Ipar 4.0 - Házi feladat kidolgozás

Csaba Hajdu

2024/2025//II.

Tartalomjegyzék

1. Bevezetés **2**

2. Kidolgozott házi feladatok **3**

2.1. AI vezérelt célfelismerés, önvezetés és kiberbiztonság szárazföldi, harcászati járművek . . . 3

2.2. CPS ÉS MI SZEREPE A PRECÍZIÓS NÖVÉNY TERMESZTÉSBEN ÉS ÁLLAT TARTÁSBAN VASAS GERGŐ . . . 35

2.3. Okosotthonok kiberbiztonsági kihívásai CPS környezetben . . . 61

2.4. OKOSOTTHON KIÉPÍTÉSÉNEK LEHETŐSÉGEI . . . 86

2.5. Talajnedvesség-vezérelt IoT locsolórendszer ESP8266-tal Pálmási Ákos . . 119

2.6. A Bluetooth fejlődése, architektúrája, újszerű alkalmazásai beágyazott rendszereken . . . 126

2.7. Védelem biztosítása az automatizált ipari termelésben . . . 151

2.8. Az 5G internet jellemzése , és haszna az iparban, a . . . 173

2.9. Business analytics az ipari termelésben Kocsis Ákos Gazdaságinformatkus Bsc, akoskocsis2005@gmail.com . . . 199

2.10. Önvezető járművek, okos tömegközlekedés és városi stratégiák, drónok és autonóm légi közlekedés a városokban . . . 221

2.11. Az intelligens robotika fejlődése és a KUKA ipari robotok szerepe A KUKA robotok és a robotika Pálfalvi Áron . . . 247

2.12. Okosotthonok energiahatékonysági megoldásai: Fenntarthatóság és költségcsökkentés a modern technológiák segítségével . . . 271

2.13. A digitális ikrek és a mesterséges intelligencia kapcsolata az iparban Kovács Ábel . . . 297

2.14. Szövegszerkesztési Sablon az Ipar 4.0 Technológiák című Tárgyhoz Okosvárosok energiafelhasználása, a sablon az ACM megfelelő sablonján alapul . . . 317

2.15. A mobilkommunikáció fejlődése: Az 1G-től a 6G-ig, technológiai architektúrák, eszközök és ipari hatások . . . 340

2.16. Zero Trust biztonsági modell alkalmazása a CPS rendszerekben . . . 367

2.17. Okosgyárak CPS rendszereinek fejlesztése mesterséges-intelligenciával MI-CPS rendszerek az Ipar 4.0 okosgyáraiban Innovatív megoldások és fejlesztési módszertanok a CPS-ek mesterséges intelligencia alapú integrációjára 394
2.18. Műholdas rendszerek integrációja valós idejű ipari alkalmazásokban beágyazott és számítógépes rendszerek segítségével 421
2.19. Robotika és mesterséges intelligencia az iparban Az ipari automatizáció, gyártás és logisztika fejlődése a modern technológiák tükrében SZÁSZ BOTOND 447
2.20. A mesterséges intelligencia alkalmazásai a kiberfizikai rendszerekben a . . 469
2.21. Bluetooth technológia fejlődése, architektúrája és gyakorlati alkalmazása az Ipar 4.0 környezetben 504
2.22. IIoT avagy Industrial Internet of Things Kovács Ármin Krisztián 513
2.23. Beágyazott rendszerek szerepe az önvezető járművek valós idejű döntéshozatalában 539
2.24. Az 5G hálózatok alkalmazása CPS keretrendszerekben 563
2.25. 5G hálózat szerepe az okosotthonok IoT eszközeinek valós idejű kommunikációjában 588
2.26. Zsarolóvírusok elleni védekezés a CPS rendszerekben SZILÁGYI MÁRK . 611
2.27. Légiközlekedés, beágyazott rendszerek technológiái 656
2.28. TOTP időszinkronizáció hatásai és támadhatósága különböző implementációkban 680
2.29. StulczBendegúzMilán HT9NZQ Privát 5G hálózatok kiépítése noneptun . . 706
2.30. Az ipar kezdetei – Ókori Egyiptom Ha az iparról beszélünk a történelem kezdeti időszakaiban, akkor Egyiptom az egyik legkorábbi civilizáció, ahol már egész jól szervezett és sokféle „ipari tevékenység” zajlott – persze nem abban az 743
2.31. Digitális ikrek a jövő iparában: Architektúrák, kihívások és alkalmazások az autóiparban Digitális ikrek az autóiparban 761
2.32. Parkolóház kapuvezérlése Arduino Nano segítségével 784
2.33. vezérlésében szerelősoron 793
2.34. IoT-rendszerek szerepe az okosotthonok kommunikációjában és biztonságában az Ipar 847
2.35. Varga Dániel, ... 888
2.36. Okosgyárak kibervédelmi megoldásai 916
2.37. A mesterséges intelligencia használata a gyógyszerfejlesztésben 944
2.38. Szenzorok és alkalmazásuk az Ipar 970
2.39. Alacsony energiaigényű hálózatok szerepe az okosgyárakban 993

2.40. Az okosotthonok fejlődése és hatása a mindennapi életre, az energiamenedzsment szerepe Intelligens rendszerek az otthonokban 1020
2.41. A hibrid rendszerek jelentősége az Ipar 1044
2.42. Labdaszállító berendezés 1073
2.43. Kiberbiztonság az okosotthonokban – Honnan tudjuk, hogy tényleg biztonságban leszünk? 1109
2.44. Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben 1147
2.45. Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben 1174
2.46. LoRa-WAN technológia LoRa-WAN technológia alkalmazása CPS rendszerekben 1201
2.47. Felhőalapú szolgáltatások hatása a videójáték-iparra 1226
2.48. A biztonságtechnika szerepe 1252
2.49. GSM technológiák összehasonlítása, alkalmazása CPS rendszerekben . . 1276
2.50. IoT hálózatok biztonsági kihívásai és megoldásai ipari környezetben . . . 1300
2.51. Kiberbiztonság a CPS-rendszerekben 1322
2.52. Okosvárosok és beágyazott rendszerek: Technológiai megoldások és alkalmazások az 1383
2.53. Okosvárosok és beágyazott rendszerek: Technológiai megoldások és alkalmazások az 1412
2.54. Mesterséges Intelligencia és alkalmazásai CPS keretrendszerekben Orvosi diagnosztika, személyre szabott gyógyászat 1442
2.55. Az Ipar 4.0 technológiák alkalmazása a Siemens Amberg okosgyárában Digitalizáció, automatizálás és fenntarthatóság az elektronikai gyártásban . 1464
2.56. IOT ÉS OKOSGYÁRTÁS A GYÁRTÁSI FOLYAMATOKBAN 1489
2.57. MQTT protokoll alkalmazása okos éttermekben: Valós idejű szenzoradatok kezelése és integrációja egy IoTalapú vendéglátóipari rendszerben 1517
2.58. Smart megoldások és technológiájuk okoslakás, okosotthon 1541
2.59. Humán-robot interakció szerepe és tervezési szempontjai a kiber-fizikai rendszerekben (CPS) Vizkeleti Gergő, ... 1566
2.60. Szimulációs Gyártósor esszé 1591
2.61. Az Okosotthonok jövője: automatizált intelligens rendszerek, felhőalapú támogatás és energiahatékonyság 1626

1. fejezet

Bevezetés

Az Ipar 4.0 tantárgy célja, hogy a hallgatók átfogó képet kapjanak a modern ipari digitalizáció alapelveiről, az intelligens gyártási rendszerek felépítéséről, valamint a kiber-fizikai rendszerek (CPS) szerepéről a jelen és a közeljövő termelési folyamataiban. A tárgy egyik legfontosabb eleme a technológiák gyakorlatias megközelítése: nem csupán elméleti fogalmakat tárgyalunk, hanem valódi ipari példákon keresztül vizsgáljuk, hogyan alakítja át a digitalizáció a gyárakat, az ellátási láncokat és a mérnöki munkát.

Ez a dokumentum a félév során beadott hallgatói esszéket gyűjti egybe, amelyek az Ipar 4.0 témakörének különböző részterületeit dolgozzák fel. A dolgozatok az automatizálástól és robotikától kezdve a mesterséges intelligencia ipari alkalmazásain át a kibervédelemig és okos rendszerekig számos izgalmas témát érintenek. A hallgatók saját érdeklődési körüknek megfelelően választottak témát, így a gyűjtemény jól tükrözi az Ipar 4.0 világának sokszínűségét és az ezek mögött álló mérnöki gondolkodásmódot.

A dokumentum célja kettős: egyrészt betekintést adni abba, milyen problémák, technológiák és trendek foglalkoztatják a mérnökhallgatókat; másrészt inspirációt nyújtani mindazok számára, akik a modern ipari digitalizáció területén szeretnének elmélyülni. A dolgozatok önállóan értelmezhetők, ugyanakkor együtt egy olyan panorámát adnak, amely jól kiegészíti a tantárgy előadásait és laborjait.

Bízom benne, hogy ez az esszégyűjtemény hozzájárul ahhoz, hogy a hallgatók még tudatosabban és magabiztosabban mozogjanak az Ipar 4.0 technológiáinak világában, és tovább erősíti azt a mérnöki szemléletet, amelyre a jövő gyártástechnológiája épül.

2. fejezet

Kidolgozott házi feladatok

2.1. AI vezérelt célfelismerés, önvezetés és kiberbiztonság szárazföldi, harcászatijárművek

2024/2025/2

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

AI vezérelt célfelismerés, önvezetés és kiberbiztonság szárazföldi, harcászatijárművek esetében

A pusztító frigy: acél és adat

Nagy Gergő Roland
[redacted]

Abstract:

This paper presents an in-depth examination of the core technologies that underpin AI-driven target recognition, autonomous navigation, and cybersecurity in modern ground combat vehicles.

AI-based target recognition is achieved through real-time processing of electro-optical, infrared, LiDAR and radar sensor feeds by convolutional neural networks (YOLO, Faster R-CNN) running on vehicle-mounted edge-AI modules (GPUs and Neural Compute Sticks). This enables the fire-control system to update target coordinates with minimal latency—even in environments degraded by dust, smoke, electromagnetic interference, or extreme temperatures.

For autonomous navigation, the vehicle relies on a multi-sensor approach: LiDAR, radar, and stereo-camera data are fused via SLAM algorithms in concert with GNSS and inertial measurement units (IMUs). GPU- and FPGA-accelerated obstacle-avoidance and path-planning modules execute dynamic speed and steering control, and support on-the-fly route re-planning. In convoy operations, adaptive following and team-communication–based coordination ensure that multiple vehicles maintain formation and share situational awareness in real time.

Cybersecurity is enforced through a hardware Root of Trust architecture, endpoint encryption, and multi-factor authentication to prevent unauthorized access. Machine-learning–based intrusion detection systems continuously monitor inter-module communications for anomalies, while quantum-secure key-exchange protocols and dynamic network segmentation mitigate Man-in-the-Middle and denial-of-service threats. Authenticated software updates and regular security audits complete the defense-in-depth strategy, preserving system integrity throughout the vehicle’s operational lifecycle.

By integrating these tightly coupled technologies, next-generation combat vehicles achieve enhanced survivability, reduced crew risk, and adaptive decision-making on the battlefield.

Tartalomjegyzék

Abstract: 1
Bevezetés 3
Szenzorok és adatgyűjtés 4
Célfelismerést támogató rendszerek 4
Elektor-optikai és Infravörös szenzorok 4
Milliméter-hullámhosszúságú radar 5
LiDAR szenzorok 6
Katonai felhasználás 7
Konvolúciós neutrális hálózatok 8
YOLO 9
Faster R-CNN 10
Összehasonlítás 11
Járműfedélzeti edge-AI modulok 11
Navigáció 13
Sztereó kamerák 13
SLAM algoritmusok 13
GNSS és IMU 14
FPGA-gyorsított útvonal tervezés és akadályelkerülés 15
V2X kommunikációs rendszerek 16
Kiberbiztonság 18
A hardveres root-of-trust 18
Fix funkciójú 18
Programozható 18
Katonai felhasználás 18
Végponti titkosítás 20
Többlépcsős hitelesítés 21
Gépi tanulás alapú behatolás-észlelő rendszerek 22
Kvantum kulcscsere protokollok 23
Dinamikus hálózati szegmentálás 24
Hitelesített szoftverfrissítések fontossága 24
Rendszeres biztonsági auditok 25
Összefoglalás és konklúzió 27
Források: 28

Bevezetés

A modern szárazföldi harcjárművek ma már nem csupán acélból és hajtóművekből állnak, hanem komplex, egymással szoros kölcsönhatásban működő intelligens rendszerekből, amelyek valós időben gyűjtik, értelmezik és használják fel a környezetről szóló adatokat. E három pillér – az AI-alapú célfelismerés, az autonóm navigáció és a kiberbiztonság – együttes alkalmazása lehetőséget teremt arra, hogy a járművek önálló döntéshozatallal rendelkező, adaptív harci platformokká váljanak.

Az AI-alapú célfelismerő modulok összetett szenzorhálózatokra támaszkodnak: az elektro-optikai, infravörös és radaradatokból gépi tanulási modellek állítanak elő valós idejű, megbízható helyzetképet, amely a tűzvezető rendszerek számára pontos célkoordinátákat biztosítanak még kedvezőtlen körülmények között is.

Az autonóm navigációs rétegben a terep felmérését LiDAR, radar és stereokamera adatok szolgáltatják, amelyeket SLAM-eljárások és GNSS/IMU integráció egészít ki. Az így kapott térinformatikai alapra épülnek az út- és manővertervező algoritmusok, valamint az akadályelkerülő mechanizmusok, melyek akár konvojműveletek során is képesek adaptív követésre és kooperatív manőverezésre.

A kiberbiztonsági réteg feladata, hogy megvédje a jármű belső és külső kommunikációs csatornáit: a hardveres root-of-trust, a titkosított adatátvitel és az anomáliadetektáló rendszerek együttesen akadályozzák meg a jogosulatlan beavatkozásokat, miközben a folyamatos szoftverfrissítések és auditok garantálják a rendszerek integritását.

Ez a dolgozat azt vizsgálja, hogyan építhető fel és milyen műszaki követelmények mentén működhet hatékonyan ez a háromrétegű architektúra, miközben a harcászati igények és a valós idejű műveleti körülmények szigorú kereteit is szem előtt tartja.

Szenzorok és adatgyűjtés

A szenzor vagy érzékelő egy olyan eszköz, amely képes a környezeti változásokat detektálni és képes reagálni ezekre a változásokra. Fő feladata a fizikai jelenségek digitális vagy analóg jellé való alakítása. [1]

A megfelelő döntéshozatalokhoz szükséges adatok gyűjtéséről a következő rendszerek a felelősek:

Célfelismerést támogató rendszerek

Elektor-optikai és Infravörös szenzorok

Az EO/IR (Electro-Optikai/Infravörös) szenzorok két, egymást kiegészítő alrendszerből állnak: az EO-kamerák a látható és szabad szemmel nem látható infravörös fény tartományban rögzítenek nagyfelbontású képeket, míg az IR-detektorok a tárgyak által kibocsátott hőmennyiség alapján hőtérképet készítenek (1. ábra). [2]

1. ábra Példa az EO/IR szenzorok képalkotására

forrás: https://www.flyeye.io/drone-acronym-eo-ir/

A modern EO/IR payload-okban mindkét adatsáv párhuzamosan fut, és az IR-hőtérképet (2.ábra) összefésülik az EO-képpel, így az operátor egyszerre kap részletgazdag vizuális és hőinformációt ugyanarról a jelenetről. Emellett a pan-tilt-zoom (PTZ) mechanika lehetővé teszi a célterület szabad forgatását és nagyítását, ami AI-asszisztált célkövetéssel egészül ki [2].

Katonai járművekhez a Leonardo DRS által fejlesztett rendszerek elsősorban hűtés nélküli hosszúhullámú IR-detektorokon alapulnak, amelyek többféle látómező (FOV) között válthatók, ezzel távoli fenyegetésfelderítést és közeli célpontkövetést biztosítanak kedvező méret-tömeg-teljesítmény arány mellett. A Driver's Vision Enhancer (DVE) család kibővített látómezőt nyújt a páncélozott járművek számára, jelentősen javítva a manőverezést és a helyzetfelismerést korlátozott látási viszonyok között is [3].

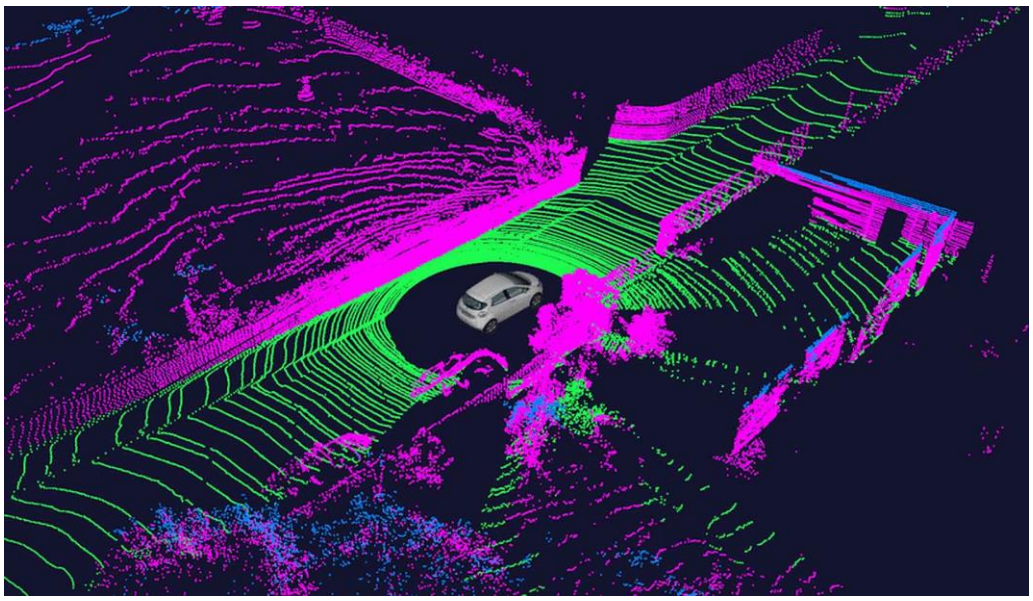
2. ábra Példa egy IR rendszer által készített képre

forrás: https://optics.org/news/3/2/15

Milliméter-hullámhosszúságú radar

A fedélzeti milliméterhullámú radar 30–300 GHz-es frekvenciatartományban dolgozik, ahol az 1–10 mm-es hullámhossz rövid impulzusokat vagy folyamatosan frekvenciamodulált jeleket (FMCW) bocsát ki. A radar ezt követően méri a visszavert jel időbeli késését („Time-of-Flight"), így pontos távolságadatot kap a célpontokról; a Doppler-effektuson (a hullám frekvenciája és hullámhosszában megjelenő változásra ad magyarázatot, miszerint, ezeknek a változásoknak az oka a hullámforrás és a megfigyelő egymáshoz képest való elmozdulása, mozgása. [4]) alapuló frekvenciaeltolódás segítségével pedig a mozgó tárgyak sebességét is meghatározza. A fázisvezérelt vagy többnyalábos antenna-tömbök (phased-array / multi-beam) lehetővé teszik a célpontok irányának (azimut és eleváció) kalkulálását, így a rendszer egyszerre képes nagy felbontású, valós idejű 3D-pontfelhő (3. ábra) előállítására és csekély késleltetéssel történő időbeli frissítésére. [5]

A harcjárművek számára a milliméterhullámú radar alapvető funkciója a környezet folyamatos figyelése és a célpontok valós idejű detektálása és követése. A radar jelei füstön, poron, esőn vagy ködön át is áthatolnak, így kedvezőtlen körülmények között is megbízható helyzetadatot szolgáltatnak. A beérkező visszaverődések jelalakjának és Doppler-eltolódásának algoritmikus feldolgozása révén a rendszer meghatározza a célpont(ok) helyzetét, sebességét és mozgásvonalát, ami a tűzvezető és a navigációs alrendszerek számára kritikus adatokat biztosít. Így a páncélosok önállóan képesek felismerni, követni és – szükség esetén – támadási parancsokra előkészíteni a célpontokat, miközben csökkentik a személyzet kockázatát és növelik a jármű túlélőképességét a harctéri környezetben. [5]



3. ábra Példa egy 3D-s pontfelhőre

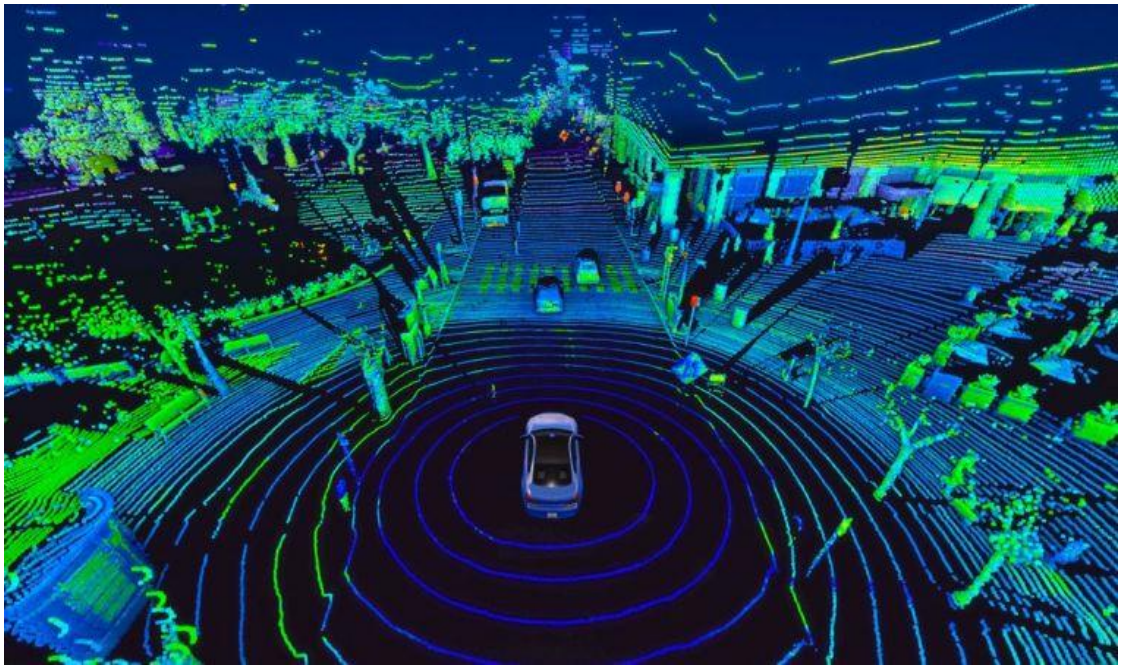
forrás: https://keymakr.com/blog/how-3d-point-cloud-segmentation-will-make-the-future-hands-free/

LiDAR szenzorok

A LiDAR (Light Detection and Ranging) rendszerek lényegében radarok lézeres párjai: infravörös lézerimpulzusokat bocsátanak ki, majd a környezeti felületekről (föld, vegetáció, épületek stb.) visszaverődő jeleket detektálják. Maga a sugárzás egy forgó tükrökből álló szkenneren keresztül történik, amely biztosítja, hogy a lézerimpulzusok a tér minden irányába eljussanak. Amikor az impulzus visszatér, fotodiódák vagy speciális avalanche photodiódák érzékelik a fényt, és mind az érkezési időt, mind a beesési szöget rögzítik (4. ábra). [6]

A visszaverődés időbeli késéséből – ahol a pulzus oda- és visszaútjának idejét a fénysebességgel és egy kettővel történő osztással számítjuk ki – tisztán kivehetővé válik, hogy milyen távolságra helyezkedik el a célpont. Mivel a LiDAR másodpercenként több százezer, de akár millió impulzust is képes leadni, minden egyes visszaérkezett lézerimpulzus egy pontot képez a 3D-s pontfelhőben, amely így rendkívül részletes digitális modellé áll össze. A mérési pontok abszolút helyzete GNSS-vevők (GPS) és inerciális mérőegységek (IMU) segítségével kiegészül, így minden pont GPS-koordinátákkal és a jármű térbeli orientációs adataival együtt kerül a rendszerbe.[6]

A képalkotás után a pontfelhő valós időben vagy utólag is szoftveres eljárásokon megy keresztül: megtisztítják a zajos adatokat, klaszterezéssel csoportosítják a hasonló visszaverődéseket, majd felület-rekonstrukciót végeznek. Ennek eredményeként jön létre a végső digitális domborzatmodell (DTM) vagy a teljes digitális terepmodell (DEM), amely a harctér geometriáját és az akadályok pontos elhelyezkedését is megmutatja.[6]



4. ábra Példa a LiDAR szenzor képalkotására

forrás: https://www.gim-international.com/content/article/multibeam-lidar-for-mobile-mapping-systems

Katonai felhasználás

A hadsereg a LiDAR műszert elsősorban a nagy felbontású és nagy impulzusszámú adatgyűjtés miatt alkalmazza, amely lehetővé teszi a mozgó célpontok pontos detektálását és követését, még kis méretű objektumok esetén is kritikus fontosságú pontossággal. Ugyanezen képességek révén gyorsan előállíthatóak részletes 3D taktikai térképek mind városi, mind nyílt terepen, segítve a missziótervezést és az ellenséges erők elhelyezkedésének felderítését. A LiDAR-alapú „Line of Sight" számítása során a 3D pontfelhők geometriai elemzésével határozható meg a potenciális megfigyelő- és tüzérségi pozíciók optimális elhelyezése, továbbá támogatja a kommunikációs és rádiósávok tervezését is. [7]

Aknaellenes műveleteknél LiDAR-szkennerek telepíthetők pilóta nélküli felszíni járművekre (USV), ahol a felszíni aknák felderítésében nyújtanak kulcsfontosságú képességeket. Emellett önvezető harcjárművekben a LiDAR-adatok akadályelkerülésre, környezeti térkép folyamatos frissítésére és megbízható navigációra szolgálnak, még GPS-jel kiesése vagy zavaros környezet esetén is.[7]

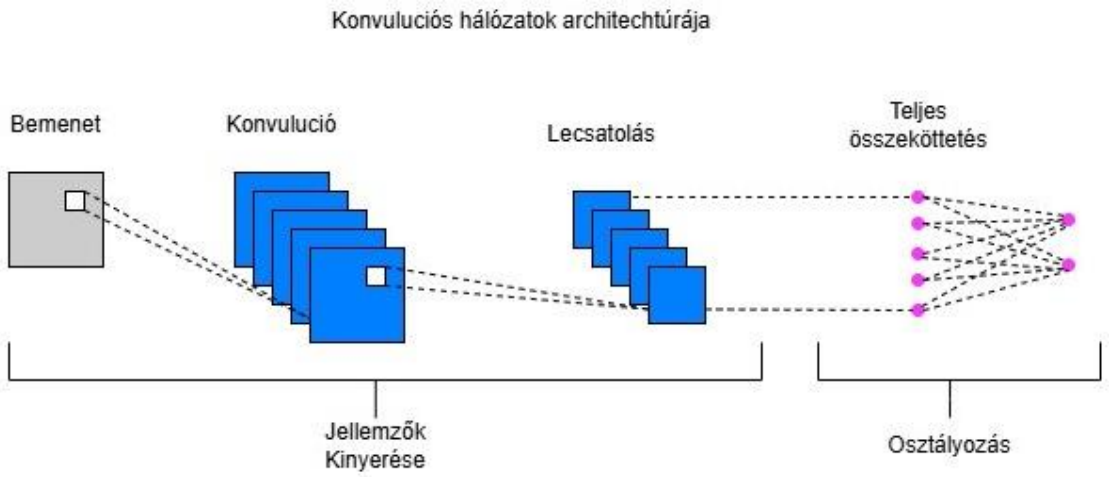
Konvolúciós neutrális hálózatok

A konvolúciós neurális hálózatok (CNN) lényege, hogy a képadatokból automatikusan tanuljanak kiemelkedően releváns jellemzőket úgy, hogy lokálisan összekapcsolt, többszintes rétegeken keresztül fokozatosan építik fel a bemenet hierarchikus reprezentációját. Az első rétegekben kisebb, általában 3×3 vagy 5×5 méretű szűrők pásztázzák végig a bemeneti képet, és – terhelésmegosztás révén – ugyanazt a mintázatkinyerő műveletet alkalmazzák minden pozícióban, ezzel éleket, vonalakat és egyszerű textúrákat érzékelve. A konvolúciós művelet eredménye egy úgynevezett jellemzőtérkép (featuremap), amely a bemenet bizonyos tulajdonságainak intenzitását reprezentálja. A jellemzőtérképek továbbhaladását speciális aktivációs függvények, például a ReLU (Rectified Linear Unit) nem linearizálják, ami lehetővé teszi a hálózat számára, hogy a valóság komplex összefüggéseit is leképezze. [8]

A konvolúciós blokkok után rendszerint lecsatoló (pooling) rétegek következnek, melyek a jellemzőtérképek térbeli felbontását csökkentik, és ezzel együtt a számítási igényt és az overfitting kockázatát is mérséklik. A leggyakoribb pooling-módszer a max-pooling, ahol egy adott ablakméretben a legnagyobb aktiváció értéke kerül továbbításra, így a hálózat ellenálóvá válik a kisebb eltolódásokkal és torzulásokkal szemben. [8]

A konvolúciós és pooling rétegeket többször egymás után alkalmazva a hálózat egyre magasabb szintű, egyre összetettebb mintázatokat ismer fel: míg az alsó rétegek éleket és sarkokat, addig a mélyebb rétegek már objektumrészeket vagy akár teljes objektumokat is képesek detektálni. A rétegezett felépítés végén a kinyert jellemzők egy vagy több teljesen összekapcsolt (fully connected) rétegbe kerülnek, ahol a tanult reprezentációk alapján történik meg az osztályozás: a softmax vagy egyéb kimeneti aktivációs függvény segítségével adódnak a valószínűségek az adott kategóriákra. [8]

A tanulási folyamat során a CNN a visszaterjesztés (backpropagation) elvét alkalmazza, amely a kimeneti hibát visszafelé osztja szét a hálózaton, és gradiensalapú optimalizációval (például stochasztikus gradient descent) frissíti a súlyokat. A súlymegosztás, a lokális összekapcsolás és a mély, hierarchikus szerkezet együttesen teszik lehetővé, hogy a CNN-ek hatékonyan működjenek nagyfelbontású képfeldolgozási feladatokban anélkül, hogy a paraméterek száma kezelhetetlenné válna, miközben képesek általánosítani a látott mintázatokra (5. ábra). [8]



5. ábra Konvulúciós hálózatok architechtúrája
Saját ábra a https://zilliz.com/glossary/convolutional-neural-network cikkben található kép alapján

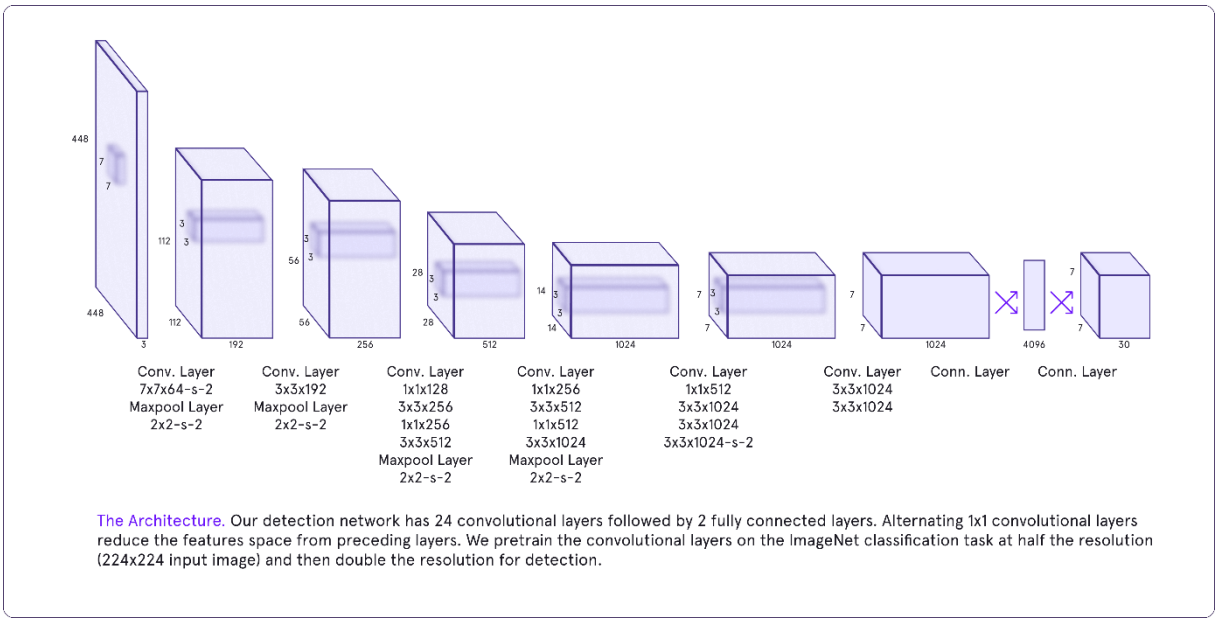
YOLO

YOLO egy egylépcsős (single-shot) objektumdetektáló architektúra, amely a teljes bemeneti képet egyetlen konvolúciós hálózati előrecsatolással (forward pass) dolgozza fel (6. ábra). [9], [10]

A bemenetet S×S méretű rácsokra osztja, és minden cella felelős B darab bounding box-előrejelzésért és osztályvalószínűségek becsléséért. A hálózat „anchor box" sablonokat használ, amelyekhez eltolási vektorokat (offset regression) számít, hogy a dobozok pontosan illeszkedjenek a tényleges objektumok köré. A detektált átfedő dobozok között a Non-Maximum Suppression (NMS) algoritmus szűr ki redundanciát, így minden tárgynak csak egy végső becslése marad. [9]

A Non-Maximum Suppression (NMS) egy olyan objektumfelismerési eljárás, amely a detektor által egy képben található, egymással átfedő határoló kereteket egymás után feldolgozva megtartja mindig csak a legmagasabb bizalmi pontszámú keretet, majd a kiválasztott kerettel túlságosan átfedő (IoU > küszöbérték, jellemzően 0,5) többit elnyomja, így minden objektumra egyetlen, pontos és magas pontosságú jelölés marad a végén; ezáltal csökken a redundancia, nő a észrevételi pontosság és javul a számítási hatékonyság. [11]

A legújabb YOLO-verziók (YOLOv5, YOLOv7) tovább finomították ezt a sémát: bevezettek CSPDarknet-11/53 jellegű gerinchálózatot, Spatial Pyramid Pooling (SPP) és Path Aggregation Network (PAN) modulokat a méret- és arányváltozások kezelése érdekében, miközben 30–45 FPS közötti feldolgozási sebességet tartanak. [9]



6. ábra Teljes YOLO architechtúra

forrás:https://imgur.com/yvum3vg

Faster R-CNN

A Faster R-CNN kétlépcsős (two-stage) detektor, amely elsőként egy Region Proposal Network (RPN) segítségével generál lehetséges célterületeket (region proposals), majd ezeket finomítja és osztályozza egy különálló detektáló rész (7.ábra).[10], [12]

A bemenetet egy előre betanított konvolúciós gerinchálózat dolgozza fel, és az így nyert jellemzőtérképből az RPN több méretű és arányú anchor box-ot használva becsli az objectness-et és a bounding box-eltolásokat. A kiválasztott javaslatokat a RoI pooling egységes méretűre alakítja, majd párhuzamosan alkalmaz egy klasszifikációs és egy doboz-regressziós fejet, így kapva meg a végső osztály- és pozícióelőrejelzéseket. [12]

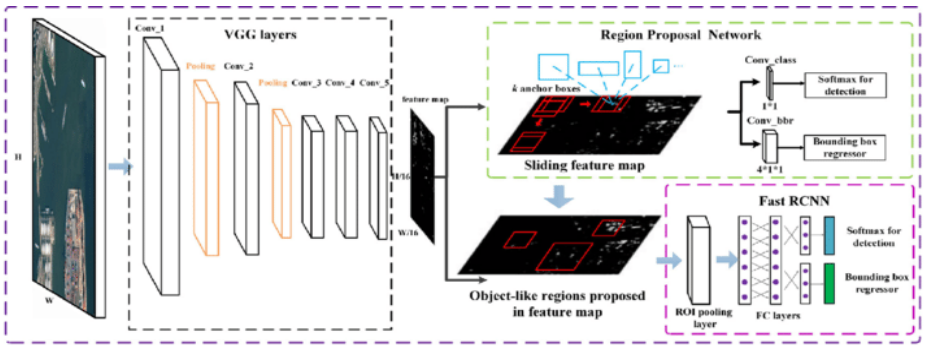
A Faster R-CNN erőssége a pontos lokalizáció és osztályozás: a javaslat-finomítás révén nagyon alacsony a hamis pozitív találatok aránya, különösen zsúfolt vagy átfedő objektumok esetén. Ez teszi alkalmassá a tüzérségi célmegjelölő és felderítő rendszerekben, ahol a harcijárműveknek pontos kontúr- és típusinformációra van szükségük (pl. ellenséges tankok, lövegtalp-nyomok vagy rejtett gyalogos egységek) a hatékony célzás és tüzelés érdekében. [12]

Összehasonlítás

Mindkét modell objektumdetektálásra szolgál, de a kiemelt különbség a valós idejű reagálás és a pontosság közötti kompromisszum. A YOLO 30–45 FPS körüli feldolgozási sebességével ideális a kritikus késleltetés nélküli feladatokra, ugyanakkor apró vagy erősen átfedő objektumok esetén akadhatnak pontossági korlátjai. [9]

Ezzel szemben a Faster R-CNN 5–7 FPS körüli sebességet produkál, de region proposal alapú kétlépcsős struktúrájának köszönhetően magasabb lokalizációs és osztályozási pontosságra képes, különösen változatos méretű és komplex elrendezésű objektumok esetén. [10], [12]

Hatékony szárazföldi harcjármű-alkalmazásokban a YOLO gyors döntéshozatalára hagyatkoznak, ha a célkövetés és veszélyészlelés reakcióideje élet-halál kérdés (pl. passzív védelmi rendszerek), míg a Faster R-CNN részletes célpont-feldolgozást biztosít a tüzérségi előkészítésnél és a harctéri felderítésnél, ahol a pontosság és a hamis pozitív találatok minimalizálása a fő szempont. [12]



7. ábra Faster R-CNN achitechtúra

forrás:https://www.researchgate.net/figure/The-architecture-of-Faster-R-CNN_fig2_324903264

Járműfedélzeti edge-AI modulok

A modern szárazföldi harcjárművek fedélzeti rendszereiben „rugged” beágyazott GPU-megoldások (3U/6U VPX formátumú grafikai és GPGPU kártyák) biztosítják a valós idejű adatvizualizáció, szenzor-fúzió és AI-alapú analitika magas párhuzamos számítási teljesítményét, miközben –40 °C és +85 °C közötti hőmérsékleti tartományt, IP67-es védettséget, fokozott rezgés- és ütésállóságot, valamint MIL-Spec követelményeknek megfelelő megbízhatóságot nyújtanak. [13]

Például az Abaco GVC1001 „evaluation embedded computer” a NVIDIA Jetson AGX Xavier SoM-re épít, amely egy Volta architektúrás GPU-val (512 Tensor Core) és nyolcmagos ARM CPU-val akár 5,7 TFLOPS lebegőpontos teljesítményt kínál. A GVC1001 két 10 Gigabit Ethernet és két CANbus port segítségével képes több kamera és járműszenzor adatfolyamát párhuzamosan fogadni, miközben a beépített 256 GB-os NVMe SSD-n tárolja a missziós és mozgó térkép adatokat. A beágyazott JetPack környezet és az Abaco AXIS ImageFlex eszköztára révén olyan alkalmazások valósíthatók meg, mint a 360°-os helyzetfelismerés, EO-szenzor-feldolgozás, DVE („degraded visual environment”) támogatása, mozgó térképek generálása, valamint a széles területű tartós megfigyelés, hiperspektrális szenzor-fúzió, akna- és robbanóeszköz-észlelés. [14]

Curtiss-Wright Parvus® DuraCOR 312 és AGX-Xavier moduljai a NVIDIA Jetson család katonai-ipari változatait alkalmazzák. A DuraCOR 312 a Jetson TX2i SoM-et építi be, mely 256 Pascal GPU-magot és négymagos ARMv8 CPU-t egyesít, SWaP-érzékeny alkalmazásokhoz optimalizált pasztázott energia-profilokkal (Max-Q/Max-P), ECC-memóriával, valamint –40 °C…+85 °C üzemeltetési tartománnyal és IP67-es burkolattal. A modul CANbus, Mini-PCIe, M.2 és SATA interfészén keresztül több bővítőhelyet és tárolási opciót kínál, míg a 50 ms-os energia-tárolás (power hold-up) és a teljesen ventillátormentes kialakítás garantálja a magas szintű rendelkezésre állást extrém környezetben is. [15]

A DuraCOR AGX-Xavier a Jetson AGX Xavier Industrial SoM-et használja, amely 512 CUDA-maggal, dedikált tensor-magokkal és további mélytanulás-gyorsító motorokkal akár 22 TOPS-nyi inferencia-teljesítményt (vagy 11 TFLOPS CUDA-számítást) nyújt. A MIL-STD-810H szerint tanúsított modul 10 Gigabit Ethernet, USB 3.1, DVI/HDMI és opcionális GMSL kamerainterfészek sorát kínálja, valamint kicserélhető NVMe SSD-t és mini-PCIe/PCIe104 bővítményeket támogat, lehetővé téve a folyamatos, nagyszabású szenzor-adatfeldolgozást, célfelismerést és mozgástervezést a harcjármű fedélzetén, zord körülmények között is. [15]

Ezekkel a hardver eszközökkel biztosítva van a folyamatos adatfeldolgozás és adattovábbítás. Esetleges analitikák is készíthetők a jármű személyzetének, valamint azonnali veszélyfelismerést is szolgáltatnak az alrendszerek, amelyek nagyban növelik a személyzet és a jámű túlélési esélyeit.

Navigáció

Sztereó kamerák

A sztereó kamera rendszerek működésének alapja, hogy két, ismert távolságra egymástól elhelyezett kamerát használ ugyanannak a jelenetnek a párhuzamos felvételezésére, és ezek fényképei közötti geometriai eltérések (diszparitás) alapján számítja ki a tárgyak távolságát és a térbeli elhelyezkedésüket. [16]

A két kamera optikai tengelye párhuzamos vagy enyhén konvergáló, így a képek egymásra történő leképezése (rektilikáció) után megkereshető a megfelelő pixelek közti eltolódás, amelyből trigonometriai úton egy mélységtérkép (depth map) állítható elő. Ez a mélységtérkép adja meg minden képponthoz a kamera és a tárgy közti távolságot, ami alapján háromdimenziós pontfelhő generálható és valós idejű térinformáció szolgáltatható a navigációs és akadályelkerülő algoritmusok számára. [16]

Katonai környezetben a Jet Propulsion Laboratory által fejlesztett passzív sztereó-víziót (látható vagy LWIR szenzorokkal) számos UGV-programban alkalmazták a terep valós idejű feltérképezésére és az útvonal biztonságának biztosítására. A megoldás a diszparitásadatokból előállított mélységi térkép segítségével képes volt negatív akadályok—például árkok, gödrök és meredek lejtők—felismerésére, valamint a terep stabilitásának értékelésére, így a robotok elkerülhették a megbillentő veszélyeket. [17]

Ez a rendszer kifejezetten jó akadályok felismerésre, amelyek esetleg végzetessé tennék a jármű sorsát. Bizonyos esetekbe az erre való támaszkodás kifejezetten előny lehet hisz ez a rendszer passzívan működik, így nehezen detektálható, nagyban növeli a járművek túlélőképességét.

SLAM algoritmusok

A SLAM (Simultaneous Localization and Mapping) lényege, hogy egy autonóm jármű vagy robot még teljesen ismeretlen környezetben is képes egyszerre felépíteni a környezet térképét és meghatározni saját helyzetét ezen a térképen. A módszer alapja az, hogy valós időben folyamatosan gyűjti és feldolgozza a különböző szenzorok – például LiDAR, vizuális kamerák és inerciális mérőegységek (IMU) – adatfolyamát, majd ezekből egyre pontosabb 2D/3D rekonstrukciót hoz létre. Így a gép nemcsak abszolút pozícióadatok nélkül tud navigálni, hanem folyamatosan finomítja a róla és környezetéről alkotott belső modellt is. [18]

A SLAM-algoritmus működésének szívét a következő lépések alkotják. Először beérkeznek a szenzoradatok: a LiDAR távolságmérései, a kameraképek és az IMU-gyorsulás információk mind időbélyeggel ellátva rögzülnek. Ezt követően a rendszer detektálja és követi a környezet egyedi jellemzőpontjait – éleket, sarkokat vagy más jól azonosítható mintázatokat –, hogy a mozgás közben ezek ismételt észleléséből becslést készítsen a saját elmozdulására. A harmadik fázisban ezen jellemzőpontok és távolságmérések alapján folyamatosan épül a környezet pontfelhője vagy gráfszerkezete, amely egyre gazdagabb, részletesebb térképet eredményez. Miközben a térkép bővül, az algoritmus az újonnan felismert jellemzőpontokra támaszkodva lokalizálja magát, így még GPS-jel hiányában vagy jelezavarás esetén is pontosan tudja, hol tartózkodik. Végül a dinamikusan frissülő modellre építve a jármű azonosítja és elkerüli a felbukkanó akadályokat, valamint tervezett célpontja felé optimalizált útvonalat generál. [18]

Katonai alkalmazásában és gyakorlatban SLAM nélkülözhetetlen ott, ahol a hagyományos navigációs módszerek (például GPS) nem használhatók: alagutakban, beltéri csarnokokban, erdőben vagy hidak alatt. Ilyen környezetekben a SLAM lehetővé teszi, hogy az autonóm rendszerek akadályérzékelés nélkül is biztonságosan manőverezzenek, miközben valós idejű térképet készítenek a környezetről. Az így felépült, pontos környezeti modell nemcsak a valós idejű repülést és terepfelmérést támogatja, hanem a felhőkép generálás, az infrastrukturális ellenőrzés, a keresés-mentés és a raktárfeltérképezés feladatainál is kritikus fontosságú valós idejű adatokkal szolgála Visual SLAM különösen értékes GPS-megvonásos vagy elektronikus zavarásnak kitett harci környezetekben. [18], [19]

GNSS és IMU

Global Navigation Satelite Systems

A műholdas helymeghatározó rendszerek (GNSS) alapvetően három vagy több műhold és a fedélzeti vevő közötti időbeli késések mérésén alapulnak. A GNSS-műholdak – például az amerikai GPS, az európai Galileo, az orosz GLONASS és a kínai BeiDou konstelláció – mindegyike 1,1–1,6 GHz-es rádiósávban sugároz pontos időjelzéseket atomórák segítségével. [20]

A vevő egyszerre fogad legalább három műhold jelét: mivel a rádiójelek a fénysebességgel terjednek, a távoli és közeli műholdakról érkező impulzusok közötti időeltérés alapján a vevő kiszámítja saját háromdimenziós pozícióját. A negyedik jel pedig a vevő órájának korrekciójára szolgál, így egyszerre biztosítva a hely- és időszinkron pontosságát. [20]

Katonai környezetben a GNSS-jelekhez általában titkosított, úgynevezett M-Code vagy hasonló védett air-interface tartozik, amely csak jogosult haditechnikai eszközök számára dekódolható. Ez a titkosítás védelmet nyújt az ellenséges jel zavarás (jamming) és megtévesztés (spoofing) ellen, mivel a kódolt jelek kiszűréséhez és helyes dekódolásához szükséges kulcsok nélkül lehetetlenné válik a műveleti pontosság rontása. [20]

Inerctial Mesurement Unit

Az inerciális mérőegység (IMU) háromtengelyes gyorsulásmérők és giroszkópok – valamint gyakran egy fémsáv-vagy fluxgate-magnetométer – kombinációja, mely folyamatosan méri a jármű lineáris gyorsulását és szögsebességét. A MEMS-alapú giroszkópok három ortogonális tengely mentén szolgáltatnak anguláris sebességadatot, míg a MEMS-gyorsulásmérők a három tengelyen mért lineáris gyorsulást adják át a fedélzeti számítógépnek.

Ezek a szenzorok gyári kalibrációval, hőkompenzációval és beépített önellenőrző („built-in test”) funkcióval készülnek, így –40 °C és +85 °C közötti hőmérsékleti tartományban is megbízható, alacsony zajszintű és kis eltéréssel dolgoznak. [21]

Egy IMU önmagában csak relatív mozgásadatot szolgáltat, ezért az IMU-k által generált anguláris és gyorsulási jeleket időben integrálva az eszköz fokozatosan „elfáradhat” (drift), és a helyzetbecslés pontatlanná válhat. A taktikai minősítésű IMU-megoldásoknál ezért általában kalman-szűrővel kiegészített Attitude and Heading Reference System (AHRS) van, amely a giroszkópok és gyorsulásmérők adatait a magnetométerrel, valamint külső GNSS-adatokkal fúzióhoz használja, ezzel minimalizálva a zavarásból és zajból eredő hibákat. [21]

Ezért a legmagasabb szintű navigációs pontosság eléréséhez a GPS/GNSS vevőket rendszerint közvetlenül összekapcsolják egy taktikai IMU-val, létrehozva a GPS-INS (Inertial Navigation System) rendszert. Itt a GNSS pozíció- és időinformációja folyamatosan korrigálja az IMU integrációs eredményeit, míg az IMU az GNSS-jel rövid kiesései vagy zavarai esetén is garantálja a helyzetismeret folytonosságát. A modern, rendszerekben több antennával szerelt INS-ekel integrált, gyro-kompenzált mágneses iránytűvel és nagy megbízhatóságú GNSS-vevőkkel akár statikus és dinamikus körülmények között is pontos irányt, dőlést és gördülő mozgást biztosítanak. [21]

FPGA-gyorsított útvonal tervezés és akadályelkerülés

Az FPGA-alapú (Field-programmable gate array/ mezőprogramozható kapuáramkört) útvonaltervezés és akadályelkerülés két, egymást kiegészítő megközelítést használ a járművek valós idejű autonóm irányításához: egy Q–learning alapú gyorsítót és egy gyorsításon és sebesség–akadályokon (Acceleration–Velocity Obstacles, AVO) nyugvó ütközéselkerülő modult. [22], [23]

A Q–learninges útvonaltervezés esetében az FPGA-ra implementált gyorsítóarchitektúra célja, hogy a megerősítéses tanuláson alapuló algoritmus iterációit és frissítéseit párhuzamosan, alacsony késleltetéssel hajtsa végre. A környezet diszkrét állapotainak (rács cellák, robot pozíciója és célpontja közti relációk) és az akciókészletnek (fel, le, balra, jobbra lépések) megfelelő Q-táblát a hardver egy SRAM-ban tárolja. Minden iterációban a vezérlő egység beolvassa a jelenlegi állapot- és akcióindexeket, lekéri a Q-értéket, majd a párhuzamosan futó max-kereső modul kiszámítja a következő állapothoz tartozó legmagasabb várható jutalommal bíró Q-értéket. Ezután a Bellman-egyenlet szerinti frissítési képlet FPGA-logika segítségével – beleértve az úthossz-korrekciót és a tanulási rátát – azonnal kiértékelésre kerül, és a Q-tábla frissül. A rendszer úgy van méretezve, hogy több Q-tábla-blokk is párhuzamosan fusson, így a tanulás és a döntéshozatal ciklusideje mikroszekundumos tartományban marad. [23]

Az AVO (Acceleration Velocity Obsticle) -alapú ütközéselkerülésnél az FPGA egy másik modult valósít meg, amely a célfelé tartó sebességvektor és a környező akadályok által generált „tiltott” sebességterületek metszet vizsgálata alapján választja ki az optimális gyorsulást. A jármű és a környező akadályok hely- és sebességadatait FIFO-csatornán keresztül fogadva a párhuzamos AVO-számító egységek minden akadályra kiszámítják a „velocity obstacle” értékeket – azaz azt a sebesség akadályt, amely a következő időablakban ütközéshez vezetne. Ezt követően a gyorsulási opciók halmazából (fix léptékű akciómátrix) a blokk kiszűri azokat, amelyek átfedésben vannak bármely gyorsulási akadállyal, majd a fennmaradó alternatívák közül a célirányhoz legközelebbi vektorral rendelkező gyorsulást választja ki, garantálva a determinisztikus, 10–50 milliszekundum alatti ciklusidőt az ütközések elkerülésére. [22]

E két FPGA-gyorsítómodul együttműködése lehetővé teszi, hogy egy autonóm szárazföldi harcjármű Q-learning alapú útvonaltervezéssel adaptív módon válassza ki a legoptimálisabb mozgásterepet ismeretlen terepen, miközben párhuzamos AVO-alapú gyorsulás- és sebességszabályozással valós időben elkerüli a statikus és dinamikus akadályokat, ezzel növelve a túlélőképességet és minimalizálva a késleltetést.

V2X kommunikációs rendszerek

A V2V (Vehicle-to-Vehicle) és V2X (Vehicle-to-Everything) kommunikáció alapját a járművek közötti, illetve a járművek és a külvilág – például infrastruktúra, gyalogosok, hálózatok – közötti valós idejű adatcsere képezi. A V2V rendszerekben a járművek rádiófrekvenciás protokollokon keresztül (például DSRC 5,9 GHz-en vagy C-V2X LTE/5G hálózatokon) megosztják egymással a sebesség-, pozíció- és irányadatokat, míg a V2X a V2V-n túl kiterjeszti ezt a képességet forgalomirányító lámpákra (V2I), gyalogosokra (V2P) és távközlési hálózatokra (V2N), ezzel egy komplex, minden felhasználót és entitást összehangoló rendszert létrehozva. [24]

A DSRC (Dedicated Short-Range Communications) alacsony késleltetésű, rövid hatótávolságú (~300 m) rádiósávot használ (5,9 GHz), kifejezetten biztonságkritikus alkalmazásokra tervezve, míg a C-V2X (Cellular V2X) az LTE és az 5G mobilhálózatokat építi be, ezzel hosszabb távra és nagyobb sűrűségű forgalomra is skálázható, megnövelt megbízhatóságot és hatékonyabb spektrumhasználatot kínál.[24]

Az 5G New Radio (NR) kiemelkedően megbízható, alacsony késleltetésű (URLLC) képességeivel támogatja a nagy átviteli sebességet és a nagy adatforgalmat igénylő feladatokat – például HD térképfrissítéseket vagy többeszközös kooperatív manőverezést –, míg a 802.11p (Wi-Fi for V2X) vezetéknélküli LAN-sávokra építve egészíti ki az ökoszisztémát. A modulok CBW (Channel Bandwidth) konfigurációkat, QAM-modulációs sémákat és adattovábbítási protokollokat (CAM – Cooperative Awareness Message, DENM – Decentralized Environmental Notification Message) támogatnak, amelyek a járművek, infrastruktúra és felhasználók közötti biztonságos, hitelesített kommunikációt garantálják. [24]

A járműfedélzeti V2X modulok beágyazott rádiós egységek, amelyek több antennával (pl. MIMO-config) rendelkeznek a spektrum optimális kihasználása érdekében, és általában dedikált mikrovezérlővel, biztonsági chip-párral (TPM), valamint ipari környezeti specifikációkkal (–40 °C…+85 °C, MIL-Spec ütés és rezgésállóság) készülnek [25]

Katonai rendszerekbe integrálva ezeket a V2X technológiákat több rétegben biztosítjuk a túlélőképességet és a műveleti hatékonyságot. Először is, a C-V2X modulok M-Code-hoz hasonló, katonai célú, titkosított légi interfészeket (S-vírus ellenálló moduláció) és PKI-alapú hitelesítést alkalmaznak az ellenséges jel zavarás (jamming) és megtévesztés (spoofing) elleni védelem érdekében. Másodszor, a járművek konvojműveletei során a V2V-n átadott pozíció- és mozgás adatokat dedikált parittya-topológiájú hálózatok (pl. Rajant mesh) egészítik ki, így többrétegű, redundáns útvonalakon biztosítják az elkülönített, de együttműködő jármű, vagy gyalogsági egységek folyamatos szinkronizálását és helyzetmegosztását. [25]

A valós idejű adatfúzióra épülő vezetési parancsok és veszély-, fenyegetés-észlelés azonnali kiértékelését a beágyazott edge-AI számítási egységek (GPU/FPGA SoM-ek) végzik, amelyek a V2X-ről érkező információkat integrálva egy komplex C2 (Command and Control) réteggel közvetlenül a harcijárműn belüli fegyvervezérlésnek, vezetési modulnak, valamint a központi taktikai hálózatnak szolgáltatják. [24]

A katonai V2X infrastruktúra továbbá képes dinamikus hálózati szeparációra – ahol külön frekvenciasávokra oszthatók a parancs-irányító, hírszerzési, felderítési és hitelesítési csatornák –, ezzel is csökkentve az ellenséges hálózati támadások célba jutását és biztosítva a műveleti biztonságot.

Kiberbiztonság

A hardveres root-of-trust

A hardveres Root-of-Trust (RoT) a számítástechnikai rendszer–legyen az bármilyen elektronikus rendszer–legfontosabb biztonsági alapját képezi, amelybe a rendszer azon kriptográfiai kulcsait és biztonsági primitívjeit helyezik, amelyekre minden további védelmi funkció támaszkodik. [26]

A RoT feladata, hogy a rendszer bekapcsolásakor induló biztonságos indítási (secure boot) folyamat első, megbízható lépését szolgáltassa, és ebből kiindulva építse fel a szoftveres bizalomláncot (chain of trust), biztosítva, hogy csak aláírt, hitelesített komponensek kerüljenek futtatásra (10. ábra). [27]

A hardveres Root-of-Trust két fő típusa létezik: fix funkciójú (8. ábra) és programozható (9. ábra). [27]

Fix funkciójú

A fix funkciójú RoT tipikusan beégetett, firmware-vezérelt egység, amely előre meghatározott kriptográfiai műveletekhez–például kulcskezeléshez, adat-titkosításhoz és tanúsítvány-ellenőrzéshez–nyújt biztonságos végrehajtó környezetet, és leginkább IoT eszközökben, egyszerű rendszerarchitektúrákban alkalmazzák. [27]

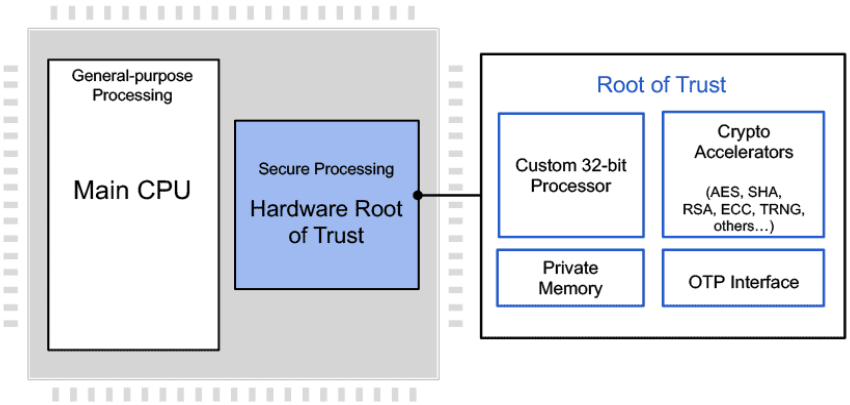
Programozható

A programozható hardveres RoT egy dedikált, beágyazott processzort (security core) tartalmaz, amely nemcsak az alapvető kriptográfiai feladatokat végzi, hanem új algoritmusok és biztonsági alkalmazások futtatására is képes, így rugalmasan frissíthető és bővíthető a fejlődő támadásokkal szemben. [27]

Katonai felhasználás

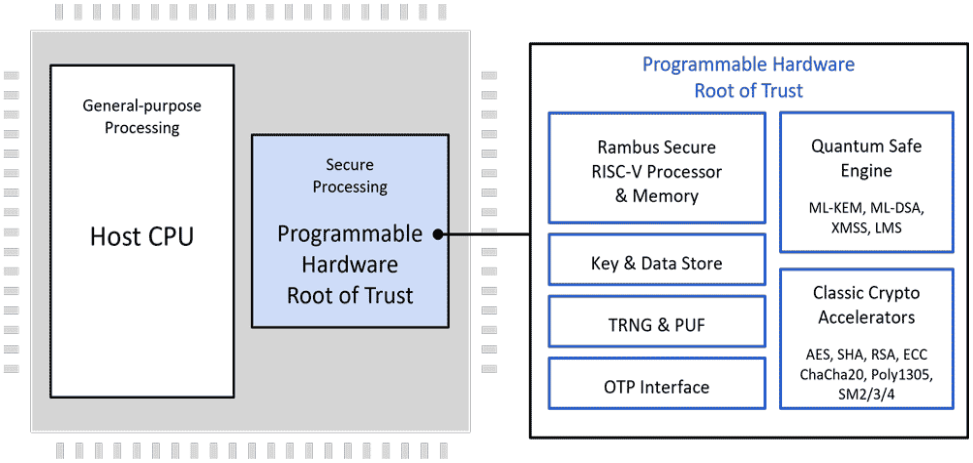
A katonai rendszerekben a hardveres RoT kritikus szerephez jut: egyrészt a zárt lökésű, alacsony késleltetésű secure boot révén garantálja, hogy a harcijárművek, radarok vagy kommunikációs modulok csak megbízható, aláírt firmware-el induljanak, így kizárva a rootkit vagy bootloader-szintű rosszindulatú beavatkozás lehetőségét. Másrészt a programozható RoT-ok speciális, katonai titkosítási protokollokat (például AES, ECC és a jövőbiztos poszt-kvantum algoritmusok) képesek hardveresen végrehajtani, miközben a fizikai elszigeteltség és a több rétegű anti-tamper védelem megakadályozza a side-channel támadásokat és az adatkinyerést célzó behatolásokat. [27]

Emellett a hardveres RoT lehetővé teszi a járműfedélzeti kulcsok és hitelesítő adatok biztonságos tárolását olyan nem-felejtő memóriákban, amelyek írásvédettek és kriptográfiai (pl. SHA-256) protokollokkal védettek, így a klónozás (spoofing) és a DoS-támadások sem férnek hozzá a kulcsokhoz. A Root-of-Trust beágyazása a katonai platformokba – legyen szó páncélosokról, UAV-kről vagy parancsnoki egységekről – tehát nem csupán a rendszer integritását és rendelkezésre állását növeli, hanem a teljes hálózati és alkalmazásszintű bizalmi architektúrát is megalapozza. [26], [27]



8. ábra Példa egy fix funkciójú Root of Trust architektúrára

forrás: https://www.rambus.com/security/root-of-trust/rt-1660/



9. ábra Példa egy programozható Root of Trust architektúrára

forrás: https://www.rambus.com/security/root-of-trust/rt-6xx/

10. ábra Root of Trust elemei

saját ábra a https://www.beningo.com/5-elements-to-secure-embedded-system-part-2-root-of-trust-rot/# ábrája alapján

Végponti titkosítás

A végponti titkosítás (endpoint encryption) az a folyamat, amelynek során az eszközön tárolt adatok – legyenek azok operációs rendszerfájlok, alkalmazásadatok, bejegyzések vagy érzékeny parancsnoki- és szenzorinformációk – titkosítási algoritmusok alkalmazásával védelmet kapnak a jogosulatlan fizikai hozzáférés ellen. Ez a védelemforma a modern endpoint security stratégiák – például a Check Point Harmony Endpoint – alapkövetelménye, hiszen így ellehetetlenítjük, hogy akár ellenséges erők, akár beépült rosszakaró személyek fizikailag megszerzett eszközről olvashassák ki az adatokat.[28]

A titkosítás arra is választ ad, hogy a – gyakran elszigetelt, vagy GPS-jel hiányos környezetben működő – harcjárművek fedélzeti számítógépeihez való fizikai hozzáférés esetén ne lehessen visszafejteni a tárolt üzemeltetési és felderítési adatokat. A leggyakoribb támadási módok közé tartoznak az ellopott vagy megsemmisített járműről készült memóriaadatok „használata”, az eszközök selejtezésekor elhagyott háttértárak, valamint az úgynevezett „evil maid” típusú akciók, amikor egy rosszindulatú szereplő illetéktelenül fér hozzá a géphez és közvetlenül próbál adatokat kinyerni vagy fertőzni. [28]

A titkosítási mechanizmusok alapját a széles körben elfogadott, nyilvános kulcsos és szimmetrikus algoritmusok – például az AES (Advanced Encryption Standard) és az RSA – adják. A megvalósítás szintje szerint megkülönböztetünk teljes lemeztitkosítást (Full-Disk Encryption, FDE), ahol az eszköz minden tartalma egyetlen titkos kulccsal védett, és fájlszintű hozzáférés csak a felhasználói hitelesítés után engedélyezett, valamint részleges, fájlszintű titkosítást, ahol csak az előre kijelölt fájlok vagy mappák kerülnek titkosításra, finomabb szabályozást és költséghatékonyabb erőforrás-felhasználást téve lehetővé. [28]

A titkosítás mindezek mellett az EPP-platformok (Endpoint Protection Platforms) – amelyekbe beépítik az antivírus, az rosszindulatú szoftver ellenei védelmet, a személyes tűzfal és az behatolás megelőző modulokat – alapvető komponense. Az EPP-megoldások egyik kulcsfunkciója éppen a „data encryption”, azaz az adattitkosítás. Így egyetlen, központosított védelmi platformon belül valósítható meg az adatbiztonság, a behatolás-észlelés és a reagálás is. [29]

Katonai földi harcjárművek esetében a végponti titkosítás ma már nélkülözhetetlen: a páncélozott járművekben futó érzékeny operációs rendszerek és az azokhoz kapcsolódó adatbázisok teljesítményeiket illető metrikákat, a térképadatokat, a célpontkoordinátákat és a hálózati kommunikáció naplóit kizárólag titkosított formában tárolják. Emellett az utánpótlást és karbantartást végző modulok USB- vagy más cserélhető adathordozóit is automatikusan titkosítják, így megakadályozva a tranzit közben történő adatlopást. Így minimalizálható, hogy GPS-jel zavarással vagy kieséssel, vagy elektronikus interferencia esetén sem sérüljenek a műveleti adatok, és a jármű személyzete akár hálózati kapcsolat nélküli környezetben is biztonságosan meghozhassa döntéseit. [28]

Többlépcsős hitelesítés

A többtényezős hitelesítés (MFA) alapja, hogy a felhasználó kilépéskor ne csak egyetlen jelszó vagy PIN használatával, hanem legalább két, egymástól eltérő kategóriájú tényező – „amit tud” (jelszó/PIN), „amit birtokol” (hardveres tokén vagy mobilos alkalmazás) és/vagy „ami ő maga” (biometrikus azonosító) – együttes igazolásával férhessen hozzá a rendszerhez. [30]

Három fő összetevője van: a hitelesítők (authenticators), amelyek előállítják a bizonyítékot arról, hogy a felhasználó valóban rendelkezik a „what you have” tényezővel; az érvényesítők (validators), amelyek ellenőrzik, hogy a bemenetet valóban az adott hitelesítő generálta; valamint az identitás- és hitelesítőkezelést biztosító életciklus-menedzsment, amely gondoskodik a kulcsok vagy tokenek kiadásáról, visszavonásáról és lejáratáról. [30]

A NIST SP 800-63-3 szabvány három Assurence Level (AAL) szerinti besorolást határoz meg: a kormányzati rendszerek hivatalos információs rendszereihez AAL 2, míg a különösen érzékeny vagy küldetéskritikus rendszerekhez akár AAL 3 szintet írnak elő. Az AAL 2-megoldások esetén elegendő, ha az authentikátor hardveres (például egy FIPS 140-2 minősítésű tokén) vagy szoftveres (például egy hitelesítő mobilapp) formában valósítja meg a „what-you-have” tényezőt, és ehhez kapcsolódik egy PIN- vagy biometrikus aktiváció, amely igazolja a „what-you-know/are” tényezőt. Ezzel szemben az AAL 3 rendszereknél kötelező a hardveres, kriptográfiai (TPM vagy HSM) kulcsok használata és a felhasználó biometrikus azonosítása is, hogy a fizikai és logikai védelem egyaránt garantált legyen. [30]

A biztonságos MFA-megvalósítás védelmet nyújt az olyan támadásokkal szemben, mint a jelszótároló vagy –naplózó rosszindulatú szoftverek, a visszajátszásos (replay) és a beékelődéses támadás (man-in-the-middle) kísérletek. Semmilyen MFA-mechanizmus sem nyújt védelmet egy teljesen kompromittált eszközzel szemben, ezért ahol csak lehetséges, központilag menedzselt eszközön (GFE) kell futtatni az authentikációs klienseket. [30]

A szárazföldi katonai járművekben az MFA-t több szinten alkalmazzák a teljes operációs folyamatra kiterjedően. A parancsnoki- és tűzvezetőállomások konzoljai csak akkor aktiválják a harci- és navigációs szoftvereket, ha a kezelő sikeresen végrehajtotta a több tényezős hitelesítést (például személyre kiosztott PIV-token + PIN + ujjlenyomat). Ugyanezt a szigorúságot alkalmazzák a járműfedélzeti Ethernet- és CAN-busz alrendszereinek belépésvezérlésénél is: az érzékelők, kommunikációs és navigációs modulok csak a sikeres MFA után csatlakozhatnak, ezzel kizárják a jogosulatlan eszközök fizikai csatlakoztatásának veszélyét. [30]

Gépi tanulás alapú behatolás-észlelő rendszerek

A nagy és kiegyensúlyozatlan hálózati adatállományok esetén a hagyományos aláírásalapú behatolás-észlelő rendszerek (IDS) gyakran túl lassúak vagy pontatlanok. Ezért az új rendszerben először véletlenszerű túlmintavételezéssel (Random Oversampling) kezelik az osztályok közti egyensúlyhiányt, majd klaszterezésre épülő stacking feature embeddinggel meta-jellemzőket hoznak létre, végül főkomponens-analízist (PCA) alkalmaznak a dimenziók csökkentésére. Ezek után döntési fa (DT), véletlen erdő (RF) és extra fa (ET) klaszterekkel tanítják a rendszert, amely az UNSW-NB15, a CIC-IDS-2017 és a CIC-IDS-2018 adathalmazokon 99,59–99,99 %-os pontosságot ért el, ezzel folyamatosan meghaladva a korábbi state-of-the-art módszerek teljesítményét. [31]

Az új, IoT-hálózatokhoz tervezett, anomáliákon alapuló behatolás-észlelő rendszer (AIDS) készült, ahol a nagy mennyiségű, heterogén és erőforrás-korlátos adatokra egy ritka automatikus kódoló (Sparse Autoencoder, SAE) és egy konvolúciós neurális háló (CNN) kombinációját alkalmazzák. A SAE először kis sűrűségű reprezentációfelépítéssel csökkenti az adatok dimenzióját, majd a CNN bináris klasszifikátorként működik: a Bot-IoT adatbázison elért 99,9 %-os pontosság, 100 %-os visszahívás (recall) és 0,03 %-os téves riasztási arány (FPR) bizonyítja, hogy a modell hatékonyan kezel nagy, zajos IoT-adatfolyamokat és alacsony késleltetésű detektálást tesz lehetővé. [32]

A mélytanulásos IDS-ek a bemeneti adatokat (nyers csomagok, hálózati folyamatok, naplófájlok) egymástól elkülöníti, majd a detektálásra használt architektúrák (CNN, RNN, autoenkóder, hibrid megoldások) és a telepítési stratégiák (edge-től a felhőig) szerinti csoportosítás következik. E felosztás mentén elemzi az alkalmazott értékelési módszerek hatékonyságát, a válaszidőt, a skálázhatóságot és a hamis pozitív riasztások arányát, kiemelve, hogy a mélyháló-technológiák jelentősen javítják az ismeretlen támadások detektálását, ugyanakkor komoly terhelést tesz az erőforrás-szegény környezetekre, ezért katonai alkalmazásban különösen fontos a modulok méretezése és optimalizálása. [33]

E három, egymást kiegészítő megközelítésből összeálló portfólió lehetővé teszi, hogy a modern szárazföldi harcjárművek fedélzeti kommunikációs és szenzorhálózatait valós időben monitorozó IDS-ek hatékonyan kezeljék a nagy és kiegyensúlyozatlan adatáramokat, alkalmazkodjanak a változó és strukturálatlan IoT-környezethez, valamint gyorsan és pontosan észleljék az új típusú hálózati behatolásokat. Így a legénység védelme érdekében minimalizálható a rejtett vagy kifinomult hálózati támadások kockázata, miközben fenntartható marad a késleltetés és a számítási erőforrás-használat egyensúlya.

Kvantum kulcscsere protokollok

A kvantumkulcs-elosztás (QKD) a kvantummechanika alaptörvényeire építve olyan titkosított kommunikációs módszer, amely két fél között kriptográfiai kulcsanyag előállítását és megosztását teszi lehetővé oly módon, hogy a fizika törvényei garantálják az adatok védelmét. A hagyományos kulcsszétosztás matematikai nehézségekre épül, melyek a jövőbeli kvantumszámítások megjelenésével kiszolgáltatottá válnak, ezzel szemben a QKD a no-cloning tételre és a mérési zavarhatás elvére alapoz, azaz bármely lehallgatási kísérlet megváltoztatja a kvantumállapotot, észlelhetővé téve a támadót az érintett felek számára; ez a biztonsági funkció semmilyen hagyományos módszerben nem áll rendelkezésre. [34]

A megvalósítás során egy sor foton kerül átküldésre optikai szálon vagy szabad térben a kulcs két pontja közötti összeköttetésben, a fotonok kvantumállapotának véletlenszerű jellege egy qubit-sorozatot generál, amelyet végül egy, a küldő és a vevő által közösen elvégzett hibajavítási és adatvédelmi fázis után titkosító kulcsként használnak fel. [34]

Katonai környezetben a QKD modulok a járművek fedélzeti kommunikációs architektúrájába integrálva a parancsnoki lánc bizalmát erősítik, hiszen a kulcscsere fizikailag elkülönített, dedikált szálas vagy szabad térben működő optikai linkeken zajlik, és a no-cloning elv értelmében minden lehallgatási kísérlet azonnal láthatóvá válik, így a járművek közötti érzékeny parancsok, tűzvezetési adatok és koordináták védelme jelentősen fokozható.[34]

Ugyanakkor ez a megközelítés speciális hardvereszközöket igényel – kvantumfoton-forrásokat, egykópiás fotondetektorokat és precíziós optikai elemeket –, amelynek telepítési és fenntartási költsége, valamint a jelenlegi technológiák 100–300 km alatti hatótávolsága jelentős infrastruktúra-igényt támaszt, továbbá a rendszerben megbízható, bizalmi hídnak tekintett köztes pontok (trusted relays) alkalmazását teszi szükségessé. [35]

A QKD által generált kulcsanyag kizárja a klasszikus visszafejtési és hamisítási eljárásokat de, a gyakorlatban számos technikai korlát befolyásolja a hatékonyságot: a QKD csak a titkosítási kulcsok előállításáért felel, önmagában nem ellenőrzi a forrást, ezért aszimmetrikus kriptográfia vagy előre megosztott titkos kulcsok nélkülözhetetlenek a forráshitelesítéshez; a kvantumcsatorna érzékenysége a szolgáltatásmegtagadásos (DoS) támadásoknak (például fotonblokkolás) is teret ad; továbbá a teljes QKD-hálózat biztonságos ellenőrzése rendkívül alacsony hibahányadot követel, ami a fizikai és mérnöki megvalósítás során komoly kihívásokat jelent. [35]

Ennek ellenére a QKD a jövőbeni kvantumszámítógépek fenyegetéseivel szemben is ellenálló kulcscserét kínál, ezért a katonai járművekben a hagyományos és poszt-kvantum kriptográfiai módszerekkel kombinálva biztosítható a kommunikáció megbízhatósága és a parancsok sértetlensége a következő évtizedekben is. [34], [35]

Dinamikus hálózati szegmentálás

A hálózati szegmentáció olyan biztonsági elv, mely a korábbi, monolitikus, „mindent egy kalap alá” üzemmódból kifolyólag kialakult támadási felületet kisebb, elkülönített alhálózatokra bontja, ezzel minimalizálva az esetleges behatolások terjedését. A U.S. Air Force 2024-ben kiadott Zero Trust stratégiájában világosan megfogalmazódott, hogy a hagyományos, csak peremvédelmi szegmensekre épülő megközelítés helyett a megoldás a data center–, hoszt– és mikro-szolgáltatás-szerű (micro-service) hálózati izolációban rejlik, amely az egyes szolgáltatások és erőforrások között szigorú, dinamikusan alkalmazott biztonsági szabályokat érvényesít. [36]

A logikai szegmentáció nem feltétlenül igényel új fizikailag elkülönített berendezéseket: a VLAN-ek, alhálózatok (subnetting) és virtuális alagutak (VPN) már önmagukban is képesek olyan önálló, zárt „buborékokat” létrehozni, amelyeken belül a forgalom csak szigorú, előre definiált szabályok szerint haladhat. [37]

A szegmentáció lényege a bizalmi zónák (security zones) kialakítása és a köztük lévő forgalom mérése, alakítása, valamint a hardveres vagy szoftveres tűzfalakon keresztüli ellenőrzés, melynek célja a kártékony vagy jogosulatlan kommunikáció blokkolása. [38]

Amikor ezt a katonai szárazföldi járművek fedélzeti hálózatára adaptáljuk, a CAN-busz, a járműbelsői Ethernet és az érzékelői adatcsatornák felosztása – például parancsnoki/szituációs tudatossági, szenzor-adatgyűjtő, fegyver-vezérlő és ECM-blokkokra – garantálja, hogy amennyiben egy alrendszer fertőzötté válik, a rosszindulatú kód nem tud oldalirányban terjedni a többi, kritikus funkciót ellátó szegmensre. [37]

Minden egyes szegmens közötti átjárás – akár csomag-irányítás, akár szolgáltatás-hívás – csak kriptográfiai hitelesítés és szigorú hozzáférés-ellenőrzés után engedélyezett, ezzel védve a belső kapcsolódást célzó „mellékkapcsolt” támadások, a busz-túlterheléses DoS-kísérletek, valamint az ellenséges forgalomtorzítási (MITM) forgatókönyvek ellen. [36]

Mindez nem csak a jármű önvédelmét szolgálja, hanem a missziókritikus adatcsere titkosságát és sértetlenségét is, hiszen a parancskoordináták, a valós idejű helyzetjelentések és a célpontadatai soha nem hagyják el a nekik fenntartott, külön – Zero Trust elvek mentén – validált szegmenst. Így egy esetleges belső kompromittálódás vagy ellenséges behatolás esetén a kár lokalizálható és korlátozható, ezzel is növelve a jármű túlélőképességét és a személyi kockázatokat minimalizálva a hadszíntéren. [37], [38]

Hitelesített szoftverfrissítések fontossága

A hitelesített szoftverfrissítés lényege, hogy minden egyes firmware- vagy szoftvercsomagot a gyártó privát kulcsával digitálisan aláírnak, és csak ezzel az aláírással hitelesített csomag telepíthető az ECU-kon (Electronic Control Unit) belül. [39]

A frissítéscsomag előkészítésekor a teljes csomag tartalmáról kriptográfiai hash-értéket képeznek, majd ezt a hash-t titkosítva – illetve opcionálisan tanúsítványláncon keresztül igazolva – a csomaggal együtt továbbítják. A járműfedélzeti update-ügynök a fogadáskor először a beégetett gyártói nyilvános kulcs segítségével dekódolja az aláírást, majd összehasonlítja a kapott hash-t a csomag tényleges tartalmából számított értékkel. Amennyiben bármelyik ellenőrzés – érvénytelen aláírás, eltérés a hash-értékek között vagy visszavont tanúsítvány használata – sikertelen, a frissítés azonnal megszakad, és a rendszer naplózza az eseményt, ezáltal megakadályozva a rosszindulatú kód vagy a manipulált csomag beépülését. [39]

Katonai szárazföldi harcjárművekben a hitelesített frissítés kulcsfontosságú a kritikusan biztonságérzékeny modulok – például a tűzvezérlő algoritmusok, a navigációs és kommunikációs rendszerek – integritásának és megbízhatóságának megőrzéséhez. Egy ilyen rendszerrel kizárható a távoli, ellenőrzés nélküli frissítések útján történő backdoor-telepítés, a supply-chain támadások (például beszállítói kompromittálás) és az utánközlő (replay) kísérletek lehetősége, miközben garantálja, hogy csak a hiteles forrásból származó, gyártó által jóváhagyott kód fusson a jármű fedélzetén. [39]

Rendszeres biztonsági auditok

A modern katonai járművek fedélzeti rendszereinek villamosítása újabb sebezhetőségi dimenziókat nyit meg, ezért elengedhetetlenné vált a rendszeres biztonsági auditok és frissítések alkalmazása. A “smart” és opcionálisan pilóta nélküli harcjárművek egyre bonyolultabb, számítógépesített és hálózatba kötött rendszereket tartalmaznak, melyekben a szoftveres komponensek folyamatos vizsgálata és hitelesítése nem csupán ajánlott, hanem kifejezetten kötelező eleme a védelemnek. A rendszeres auditok keretében nemcsak a frissítések telepítésének folyamatát ellenőrzik – így biztosítva, hogy kizárólag hiteles, aláírt firmware kerüljön az egységekbe –, hanem a járművek hálózati és fizikai interfészeiről begyűjtött naplóadatokat, konfigurációkat és biztonsági beállításokat is átvilágítják. [40]

Ezeknek az auditoknak a technikai keretrendszerét a NIST SP 800-115 gyakorlatias ajánlásai szolgáltatják, amelyben a dokumentum részletes útmutatást ad a biztonsági tesztek és vizsgálatok megtervezéséhez, végrehajtásához, az eredmények elemzéséhez és a hibák korrekciójához. A szabvány hangsúlyozza, hogy a tesztelés nem egyszeri esemény, hanem ciklikusan, például negyedéves vagy félezredéves ütemezésben kell történnie, így a járművek szoftverösszetevői, operációs rendszerei és kommunikációs protokolljai mindig naprakészek maradnak a legújabb sebezhetőségekkel szemben. A NIST-ajánlások kiterjednek a sebezhetőség-felismerés módszereire (segedeltek használata, scanning eszközök, penetrációs tesztelés) és az auditok dokumentációjára, amely lehetővé teszi a vezetőség számára, hogy átláthatóan kövesse a biztonsági helyzet változását és a javítóintézkedések hatékonyságát. [41]

Katonai környezetben ezek a rendszeres auditok a jármű fedélzeti elektronikájának, akkumulátor- és töltőinfrastruktúrájának, valamint a hálózati alrendszereknek (pl. CAN-busz, Ethernet, V2X) az integritását és megbízhatóságát garantálják. A negyedéves auditok során az illetékes biztonsági csoportok minden szoftverkomponenst, tanúsítványt és konfigurációs beállítást ellenőriznek, valamint penetrációs teszteket hajtanak végre a járművek belső hálózatán, így az esetleges supply-chain támadások (backdoor-beszúrások) vagy a töltőállomásokon keresztüli rosszindulatú behatolások már a telepítésük előtt felfedhetők és megszüntethetők. [40], [41]

A rendszeres biztonsági auditok védelmet nyújtanak az olyan támadások ellen is, mint a firmware-manipuláció, a jogosulatlan konfigurációváltoztatás vagy a hálózati infrastruktúra kompromittálása. Segítségükkel a biztonságért felelős mérnökök időben azonosíthatják a beállítási hibákat, a gyenge jelszavakat, a lejárt tanúsítványokat és a nem-hitelesített szoftverösszetevőket, melyek egyébként lehetővé tennék a Parancsnoki és Irányító (C2) rendszerek feltörését, a járművezetés eltérítését vagy a töltőhálózat leállítását. Így a rendszeres auditok nem csupán az üzembiztonságot növelik, hanem a legénység és az üzemeltetési adatok védelmét is kritikus fontosságú módon szolgálják. [40], [41]

Összefoglalás és konklúzió

A bemutatott háromrétegű architektúra – a több-modalitású érzékelők és valós idejű adatgyűjtés, az autonóm navigációs és mozgásvezérlő eljárások, valamint a kiberbiztonsági mechanizmusok szoros összjátékán alapuló védelem – együttesen képes olyan holisztikus harci platformot létrehozni, amely egyszerre reagál gyorsan a környezeti kihívásokra és ellenáll a komplex külső fenyegetéseknek. A LiDAR, milliméterhullámú radar és EO/IR kamerák által szolgáltatott gazdag terep- és céladatokat a mélytanuló konvolúciós hálózatok, a SLAM és a GNSS/IMU integráció biztosítja, míg az FPGA- és GPU-gyorsítókkal felvértezett edge-AI modulok garantálják az alacsony késleltetésű, megbízható döntéshozatalt. Ezt a képességet egészíti ki a hardveres Root of Trust, a végponti titkosítás, a többtényezős hitelesítés, az anomáliadetektáló IDS-ek, a dinamikus hálózati szeparáció és a kvantumbiztos kulcscsere, amelyek együtt hoznak létre egy több szinten elhelyezkedő, egymást erősítő védelmi ökoszisztémát.

A jövő harcjárművei számára ez az integrált megközelítés nem csupán technológiai fejlődést jelent, hanem új taktikai szabadságot és túlélőképességet biztosít: a kritikus parancsok és céladatok a legszigorúbb körülmények között is titkosan, sértetlenül jutnak célba, a navigáció és célkövetés pedig kiszámíthatóan pontos marad, még ha a GPS-jelek el is vesznek, vagy elektronikus interferencia terheli a környezetet. A következő generációs fejlesztések feladata, hogy mindezeket a komponenseket tovább finomítsa – részben algoritmikus optimalizációval, részben poszt-kvantum kriptográfiára való átállással –, és a katonai standardok szigorú környezeti, megbízhatósági és biztonsági követelményeinek még magasabb szintű kielégítését tegye lehetővé. Csak egy ilyen, maradéktalanul védett és adaptív rendszer képes kiteljesíteni a szövetséges erők követelményrendszerét a modern, összetett hadszíntéren, és garantálni a legénység biztonságát, valamint a misszió sikerét a következő évtizedekben.

Források:

[1] “What Is A Sensor and What Does it Do?,” Data Acquisition | Test and Measurement Solutions. Accessed: May 14, 2025. [Online]. Available: https://dewesoft.com/blog/what-is-a-sensor

[2] Stoner J., “What is EO/IR (Electro-Optical/Infrared) & How Does it Work?,” Fly Eye. Accessed: May 15, 2025. [Online]. Available: https://www.flyeye.io/drone-acronym-eo-ir/

[3] “Vehicle EO/IR Sensors,” Leonardo DRS. Accessed: May 15, 2025. [Online]. Available: https://www.leonardodrs.com/what-we-do/our-solutions/advanced-sensing/ground-vehicle-eo-ir-sensors/

[4] “Doppler-effektus,” *Wikipédia*. Apr. 01, 2025. Accessed: May 15, 2025. [Online]. Available: https://hu.wikipedia.org/w/index.php?title=Doppler-effektus&oldid=28014014

[5] “(PDF) Vehicle-mounted Millimeter-wave Radar Target Recognition Technology,” *ResearchGate*, Jan. 2025, Accessed: May 15, 2025. [Online]. Available: https://www.researchgate.net/publication/387964933_Vehicle-mounted_Millimeter-wave_Radar_Target_Recognition_Technology

[6] “LiDAR: What Is It and How Does It Work?,” YellowScan. Accessed: May 15, 2025. [Online]. Available: https://www.yellowscan.com/knowledge/how-does-lidar-work/

[7] “Military LiDAR Solutions for Defense Applications,” Defense Advancement. Accessed: May 15, 2025. [Online]. Available: https://www.defenseadvancement.com/suppliers/military-lidar/

[8] “What are Convolutional Neural Networks? | IBM.” Accessed: May 15, 2025. [Online]. Available: https://www.ibm.com/think/topics/convolutional-neural-networks

[9] “YOLO Algorithm for Object Detection Explained [+Examples].” Accessed: May 15, 2025. [Online]. Available: https://www.v7labs.com/blog/yolo-object-detection

[10] H. Amit, “Object Detection with YOLO and Faster R-CNN,” Biased-Algorithms. Accessed: May 15, 2025. [Online]. Available: https://medium.com/biased-algorithms/object-detection-with-yolo-and-faster-r-cnn-c2c1eda63dad

[11] “What is Non-Maximum Suppression?,” GeeksforGeeks. Accessed: May 15, 2025. [Online]. Available: https://www.geeksforgeeks.org/what-is-non-maximum-suppression/

[12] G. Boesch, “The Fundamental Guide to Faster R-CNN,” viso.ai. Accessed: May 15, 2025. [Online]. Available: https://viso.ai/deep-learning/faster-r-cnn-2/

[13] “Military GPU | Rugged Mil-Spec Graphics Cards & GPGPU Boards,” Defense Advancement. Accessed: May 15, 2025. [Online]. Available: https://www.defenseadvancement.com/suppliers/graphics-cards-gpu-video-processing-boards/

[14] “Aitech’s NVIDIA Jetson AGX Orin-based Supercomputer Increases Rugged AI Processing in Military Applications,” Military Aerospace. Accessed: May 15, 2025. [Online]. Available: https://www.militaryaerospace.com/directory/board-products/communications-network-controllers/press-release/55288307/aitech-aitechs-nvidia-jetson-agx-orin-based-supercomputer-increases-rugged-ai-processing-in-military-applications

[15] “NVIDIA Jetson | Curtiss-Wright Defense Solutions.” Accessed: May 15, 2025. [Online]. Available: https://www.curtisswrightds.com/media-center/blog/nvidia-jetson-military-aerospace

[16] "stereo camera - an overview | ScienceDirect Topics." Accessed: May 15, 2025. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/stereo-camera

[17] "(PDF) Unmanned ground vehicle perception using thermal infrared cameras," *ResearchGate*, doi: 10.1117/12.884349.

[18] Stoner J., "What is SLAM (Simultaneous Localization and Mapping)?," Fly Eye. Accessed: May 15, 2025. [Online]. Available: https://www.flyeye.io/drone-acronym-slam/

[19] X. Yan, W. Guo, Y. Wang, and S. Li, "Application of Visual SLAM Technology in Military Intelligent Unmanned Systems," in *Proceedings of the 2024 4th International Conference on Artificial Intelligence, Big Data and Algorithms*, in CAIBDA '24. New York, NY, USA: Association for Computing Machinery, Október 2024, pp. 206–211. doi: 10.1145/3690407.3690442.

[20] "Military Satellite Navigation Technology (GPS/GNSS) Systems," Defense Advancement. Accessed: May 15, 2025. [Online]. Available: https://www.defenseadvancement.com/suppliers/military-satellite-navigation-gps-gnss/

[21] "Navigation Grade IMU | GPS/INS | Weapon Orientation Modules," Defense Advancement. Accessed: May 15, 2025. [Online]. Available: https://www.defenseadvancement.com/company/inertial-labs/

[22] "(PDF) Field Programmable Gate Array (FPGA) based Collision Avoidance using acceleration velocity obstacles," in *ResearchGate*, doi: 10.1109/ROBIO.2012.6491318.

[23] "(PDF) A FPGA-based Accelerator Implementation for Path Planning using Q_learning Algorithm," *ResearchGate*, Accessed: May 15, 2025. [Online]. Available: https://www.researchgate.net/publication/360095053_A_FPGA-based_Accelerator_Implementation_for_Path_Planning_using_Q_learning_Algorithm

[24] "(PDF) Wireless Communication Between Vehicles: Exploring the Potential of V2V and V2X Communication for Improved Efficiency, Safety, and Sustainability," *ResearchGate*, Accessed: May 15, 2025. [Online]. Available: https://www.researchgate.net/publication/372824335_Wireless_Communication_Between_Vehicles_Exploring_the_Potential_of_V2V_and_V2X_Communication_for_Improved_Efficiency_Safety_and_Sustainability

[25] "What Is Vehicle to Everything (V2X)?," Built In. Accessed: May 15, 2025. [Online]. Available: https://builtin.com/articles/v2x-vehicle-to-everything

[26] "What is a Root-of-Trust (RoT)?," Trusted Computing Group. Accessed: May 15, 2025. [Online]. Available: https://trustedcomputinggroup.org/about/what-is-a-root-of-trust-rot/

[27] "Hardware Root of Trust: Everything you need to know," Rambus. Accessed: May 15, 2025. [Online]. Available: https://www.rambus.com/blogs/hardware-root-of-trust/

[28] "What is Endpoint Encryption?," Check Point Software. Accessed: May 15, 2025. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-security/what-is-endpoint-encryption/

[29] "(PDF) Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat," in *ResearchGate*, Apr. 2025. doi: 10.1109/CyberC.2019.00023.

[30] "MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.pdf." Accessed: May 15, 2025. [Online]. Available: https://media.defense.gov/2024/Jul/31/2003515137/-1/-1/0/MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

[31] Md. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *Journal of Big Data*, vol. 11, no. 1, p. 33, Feb. 2024, doi: 10.1186/s40537-024-00886-w.

[32] M. A. Alsoufi *et al.*, "Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks," *CMES*, vol. 141, no. 1, pp. 823–845, 2024, doi: 10.32604/cmes.2024.052112.

[33] "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues | Request PDF," *ResearchGate*, doi: 10.1016/j.knosys.2019.105124.

[34] "What is Quantum Key Distribution (QKD) and How Does it Work?," Search Security. Accessed: May 15, 2025. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

[35] "National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC." Accessed: May 15, 2025. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[36] "Segmentation is Key in U.S. Air Force's Zero Trust Strategy – How Other Agencies Can Follow Suit," Cyber Defense Magazine. Accessed: May 15, 2025. [Online]. Available: https://www.cyberdefensemagazine.com/segmentation-is-key-in-u-s-air-forces-zero-trust-strategy-how-other-agencies-can-follow-suit/

[37] "What Is Network Segmentation? How It Works & Why It Matters," Nile. Accessed: May 15, 2025. [Online]. Available: https://nilesecure.com/network-security/what-is-network-segmentation-how-it-works-why-it-matters

[38] "What Is Network Segmentation?," Cisco. Accessed: May 15, 2025. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[39] R. Bielawski, R. Gaynier, D. D. Ma, S. Lauzon, and D. A. Weimerskirch, "Cybersecurity of Firmware Updates".

[40] K. Csenkey and A. Rapin, "Power and Tension: The Cyber Security Problems of Military Electrification," War on the Rocks. Accessed: May 15, 2025. [Online]. Available: https://warontherocks.com/2024/06/power-and-tension-the-cyber-security-problems-of-military-electrification/

[41] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment.," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115.

2.2. CPS ÉS MI SZEREPE A PRECÍZIÓS NÖVÉNY TERMESZTÉSBEN ÉS ÁLLAT TARTÁSBAN VASAS GERGŐ

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

IPAR 4.0 TECHNOLÓGIÁK

CPS ÉS MI SZEREPE A PRECÍZIÓS NÖVÉNY TERMESZTÉSBEN ÉS ÁLLAT TARTÁSBAN

VASAS GERGŐ

[redacted]

(GKNB_INTM087)

2024/25/2

Tartalomjegyzék

BEVEZETÉS 3

Mi a kiberfizikai rendszer fogalma? 3

Mi a mesterséges intelligencia fogalma? 4

MI A PRECÍZIÓS GAZDÁLKODÁS? 4

Precíziós mezőgazdaság fejlődése 5

CPS ÉS MI SZEREPE A NÖVÉNYTERMESZTÉSBEN 7

Kiberfizikai rendszerek 7

I. Talaj nedvességét mérő szenzorok 8

II. Növénymegfigyelés 9

Mesterséges intelligencia a növénytermesztésben 12

I. Betegség felismerés gépi látással 13

II. Automatikus beavatkozás 14

III. Osztályozás és válogatás minőség szerint 14

CPS és MI szerepe az állattartásban 15

Kiberfizikai rendszerek 15

I. Egészségügyi monitoring rendszerek 15

II. Drónok használata a precíziós állattartásban 16

Mesterséges intelligencia az állattartásban 17

I. Automatizálás az állattartásban 18

II. Mesterséges intelligencia szerepe a szarvasmarha szelekcióban 19

A PRECÍZIÓS MEZŐGAZDASÁG KÖRNYEZETRE GYAKOROLT HATÁSA 20

A PRECÍZIÓS MEZŐGAZDASÁG ELTERJEDÉSÉNEK NEHÉZSÉGEI 21

1. Szakértelem és tudás hiánya 21

2. Magas technológiai költségek 21

3. Társadalmi hatások 21

4. Bizalmi nehézségek 21

KONKLÚZIÓ 22

ÁBRA JEGYZÉK 23

FORRÁSOK 24

BEVEZETÉS

A kiberfizikai rendszerek (Cyber-Physical Systems – CPS) és a mesterséges intelligencia (MI) alkalmazása egyre meghatározóbb szerepet játszik a modern mezőgazdaságban. Az Ipar 4.0 forradalmának köszönhetően olyan változások mentek végbe, amelyek nagymértékben megváltoztatták a mezőgazdasági szektor működését. Ezek a fejlesztések lehetővé tették, hogy a korábban idő- és munkaigényes folyamatok egyszerűbben, precízebben és gyorsabban valósuljanak meg, mint az Ipar 4.0-t megelőzően. A CPS és az MI alkalmazása nemcsak a termelés optimalizálását segíti elő, hanem hozzájárul egy sokkal környezetbarátabb és fenntarthatóbb gazdálkodási forma kialakításához is.

Mi a kiberfizikai rendszer fogalma?

A kiberfizikai rendszerek (CPS) olyan intelligens rendszerek, amelyek a fizikai eszközök (például szenzorok, gépek) és a számítógépes elemek (mint az algoritmusok, szoftverek, hálózatok) szoros együttműködésén alapulnak. Ezek a rendszerek képesek adatokat gyűjteni a környezetükből, azokat valós időben elemezni, majd az eredmények alapján önálló döntéseket hozni. [1] (1.ábra)

1. ábra CPS rendszer bemutatása talajnedvesség esetén- https://compactionprevention.com/the-innovation/

A CPS célja, hogy nagyobb hatékonyságot, pontosságot és megbízhatóságot biztosítson olyan területeken, mint például a mezőgazdaság.

Mi a mesterséges intelligencia fogalma?

A mesterséges intelligencia (MI) olyan számítógépes algoritmusok összességét jelenti, amelyek képesek az önfejlesztésre és tanulásra. Az MI képes olyan feladatok elvégzésére, amelyeket korábban kizárólag emberek tudtak megoldani. A mesterséges intelligencia egy gyűjtőfogalom, amely több technológiát is magába foglal, például a gépi tanulást, a gépi látást és a természetes nyelvfeldolgozást. [2] (2.ábra)

2. ábra A mesterséges intelligencia bemutatása

https://www.neilsahota.com/what-is-artificial-intelligence-how-does-it-work/

MI A PRECÍZIÓS GAZDÁLKODÁS?

A precíziós gazdálkodás egy modern mezőgazdasági eljárás, amely során digitális és műholdas technológiák segítségével optimalizálják az erősforrások, mint például a műtrágya vagy a vegyszerek adagolását és ezzel csökkentve a költségeket és a környezetre kitett természeti hatásokat.[3]

Az eljárás alapelve 1980-as években jelent meg az Amerikai Egyesült Államokban, viszont elterjedése csak az elmúlt 5 év technológiai fejlődése következtében terjedt el igazán a CPS és MI alapú rendszerek használatát követően.[3]

A kiberfizikai rendszerek (CPS) és a mesterséges intelligencia (MI) segítségével a mezőgazdaságban valós időben gyűjthetjük és elemezhetjük az adatokat. A CPS rendszerek érzékelői például mérik a talaj nedvességét, amit az MI feldolgoz, és az így nyert adatok alapján előrejelzéseket, illetve javaslatokat ad az optimális gazdálkodáshoz. Így a gazdák könnyebben és pontosabban meghatározhatják, mikor érdemes öntözni, műtrágyázni, takarmányozni vagy betakarítani, ezáltal javítva a termelés hatékonyságát.

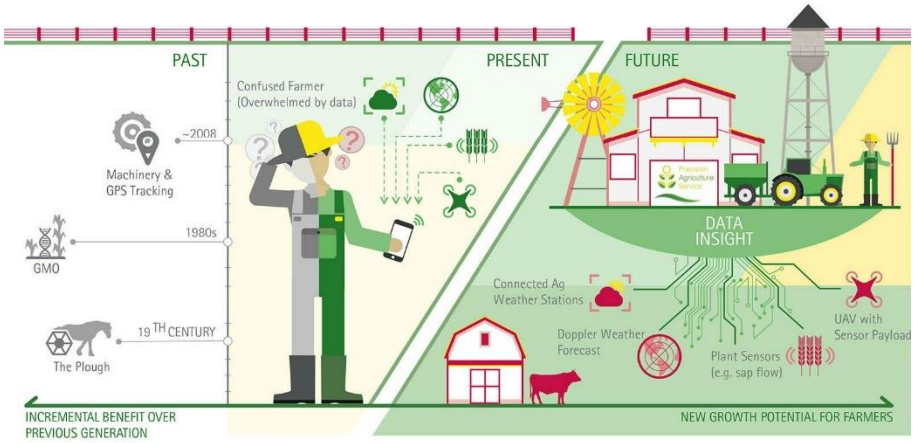
Precíziós mezőgazdaság fejlődése

A precíziós mezőgazdaság fejlődése az 1970-es években kezdődött, amikor a GPS-es helymeghatározó rendszereket először mezőgazdasági gépekre is elkezdték felszerelni. 1984-ben már olyan térképeket készítettek GPS segítségével, amelyek megmutatták a termőföld minőségét, majd 1991-től olyan digitális térképeket is használtak, amelyek segítettek az egyes területekre szabott gazdálkodásban. [5] (3,4.ábra)

A kilencvenes évek második felétől különféle érzékelőket kezdtek használni, például légi és műholdas eszközöket, hogy felmérjék a növények állapotát. 1999-től már a talaj jellemzőit is vizsgálták, például az elektromos vezetőképességet, hogy pontosabb képet kapjanak a föld állapotáról. [5] (3,4.ábra)

2000 körül megjelentek a nagy pontosságú helymeghatározást biztosító rendszerek (RTK), majd ezeket 2002-re már gyomirtásra és nagyon pontos vetésre is elkezdték használni. 2003-ban bevezették az automatikus kormányzást a traktorokon, 2008-ra pedig olyan rendszerek jelentek meg, amelyek irányított útvonalon mozgatták a gépeket.[5] (3,4.ábra)

2011-től drónokat is használnak a területek felmérésére, 2015-től pedig megjelentek az első robotok is, amelyek főleg kertészeti növények gondozásában segítenek.[5](3,4.ábra)



3. ábra Precíziós gazdálkodás idővonala - https://web.archive.org/web/20200309230626/https://www.accenture.com/us-en/insight-accenture-digital-agriculture-solutions

Évszám	Elért eredmény
1970–1980	A GPS technológia bevezetése, az első helymeghatározó kombájnra szerelve
1984	Az első minőség helymeghatározó térképek bemutatása (GPS-sel)
1991	Alkalmazási térképek (GIS alapú) bevezetése
1995–1998	Földi és műholdas/légi érzékelő rendszerek a termés állapotának mérésére (klorofil tartalom)
1999 – 2002	A talaj elektromos vezetőképesség-mérésének és légi/műholdas mérésének bevezetése
2000	A mezőgazdaságban alkalmazott RTK rendszerek bevezetése
2000 – 2002	Első próbálkozás gyomirtó rendszerrel és precíz vetéssel
2003	Az automata kormányzás bevezetése a mezőgazdaságban
2008	Az első irányított közlekedési rendszerek bevezetése a gazdálkodók körében
2011	UAV-ok (drónok) bevezetése az alkalmazási térképekhez
2015	Az első robotrendszerek bevezetése a nagy értékű növények termesztésében/kertészetben

4. ábra Precíziós gazdálkodás idővonala az Egyesült Államokban

https://korforgas.uni-mate.hu/documents/3045980/0/MATE-KGEK+-+2023-02+VL+Precíziós+MG.pdf/73c8a9ae-ae89-1612-c29c-b2d2e331e666?t=1682348604228- alapján saját szerkesztés

CPS ÉS MI SZEREPE A NÖVÉNYTERMESZTÉSBEN

5. ábra Precíziós növénytermesztés-

https://agrowebsystem.com/a-precizios-ultetes-adatelemzese/

A precíziós növénytermesztés (5.ábra) egy modern módszer, amely során a földet kisebb részekre bontva, az adott területre specifikus jellemzőihez igazodva végzik el a munkát. Ezáltal az öntözést, trágyázást vagy növényvédelmet mindig a konkrét igényekhez igazítják. Ennek köszönhetően nemcsak jobb minőségű és nagyobb hozamú termést lehet elérni, hanem csökkenthetőek a környezetre gyakorolt hatások és a felesleges költségek is. A cél, hogy a föld lehetőségeit maximálisan kihasználva egészséges, vegyszerektől mentes élelmiszereket és takarmányokat állítsunk elő. [4]

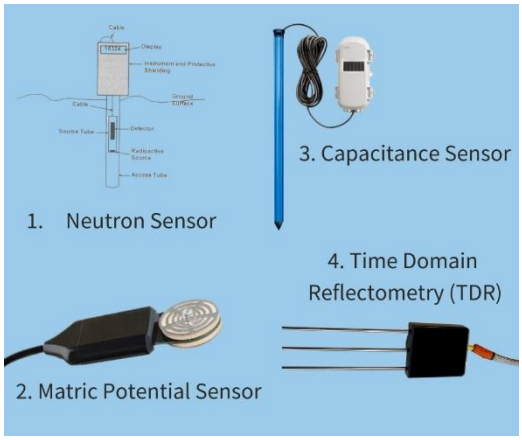
A precíziós gazdálkodás megvalósításához számos modern technológia áll rendelkezésre, amelyek segítenek pontosan meghatározni a föld állapotát és annak megfelelően meghozni a döntéseket.

Kiberfizikai rendszerek

A precíziós gazdálkodás alapja, hogy megbízható adatokra támaszkodva mindig a legmegfelelőbb döntést tudjuk meghozni. Ehhez különféle mérőeszközöket és szenzorokat használunk, amelyek segítségével adatokat gyűjtünk a föld állapotáról, a növényekről vagy éppen az időjárásról. Ezeket az adatokat aztán továbbítjuk feldolgozásra, ahol elemzik az információkat sokszor akár mesterséges intelligencia használatával. A szenzorok többféle területen alkalmazhatók, attól függően, hogy éppen mire van szükség: talajnedvesség mérésére, növénymegfigyelésre, kártevők észlelésére, de akár a környezeti tényezők (például hőmérséklet, páratartalom, fényintenzitás) folyamatos monitorozására is.

I. Talaj nedvességét mérő szenzorok

A talaj nedvességtartalmának mérése különösen fontos a precíziós növénytermesztésben, mivel a növények megfelelő vízellátása közvetlen hatással van a terméshozamra. A talaj nedvességét különböző technológiák segítségével mérhetjük, amelyek pontos adatokat szolgáltatnak a gazdálkodók számára, lehetővé téve számukra, hogy megfelelő intézkedéseket hozzanak az optimális öntözés elősegítése érdekében. A talaj nedvességtartalmát leggyakrabban szenzorok alkalmazásával (6.ábra) határozzák meg, amelyek elektromágneses elveken alapulnak, és segítenek meghatározni a talaj vízfelvételi képességét. Például ilyenek a TDR (Time Domain Reflectometry) szenzor.



6. ábra Nedvesség mérő szenzorok

https://www.earthscout.com/blog/measuring-soil-moisture-why-tdr-soil-sensors-are-preferred-for-precision-irrigation-scheduling/

TDR (Time Domain Reflectometry)

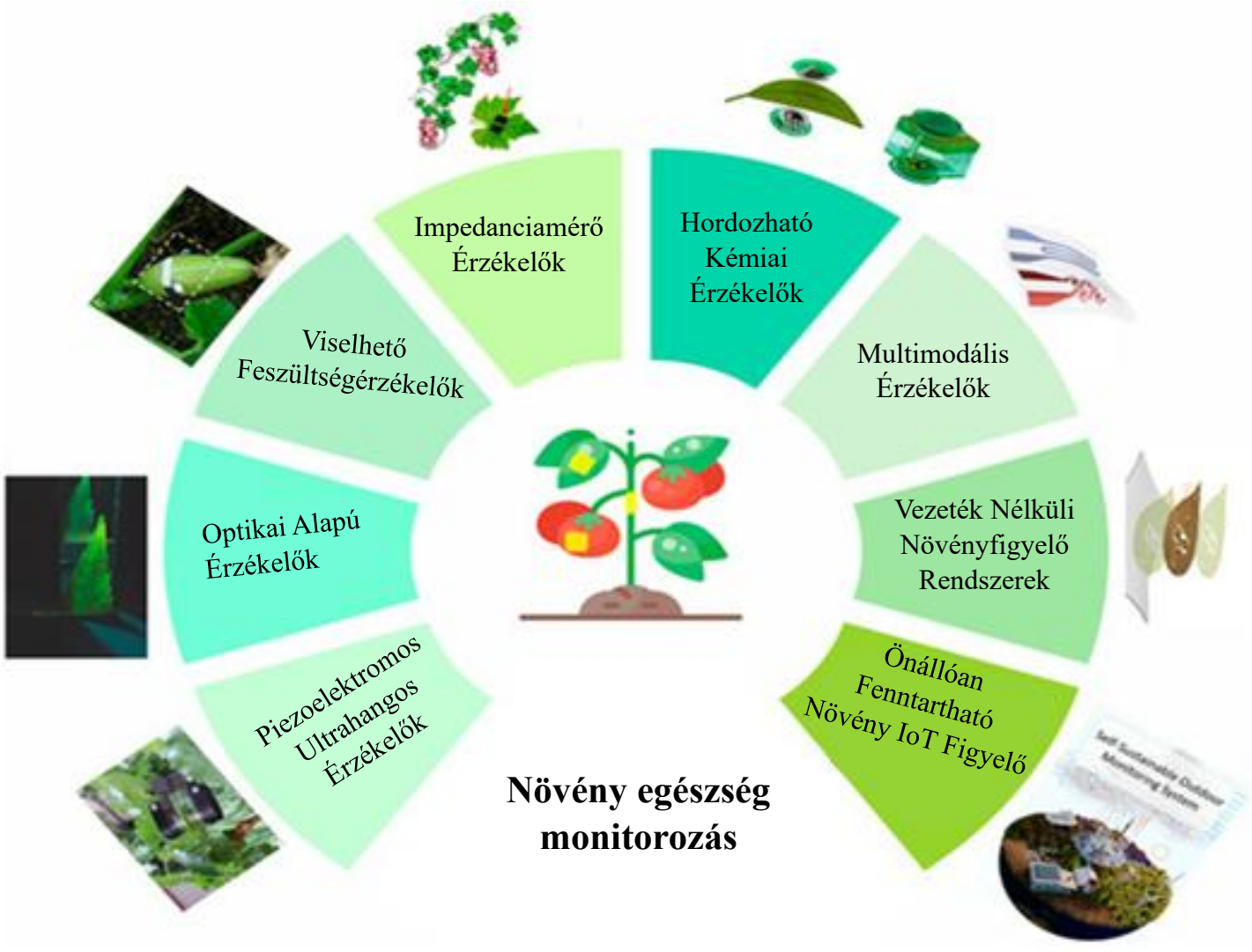
A Time Domain Reflectometry (TDR) mérés során elektromos jeleket küldünk a talajba, és mérjük a visszaverődési időt. Mivel a víz elektromos vezetőképessége eltér a száraz talajétól, a visszaverődési idő alapján meghatározható a talajban lévő víz mennyisége.[6]

A TDR szenzorok kezdetben kutatási célokra voltak használva, mert drágák és bonyolultan használhatók voltak. Az évek múltával, viszont a technológia sokat fejlődött és pontosabb méréseket tesz lehetővé ráadásul használata is egyszerűbbé vált, ebből kifolyólag a mezőgazdaságban is elkezdett elterjedni használata nem csak kutatási munkák során. Nagy előnye, hogy gyorsan reagál a talajnedvesség változására és nem befolyásolja a talaj só tartalma sem működését. A mérést rendkívül pontosan milliárd vagy billiomod részre lebontva végzi, így a mért értékek pontosak lesznek. [7] (7.ábra)

7. ábra TDR szenzor - https://soilsensor.com/articles/time-domain-reflectometry-tdr/

II. Növénymegfigyelés

A precíziós növénytermesztés egyik legfontosabb része a növények állapotának folyamatos és valós idejű megfigyelése. A növények víztartalma, növekedési üteme, tápanyagellátottsága vagy éppen a betegségeik olyan információkat adnak, amelyek alapján időben lehet beavatkozni esetleges probléma felmerülése esetén. Ez nemcsak a terméskiesés megelőzésében segít, hanem az erőforrások például a víz vagy a műtrágya hatékonyabb felhasználását is lehetővé teszi. Egyes betegségek már korai szakaszban is kimutathatók, például a növény által kibocsátott VOCs vagy a megváltozott víztartalom alapján



8. ábra Növény egészség megfigyelés –

https://www.mdpi.com/2079-6374/14/12/629?utm

– alapján saját magyar feliratos szerkesztés

A mai megfigyelőrendszerek különféle szenzorokra épülnek (8.ábra), amelyek képesek érzékelni a növényekből származó fizikai, kémiai és biológiai jeleket. Az így nyert adatok alapot adnak az automatikus döntéshozatalhoz, és nagyban hozzájárulnak a gazdálkodás hatékonyságához és fenntarthatóságához.

Optikai Alapú Érzékelők

Az optikai szenzorok segítenek a növények egészségének követésében, mivel gyorsan és károsodás nélküli módon mérhetők. Ezekkel mérhetjük a nitrogén szintet, a klorofill tartalmat és a növényi stresszt. A CO2 szintjének ellenőrzése fontos a fotoszintézishez. Az optikai szenzorok, mint a hőképek és spektrális mérés, segítenek a növényi betegségek és stressz korai felismerésében, ami javítja a terméshozamot és a növények ellenálló képességét.[8]

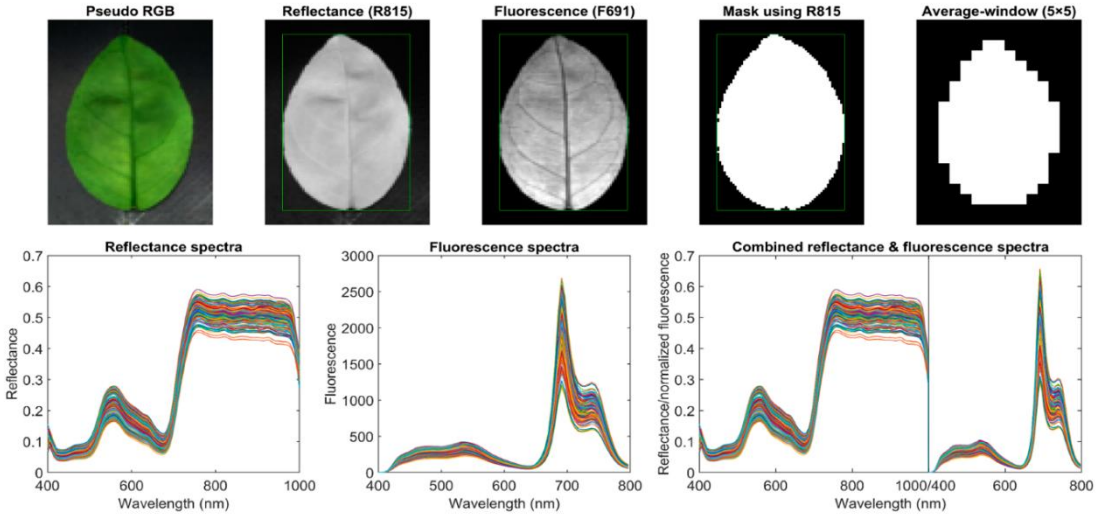
Felhasználási példák

1. ***CO2 szint monitorozása üvegházi környezetekben (2022, H. Zhou et al.)***

   A CO2 szintjének monitorozása üvegházi környezetekben optikai érzékelők segítségével. Ez biztosítja a fotoszintézis hatékonyságát és az optimális CO2 koncentrációkat a növények növekedéséhez.[8]

II. ***Hiperspektrális reflektancia betegségek észlelésére (2012)***

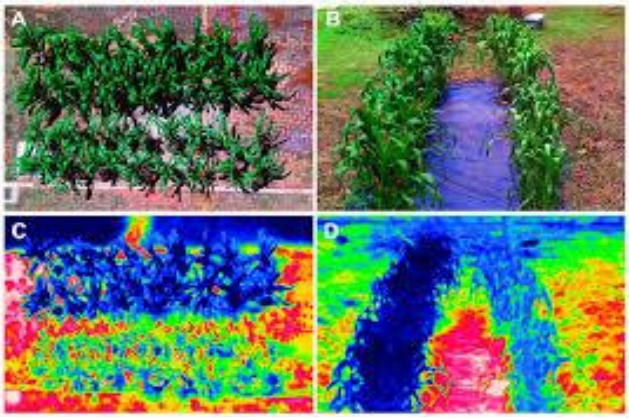
   A hiperspektrális reflektanciát használják a növényi betegségek korai stádiumú felismerésére. Például cukorrépa leveleinek betegségeit észlelik, mielőtt látható tünetek jelentkeznének. [8] (9.ábra)



9. ábra Hiperspektrális reflektancia - https://www.mdpi.com/2311-7524/10/11/1124

III. Hőkamerás képalkotás a szárazság észlelésére

A kutatás azt vizsgálta, hogyan lehet hőkamerával felismerni, ha a növény – például a kukorica – nem kap elég vizet. A növények leveleinek hőmérséklete árulkodó: ha melegebbek, az azt jelzi, hogy kevesebb vizet párologtatnak, vagyis vízhiányos állapotban vannak. Ez a módszer segíthet abban, hogy olyan növényfajtákat találjunk, amelyek jobban bírják az aszályos körülményeket.[8] (10.ábra)



10. ábra Hőkamerás képalkotás - https://www.researchgate.net/figure/Thermographic-image-data-used-to-evaluate-drought-stress-in-maize-plants-In-A-C-the_fig2_347414760

Viselhető Feszültségérzékelők

A vezeték nélküli növénymonitorozó rendszerek lehetővé teszik a növények egészségének és növekedésének folyamatos figyelemmel kísérését anélkül, hogy beavatkoznának a fiziológiai működésükbe. Ezek a rendszerek különféle érzékelő technológiákat alkalmaznak, mint például hőmérséklet, páratartalom és fényérzékelők, amelyek valós időben mérik a növények fiziológiai állapotát. Az érzékelők az adatokat digitális jelekké alakítják, amelyeket egy mikrovezérlő (MCU) segítségével dolgoznak fel, majd vezeték nélküli kommunikációs rendszeren, például Bluetooth vagy NFC segítségével továbbítanak.

I. Vékony, rugalmas, viselhető eszközök

Ezek a szenzorok a növények víz- és hőmérsékleti állapotát mérik. Beépített hőmérséklet-érzékelőkkel rendelkeznek, amelyek segítenek meghatározni a növények vízmozgást. Az adatokat Bluetooth segítségével továbbítják, így a gazdák okostelefonjukon nyomon követhetik a növények vízfogyasztását és egészségi állapotát.

II. NFC alapú gázérzékelők

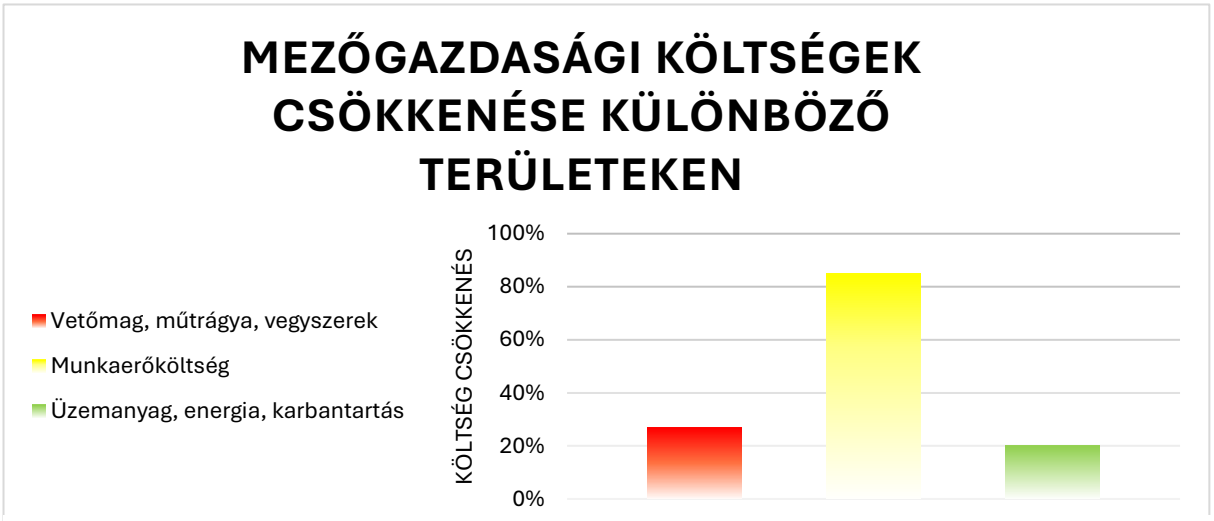
Ezek az érzékelők a NFC technológia segítségével mérik a növények stresszét jelző gázokat. A rendszer vezeték nélküli módon kommunikál, és lehetővé teszi, hogy valós időben figyeljük a növények állapotát, anélkül, hogy zavaró hatást gyakorolnánk a növényekre.

Mesterséges intelligencia a növénytermesztésben

A mezőgazdaság, azon belül is a növénytermesztés, hatalmas kihívásokkal néz szembe a 21. században. A klímaváltozás egyre kiszámíthatatlanabb időjárási viszonyokat idéz elő, a termőföldek területe folyamatosan csökken, miközben a világ népessége folyamatosan növekszik. Ezek a tényezők együtt komoly nyomást gyakorolnak az élelmiszertermelésre. A hagyományos növénytermesztési eljárások már egyre kevésbé képesek hatékonyan reagálni ezekre a kihívásokra, ezért szükség van korszerű, adat vezérelt megoldásokra. A mesterséges intelligencia (AI) alkalmazása lehetővé teszi például a talajadottságok pontos elemzését, így meghatározható, hogy egy adott területen milyen növények termesztése lehet a leghatékonyabb a talaj termékenységi mutatói alapján. Az ilyen jellegű elemzések hozzájárulnak a terméshozam növeléséhez és a gazdálkodás fenntarthatóságához, ezért kiemelten fontos, hogy a jövőben az AI a mezőgazdaság alap pillérévé váljon.

12. ábra See and Spray Ultimate - https://www.deere.com/en/sprayers/see-spray-ultimate/

Az Ark Invest kutatása alapján a mesterséges intelligencia és a precíziós mezőgazdaság több,mint 22%-al csökkentheti az éves mezőgazdasági költségeket. A See and Spray Ultimate permetezőgép (11.ábra), az ExactShot Planter és az autonóm technológia kombinációjának segítségével a vetőmagok, trágyák és vegyszerek mennyisége körülbelül 27%-kal, a munkaerőköltségek

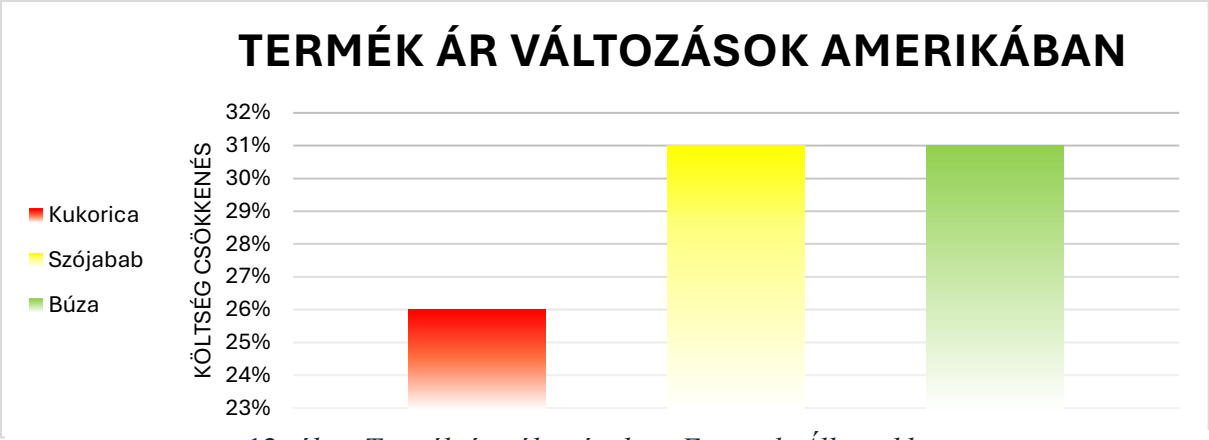


11. ábra Mezőgazdasági költségek csökkenés különböző területeken - https://www.futurefarming.com/smart-farming/will-ai-and-precision-agriculture-lower-farming-costs/

- saját diagram szerkesztése

akár 85%-kal, a járműfenntartási költségek, mint az üzemanyag vagy a javítási költségek pedig 20%-kal csökkenhetnek.[9] (12.ábra)

A kutatás továbbá kitért arra is, hogy a mesterséges intelligencia segítségével a kukorica 26%-kal, míg a szójabab és a búza költsége egyaránt 31%-kal is csökkenhet 1 acre-en (1 acre ~ 0,4047 hektár) az Egyesült Államokban.[9] (13.ábra)



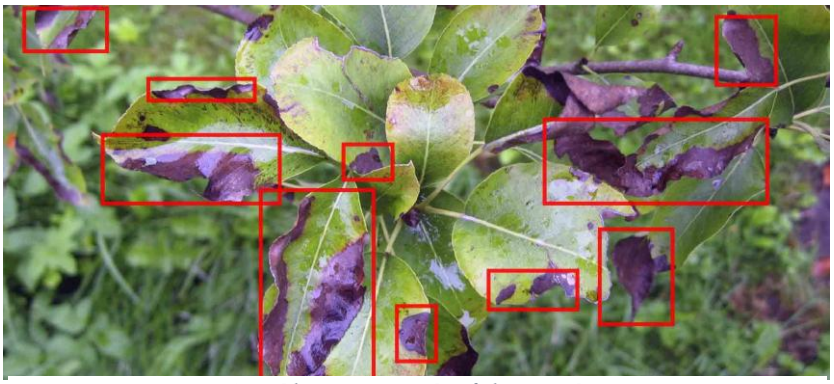
13. *ábra Termék ár változások az Egyesült Államokban - https://www.futurefarming.com/smart-farming/will-ai-and-precision-agriculture-lower-farming-costs/*

-saját szerkesztésű diagram

I. Betegség felismerés gépi látással

Különösen fontos alkalmazási terület a betegségek korai felismerése. A mesterséges intelligencia által támogatott képfelismerő rendszerek képesek már a legkisebb elváltozásokat is azonosítani a növényeken, amelyeket az emberi szem gyakran figyelmen kívül hagy. Ezek az AI rendszerek képeken keresztül ismerik fel a betegségeket vagy kártevőfertőzéseket, lehetővé téve a gyors és célzott beavatkozást, és csökkentve a vegyszerek túlzott használatát [10][11]. (14.ábra)

Egy kutatásban a fekete rothadás felismerését vizsgálták. Egy mély konvolúciós neurális hálót (Deep Convolutional Neural Network) tanítottak be, amelyhez olyan képeket használtak, amelyeken a rothadás négy különböző fázisát botanikusok jelölték



14. ábra Betegség felismerés - https://bitrefine.group/industries/precision-agriculture/88-industries/agriculture-food/agriculture-solutions/184-plant-disease-detection

meg a fertőzés súlyossága szerint. Az AI a betanítást követően 90,4%-os pontossággal tudta beazonosítani, hogy a növény milyen mértékben fertőzött. [11] (14.ábra)

Egy másik kutatásban YOLO v3 segítségével paradicsomokat elemeztek. A kutatók digitális fényképezőgéppel és okostelefonnal rögzítették a képeket és összesen 13 problémát tudtak azonosítani. A betanított AI modell ezután 92,39%-os pontossággal 20,39 ezredmásodperc alatt képes volt felismerni a paradicsom betegségét, ami jól mutatja az AI használata mennyivel fel tudja gyorsítani a mezőgazdasági folyamatokat. [11] (15.ábra)

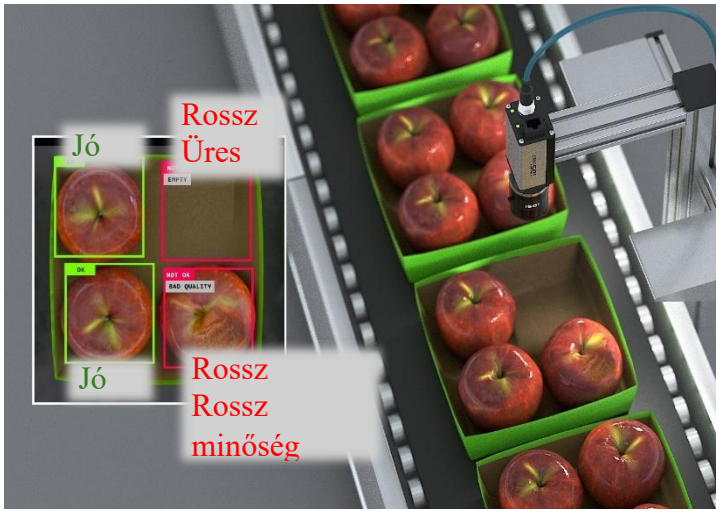
15. ábra Paradicsom betegség felismerése - https://indatalabs.com/blog/agriculture-and-computer-vision

II. *Automatikus beavatkozás*

Az AI ugyanakkor nemcsak a megfigyelésben segít, hanem az automatikus beavatkozásban is. Az intelligens permetező rendszerek képesek csak a fertőzött vagy gyomos területekre kijuttatni a szükséges vegyszert, így minimálisra csökkentve a környezeti terhelést. Az automatikus gyomirtó robotok pedig képesek felismerni és eltávolítani a gyomnövényeket anélkül, hogy a termesztett növényeket károsítanák, amely az AI által tanított képfelismerés és mintázatfelismerés segítségével valósítható meg [11].

III. *Osztályozás és válogatás minőség szerint*

Betakarítás után az AI továbbra is hasznos szerepet tölt be: a terméseknek osztályozásában és válogatásában. A mesterséges intelligencia rendszerek képesek képfelvételek alapján megállapítani a zöldségek és gyümölcsök méretét, alakját, színét és érettségét, így automatikusan elkülönítik a piacképes terményt a hibás vagy alacsonyabb minőségű daraboktól. Ez a folyamat sokkal gyorsabb és pontosabb, mint az emberi munka, ráadásul jelentős munkaerő-megtakarítással is jár [11]. (16.ábra)



16. ábra AI alapú válogatás - https://en.ids-imaging.com/technical-articles-details/items/detecting-sorting-counting.html

CPS és MI szerepe az állattartásban

A precíziós állattartás célja, hogy minden egyes állat igényeit egyedileg figyelembe véve biztosítsa a legjobb egészségügyi állapotot, a takarmányozás hatékonyságát és a termelés optimalizálását. A CPS (Cyber-Physical Systems) rendszerek és a mesterséges intelligencia ebben kulcsszerepet játszanak, mivel lehetővé teszik az állatok viselkedésének, egészségi állapotának és környezeti feltételeinek valós idejű nyomon követését és elemzését.

Kiberfizikai rendszerek

A precíziós állattartás alapját képezik a különféle szenzorok, amelyek az állatok fizikai és biológiai paramétereit mérik. Az érzékelők segítségével lehetőség van az állatok mozgásának, testhőmérsékletének, pulzusának, valamint a légzésük figyelemmel kísérésére. A szenzorok a takarmányozás hatékonyságának mérésére is alkalmazhatók, például a takarmány felvételének nyomon követésére, így biztosítva a megfelelő táplálkozást az állatok számára.

I. Egészségügyi monitoring rendszerek

Az Egyesül Államokban a tejtermelők egyre gyakrabban használnak okos nyakörveket (17.ábra) és egyéb eszközökét, hogy internetes kapcsolat segítségével valós időben nyomon tudják követni a tehenek egészségügyi állapotát és viselkedését. Ezek a viselhető eszközök mikrofonnal, hő és mozgás érzékelővel vannak felszerelve, amellyel megfigyelhetik a tehenek aktivitását. Az eszközök a mesterséges intelligencia és azon belül is a gépi tanulás segítségével jelzik, ha az állat szokatlanul viselkedik, mert mondjuk betegség miatt megváltozott az aktivitása, mint például a mozgása lecsökken vagy a szokásosnál többet pihen ezzel jelezve, hogy esetleg betegség merül fel az állattal kapcsolatban. [12]

17. ábra Tehén okos nyakörvvel - https://www.fwi.co.uk/livestock/heat-collars-help-dairy-farmer-improve-submission-rates

II. Drónok használata a precíziós állattartásban

A precíziós állattartás fejlődésével párhuzamosan egyre fontosabb szerepet kapnak az UAV (pilóta nélküli légijárművek), más néven a drónok, amelyek lehetővé teszik az állatok hatékony és távoli megfigyelését. Drónok segítségével emberi jelenlét nélkül, valós időben adatokat lehet gyűjteni az állatok számáról, elhelyezkedéséről és viselkedéséről. A drón-technológia egyik nagy előnye, hogy minimálisra csökkenti az állatok stresszelését, miközben pontos és valós idejű információt továbbítanak a gazdák számára. (18.ábra)

18. ábra Drón technológia az állat monitorozásban - https://www.dailypost.co.uk/news/local-news/drone-sheep-flocks-farmers-sheepdog-17478918

A SPADE projekt során juhok automatikus drónos megfigyelését valósították meg SheepCounter nevű adatbázis (19.ábra) segítségével, amely egy nyilvános adathalmaz, ami 1727 képet tartalmaz többnyire fehér bárányokról réten. A képek nagy felbonásúak és nappal készültek. A kutatás célja egy olyan technológiai megoldás fejlesztése volt, amely valós időben terepen is alkalmazható. A kutatás során a YOLO különböző fajtáit használták (YOLOv4,YOLOv5,YOLOX nano) és emellett egyéb technológiákat, mint az SSD és a Faster R-CNN. Ezeket a modelleket a SheepCounter képein tanították és tesztelték, az algoritmusok teljesítményét AP,mAP és mAR mutatók alapján értékelték. [13]

	Tanítás	Érvényes	Teszt	Összes
Képek száma	1203	350	174	1727
Hány bárány van a képen	32,0	32,39	32,2	32,1
Összes találat	38495	11337	5603	55435
Kis méretű kép az állatról	147	39	32	218
Közepes méretű kép az állatról	6209	2359	984	9552
Nagy méretű kép az állatról	32139	8939	4587	45665

19. ábra SheepCounter –

https://spade-horizon.eu/wp-content/uploads/2024/05/Scientific-Publication-SPADE-EU-Project_Comparison-of-Object-Detection-Algorithms-for-Livestock-Monitoring-of-Sheep-in-UAV-images.pdf

- saját szerkesztésű táblázat

Az eredmények azt mutatták, hogy a kisebb, alacsony erőforrás igényű modellek, mint a YOLOv8 és az SSD Lite jól alkalmazhatók valós idejű drónos megfigyelésre, amíg a nagyobb modellek, mint az SSD ResNet50 magasabb pontossággal határozták meg az állatot, de lassabban dolgozta fel az adatokat. [13]

Mesterséges intelligencia az állattartásban

A mesterséges intelligencia szerepe az állattartásban az adatok elemzésében és a döntéshozatali folyamatok automatizálásában rejlik. Az AI segítségével az állatok viselkedésének és egészségi állapotának elemzése valós időben történhet, így az esetleges problémák gyorsan észlelhetők, és azonnali beavatkozásra is lehetőség van. Az MI segítségével optimalizálható a takarmányozás, az állatok mozgásának nyomon követése, valamint a környezeti tényezők, például a hőmérséklet és páratartalom folyamatos figyelése.

I. Automatizálás az állattartásban

Az automatizálás az állattartásban széleskörűen alkalmazható több területen is, mint az állatok egészségének és viselkedésének megfigyelése, vagy a takarmányozás automatizálása. Ezeket a rendszereket több mezőgazdasági környezetben is használják például baromfi és sertés telepeken is.

A mesterséges intelligencia az automatizált állattartás fontos eleme, amely a hagyományos eljárásokkal szemben sokkal precízebb és gyorsabban reagál szükség esetén. Szenzorok segítségével folyamatosan érzékeli a környezeti változásokat, például a hőmérsékletet, páratartalmat, levegőminőséget és a fény erősségét, így biztosítva az állatok számára az optimális feltételeket. Például a baromfitelepen a rendszer a begyűjtött adatok alapján a hőmérséklet ingadozás kiküszöbölésére automatikusan vezérli a szellőztető berendezéseket, hogy a baromfik megfelelően tudjanak fejlődni. [14]

Az MI használatával a takarmányozás és az itatás is optimalizálható, amely során a rendszer valós idejű adatok alapján szabályozzák az állatok étel és ital ellátását biztosítva az állatok megfelelő élelmezését. Ezáltal, hogy mindig a megfelelő mennyiségű táplálék jut el az állatokhoz jelentős mértékben mérsékelhetők a költségek, és az emberi munkaerő se szükséges a folyamatosan ismétlődő, monoton folyamatok végrehajtásához. [14] (20.ábra)

20. ábra Automatizált etetés –

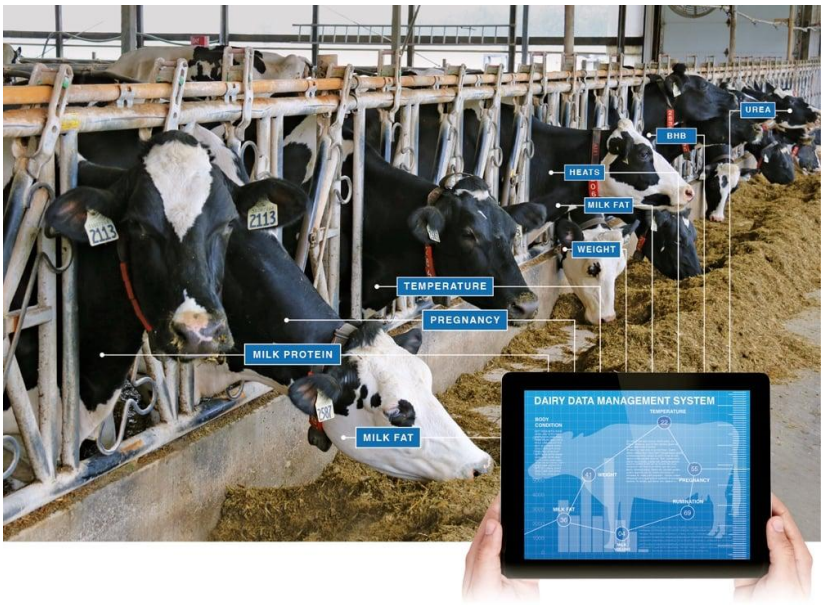
https://www.lelyna.com/us/solutions/feeding/

A mesterséges intelligenciának köszönhetően a gazdák képesek előrejelzéseket kapni az állatok egészségügyi helyzetének változásáról értesülni még mielőtt komolyabb baj történne. Például képes egy tehén tejhozamának csökkenését vagy egy baromfi megbetegedését azelőtt jelezni, mielőtt a tünetek megjelennének, így időben be tudjanak avatkozni. Ez csökkenti a betegségek miatti halálozásokat, az állat jóllétet növeli és hosszútávon fentarthatóbbá teszi a gazdálkodást. [14]

II. Mesterséges intelligencia szerepe a szarvasmarha szelekcióban

A mesterséges intelligencia sokat segít a szarvasmarha tenyésztésben, mivel képes elemezni az állatok genetikai adatait, teljesítményét és korábbi egészségügyi állapotát. Így a tenyésztők jól megalapozott döntéseket képesek hozni. Az AI például figyelembe veszi a tehén tejtermelésének mennyiségét, korábbi betegségeit, vemhességének alakulását, valamint az utódok növekedési ütemét is. [15]

Ezek az eszközök megtudják mondani, melyik bika és tehén a legjobb választás a párosításhoz, így egészségesebb és termelékenyebb utódok születhetnek. Előre tudják jelezni, mikor vannak termékeny állapotban, segít felismerni a vemhességet és figyeli hogyan fejlődnek az állatok. Ezen folyamatoknak köszönhetően a hibák száma csökken, a tejhozam nő és az állatok egészsége javul. [15] (21.ábra)



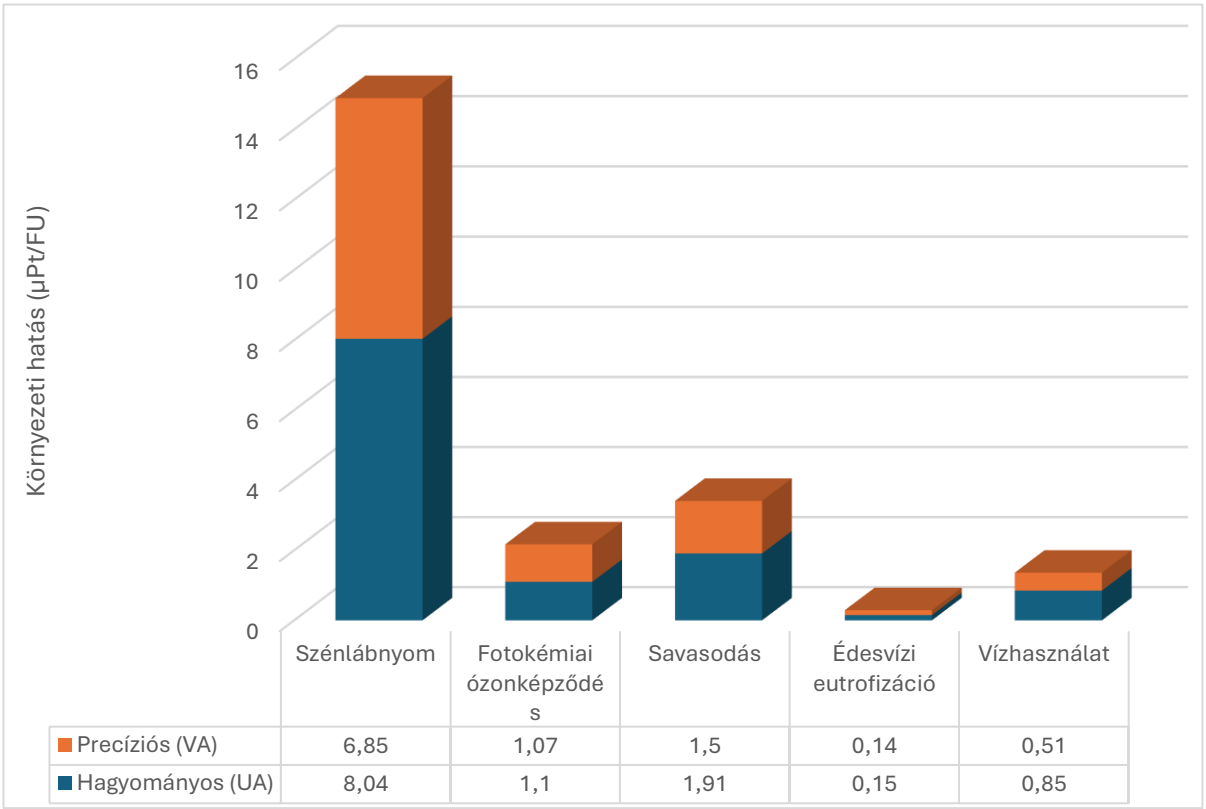
21. ábra Mesterséges intelligencia használata a tehén tenyésztésben - https://farmtario.com/livestock/the-big-data-dairy-challenge/

A gyakorlatban a hatása már most érezhető, mivel több tej, jobb hús minőség és kevesebb veszteség van, mint az AI használatát megelőzően. A mesterséges intelligencia használatának köszönhetően az állatállomány gyorsabban fejlődik, és kevesebb pénz felhasználásával lehet üzemeltetni a gazdaságot. [15]

A PRECÍZIÓS MEZŐGAZDASÁG KÖRNYEZETRE GYAKOROLT HATÁSA

Délkelet-Spanyolországban, Murica régióban végeztek egy kutatást, amelyben a hagyományos és precíziós mezőgazdaság teljesítményét hasonlították össze. A vizsgálat egy 405 hektáros nektarin ültetvényen történt, és a teljes termelési folyamatot elemezte a műtrágya előállításától egészen a gyümölcs betakarításáig. A cél az volt, hogy összehasonlítsák a két módszer környezeti terhelését és gazdasági hatékonyságát. [16]

A precíziós mezőgazdasági módszerek jelentős erőforrás megtakarítást eredményeztek a hagyományos technológiákhoz képest. A kutatás szerint a hagyományos mezőgazdasági folyamatokhoz képest a precíziós mezőgazdaságnak köszönhetően a műtrágya felhasználás 46%-kal, a permetező szerek használata 51%-kal és az öntözésre fordított víz mennyisége 28%-kal csökkent. Ezek a csökkenések nem csak környezet védelmi szempontból jelentősök, így a gazdáknak a kutatás alapján például permetező szerekre évi 665 euróval kevesebb pénzt kell költeni hektáronként, ami egy több száz hektáros ültetvény esetén jelentős költségmegtakarítást jelent. [16] (22.ábra)



22. ábra Mezőgazdasági eljárások összehasonlítása µPt/FU alapján (környezeti hatás/egységnyi gyümölcs) –

https://www.mdpi.com/2073-4395/12/7/1545

-saját szerkesztésű diagram

A PRECÍZIÓS MEZŐGAZDASÁG ELTERJEDÉSÉNEK NEHÉZSÉGEI

A precíziós mezőgazdaság az ipar 4.0 technológiáknak köszönhetően forradalmasíthatja a mezőgazdasági telelést. Ezek a technológiák lehetővé teszik a fenntarthatóbb gazdálkodást és közben csökkentik a pazarlást és növelik a hatékonyságot. Viszont rengeteg kihívással jár az elterjedése. [17]

1. *Szakértelem és tudás hiánya*

   Az informatikai szakemberek sokszor nem értenek a mezőgazdasághoz, amíg a mezőgazdaságban jártas emberek nem értenek az új technológia használatához. Ez a tudásbeli eltérés megnehezíti az új rendszerek bevezetését. [17]

2. *Magas technológiai költségek*

   A szenzoros rendszerek, önműködő gépek és mesterséges intelligencia alapú megoldások gyakran jelentős beruházást igényelnek. A kisebb gazdaságok számára ezek a költségek sokszor elérhetetlenek, így jellemzően csak a nagyobb, tőkeerős szereplők tudják kihasználni az előnyeiket. Ez pedig fokozza a gazdaságok közötti különbségeket. [17]

3. *Társadalmi hatások*

   Az automatizálás bekövetkeztével az alacsony képzettséget igénylő munkákra való igény csökken, ami munkanélküliséghez vezethet. Viszont egyre nagyobb szükség lesz, majd a jövőben ezzel arányosan magasan képzett munkaerőre. [17]

4. *Bizalmi nehézségek*

   Sok gazdálkodó óvatosan vagy bizalmatlanul áll az új technológiákhoz, különösen, azok, akik kevésébé jártasak a digitális megoldásokban. Emellett a fejlesztések gyakran nyugati szemléletet tükröznek, amely nem mindig alkalmazkodik a helyi körülményekhez vagy a kulturális sajátosságokhoz. Ez különösen a fejlődő országokban jelenthet akadályt, ahol a nyelvi, oktatási és politikai különbségek is nehezítik az alkalmazást. [17]

KONKLÚZIÓ

A mesterséges intelligencia és kiberfizikai rendszerek egyre fontosabb szerepet töltenek be a mezőgazdaságban. Ezek a technológiák lehetővé teszik a gazdálkodások számára, hogy a gazdasági folyamatokat költséghatékonyabban és környezetkímélőbben valósítsák meg. Ahogy a dolgozat során már kifejtettem a növénytermesztésben és az állattenyésztésben is megfigyelhető, hogy az MI és CPS használata segítik a folyamatok optimalizálását,aminek következtében az erőforrások pazarlás és a környezetre kiható hatása is csökken a gazdasági folyamatoknak. Ennek eredménye képpen kevesebb a víz és műtrágya felhasználás és a széndioxid kibocsátsá is mellette,viszont a költségek is csökkennek ,ami hosszú távon a gazdáknak megtérül.

Viszont az is kiderült, hogy a precíziós mezőgazdaság elterjedése nem egyszerű és sok tényező van, amitől jelenleg nem mindenhol használják a sok előnye ellenére is. Ezek a kihívások azonban nem megoldhatatlanok, a technológiák fejlődésével olcsóbbá és elérhetőbbé válhatnak, ami által a kisebb tőkével rendelkezők is hozzá férhetnek.

A mesterséges intelligencia és a kiberfizikai rendszerek használata nemcsak, hogy megkönnyíti a gazdálkodást, de fenntarthatóbbá és költséghatékonyabbá is teszi. Ahogy ezek a technológiák fejlődnek és egyre olcsóbbak lesznek, egyre több gazdálkodó számára elérhetővé válnak, és alapjaiban változtatják meg azt, ahogy a mezőgazdaság működik.

ÁBRA JEGYZÉK

1. ábra CPS rendszer bemutatása talajnedvesség esetén- https://compactionprevention.com/the-innovation/ 3
2. ábra A mesterséges intelligencia bemutatása 4
3. ábra Precíziós gazdálkodás idővonala - https://web.archive.org/web/20200309230626/https://www.accenture.com/us-en/insight-accenture-digital-agriculture-solutions 5
4. ábra Precíziós gazdálkodás idővonala az Egyesült Államokban 6
5. ábra Precíziós növénytermesztés- 7
6. ábra Nedvesség mérő szenzorok 8
7. ábra TDR szenzor - https://soilsensor.com/articles/time-domain-reflectometry-tdr/ 8
8. ábra Növény egészség megfigyelés – 9
9. ábra Hiperspektrális reflektancia - https://www.mdpi.com/2311-7524/10/11/1124 10
10. ábra Hőkamerás képalkotás - https://www.researchgate.net/figure/Thermographic-image-data-used-to-evaluate-drought-stress-in-maize-plants-In-A-C-the_fig2_347414760 11
11. ábra Mezőgazdasági költségek csökkenés különböző területeken - https://www.futurefarming.com/smart-farming/will-ai-and-precision-agriculture-lower-farming-costs/ 12
12. ábra See and Spray Ultimate - https://www.deere.com/en/sprayers/see-spray-ultimate/ 12
13. ábra Termék ár változások az Egyesült Államokban - https://www.futurefarming.com/smart-farming/will-ai-and-precision-agriculture-lower-farming-costs/ 13
14. ábra Betegség felismerés - https://bitrefine.group/industries/precision-agriculture/88-industries/agriculture-food/agriculture-solutions/184-plant-disease-detection 13
15. ábra Paradicsom betegség felismerése - https://indatalabs.com/blog/agriculture-and-computer-vision 14
16. ábra AI alapú válogatás - https://en.ids-imaging.com/technical-articles-details/items/detecting-sorting-counting.html 14
17. ábra Tehén okos nyakörvvel - https://www.fwi.co.uk/livestock/heat-collars-help-dairy-farmer-improve-submission-rates 15
18. ábra Drón technológia az állat monitorozásban - https://www.dailypost.co.uk/news/local-news/drone-sheep-flocks-farmers-sheepdog-17478918 16
19. ábra SheepCounter – 17
20. ábra Automatizált etetés – 18
21. ábra Mesterséges intelligencia használata a tehén tenyésztésben - https://farmtario.com/livestock/the-big-data-dairy-challenge/ 19
22. ábra Mezőgazdasági eljárások összehasonlítása µPt/FU alapján (környezeti hatás/egységnyi gyümölcs) – 20

FORRÁSOK

[1] E. R. Griffor, C. Greer, D. A. Wollman, és M. J. Burns, „Framework for cyber-physical systems: volume 1, overview”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 1500-201, jún. 2017. doi: 10.6028/NIST.SP.1500-201.

[2] „What Is Artificial Intelligence? Definition, Uses, and Types”, Coursera. Elérés: 2025. május 3. [Online]. Elérhető: https://www.coursera.org/articles/what-is-artificial-intelligence

[3] Andras, „Mi az a precíziós gazdálkodás és hogyan kezdjünk hozzá?”, Agrárközösség. Elérés: 2025. május 6. [Online]. Elérhető: https://agrarkozosseg.hu/mi-az-a-precizios-gazdalkodas-es-hogyan-kezdjunk-hozza/

[4] A. C. Dobos, Precíziós növénytermesztés, Debrecen: Debreceni Egyetem, Agrár- és Gazdálkodástudományok Centruma, 2011. [Online]. Elérhető: https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/12423/2011-0085_precizios_novenytermesztes.pdf?sequence=2&isAllowed=y

[5] „73c8a9ae-ae89-1612-c29c-b2d2e331e666.pdf”. Elérés: 2025. május 6. [Online]. Elérhető: https://korforgas.uni-mate.hu/documents/3045980/0/MATE-KGEK+-+2023-02+VL+Prec%C3%ADzi%C3%B3s+MG.pdf/73c8a9ae-ae89-1612-c29c-b2d2e331e666?t=1682348604228

[6] C. M. P. Vaz, S. Jones, M. Meding, és M. Tuller, „Evaluation of Standard Calibration Functions for Eight Electromagnetic Soil Moisture Sensors”, *Vadose Zone J.*, köt. 12, sz. 2, o. vzj2012.0160, 2013, doi: 10.2136/vzj2012.0160.

[7] S. Wieland, „Measuring Soil Moisture: Why TDR Soil Sensors are Preferred for Precision Irrigation Scheduling”, EarthScout. Elérés: 2025. május 9. [Online]. Elérhető: https://www.earthscout.com/blog/measuring-soil-moisture-why-tdr-soil-sensors-are-preferred-for-precision-irrigation-scheduling/

[8] L. Wang, M. Xiao, X. Guo, Y. Yang, Z. Zhang, és C. Lee, „Sensing Technologies for Outdoor/Indoor Farming”, Biosensors, köt. 14, sz. 12, Art. sz. 12, dec. 2024, doi: 10.3390/bios14120629.

[9] E. Asscheman, „Will AI and precision agriculture lower farming costs?”, Future Farming. Elérés: 2025. május 10. [Online]. Elérhető: https://www.futurefarming.com/smart-farming/will-ai-and-precision-agriculture-lower-farming-costs/

[10] „How exactly is AI used in agriculture? - growAG”. Elérés: 2025. május 10. [Online]. Elérhető: https://www.growag.com/highlights/article/how-exactly-is-ai-used-in-agriculture-1

[11] „AI in Agriculture: 8 Practical Applications [2024 Update]”. Elérés: 2025. május 9. [Online]. Elérhető: https://www.v7labs.com/blog/ai-in-agriculture

[12] B. Lin, „Cow Wearables Help America’s Dairy Farmers Detect Bird Flu and Other Illnesses”, Wall Street Journal, 2025. március 20. Elérés: 2025. május 12. [Online]. Elérhető: https://www.wsj.com/articles/cow-wearables-help-americas-dairy-farmers-detect-bird-flu-and-other-illnesses-57470646

[13] O. Doll és A. Loos, „Comparison of Object Detection Algorithms for Livestock Monitoring of Sheep in UAV images”.

[14] P. A. Vlaicu, M. A. Gras, A. E. Untea, N. A. Lefter, és M. C. Rotar, „Advancing Livestock Technology: Intelligent Systemization for Enhanced Productivity, Welfare, and Sustainability”, AgriEngineering, köt. 6, sz. 2, Art. sz. 2, jún. 2024, doi: 10.3390/agriengineering6020084.

[15] „Best AI Breeding Tools for Cattle Selection: A Comprehensive Guide - Cattle Daily”. Elérés: 2025. május 15. [Online]. Elérhető: https://cattledaily.com/best-ai-breeding-tools-for-cattle-selection/

[16] P. Núñez-Cárdenas, B. Diezma, G. San Miguel, C. Valero, és E. C. Correa, „Environmental LCA of Precision Agriculture for Stone Fruit Production”, Agronomy, köt. 12, sz. 7, Art. sz. 7, júl. 2022, doi: 10.3390/agronomy12071545.

[17] E. M. B. M. Karunathilake, A. T. Le, S. Heo, Y. S. Chung, és S. Mansoor, „The Path to Smart Farming: Innovations and Opportunities in Precision Agriculture”, Agriculture, köt. 13, sz. 8, Art. sz. 8, aug. 2023, doi: 10.3390/agriculture13081593.

2.3. Okosotthonok kiberbiztonsági kihívásai CPS környezetben

Okosotthonok kiberbiztonsági kihívásai CPS környezetben

Tihanyi Levente

Gazdaságinformatikus Bsc, tihanyil724@gmail.com

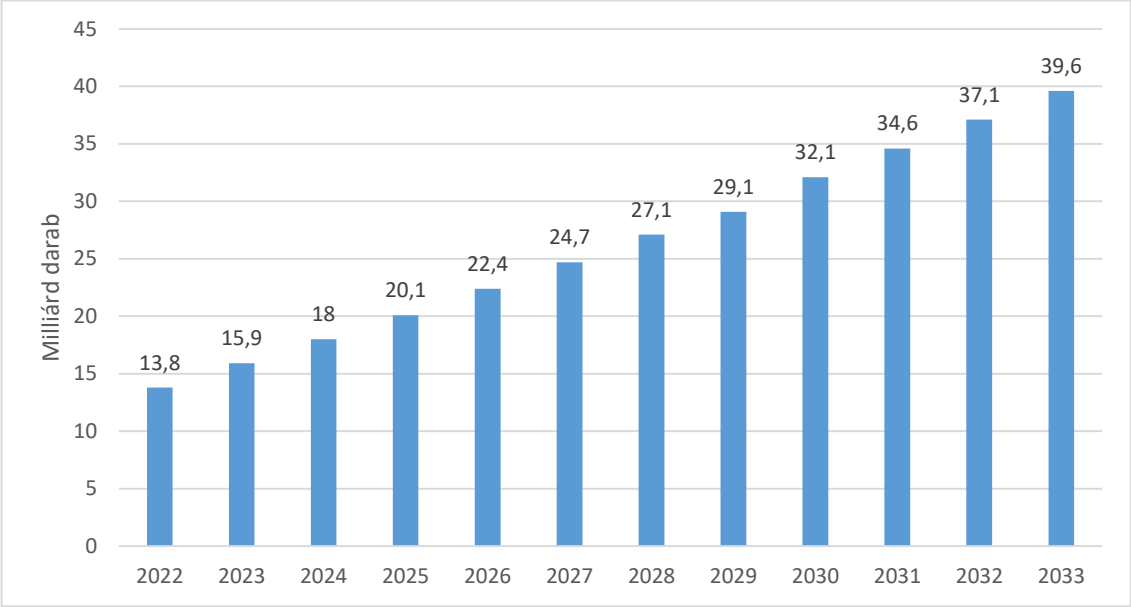
I. BEVEZETÉS

Az okosotthonok egyre elterjedtebbek manapság és technológia fejlődésével ezek az épületek az elkövetkezendő években integrálódni fognak a mindennapokba. Az okosotthon rendszerszinten kezeli a lakásunkat a villanytól egészen a fűtőberendezésekig, hogy minél kényelmesebben és biztonságosabban élhessünk.

Egy lakás nem attól lesz okos, hogy minél több okoseszközt tartunk és azokat telefonról vezérelve adunk nekik instrukciókat. A valódi okosotthon tanul, megfigyeli szokásainkat, elvégzi a mindennapi feladatainkat utasítás nélkül. Emellett ezek a technológiák támogatják az időseket, illetve fogyatékkal élőket, akik különleges bánásmódban részesülnek.

A kiber-fizikai rendszerek, rövidítve CPS, egy feltörekvő paradigma, amely az utóbbi időben különös figyelmet kapott a kutatás és fejlesztés területén. A CPS átalakította a fizikai világgal való kapcsolatunkat azáltal, hogy intelligens kommunikációt vezetett be a fizikai világ és annak kiberkomponensei között. A mai kor növekvő igényeinek kielégítésére a CPS számos alkalmazási területen megjelent, különösen az okosotthonokban.

Fontos még megemlíteni az IoT-t vagyis a dolgok internetjét, ami lehet bármilyen számítástechnikai eszköz, számítógép, tablet, autó, konnektor vagy akár villanykörte is. Az IoT minden összekapcsolt technológiai eszköz, gép és kapcsolat fogalma. Akkor is IoT-ről beszélünk, ha egy nagyobb rendszer több alrendszer foglal magába, mint például egy okos ház. Az IoT eszközök népszerűsége egyre jobban nő ahogy azt az ábra is mutatja. (1.ábra)



1. ábra: IoT kapcsolatok száma világszerte (2022-2023), előrejelezve (2024-2033)
https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ - alapján saját szerkesztés

Más IoT rendszerekhez hasonlóan az okosotthonok is ki vannak téve kiberfenyegetéseknek, amelyek veszélyeztetik a magánszférát és a fizikai biztonságot vagy károsíthatja a berendezéseket. Előfordulhat, hogy egyes készülékek nem biztonságosak. Vannak olyan IoT eszközök, amik nagyon olcsón, illetve sietve, tesztelés nélkül kerülnek a piacra és a gyártók a biztonságon próbálnak spórolni. Ilyen példa lehet, amikor Angliában egy babamonitoron kezdett el egy idegen személy a babához beszélni. Az is előfordulhat, hogy az otthoni hálózat eleve nem biztonságos és az adatok könnyen elérhetők a behatolók számára.

Ezért tartom fontosnak, hogy kiberbiztonsági intézkedéseket hozzunk az okos épületek biztonságának érdekében. A dolgozatomban ezekre a kiberbiztonsági kihívásokra és megoldásokra szeretnék fókuszálni CPS környezetben.

II. CYBER-PHYSICAL SYSTEMS (CPS) OKOSOTTHON KÖRNYEZETBEN

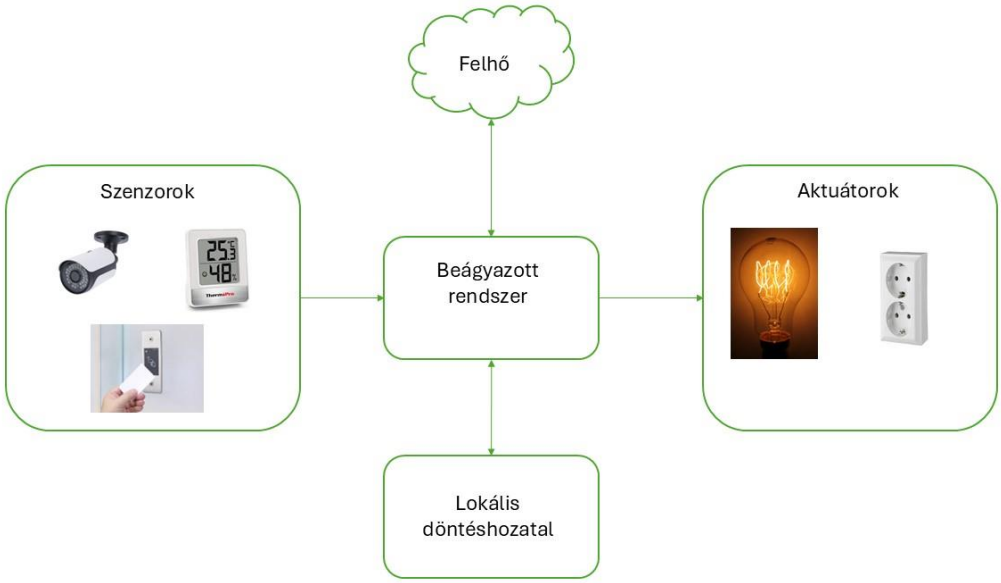
Az okos épületek az egyik legjellemzők képviselője a CPS rendszerek számára. Egy jól megtervezett CPS rendszer csökkenti az energiafogyasztást, növeli az épület biztonságát, valamint javítja az épületben lévő emberek kényelmét.

A kiber rendszerek és a fizikai világ egyesülése az információs technológia egyik fejlődésének tekinthető, főleg a vezeték nélküli hálózatok terén. A fizikai rendszerhez tartozik az a környezet, amit irányítani, felügyelni kell, addig a kiber rendszerhez olyan beágyazott eszközökre utalnak, amelyet következő generációs mérnöki rendszernek nevezünk. Ezeknek az eszközöknek a feladat az információfeldolgozás és a CPS-alapú rendszer környezetével való kommunikáció. Egy CPS-alapú rendszerben a kommunikációs hálózat, szenzorok és aktuátorok együtt alkotják meg azt az interfészt, ami összeköti a fizikai világot a kiberarchitektúrával. [1]

Az aktuátorok a vezérlőrendszerek végrehajtó szervei. Feladatuk, hogy a vezérlő algoritmus kimenő jeleit konkrét akcióvá alakítsák át. Mechanikai elmozdulás, valamely elem bekapcsolása vagy kikapcsolása vagy éppen pozicionálás. Az információt, illetve a vezérlőrendszer döntését az aktuátor egy digitális kód alakjában kapja, amit később jellé alakit át. [1]

A vezet nélküli hálózatoktól eltérően, ahol egy adott célra rendeltetett eszköz van a fizikai környezetbe beágyazva, az okosházak eszközei gyakran több érzékelővel és működtető egységgel vannak felszerelve, hogy többcélú alkalmazásokat tudjanak kiszolgálni. Azokat a szenzorokat, amelyeket különböző alkalmazások különböző időpontban használnak, heterogén szenzoroknak nevezzük. Azonban a rendelkezésre álló érzékelőknek csupán egy részét használja az CPS-alkalmazás a saját igényeinek megfelelően. [1]

A következő ábra egy CPS modell mutat be az okosotthon környezetében és ábrázolja, hogyan működnek együtt a különböző komponensek. (2.ábra)



2. ábra CPS modell az okosotthon környezetben - saját szerkesztés

A szenzorok felelnek a fizikai világ különböző adatainak begyűjtéséért. Ilyen eszköz lehet egy biztonsági kamera, ami mozgás vagy képi információt kezel, hőmérő, ami méri a hőmérsékletet ez főleg egy termosztát vezérlésénél különösen hasznos, vagy egy RFID, ami az eszközök azonosítására, például ajtónyitás, szolgál. A szenzorok célja továbbítani ezeket az adatokat a központi feldolgozó egység felé.

A beágyazott rendszer összegyűjti ezeket az adatokat és irányítja az aktuátorokat. További feladat az adatfeldolgozás, döntéshozatal, valamint kommunikáció a felhőalapú rendszerekkel.

A lokális döntéshozatal önálló döntéseket hoz a kapott szenzorok alapján. Ilyen döntés lehet, hogy hőmérséklet alapján szabályozza a fűtést vagy ha az ember belép a szobába felkapcsolja a villanyt. Ez a blokk a döntéseit helyben hozza meg ami csökkenti a hálózati késleltetést és növeli a biztonságot az által, hogy nem mindet adatot továbbit ilyenkor a felhőbe.

A felhő alapú szolgáltatások szinkronban vannak a beágyazott rendszerrel. Ilyen lehet, amikor egy eszközt távolról vezérlünk az okostelefonnal vagy a biztonsági naplók tárolása.

Az aktuátorok azok az eszközök, amelyek a döntések hatására fizikailag reagálnak. Ilyen lehet az izzó felkapcsolása vagy a konnektor ki/be kapcsolása.

A következőben egy valós példán keresztül szeretném bemutatni egy CPS eszköz működését. Az intelligens világítás talán az első dolog, ami az ember eszébe jut, ha okosotthonról beszélünk. Ez a leggyakrabban alkalmazott funkció, ahol a manuális kapcsolók helyett szenzorok, beágyazott vezérlők és aktuátorok működnek. Ez a rendszer nem csupán kényelmet nyújt, hanem segíti az energiamegtakarítást és biztonságérzetet is ad.

A működés azon alapszik, hogy a világítás automatikusan bekapcsol, amikor mozgást érzékel a szobában és egy előre meghatározott idő elteltével kikapcsol.

A szenzorok adatot gyűjtenek egy mozgásérzékelőn keresztül. Ilyen szenzor lehet a PIR (passive infrared sensor) ami az objektumok által kibocsátott infravörös fényt mérik. Majd ezt az adatok a beágyazott rendszer feldolgozza és értelmezi. A lokális döntéshozatal, ha mozgást érzékel, akkor aktiválja az aktuátorokat. A lámpák lekapcsolnak majd, ha nincs mozgás a szobában egy meghatározott időn belül lekapcsol.

III. BEÁGYAZOTT RENDSZEREK AZ OKOSOTTHONBAN

Az okosotthonok fejlődése összekapcsolódik a beágyazott rendszerek technológia fejlődésével. Ezek az általában alacsony fogyasztású de nagy teljesítményre képes rendszerek az okosotthonok közepét alkotják, ők felelnek az adatok összegyűjtéséért, feldolgozásáért és értelmezéséért, amik által később az aktuátorokat vezérelve segíti a kényelmes és biztonságos életet.

A beágyazott rendszerek összegyűjtik a szenzoroktól kapott adatokat, ezek lehet hőmérséklet, mozgás, páratartalom vagy fényérzékelések, és ezek alapján autonóm döntéseket hoznak, majd parancsokat küldenek az aktuátorok részére. Az aktuátorok végrehajtják a feladatokat, amik lehetnek világítás felkapcsolás vagy lekapcsolása, fűtés szabályozása vagy biztonsági rendszerek vezérlése. [2]

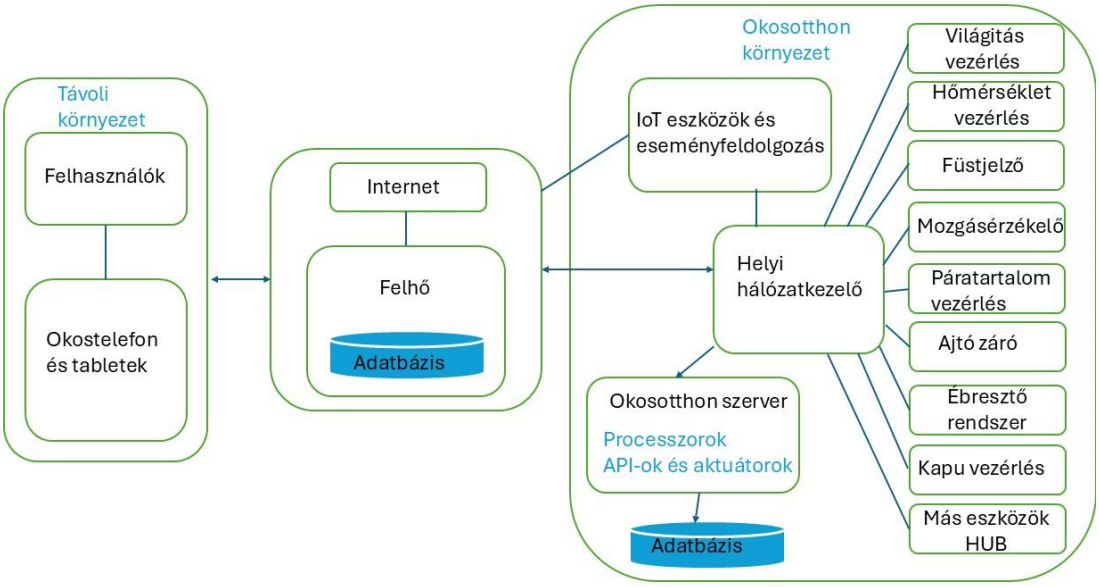
A modern okosotthonokban használatos beágyazott rendszerek, mint például az ARM Cortex-M alapú mikrokontrollerek, az ESP32 IoT chip vagy a Rasberry Pi modulok, amik mind alacsony energiaigényűek és a vezeték nélküli kommunikációs szabványokat is támogatják, amelyet nagy szerepet játszanak az IoT környezetben. Ilyen vezeték nélküli szabvány lehet a Wi-fi, ZigBee, Bluetoorh vagy éppen a Low Energy. [3]

A beágyazott rendszereknél figyelembe kell venni, hogy a rendszerek ne csak hatékonyak legyenek, hanem biztonságosak is. A támadások ellen a leggyakoribb védelmi eszközök a TPM-ek, amik hardveres biztonsági modulok, a titkosított kommunikációs csatornák és az automatikus szoftverfrissítési mechanizmusok is integrálásra kerülnek. [4]

Ezenkívül figyelembe kell még venni a rendszer hosszú távú karbantarthatóságát és megbízhatóságát ugyanis egy okosotthonban a rendszernek akár több évtizedig is működnie kell anélkül, hogy veszélyeztetne az egész rendszert.

Az Internet of Things is szorosan összekapcsolódik a beágyazott rendszerekkel, ugyanis eszek az okoseszközök valósítják meg az eszközök közötti adatcserét és döntéstámogatást. Egy jól megtervezett okosotthonban a helyi beágyazott egységek a kisebb döntéseket decentralizáltan képesek meghozni, míg a nagyobb döntéseket a központi szerverek vagy a felhőalapú rendszer dolgozza fel. [4]

IV. IOT ALAPÚ ARCHITEKTÚRA MODELL AZ OKOSOTTHONOKBAN



3. ábra IoT architektúra modell okosotthonokhoz -
https://www.researchgate.net/publication/359498890_An_Overview_of_IoT-Based_Architecture_Model_for_Smart_Home_Systems - alapján saját szerkesztés

Az ábrán látható az IoT alapú architektúra fő komponensei, valamint azok kapcsolódásai. (3.ábra) Az okosotthonok környezetében jellemzően az eszközök helyi hálózaton, LAN-on keresztül csatlakoznak. Ilyenek lehetnek a korábban említett Wi-fi, ZigBee, BLE, ANT, Z-wave vagy Bluetooth. Ezek teszik lehetővé a kommunikációt a szenzorok és az aktuátorok között. A szerver irányítja az eszközöket és naplózza azok tevékenységeit, jelentéseket készít és végrehajtja a megfelelő parancsokat. A bonyolultabb vagy már végrehajtott feladatokhoz az okosotthon szervere a felhőbe továbbítja az adatokat és távolról aktiválja a feladatokat API-k segítségével. Ezen kívűl az IoT háztartási okoseszközök is csatlakoznak az internethez bővítve ezzel az okosotthont IoT eszközökkel. Az internethez való csatlakozás után a felhasználó kommunikálhat az okosotthonnal, lehetővé téve a lakó számára a távoli aktiválást és az információk elérését. [5]

V. KOMMUNIKÁCIÓS TECHNOLÓGIÁK AZ OKOSOTTHONOKBAN [6]

Ebben a részben ismertetem a kommunikációs technológiákat, amelyeket okosotthonokban használnak, vezetékes és vezeték nélküli csoportokra lebontva.

A. Vezetékes technológiák

Ethernet

Az Ethernet talán a legnépszerűbb vezetékes kommunikációs technológia, amelyet telephelyi hálózatokban használnak és általában helyi hálózati (LAN) vagy nagy kiterjedésű hálózati (WAN) kapcsolatot biztosit. Az Ethernet szabványa az IEEE 802.3-on alapszik. Megvalósítására koaxiális, sodort érpárú vagy optaikai szálas kábelekre van szükségünk, valamint egy hub-ra vagy switchre. Az adatátviteli sebessége nagy kiterjedésű 10 Mbps-tól akár 100 Gbps-ig is terjedhet. Vezetékes hálózat révén jól védekezik a zajokkal szemben, viszont hátrányának az sorolható be, hogy a hálózat kiépítése után a változtatásokat nehéz végbevinni. A legtöbb okosotthonban sodort érpárú rétkábel használnak, ami

csillag topológiában csatlakozik a switchekhez, igy elérve 10 Mbps, 100 Mbps, 1000 Mbps vagy akár 10000 Mbps-os sebességet.

ITU G.hn

Az ITU G.hn egy vezetékes kommunikációs és hálózati szabvány, amelyet az ITU (Nemzetközi Távközlési Unió) fejlesztett ki. Fő célja, hogy egy egységes kapcsolódási lehetőséget biztosítson a digitális tartalom és médiakezelő eszközök számára, olyan már meglévő kábelhálózatokon keresztül, mint a telefon, koaxiális és adatkábelek. Az adatátviteli sebessége akár 1 Gbps is lehet. A G.hn meghatározza a fizikai és adatkapcsolati szinteket otthoni vezetékes hálózatokhoz. Felhasználása általában nagy és kissebességű szolgáltatásoknál, illetve okos hálózati alkalmazásoknál is kifizetődő.

Power Line Communication (PLC)

A PLC adatátvitelre egy már meglévő elektromos vezetékhálózatot használ. Működésének alapja az, hogy nagyfrekvenciás vivőjelet injektál a hálózatba, amelyet az átadni kívánt adattal modulál. Ez egy nagyon költséghatékony megoldás, ugyanis nem igényel újabb kábelezést vagy módosítást. Az okosotthonokban a frekvencia jellemzően 20-200 kHz között mozog. Habár a PLC technológia olcsónak számít, számos intelligens hálózati alkalmazásra nem alkalmas az interferencia, zaj, torzítás és biztonsági problémák miatt.

A HomePlug specifikációk közül jelenleg kettőt ismerünk, a HomePlug AV és a Home Plug GP személyében. A HomePlug GP a HomePlug AV egy alváltozata, alkalmazása kifejezetten intelligens hálózati alkalmazásokhoz ajánlott, és legfeljebb 10 Mbps sebességet tud biztosítani. Hatótávja akár 300 méter is lehet. A HomePlug AV 128 bites AES titkosítással védi a hálózatot. A HomePlug Command Control (HPCC) az AV egy alternatívája, amely alacsony sebességű, rendkívül olcsó alkalmazásokra lett kifejlesztve. A X10 egy nemzetközi és nyílt ipari szabvány, amely az elektromos hálózatot használja az otthoni eszközök vezérlésére, azonban kompatibilitási problémákkal, interferenciával, alacsony sebességgel és titkosítás hiánya jellemzi. További PLC technológia lehet a LonWorks és a CE Bus. PLC termékeket általában lámpák és háztartási eszközök vezérlésére használnak az okosotthonban.

Soros kommunikáció

A soros kommunikáció az adatokat bitenként továbbítja egyetlen vezetéken, ellentétben a párhuzamos adattovábbitással, ahol több bitet küldenek egyszerre a csatornán. Az RS-232 a leggyakoribb soros interfész, ami egy adó és egy vevő csatlakozást tud lehetővé tenni, legfeljebb 1 Mbps sebességgel, bár gyakran csak 115,2 kbps-ra képes. Az RS-422 és az RS-485 akár 10 Mbps adatátvitelt biztosít, akár 1200 m hatótávval.

HomePNA

A HomePNA szabvány a telefonvonalakat használja a számitógépek összekapcsolására. Internetmegosztást tesz lehetővé, akár 240 Mbps sebességgel, ami csökkenhet, ha a hálózat több mint 50 eszközt tartalmaz, legfeljebb 300 méteres hatótávval. Jelentős versenytársa az Ethernetnek és a HomePlugnak, és kulcsfontosságú szereplője az otthoni szélessávú elosztásnak.

MoCA

A MoCA (Multimedia over Coax) technológia, ami legfőképp Észak-Amerikában terjedt el, a nevéből adódóan, koaxiális kábeleken keresztül biztosit nagysebességű adatátvitelt. Ethernet szerű kereteket és MAC réteget használ. Háromszoros DES titkosítást használ, ami nagyon jól védi a hálózatot. Kifejezetten alkalmas nagy felbontású videók megosztására.

B. Vezeték nélküli technológiák

Wi-Fi

A Wi-Fi szabvány a legnépszerűbb vezeték nélküli kommunikáció, amelyet CPN-ekhez használnak. Különféle szabványokat tartalmaz, amik lehetnek a 802.11a/b/g/ac/ax. Ezek a szabványok leginkább a 2,4 GHz-es az 5 GHz-es ISM sávokat használják. A 802.11g szabvány a 2,4 GHz-es sávon működik, és 54 Mbps elméleti adatsebességet biztosít, míg a 802.11a és a 802.11n a 2,4 GHz-es és 5 GHz-es sávokon működik, és 600 Mbps elméleti adatsebességet tesz lehetővé. A hatótávolsága 100 méter is lehet. Emellett megbízható, biztonságos és nagy sebességű kommunikációt biztosít. Azonban csak rövid távú kommunikációt támogat. A WLAN (vezeték nélküli helyi hálózat) termékek költsége és energiafogyasztása is magasabb, mint más rövid távú vezeték nélküli technológiáké, mint például a ZigBee és a Z-Wave.

Zigbee

A Zigbee olyan vezeték nélküli szabvány, amely az IEEE 802.15.4 szabványra épít. Alkalmazzák olyan hálózatokban, amelyek alacsony adatátviteli sebességet igényelnek (maximum 250 kbps), valamint hosszú akkumulátor-élettartamot (akár 10 év). Egy tipikus ZigBee adatátviteli hatótávolság akár 100 méter is lehet, a teljesítménykimenettől és a környezeti jellemzőktől függően. Ha a Zigbee adatátviteli sebességét összehasonlítjuk más technológiáival, úgy tűnhet, hogy a ZigBee sokkal alacsonyabb sebességet kínál. Ezen kívül a ZigBee hálózatoknál használatos a mesh konfiguráció, amely lehetővé teszi a nagyobb megbízhatóságot és szélesebb távolságot.

Z-Wave

A Z-Wave egy szintén alacsony energiafogyasztású vezeték nélküli kommunikációs protokoll, amelyet különösen az okosotthoni eszközökhöz terveztek. A Zigbee-vel ellentétben nem az ISM 2,4 GHz-es sávot használja, ami csökkenti az interferencia lehetőségét Wi-Fi vagy Bluetooth eszközökkel. Egy Z-Wave hálózat maximum 232 eszközt képes kezelni. A tipikus hatótávolság 30 méter, de a hálózatos topológia segítségével ez is megnövelhető. Az eszközök képesek továbbítani egymás adatait, így az egész ház lefedhető. A Z-Wave különösen alkalmas világításvezérlésre, termosztátokhoz, zárakhoz és érzékelőkhöz.

Bluetooth

A Bluetooth egy rövid hatótávolságú vezeték nélküli kommunikációs szabvány, amelyet két vagy több eszköz közötti adatok átvitelére használnak. A Bluetooth a 2,4 GHz-es ISM sávban működik, és jellemzően 21 kbps adatsebességet nyújt. A szabvány jellemzően 10 méter hatótávolságú lehet, de a piacon fellelhetők akár 100 méter hatótávolságúak is. A Bluetooth-nak nincs erős biztonsági rétege a lehallgatás megakadályozására. Ezért nem felel meg a szigorú biztonsági követelményeknek, összehasonlítva más vezeték nélküli kommunikációs szabványokkal. Továbbá, alacsonyabb átvitelű hatótávolsággal rendelkezik. Lefedi mind a fizikai hozzáférési, mind a MAC réteget, és kifejezetten zajos környezetekben való működésre tervezték.

6LoWPAN

A 6LoWPAN a Low power Wireless Personal Area Networks feletti IPV rövidítése. Ez egy olyan hálózati technológia, amely lehetővé teszi az IPv csomagok hatékony továbbítását kis méretű adatkapcsolati rétegű keretekben, például az IEEE 802.15.4 által meghatározottakban. A LoWPAN kihasználja az IEEE 802.15.4 által definiált erős AES-128 szintű adatkapcsolati rétegű titkosítást. Jellemzői révén ideálisan alkalmazható olyan területeken, mint az otthonautomatizálás érzékelőkkel és beavatkozó eszközökkel, utcai világítás felügyelete és vezérlése, lakossági világítás, intelligens mérés, valamint általános IoT alkalmazások, ahol eszközök kapcsolódnak az internethez. Napjainkban a 2,4 GHz-es és az 1 GHz alatti sávok egyaránt használhatók, az IEEE 802.15.4 előnyeit kihasználva, beleértve a nagyméretű hálózatos topológia támogatását, a megbízható kommunikációt és a nagyon alacsony energiafogyasztást. Az IEEE 802.15.4 szabvány 20 és 250 kbps közötti adatátviteli sebességet biztosít, frekvenciától függően. Rövid távú kommunikációra alkalmas, jellemzően 10 és 100 méter közötti távolságban.

IEEE 802.15.3a

Az IEEE 802.15.3a az úgynevezett ultraszélessávú technológia. Ez egy nagyon rövid hatótávolságú kommunikációs technológia, jellemzően 10 méteres távolságig. Az adatátviteli sebessége kissé meghaladja a Bluetooth sebességét. Kifejezetten alkalmas nagy sebességű személyes hálózatok fizikai rétegeként való alkalmazásra.

ONE-NET

A ONE-NET egy nyílt forráskódú vezeték nélküli hálózati szabvány. Olyan olcsó, alacsony energiafogyasztású vezérlőhálózatokra tervezték, mint például otthonautomatizálás, biztonsági megfigyelés, eszközvezérlés és érzékelőhálózatok. Nem kötődik semmilyen zárt hardverhez vagy szoftverhez, és számos gyártó olcsó, kereskedelemben kapható rádiós adó-vevő egységeivel és mikrovezérlőivel megvalósítható. A ONE-NET egy dinamikus adatsebességű protokollt alkalmaz, alapértelmezett adatsebessége 38,4 kbps. A hatótávolsága akár 500 méter nyílt terepen, és akár 100 méter zárt térben. Ideális választás okos hálózati környezetben történő otthoni és épületautomatizálási alkalmazásokhoz.

VI. KOMMUNIKÁCIÓS PROTOKOLLOK [7]

Az okosotthonok működéséhez elengedhetetlen, hogy az egyes eszközök megbízhatóan tudjanak kommunikálni egymással és a központi irányítással. Ehhez különböző kommunikációs protokollok állnak rendelkezésre, amelyek mind más más módon kezelik az adatcserét, energiahasználatot és hálózati architektúrát is. Az alábbiakban három elterjedt protokollt mutatok be, amelyek gyakran szerepet kapnak az IoT rendszerekben.

1, MQTT

Az MQTT egy kis méretű és egyszerű üzenetküldési protokoll. Architektúrája nyilt és könnyen megvalósítható, ami lehetővé teszi akár több ezer távoli kliens kapcsolódását egyetlen kiszolgálóhoz. Ezeknek a tulajdonságoknak hála az MQTT alkalmas korlátozott erőforrású környezeti használatra, legfőképp ott, ahol alacsony a hálózati sávszélesség, nagy a késleltetés vagy a távoli eszközöket korlátozott feldolgozási képesség és memória jellemzi.

Az MQTT előnyei a következők. Kiterjesztett kapcsolódás az okoseszközökre akár a vállalati határokon túl is. Széleskörű skálázhatóság az eszközök telepitésénél és kezelésénél. Távoli eszközök számára optimalizált kapcsolati lehetőségeket kínál.

Az MQTT minimalizálja a hálózati sávszélességet és az eszköz erőforrás igényeit, ezen felül törekszik minél megbízhatóságra és az adatkézbesítés biztositására.

2, CoAP

Okosotthonokban gyakran előfordul, hogy az IoT eszközök eljutnak arra a pontra, hogy valaminek meg kell mozdulnia, villognia kell, vagy hangot kell adnia. Ilyen lehet, amikor a lakó érzékeli, hogy a lakás túl hideg és szeretné felmelegíteni, azáltal üzenetet küld a fűtőberendezésnek, hogy kapcsoljon be. Vagy Bluetooth-os eszköz érzékeli a lakó közeledését és ennek hatására üzenetet küld a garázsajtó felé, hogy nyíljon ki.

Ezek a telecommand példái, ahol a CoAP protokoll használatos. A telecommand hasonló a telemetriához, de amig a telemetria adatokat küld a központ felé addig a telecommand parancsokat. Ezek lefedik az összes IoT protokollt valamilyen formában.

A CoAP kompatibilis a HTTP-vel, azonban kifejezetten korlátozott erőforrású eszközökre vannak tervezve, mint például a szenzorok, amiknek a memóriája és a sávszélessége is korlátozott. Azonban fontos megjegyezni, hogy a CoAP kompakt és bináris formátumú, nem úgy, mint a HTTP. Úgy tűnhet, hogy a CoAP a HTTP részhalmaza, ám valójában jelentősen eltér tőle. A CoAP olyan platformoknál jöhet számításba, amik korlátozottak, tehát minden bit és CPU ciklus számit.

A legnagyobb különbség közöttük, hogy a HTTP-ben sok gyenge kliens van egy erős szerverrel, addig a CoAP-nál ez fordítva történik sok gyenge szerverrel és kevés erős klienssel. Ez a fordított topológia a RESTful architektúra eredménye. A CoAP webben a szenzorok és az aktuátorok irányítják az erőforrásokat. Például egy hőelem esetén az erőforrás hőmérsékleti értéke, aktuátor esetén az erőforrás az a képesség, amivel mozgatni tud valamit, például egy csapot, ajtót vagy garázsajtót.

3, SensorML

A SensorML a folyamat leírásokhoz, beleértve a szenzorok által végzett mérési folyamatokat és a magasabb szintű információk levezetésének utasításait, egy XML alapú kódolást és szabványos modelleket biztosit. A protokollba leírt folyamatok felfedezhetők és végrehajthatóak. Minden folyamatnak meg kell határoznia a bemeneteit, kimeneteit, paramétereit, valamint módszerét is. A SensorML a folyamatként modellezi a szenzorokat és a detektorokat, majd aztán ezek a modellek a valós jelenségeket adatokká alakítják.

Tehát a SensorML először lehetővé teszi, hogy a szenzorok és a folyamatok megismertessék magukat és a képességeiket. Ez a gyakorlatban azt jelenti, hogy leírja a bemeneteket, kimeneteket és a vezérelhető paramétereket. Majd a protokoll biztosítja a megfigyelések mérési és feldolgozási előzményeit, ezen felül a megfigyelések minőségével kapcsolatos tudást is támogatja. Ugyancsak támogatja a magasabb szintű információk igény szerinti levezetését és mindezt úgy, hogy előzetes ismerete lenne a szenzorrendszerről.

A SensorML úgy kapcsolódik az IoT-hez, hogy lehetővé teszi egy szenzor leírását, majd azt is, hogy linket biztosítson az ebből a komponensből származó valós idejű értékekhez.

A következő táblázatban összefoglalom a már felsorolt protokollok legfőbb tulajdonságait. (1.táblázat)

Tulajdonság	MQTT	CoAP	SensorML
Protokoll tipusa	Üzenetküldési protokoll	Telecommand/REST-alapú protokoll	Leíró protokoll XML formátumban
Használati cél	Könnyű megbízható kommunikáció korlátozott eszközök között	Parancs küldése távoli eszközöknek	Szenzorok, folyamatok, mérések strukturált leirása
Előnyei	Nagy skálázhatóság, egyszerű implementáció, kevés sávszélesség, IoT támogatás	REST támogatás, HTTP-szerű működés kis erőforrásigénnyel	Szenzorleirás, adatok elérésének lehetősége URL-en keresztül
Hátrányai	Korlátozott funkcionalitás, HTTP integrációra kevésbé alkalmas	Külön megoldások szükségesek a biztonságra és a megbízhatóságra	Külön szükséges hozzá hálózati vagy feldolgozó rendszer
Felhasználása	Szenzorhálózatok, M2M kommunikáció, IoT	Szenzorvezérlés, távoli eszközök irányítása okosotthonokban	Szezoradatok leírása, feldolgozási utasítások dokumentálása

1. táblázat Kommunikációs protokollok tulajdonságai - saját szerkesztés

VII. KIBERBIZTONSÁGI FENYEGETÉSEK

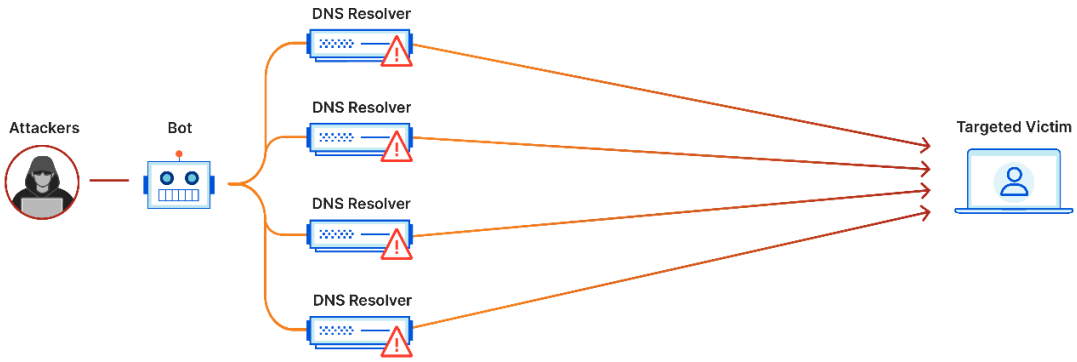
1, DDoS támadás [8]

A DDoS támadás egy olyan támadás, amely a hálózat működését azáltal zavarja meg, hogy lefoglalja a hálózat sávszélességét, ezáltal túlterheli az összes hálózati erőforrást, igy használhatatlanná teszi azokat, amelyekhez hozzáférni szeretnénk. A DDoS támadás annyiban veszélyesebb, mint a sima DoS támadás, hogy itt a támadások több ponton is jelentkeznek, igy a felhasználó nehezebben tudja beazonosítani a támadás forrását, ami miatt nehezebb is elhárítani a veszélyhelyzetet. A speciális okosotthonokban jelentkező DDoS támadások még veszélyesebbek is lehetnek, mivel a beágyazott operációs rendszer akár egyetlen hiba miatt is könnyen sebezhetővé válhat és az azonosítási mechanizmus is gyenge lehet.

Manapság a leggyakrabban előforduló kiberbiztonsági fenyegetések közé sorolható a DoS támadás, magyarul szolgáltatásmegtagadásos támadás, amely a nevéből adódóan azt jelenti, hogy erőforrások elérhetetlenné válnak a felhasználó számára. A DoS támadások végrehajtásának számos módja van, vannak, akik a kiszolgáló infrastruktúrákat célozzák meg, mások a hálózati vagy kommunikációs protokollokat használják. Más kiberbiztonsági támadásokkal összehasonlítva, amelyek szintén adatokat vagy hálózati biztonságot sértenek, a DoS nem minden esetben töri fel a biztonsági védelmet. A DoS gyakran arra is használják, hogy más káros tevékenységeket fedjenek el vele.

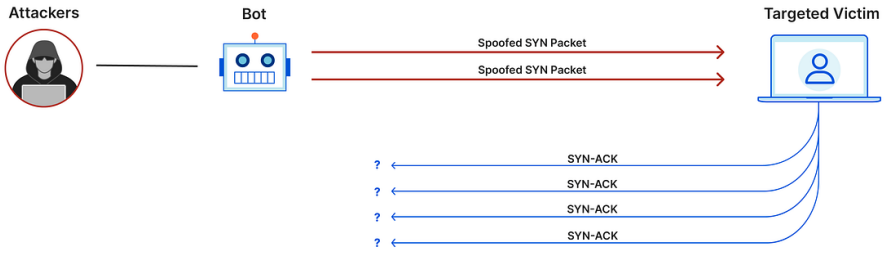
A DoS és a DDoS között alapvető különbség, hogy a DoS egyetlen internet kapcsolatot használ a támadáshoz, míg a DDoS több kapcsolatot hoz létre, hogy a kipécézett szervert hamis kérésekkel árassza el, igy terhelve azt majd használhatatlanná téve.

A DDoS támadásának egyik típusa a Volume Based Attack (Hangerő alapú támadás), ahol a támadó célja, hogy olyan módon terhelje le az áldozatának a sávszélességét, hogy ők ne tudják elérni a weboldalt. (4. ábra) Ide tartozik az UDP flood, ICMP flood, spoofed-packet flood.



4. ábra - DDoS volume based attack - https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

A következő DDoS támadási típus a protokoll alapú támadás. (5.ábra) Itt a támadó az előzővel ellentétben nem a teljes sávszélességet akarja leterhelni, hanem csak a szerver erőforrásit. Ide tartozik a SYN flood, Ping of Death, Smart DDoS.



5. ábra - DDoS protokoll alapú támadás - https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Az utolsó támadási típus az alkalmazásrétegi támadások nevet viseli. Ezek a támadások kevesebb erőforrás igényelnek, de sokkal célozottabbak, mint az előzőek. Ilyen lehet a Zero-Day DDoS, Slowloris vagy Apache, OpenBSD és Windows sebezhetőségeit célzó támadás.

Számos eszköz áll rendelkezésre a DDoS támadások végrehajtásához. Amelyek közül megkülönböztetünk helyileg vagy távolról alkalmazottakat. A következő táblázatban szeretném felsorolni a leggyakrabban használt ilyen eszközöket azok lehetséges támadásaival és megjelenési éveivel. (2.tablázat)

Eszköz	Lehetséges támadás	Év
Trinoo	UDP, TCP SYN, ACK, ICMP flood	1999
TFN	UDP, TCP SYN flood, ICMP flood, Smurf támadás	1999
TFN2K	UDP flood, SYN flood, ICMP flood, Smurf, MiM támadás	1999
Stacheldraht	Trinoo + TFN képességek	2000
Mstream	TCP ACK flood	2000
Shaft	Packet flooding	2001
Knight	TCP flood, ICMP flood, UDP flood	2001
Trinity	TCP SYN flood, UDP flood, TCP fragment	2001
TFN-Rush	TCP RST, ACK flood, IP fragmentation	2001

Stuxnet	SCADA rendszerek elleni támadás	2010
LOIC	HTTP POST flood	2013

2. táblázat A DDoS eszközök és eredetük - https://ieeexplore.ieee.org/abstract/document/9058087

A DDoS támadások ellen nem létezik konkrét védekezési módszer, ami hatékony és ténylegesen alkalmazható lenne. Most három védekezési technikát mutatok be a DDoS támadások ellen ezek név szerint a Topológiaalapú védelmi séma, Játékelmélet és fúziós alapú védelmi séma és a Szekvenciális védelmi séma.

A Topológiai védelmi séma arra épül, hogy bármilyen változást a hálózati topológiában fel lehet használni a hálózat jelerősségének javítása érdekében. Amennyiben kis számú hivatkozást cserélünk ki a topológiában, új csomópont hozzáadása nélkül, akkor a hálózati vételi teljesítmény javítható. Az intelligens otthoni hálózatokhoz az élszintű újraírás előnyösebb, mivel ez elosztott topológiákban is alkalmazható.

A Fúziós alapú védelmi sémából sok fajta létezik, de mivel az élszintű újraírás nem minden esetben lehetséges, egy játékelméleti megközelítést javasolnak a támadók azonosítására. A fúziós séma visszajelzéseken alapszik, minden csomópontból adatokat gyűjt azért, hogy eldöntse, hogy a csomópont támadás alatt áll-e vagy sem. Ez a megoldás hatékonyabb lehet, mint a topológiaalapú, azonban nagy számú eszköz esetén nagy a visszacsatolás mennyisége is, amit nehéz kezelni egy okosotthonban.

A Szekvenciális védelmi séma a hálózat csomópontjainak a visszajelzésein alapszik. Itt a támadások felismerésére a magasabb szintű csomópontok visszajelzéseket továbbítanak az alacsonyabb szintű csomópontok felé. Ezzel az alacsonyabb szinteken történő támadások jól kivédekezhetők. Ez a séma legjobban egy kisebb hálózatban működik, ugyanis ahogy nő a méret, úgy nő a különböző rétegek közötti kommunikációs idő is, ezáltal az alacsonyabb szinteken történő támadások elkerülhetik az azonnali észlelést.

A támadási pontok meghatározására nagy segítségünkre vannak az IoT eszközök. A DDoS támadások tanulmányozásához a topológialapú védelmi sémát mutatok be öt fázisban. (6.ábra)

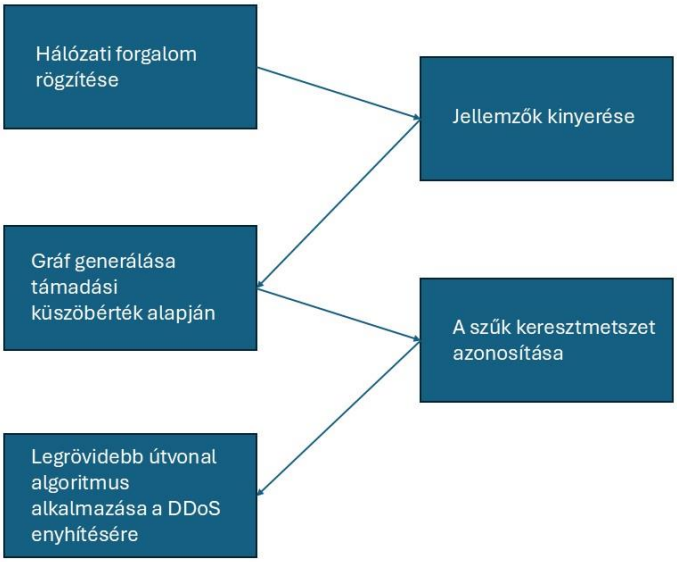
Az első lépésben a rendszer figyeli és naplózza a hálózaton zajló adatforgalmat. Ezt előrejelzés céljából csináljuk.

A második lépésben a rögzített forgalomból releváns adatokat vonunk ki.

A harmadik fázisban a már korábban említett bemeneti paraméterek segítségével hálózati gráfot generálunk, ami megmutatja a fő csomópont, hogyan kapcsolódik a többi csomóponthoz. Mindezt elérési gyakoriság és protokollhasználat alapján mondja meg.

A negyedik fázisban kiválasztjuk a szűk keresztmetszetet, ahol a legtöbb kapcsolat és a legnagyobb késleltetést tapasztaljuk.

Az ötödik fázisban a legrövidebb útvonalat meghatározó algoritmust használunk a szűk keresztmetszetre, azért, hogy megtaláljuk a csomagátvitel legrövidebb útját és hogy minimalizáljuk a késleltetést.



6. ábra - A rendszer keretrendszerének munkafolyamata - https://sci-hub.se/https://ieeexplore.ieee.org/abstract/document/9058087 - alapján saját szerkesztés

2. PDoS támadás [9]

A DDoS egy már régóta ismert fenyegetés, míg a PDoS egy újonnan feltörekvő egyre nagyobb figyelmet kapó veszélyforrás. Ezek a PDoS támadások a DDoS támadásokkal szemben, visszafordíthatatlanná következményeket okoznak a célrendszerekben. A támadások célje az infrastruktúra tartós működésképtelenné tétele, gyakran firmware szintű módosítással, amelyet phlashing-nak nevezünk.

A PDoS egy olyan támadás, ahol a támadó nem egyszerűen túlterheli a hálózatot, hanem az eszközöket fizikailag vagy szoftveresen elérhetetlenné teszi. Ez egyik ilyen módszer a firmware manipuláció a phlashing, ami egy káros firmware juttat el az eszközbe, ezzel tönkretéve azt. Ez a támadás nagyon hasonló a brickeléshez, ott is a eszköz használhatatlanná válik, amit csak hardveres javítással vagy cserével lehet orvosolni.

A PDoS támadásnak a menete három egyszerű lépésből áll. Az első lépésben a támadó talál egy sebezhetőséget és azt ki is használja, ilyen sebezhetőség lehet például egy nyitott firmware frissítési csatorna. A második lépésben bejuttatja a káros firmware vagy szoftverfrissítést az eszközbe. A harmadik lépésben pedig már az eszköz teljesen megbénul, nem tud elindul, nem reagál a bevitt inputokra.

A PDoS támadások csak az utóbbi években váltak különösen népszerűvé, a kritikus infrastruktúrák és az intelligens eszközök körében váltak gyakori célponttá. Korábban úgy gondolták, hogy ez a támadás nem lesz olyan népszerű mert nem lehet zsarolni vele, de később kiderült, hogy pusztán a rombolás is jó motiváció lehet. Ilyen vírus volt a Petya is, ahol nem a pénzszerzés volt a cél, hanem adatmegsemmisítés. Ezen felül a PDoS idő és költséghatékonyabb is mint a DDoS, mivel itt nem kell folyamatos kapcsolatot tartani a célrendszerrel.

A PDoS támadások elősegíti az IoT eszközök tenyeresé. Ezeknek az eszközöknek a száma manapság már meghaladta 20 milliárdot is. Az ilyen eszközök gyakran nem rendelkeznek megfelelő frissítésekkel, ellenőrzési vagy biztonsági mechanizmusokkal, ezzel kiváló célpontot nyújtanak az ilyen típusú támadásoknak. Akár egyetlen PDoS

támadás is hatással lehet az egész okosotthon működésére, hiszen a fizikai sérülés miatt az eszközök szoftveresen nem javíthatóak.

Védekezni nem egyszerű a PDoS támadások ellen azonban a kockázat több módon is csökkenthető. Rendszeres firmware frissítéseket eszközöljünk hiteles forrásokból és ahol lehet minden firmware frissítés esetén használjunk authentikációs védelmet. Az adatközpontban legyen éjjel-nappali biztonsági védelem, ezzel megelőzve a fizikai manipuláció lehetőségét. Hálózati monitoring és betörésészlelési rendszerek telepítése is kulcsfontosságú lehet. Végül de nem utolsó sorban fontos biztonságtudatosság növelése a vállalati környezetben.

A PDoS illetve DDoS bár nagyon hasonlónak tűnnek jelentősen eltérnek, amiket a táblázatban ismertetek is. (3-táblázat)

Jellemző	PDoS	DDos
Cél	Eszköz megsemmisítésé	Rendszer túlterhelése
Hatás	Maradandó, fizikai kár	Átmeneti kiesés
Tartósság	Hosszú távú	Rövid távú
Védekezés	Fizikai és firmware védelem	Tűzfalak, forgalomszűrés
Példa	Phlashing attack	Botnet támadás

3. táblázat - PDoS és DDoS támadás összehasonlítása - saját szerkesztés

3. Eszköz eltérítésé (Device Hijacking)

Mivel az okosotthonokban rengeteg IoT eszköz van használva és összekapacsolva ezért az egyik legjelentősebb fenyegetés a device hijacking. Ennél a támadásnál a támadó átveszi az uralmat egy vagy több okoseszköz felett. Ez nem csupán adatvédelemből egy nagy fenyegetés, hanem a fizikai biztonságot is veszélyezteti, gondoljunk csak a biztonsági kamerarendszerek feletti átvételre, okoszárak feletti átvételre vagy a termosztát feletti átvételre.

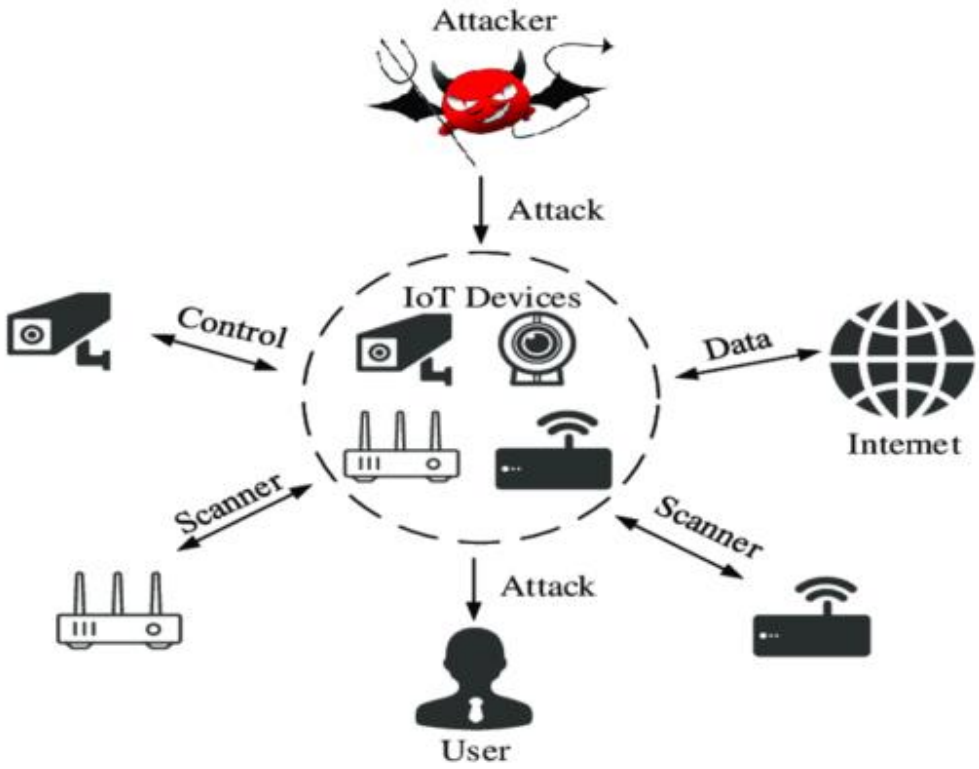
Az eszköz eltérítése során a támadó kihasználja az eszköz sebezhetőségeit, ilyen sebezhetőség lehet a nem frissített firmware, gyenge jelszavak vagy a nyílt kommunikációs protokollok, ezért, hogy távolról hozzáférhessen az eltulajdonított eszközhöz. Ez olyan veszélyeket hordoz magában, mint az okoszárak kinyitása vagy a termosztát ki esetleg bekapcsolása. Ezek a támadások különösen veszélyesek, mert nem csak adatvédelmi incidenseket jelentenek, hanem pszichológia, fizikai és gazdasági károkat is okoznak. [10]

A leggyakoribb sebezhetőségek közé tartoznak a nem megfelelő hitelesítés, a titkosítás hiánya, illetve a nyitott portokon keresztül történő kommunikáció. Az okosotthonok biztonsági architektúrája gyakran hiányos és a rendszerek nem mindig tartalmaznak megfelelő behatolást észlelő mechanizmusokat, ezzel még inkább kiszolgáltatottabbá teszi az okosotthonokat. [11]

A legtöbb device hijacking-gel kapcsolatos probléma megelőzhető lenne, ha a gyártók már a tervezés során beépítenének védelmi mechanizmusokat, például autentikált firmware frissítéseket, az adatforgalom titkosítását vagy a felhasználói jogosultságok szigorú szabályozását. Emellett nagyon fontos még a biztonságtudatos felhasználói magatartás is. A rendszeres frissítések, erős jelszavak használata, valamint a helyi hálózat védelme tűzfallal vagy akár VPN szolgáltatással mind hozzájárulnak a kockázatok csökkentéséhez. [12]

A device hijacking azért nagyon veszélyes mert ez nem csak egy technológiai probléma, hanem társadalmi és személyes biztonsági kérdés is. Az eszközök könnyen kihasználhatók a sebezhetőségek által, azonban a kockázatok nagymértékben csökkenthetőek megfelelő technológiai és felhasználói védelemmel.

Az ábrán látható a device hijacking támadás, amely során a támadó átveszi a hatalmat az IoT eszközeink felett. (7. ábra)



7. ábra - A támadás kockázata az IoT rendszer egyre intenzívebb fejlődése mellett - https://www.researchgate.net/figure/Internet-of-Things-IoT-attack_fig1_340036543

4. Adat és személyazonosságlopás okosotthonokban

Az okosotthonokban rengeteg IoT eszköz található meg, okos eszközök, kamerák, termosztát, hangvezérelt asszisztensek, amik adatokat gyűjtenek majd az adatokat a felhőbe továbbítják. Ez a központosított adattárolás ugyan megkönnyíti az adatokhoz való hozzáférést ugyanakkor fokozott kockázatot jelent a személyes adatok kiszivárgása és a személyazonosság-lopás szempontjából.

A felhőszolgáltatásokban található sebezhetőségek mindig is célpontok voltak a kiberbűnözőknek. A nem megfelelően tárolt és védett adatkapcsolatok, illetve a gyenge titkosítás fokozni tudja a felhasználói adatok kiszivárgását. Ez az okosotthonokban különösen veszélyes lehet ugyanis itt nemcsak pénzügyi vagy kapcsolattartási információk vannak, hanem hangfelvételek, videók vagy akár egészségügyi adatok. Ezek a károk nemcsak pénzügyi károkat okoznak, hanem a felhasználóknak a bizalma is megcsappanhat egy személyes adat elvesztése után. [13]

A személyazonosság lopás fő forrása általában a felhőből kiszivárgott adat. A már korábban említett helyadatok, személyes adatok, egészségügyi adatok lehetőséget ad a támadónak arra, hogy hamis identitásokat hozzanak létre, esetleg valaki másnak a személyiségét használják. Sok tanulmány szerint a felhasználók még mindig nincsenek tisztában azzal, hogy milyen típusú adatokat osztanak meg, illetve ezek hol és hogyan kerülnek feldolgozásra. Ezen szintén nem segít az átláthatóság hiánya, valamint a fejlesztők és a szolgáltatók részéről jelentkező adatvédelmi hiányosságok. [14]

A fent említett kockázatok miatt javasolt több szinten beavatkozni. Az egyik ilyen intézkedés lehetne, hogy a felhőszolgáltatók kötelezővé tennék az erős hitelesítést, a végpontok közötti titkosítást, valamint az automatikus biztonsági

frissítések alkalmazását. Emellett ugyanolyan fontos az is, hogy a felhasználók tájékozódjanak az adatvédelmi beállításokról, tudjanak róla hova menti az adataikat és miként kezeli azokat. A GDPR szigorú szabályokat ír elő az adatkezelésre vonatkozóan, azonban ezek betartása, valamint ellenőrzése nem működik kellő hatékonysággal. [15]

5. Man-in-the-middle támadás

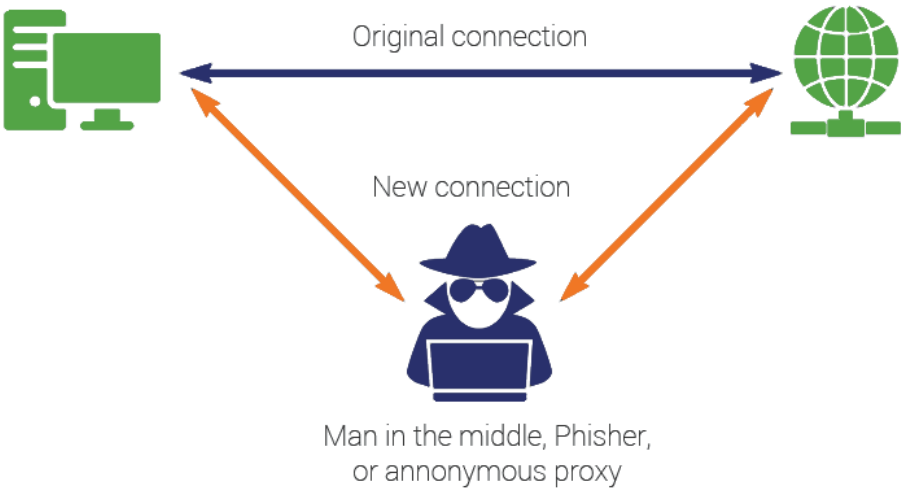
Hasonlóan az előzőekhez a Man-in-the-middle támadás is egy nagyon súlyos fenyegetés, ami arra épül, hogy a támadó beékelődik két kommunikáló fél közé és észrevehetetlenül lehallgatja, módosítja vagy manipulálja az adatforgalmat. Ez a fenyegetés is arra vezethető vissza, hogy az okosotthonokban, ahol sok IoT eszköz megtalálható, gyenge biztonsági protokollokat alkalmaznak vagy a hálózati kommunikációnak nincsen titkosítása.

A Man-in-the-middle támadás jellemzően három szakaszra bomlik. Az első szakaszban a támadó hozzáférést szerez a lehallgatni kívánt kommunikációs csatornához. A második szakaszban lehallgatja vagy módosítja az átvitt adatokat. A harmadik szakaszban pedig, továbbítja a már módosított adatokat az eredeti címzettnek úgy, hogy a kommunikáló felek nem észlelik a beavatkozást. ezek a támadások a fizikai, hálózati, alkalmazási és a szállítási rétegeket is érinti. Azok az IoT eszközök, amelyek nem támogatják a TLS/SSL titkosítást vagy nem rendelkeznek megfelelő hitelesítési mechanizmusokkal nagyobb veszélynek vannak kitéve. [16]

Az egyik leghatékonyabb védekezési módszer a Man-in-the-middle fenyegetések ellen a támadások felismerése a gépi tanuláson alapuló modellek alkalmazásával. A másik megoldás egy mesterséges intelligenciával megtámogatott behatolásmegelőző rendszer okosotthonokhoz, melyek szoftveresen definiált hálózatokban hatékonyak. Ezek a rendszerek képesek a támadásokat már a viselkedésminták alapján azonosítani és akár blokkolni is tudják a gyanús forgalmat. [17]

Azonban a Man-in-the-middle támadásoknak nem csak az IoT eszközök lehetnek a célpontjai, hanem a hozzájuk kapcsolódó mobilalkalmazások is. Ugyanis a kommunikációs csatornák nem megfelelő hitelesítési eljárások allapján működnek, igy a támadó könnyedén létrehozhat hamisítót alkalmazásokat vagy akár weboldalakat az adatok megszerzése érdekében. Itt is nagy hiba lehet, hogy a felhasználók nem frissítik az alkalmazásaikat vagy az IoT eszközök firmware-jét, igy azok is könnyen célpontokká válhatnak.

Az ábrán a man-in-the-middle támadás látható, ahol a támadó a szerver és a kliens közötti kommunikációba ékelődik be, igy lehetősége adódik a lehallgatásra, módosításra vagy a hitelesítés megkerülésére. (8. ábra)



8. ábra - Man-in-the-middle támadás - https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

VIII. TITKOSÍTÁS ÉS HITELESÍTÉS AZ IOT KÖRNYEZETBEN

Az IoT eszközök rohamos terjedésével, főleg az okosotthonokban, egyre égetőbb szükségünk van a biztonságba tudni ezeket az eszközöket. Korábban már említettem, hogy ezek az eszközök alacsony számítási kapacitással működnek, annak ellenére, hogy kényes adatokat kezelnek, amiket senki sem szeretné, ha kiszivárognának. Ezt azt eredményezi, hogy biztonságos kommunikációra van szükségünk, de az legyen energia és erőforrástakarékos.

A legkézenfekvőbb megoldás a titkosítás és hitelesítés kombinációja. A valóságban ez azonban nem ilyen egyszerű. Nem elég csak valami biztonságosnak nevezett dolgot ráhúzni a rendszerekre, hanem a védelmet már a tervezési szakaszban el kell kezdeni.

A titkosítás általában a két pont közötti adatátvitelt védi. Például amikor egy szenzor adatot küld a felhőbe, azok titkosított formában mennek át a hálózaton. A titkosítás fő célja, hogy ezeknek a szenzoroknak az adatait egy kulcs segítségével értelmetlen zajjá alakítsák át. Az adatokat csak az tudja visszafejteni, aki rendelkezik ezzel a kulccsal. Ez nagyrészben megvédi az adatot attól, hogy a támadó a csatornán elfogja.

A másik oldalon ott van a hitelesítés. Egy IoT eszközön belépési pontok tömkelege található meg, egészen a Wi-Fi modultól a Bluetooth interfészig. Amennyiben a hitelesítési mechanizmus nem megfelelő, a támadó könnyedén hozzáférhet a hálózathoz. A hitelesítés célja az lenne, hogy igazoljuk, hogy az az eszköz, amivel kommunikálunk valóban az-e, ami vagy, ez csak egy hacker által létrehozott egység. Ez a megoldás leggyakrabban jelszóalapján működik, de a fejletteb rendszerekben PKI megoldások is megtalálhatók. Azonban a probléma az, hogy ezek a hitelesítési rendszerek nagyon erőforrásigényesek. [18]

Felmerül a kérdés, hogy ezek után érdemes-e mindent okositani. Az okoseszközök sokkal kényelmesebbek, mint a nem okoseszközök, azonban sokkal kevésbé biztonságosak is. Amennyiben a gyártók szakszerűen megterveznék a rendszer titkosítási és hitelesítési részét is, legalább annyira, mint a termék funkcióit vagy a kinézetét, sokkal biztonságosabb eszközöket kapnánk. Ennek oka abban keresendő, hogy a gyártók szeretnének minél jobban spórolni a

profitszerzés maximalizálása érdekében. Ezek a sebezhetőségi pontok nemcsak a felhasználóra, de az egész infrastruktúrára is veszélyesek lehetnek.

A megoldásnak tehát nem technológiai akadályai vannak, hanem sokkal inkább gazdasági. Nem jelenthető ki az, hogy a fejlesztők nem szeretnének biztonságos eszközöket létrehozni, sokkal inkább az, hogy a nagyvállalatok nem szeretnének elesni a masszív profitoktól.

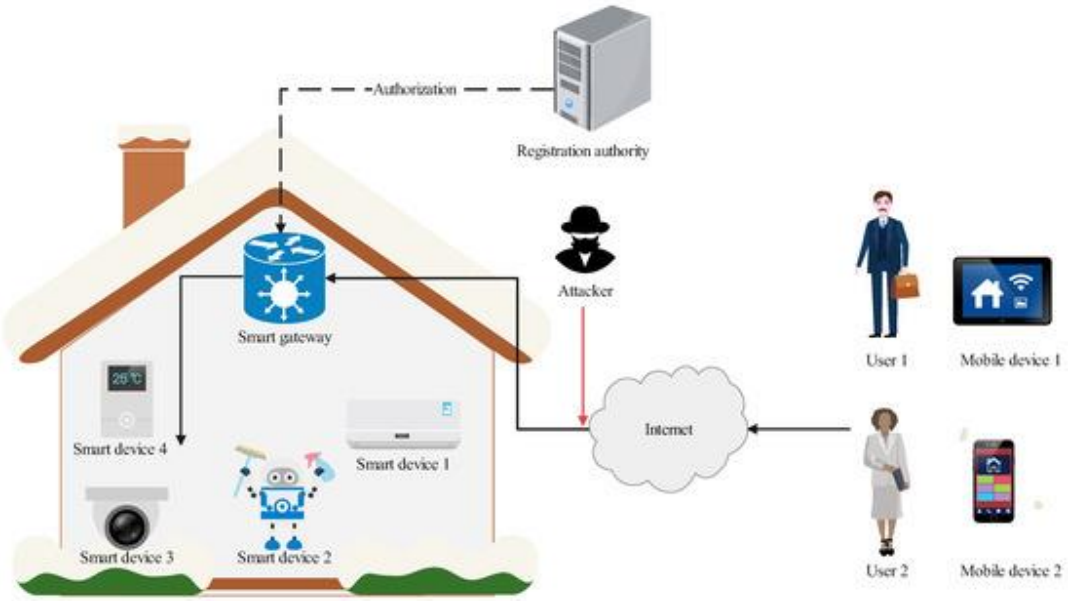
IX. HOZZÁFÉRÉS-VEZÉRLÉS ÉS JOGOSULTSÁGKEZELÉS

Az okoseszközök térhódítása miatt olyan magas szintű hálózati jelenlétet hozott magával, amely korábban elképzelhetetlennek számított. Ezzel azonban az is világossá vált, hogy az IoT világában nem lehet ugyanúgy kezelni a hozzáférést biztosítását, mint egy hagyományos számítógép esetében. A használat módja, a decentralizáltság és a folyamatos kapcsolat szükségessége azt eredményezi, hogy egy új típusú-hozzáférés vezérlési megközelítésre van szükségünk.

A régi, klasszikus jogosultsági modellek, mint a Role-Based Acces Control, sajnos dinamikusan változó környezetben nem működnek olyan jól. Például az okosotthonban lévő okoszáraknak, amelyeket lehet nyitni-zárni távolról is, más más jogosultságot kell adni felhasználótól függően.

A hozzáférés-vezérlés központi eleme, az, hogy az eszközök és a felhasználók csak a számukra engedélyezett funkciókat érhessék el. Ehhez kell a központi entitás, ami hitelesíti és szabályozza az engedélyeket, például az okosotthon központi átjárója.

Az ábrán az intelligens otthonok jogosultságkezelési mechanizmusait látható, ahol az egyes felhasználók és eszközök hozzáférése központi engedélyezésen keresztül történik. A támadó megpróbálhat jogosulatlan hozzáférést szerezni a rendszerhez, kijátszva az engedélyezési folyamatokat. (9. ábra)



9. ábra - Okosotthon jogosultságágkezelési architektúrája - https://www.mdpi.com/2227-7390/11/9/2123

A dinamikus kontextus alapú modellek ígéretesek lehetnek, hiszen ezek már képesek figyelembe venni az olyan változó körülményeket is, mint például az idő, helyszín vagy akár az eszköz viselkedési mintázatai. Azonban sajnos ezek megvalósításában hardveres és erőforrásbeli korlátok vannak. [19]

A jogosultságkezelés különösen ott nehéz, ahol több eszközt kell összehangolni vagy egy rendszerben kell együttműködniük. Ugye az se jó, ha mindenki mindenhez típusú hozzáérést se adunk, de az se jó megoldás amikor túl merev szabályokat hozunk. Ezek megoldására lehet jó megoldás az attribútum alapú modellek, de sajnos a szabálykezelés és az adminisztráció is komoly akadály lehet. Egyre több gyártó törekszik arra, hogy blokklánc alapú vagy decentralizált megközelítésű rendszerben gondolkodjanak. Ez azért jó megoldás, mert saját maguk igazolják az identitásukat és a jogosultságaikat, tehát nincs szükség központi hitelesítő szerverre. Elméletben nagyon jól hangzik, de a gyakorlatban még közel sincs azon a szinten, mint ahogy szeretnénk. [20]

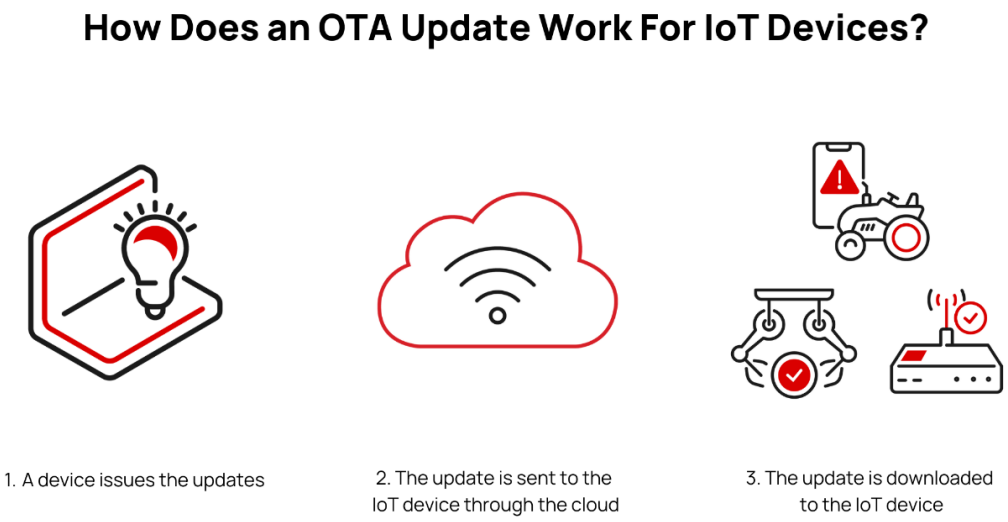
Itt is felmerül sajnos az a probléma, hogy ennek nem feltétlenül technológiai akadálya van. Itt is felmerül a gyártók részéről az, hogy minél előbb kiadják a terméket akár egy primitív hozzáférés-vezérlés nélkül. Pedig egy rosszul implementált vagy egyáltalán nem is létező jogosultságági rendszer nemcsak kényelmetlenséget, hanem adatlopást, távoli vezérlést vagy fizikai behatolás veszélye is felmerülhet.

X. OTA FRISSÍTÉSEK ÉS SZOFTVERBIZTONSÁG

Az okosotthonokban lévő intelligens eszközök folyamatosan fejlődnek, aminek az az előnye, hogy a legújabb frissítések révén új funkciókkal és fejlesztésekkel gazdagodunk. Sajnos ezeknek a rendszereknek a biztonsága nem garantált és különösen az Over-the-Air (OTA) szoftverfrissítések nagyon nagy szerepet játszanak az okosotthonok védelmében. A megfelelő frissítési mechanizmusok megóvják az eszközöket a kibertámadásoktól, azonban egy rossz frissítés akár komoly veszélyt is tud okozni.

Az Over-the-Air később már csak rövidítve OTA frissítések az okosotthonok rendszeres szoftverfrissítéseit jelölik, amelyeket közvetlenül az interneten keresztül a felhasználó közreműködése nélkül telepítenek. Ez azért nagyon hasznos, mert a gyártók távolról tudják frissíteni az eszközöket, hogy új funkciókat és biztonsági javításokat hajtsanak végre. Az OTA frissítések biztonsága alapból meghatározza az IoT eszközök védelmét. A frissítések hitelessége és integritása érdekében kulcsfontosságú a titkosított kommunikáció és a digitális aláírás használata. Az ellenőrzés és a szakszerű frissítési eljárások minimalizálják azt a kockázatot, hogy a támadó manipulálja ezeket a frissítéseket. Ebből jól látható, hogy ezek a frissítések közel se kockázatmentesek. Probléma, hogy a felhasználók nem ellenőrzik a frissítéseket, ezáltal azok automatikusan, felügyelet nélkül tudnak települni. Ez akkor veszélyes, ha a támadó valamilyen kártékony kódot juttat a frissítésbe. További veszélyforrás, ha az eszköz nincs megfelelő módon titkosítva, illetve az autentikációs mechanizmusok nem elég erősek. [21]

A képen az IoT eszközöknek az OTA frissítését mutatja be. Az első lépésben az okoseszköz jelzi, hogy frissítést igényel, majd ez a frissítés a távolról a felhőn keresztül eljut az eszközhöz és frissíti azt. (10. ábra)



10. ábra - IoT eszközök OTA frissítése - https://www.ezurio.com/resources/blog/ota-over-the-air-updates-for-iot-devices

Az okosotthonokban a szoftverbiztonság azért különösen bonyolult, mert eszközök sokszínűsége és az állandó internet kapcsolat rengeteg támadási felületet nyit meg. Az eszközök mind mind futó szoftverekkel rendelkeznek, amelyek sebezhetőséget eredményeznek. A biztonság nem csupán a frissítések biztonságára vonatkozik, hanem a tervezés egészére. A gyenge biztonsági intézkedések lehetővé teszik a támadó számára, hogy hozzáférjenek a felhasználó adataihoz, manipuláljak az eszközöket vagy éppen teljes kontroll szerezzenek felettük. Kiemelendő itt is a felhasználói magatartás, ugyanis nem mindig tartják be a gyártó által javasolt előírásokat, amivel komoly bajba sodorhatja az eszközeiket. [22]

A szoftverbiztonság és az OTA frissítések biztonságának javításának érdekében az egyik fontos lépés a biztonsági frissítések, mechanizmusok implementálása. Ez magába foglalja a frissítések titkosítását és az autentikációs megerősítést. A másik fontos lépés az, hogy a felhasználók megfelelően edukálva legyenek a rendszer frissítésének a kérdésében és hogy hogyan védekezhetnek a potenciális kockázatokkal szemben. Az új technológia fejlesztések, mint a gépi tanulás és a mesterséges intelligencia, sokat segíthetnek a kibertámadások ellen.

XI. JÖVŐBELI TRENDEK ÉS TECHNOLÓGIAI IRÁNYOK

Az okosotthonok jövőjét nagy részben befolyásolni fogja, a mesterséges intelligencia térnyerése és implementálása okosotthon környezetbe. Már a most használatos okosotthonokban is megtalálható mesterséges intelligencia, de a cél, hogy ezt egy minél biztonságosabb és kényelmesebb megvalósításban tudjuk értékelni. A cél az, hogy az AI eltanulja a felhasználó szokásait és ezekre proaktívan tudjon reagálni. Ilyen célokra léteznek olyan hangvezérlésű asszisztensek, mint az Amazon Echo vagy a Google Home, itt a kommunikáció már már megközelíti a természetes társalgást és még érzelmi intelligenciát utánzó interakciókra is képesek.

Az okosotthon környezetben az egyik legnagyobb kihívást jelenti az, hogy nincs az eszközök között kompatibilitás. Erre a Matter lehet a megoldás, ami egy nyílt forráskódú szabványt, amit már több gyártó is támogat, legyen az az Apple,

Amazon vagy Google. Ez azért lenne jó mert egy egységes kommunikációs protokollt biztositana, ami lényegesen leegyszerűsítene az eszközök integrációját és javítaná a felhasználói élményt is.

Az edge computing azt tenné lehetővé, hogy az adatokat helyben, az eszközön lehetne feldolgozni ezzel csökkentve a válaszidőt és az adatátviteli igényt. Ez azért lenne nagyon jó, mert az érzékeny adatoknál csökkentené a kockázatot azzal, hogy nem támaszkodik annyira a központi szerverre, amivel növelhető az adatbiztonság. Ezt az egyik legfontosabb fejlesztésnek tartom, mert nagyon sok kellemetlenségtől óvhatná meg a felhasználókat.

Manapság a cégek számára is egyre fontosabb a környezettudatosság, ugyanis csak egy bolygónk van és arra vigyázni kell. Az okosotthonoknál is megfigyelhető ez a fajta törekvés intelligens termosztátokkal és energiafelhasználást monitorozó eszközökkel, amik segítenek csökkenteni a háztartások energiafogyasztását és az ökológiai lábnyomukat. Szerencsére ebben a törekvésben a felhasználók is szeretik kivenni a részüket és ők is törekednek, hogy környezetbarát életmódot folytassanak.

Az okosotthonok egyre fontosabb szerepet játszanak az egészségügyi megfigyelésekben és az idős, beteg emberek önálló életvitelének támogatásában. Erre olyan eszközök állna rendelkezésre, mint a távoli egészségügyi monitorok, esésérzékelők, illetve különböző figyelmeztető jelzések egy egy tevékenység elvégzésére. Mivel a társadalmunk kezd elöregedni, ez szinten egy nagyon fontos előnye lesz az okosotthonoknak.

Végül de nem utolsósorban az is fontos, hogy az okosotthon ne csak funkcionálisan legyen kiemelkedő, hanem esztétikailag is. Erre jó példa a láthatatlan technológia, ami gyakorlatilag azt jelenti, hogy az eszközök diszkréten vannak integrálva a lakásokba úgy, hogy az gyakran észrevehetetlen. Ilyen technológia lehet a motoros függöny vagy a beépített szenzorok.

XII. ÖSSZEGZÉS

Az okosotthonok elterjedése és technológia fejlődése egy teljesen új korszakot nyitott meg a lakókörnyezetek digitalizálásában. Az okosotthonon belül megtalálhatóak IoT eszközök, beágyazott rendszerek és szenzorok, amik vezérlésével lehetőségünk nyílik sokkal energiahatékonyabban élni, ahol a kényelem és a biztonság a fő szempont.

A CPS rendszerek, amik a fizikai világot kapcsolják össze a kibertechnológia világgal, lehetővé teszik a valós idejű érzékelést, adatfeldolgozást és az automatizált válaszadást is. Ezen rendszerek működéséhez elengedhetetlenek az IoT eszközök, kommunikációs protokollok és a perifériás eszközök is.

A dolgozatom fő fókusza a kiberbiztonsági fenyegetettségekre fókuszált, amiből az 5 leggyakoribbat említettem. A DDoS, PDoS, device hijacking, man-in-the-middle és az adatlopás mind fenyegetik az okosházban lévő felhasználók biztonságát és magánéletét.

Több megoldást is belefoglaltam a dolgozatba ezek megelőzésének az érdekében, ilyenek a tervezési szinten történő védekezés, titkosított kommunikáció és hitelesítés alkalmazása, illetve a felhasználók edukálása. A jövőbeli technológiák résznél bemutatta, hogy milyen irányokban fejlődhet az okosotthon, például a mesterséges intelligencia használatával vagy az edge computing bevezetésével.

Azért választottam a témámnak az okosotthonokat mert egy nagyon aktuális témának tartom, amiben fontos, hogy minél tájékozottabbak legyünk. A jövőben egyre többen fognak okosotthonokban lakni és fontos, hogy a felhasználók minél nagyobb biztonságban legyenek a hackerekkel szemben. Ez természetesen nem csak a felhasználókon múlik, hanem a gyártókon is, akik, ha már a fejlesztés korai szakaszában figyelmet fordítanak a védekezésre, sok kellemetlenségtől óvhatnak meg minket.

Hivatkozások

[1] J. R. Jiang, “An improved cyber-physical systems architecture for Industry 4.0 smart factories,” *Advances in Mechanical Engineering*, vol. 10, no. 6, Jun. 2018, doi: 10.1177/1687814018784192.

[2] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, “Smart Home: Architecture, Technologies and Systems,” *Procedia Comput Sci*, vol. 131, pp. 393–400, Jan. 2018, doi: 10.1016/J.PROCS.2018.04.219.

[3] “IEEE Xplore: IEEE Communications Surveys & Tutorials.” Accessed: May 15, 2025. [Online]. Available: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739

[4] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *Journal of Information Security and Applications*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/J.JISA.2017.11.002.

[5] O. Djumanazarov, A. Väänänen, K. Haataja, and P. Toivanen, “An Overview of IoT-Based Architecture Model for Smart Home Systems,” *Lecture Notes in Networks and Systems*, vol. 418 LNNS, pp. 696–706, 2022, doi: 10.1007/978-3-030-96308-8_65.

[6] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Review of communication technologies for smart homes/building applications,” *Proceedings of the 2015 IEEE Innovative Smart Grid Technologies - Asia, ISGT ASIA 2015*, Jan. 2016, doi: 10.1109/ISGT-ASIA.2015.7437036.

[7] “(PDF) Towards a definition of the Internet of Things (IoT).” Accessed: May 15, 2025. [Online]. Available: https://www.researchgate.net/publication/317588072_Towards_a_definition_of_the_Internet_of_Things_IoT

[8] U. Saxena, J. S. Sodhi, and Y. Singh, “An analysis of DDoS attacks in a smart home network,” *Proceedings of the Confluence 2020 - 10th International Conference on Cloud Computing, Data Science and Engineering*, pp. 272–276, Jan. 2020, doi: 10.1109/CONFLUENCE47617.2020.9058087.

[9] “What Is a Permanent DoS (PDoS) Attack? | Data Foundry.” Accessed: May 15, 2025. [Online]. Available: https://www.datafoundry.com/what-is-a-permanent-dos-pdos-attack/

[10] D. Buil-Gil *et al.*, “The digital harms of smart home devices: A systematic literature review,” *Comput Human Behav*, vol. 145, p. 107770, Aug. 2023, doi: 10.1016/J.CHB.2023.107770.

[11] A. A. Aldridge, “Issues in Information Systems Examining the security essences of Internet of Things (IoT) devices in smart homes: challenges, vulnerabilities, and countermeasures,” vol. 25, no. 1, pp. 279–292, 2024, doi: 10.48009/1_iis_2024_123.

[12] A. M. Ansari and M. Nazir, “Risk Assessment of Security Vulnerabilities in Smart Home Using CAPEC and Defensive Goals,” *Lecture Notes in Networks and Systems*, vol. 318, pp. 705–722, 2022, doi: 10.1007/978-981-16-5689-7_63.

[13] B. M. Salih and O. K. Jasim Mohammad, “Cloud Data Leakage, Security, Privacy Issues and Challenges: Review,” *Procedia Comput Sci*, vol. 242, pp. 592–601, Jan. 2024, doi: 10.1016/J.PROCS.2024.08.113.

[14] G. P. Pinto, P. K. Donta, S. Dustdar, and C. Prazeres, “A Systematic Review on Privacy-Aware IoT Personal Data Stores,” *Sensors 2024, Vol. 24, Page 2197*, vol. 24, no. 7, p. 2197, Mar. 2024, doi: 10.3390/S24072197.

[15] N. Singh, R. Buyya, and H. Kim, “Securing Cloud-Based Internet of Things: Challenges and Mitigations,” *Sensors 2025, Vol. 25, Page 79*, vol. 25, no. 1, p. 79, Dec. 2024, doi: 10.3390/S25010079.

[16] H. Fereidouni, O. Fadeitcheva, and | Mehdi Zalai, “IoT and Man-in-the-Middle Attacks,” *Security and Privacy*, vol. 8, no. 2, p. e70016, Mar. 2025, doi: 10.1002/SPY2.70016.

[17] N. Karmous, Y. Ben Dhiab, M. Ould-Elhassen Aoueileyine, N. Youssef, R. Bouallegue, and A. Yazidi, “Deep learning approaches for protecting IoT devices in smart homes from MitM attacks,” *Front Comput Sci*, vol. 6, p. 1477501, Oct. 2024, doi: 10.3389/FCOMP.2024.1477501/BIBTEX.

[18] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, “Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios,” *Electronics 2023, Vol. 12, Page 1812*, vol. 12, no. 8, p. 1812, Apr. 2023, doi: 10.3390/ELECTRONICS12081812.

[19] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, “Access control in Internet-of-Things: A survey,” *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, Oct. 2019, doi: 10.1016/J.JNCA.2019.06.017.

[20] K. Hameed, A. Raza, S. Garg, and M. B. Amin, “A Blockchain-based Decentralised and Dynamic Authorisation Scheme for the Internet of Things,” Aug. 2022, Accessed: May 15, 2025. [Online]. Available: https://arxiv.org/pdf/2208.07060

[21] S. El Jaouhari and E. Bouvet, “Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions,” *Internet of Things*, vol. 18, p. 100508, May 2022, doi: 10.1016/J.IOT.2022.100508.

[22] M. K. Kuyucu, S. Bahtiyar, and G. Ince, “Security and Privacy in the Smart Home: A Survey of Issues and Mitigation Strategies,” *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, pp. 113–118, Sep. 2019, doi: 10.1109/UBMK.2019.8907037.

2.4. OKOSOTTHON KIÉPÍTÉSÉNEK LEHETŐSÉGEI

IPAR 4.0 TECHNOLÓGIÁK

OKOSOTTHON KIÉPÍTÉSÉNEK LEHETŐSÉGEI

Unti Alexia

[redacted]

(GKNB_INTM087)

2024/2025/2

Tartalomjegyzék

1. Bevezetés ... 3

1.1 Okosotthon történelme, fogalma ... 3

1.2 Az okosotthonok előnyei ... 5

1.3 Hátrányok, veszélyek ... 7

2. Tervezéstől a megvalósításig ... 8

2.1 Szempontok, melyeket már a ház alapjainál figyelembe kell venni ... 8

2.2 Hálózat kiépítése ... 9

2.3 A ZigBee, Z-Wave, Thread bemutatása ... 10

2.4 Az okosotthonok kiépítésének akadályai ... 13

3. Eszközök, szolgáltatások bemutatása ... 15

3.1 Intelligens asszisztensek ... 15

3.2 Apple HomeKit ... 16

3.3 Amazon Alexa ... 18

3.4 Google Home ... 19

3.5 Samsung SmartThings ... 20

3.6 Biztonsági berendezések: zárak, kamerák, riasztók ... 21

3.7 Néhány okos háztartási gép ... 23

3.8 Néhány okosotthoni eszköz költsége ... 26

4. Okosotthonok jövője ... 28

5. Összegzés ... 29

Források, Hivatkozások ... 30

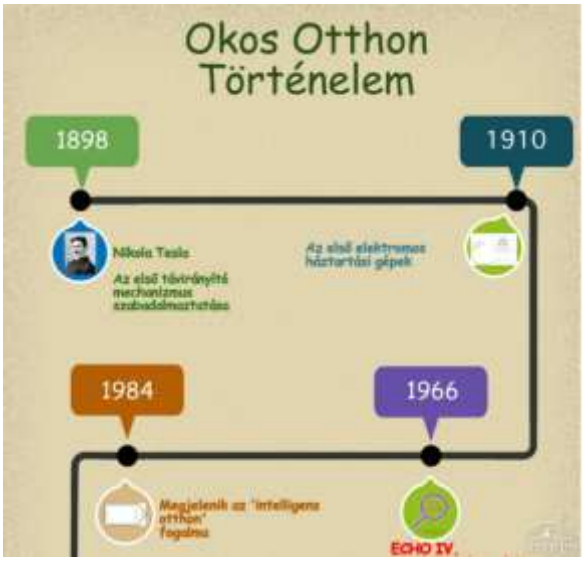
Ábrajegyzék ... 31

1. Bevezetés

1.1 Okosotthon történelme, fogalma

Napjainkban egyre nagyobb népszerűségnek örvendenek azok az eszközök, melyek az „smart”, azaz „okos” jelzővel vannak ellátva. Ezeket a technikai eszközöket és megoldásokat már a háztartásokban is alkalmazni kezdték, amelyek jelentősen megkönnyítik az emberek mindennapi életét, így egyre gyakrabban hallhatjuk az „okos otthon” kifejezést, de valójában mit értünk alattuk?

Az első lényeges történelmi esemény, amit érdemes megemlíteni, egészen 1898-ra vezethető vissza, amikor Nikola Tesla kifejlesztette az első távirányítós szerkezetet. Következő állomás a 20. század elején történt, amikor megjelentek az első háztartási gépek, amik a mindennapi életet nagyban könnyítették. Az okosotthonok fejlesztése és koncepciója folyamatosan jelen volt a technológia fejlődésével és az internet elterjedésével, viszont egyre több lehetőség nyílik az otthoni automatizálásra és a kényelem növelésére. Az első okosotthonokat már az 1970-es években is létrehozták, melyeket ECHO IV-nek neveztek, de az akkori technológiai korlátok miatt még korlátozott volt a számuk. A 2000-es évek elejétől azonban az okos otthonok fejlesztése egyre nagyobb lendületet vett, és ma már sokan használnak különböző okos otthoni



1. ábra Kép az okosotthonok történelméről

eszközöket, valamint a közeljövőben szinte már magától értetődő lesz, hogy egy új építésű ingatlan esetében a tervezésnél már okosotthon-megoldásokban gondolkodjanak a tulajdonosok, kivitelezők.

Az okosotthonokat elsősorban azért fejlesztették ki, hogy javítsák az otthoni életminőséget, és növeljék a kényelmet. Az első okosotthon-rendszerek az energiahatékonyságot és a biztonságot voltak hivatottak növelni. Az 1990-es években jelentek meg az első okosotthonrendszerek, amelyek a lakásokban a biztonságérzetet szerették volna növelni. Ekkor kezdtek alkalmazni mozgásérzékelőket, ajtónyitó szenzorokat, kamerákat és riasztókat, amelyek valamilyen módon jelentést küldtek a tulajdonosoknak vagy a biztonsági szolgálatnak, ha bármi ismeretlen történt a biztonsági berendezés által védett területe.

Az 1990-es években és a 2000-es évek elején az okosotthonok fejlesztése főként a hálózati infrastruktúrára koncentrált. Az okosotthonokban használt eszközök és rendszerek többsége vezetékes kapcsolatot használt, ami korlátozta a rendszerek funkcionalitását és rugalmasságát. A 2000-es évek közepén azonban a vezeték nélküli technológiák, mint például a Wi-Fi és a Bluetooth, széles körben elterjedtek, és ezzel megjelentek a vezeték nélküli okosotthoni eszközök is. [1]

Az okosotthon-technológia fejlődése az elmúlt években folytatódott, és napjainkban már számos eszköz és rendszer áll rendelkezésre, amelyek nemcsak megkönnyítik, hanem kényelmesebbé és élvezetesebbé is teszik az otthoni életet. Az intelligens otthoni megoldások között megtalálhatók például a hangvezérléssel működő okoshangszórók, amelyek segítségével egyszerű utasításokkal irányíthatjuk a háztartási eszközöket és rendszereket. Emellett elérhetők okostelefonról vagy táblagépről vezérelhető világítási rendszerek, valamint olyan intelligens fűtési és légkondicionáló berendezések, amelyek automatikusan a helyiség adottságaihoz igazítják a hőmérsékletet.

2. ábra A mellékelt ábra mutatja, milyen mértékben lesznek az otthonok egyre okosabbak

Az okosotthoni eszközök lehetővé teszik az otthoni élet könnyebbé és hatékonyabbá tételét, és olyan funkciókkal rendelkeznek, mint a távoli vezérlés, az automatikus beállítás és az időzített üzemmód.

Az okosotthoni rendszerek egyre több adatot gyűjtenek az otthonról és annak lakóiról, amelyeket a felhasználók hasznosíthatnak az életminőségük javítása érdekében. Ilyen eszközök például a biztonsági kamerák, mozgásérzékelők, intelligens zárak, intelligens villanykapcsolók és hőmérséklet- és páratartalomérzékelők.

Az okosotthoni eszközök által gyűjtött adatok széles skáláját tartalmazhatják, például információkat az otthonban tartózkodók jelenlétéről, mozgásáról, időbeli beosztásáról, illetve a különböző eszközök használatáról, mint például az okos TV vagy az okos hűtőszekrény. Ezek az adatok az okosotthoni rendszerek által analizálva és összefűzve, különböző információkat szolgáltathatnak az otthonban történt eseményekről.

Az okosotthoni adatgyűjtés jelentősége abban rejlik, hogy az adatok elemzése alapján az okos otthoni rendszerek képesek lehetnek az otthoni készülékek automatikus vezérlésére és az energiahatékonyság növelésére, illetve az okos biztonsági rendszerek figyelmeztetni tudják a tulajdonosokat, ha valamilyen rendellenességet észlelnek az otthonban. A technológia kulcsa, hogy az eszközök által gyűjtött adatokat általában felhőbe küldik, ahol megtörténik a rögzített adatok elemzése. [2]

3. ábra. A lakás különböző pontjáról lehetőségünk van adatot gyűjteni, melyeket telefonunkon tudunk irányítani.

1.2 Az okosotthonok előnyei

Az okosotthonok számos előnnyel járnak, amelyeket érdemes megemlíteni. Az egyik legfontosabb előnyük az, hogy javítják a mindennapi életünket. Az okosotthoni eszközök lehetővé teszik, hogy jobban kontrolláljuk az otthonunkat, kényelmesebbé tegyük az életünket, és időt takarítsunk meg. Ezen rendszerek összekapcsolják a ház különböző elemeit, így lehetővé teszik az egyszerűbb és hatékonyabb működtetést.

Továbbá, jelentős előnyként kiemelhető az is, hogy javítják a biztonságot. Az okosotthoni rendszerek beépített biztonsági funkciókkal rendelkeznek, mint például az okos zárak,

riasztórendszerek, kamerák és mozgásérzékelők. Ezen eszközök lehetővé teszik, hogy távolról is felügyeljük otthonunkat, és értesítést kapjunk, ha bármilyen gyanús tevékenységet észlelnek. Ez a funkció különösen fontos lehet, ha hosszabb időre elutazunk, vagy ha olyan helyen élünk, ahol magasabb a bűnözési arány.

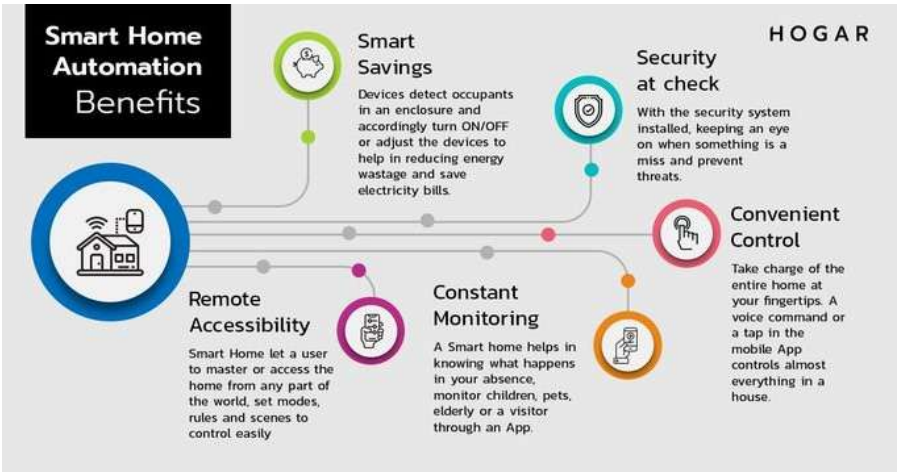
Az okosotthonok előnye még, hogy csökkenthetik az energiafogyasztást és a költségeket. Az okosotthoni rendszerek képesek optimalizálni a ház energiafogyasztását, így csökkenthetik az áram- és gázszámlákat. Az okos fűtési és hűtési rendszerek a helyiségek használatát és az időjárási körülményeket figyelembe véve szabályozzák a hőmérsékletet, így hatékonyabban használják az energiát. Az okos világítás és az elektromos készülékek automatikus kikapcsolása is hozzájárul az energiafogyasztás csökkentéséhez.

Az sem elhanyagolható tény, hogy hatással vannak a környezetvédelemre is. Az energiahatékony eszközök használatával és az energiafogyasztás optimalizálásával az okosotthonok képesek csökkenteni a szén-dioxid kibocsátást, ami hozzájárul a környezetvédelemhez. Az okosotthonokban az eszközök távolról is vezérelhetőek, így lehetőség van arra is, hogy az energiafogyasztás időbeli elosztásával optimalizáljuk a környezeti hatásokat.

Érdemes még megemlíteni, hogy remek kényelmi funkciókat, valamint szórakozási lehetőségeket biztosítanak. Az okos világítás, a hang- és videórendszer könnyen vezérelhetőek okostelefonokról vagy hangutasításokkal, és programozhatók, hogy automatikusan be- és kikapcsoljanak, amikor szükséges.

Az okos otthonok nem csak lakáson belül tudják a lakók kényelmét szolgálni, hanem még a kertben is. Az intelligens öntözőrendszerek például az időjárási adatok és a talaj nedvességtartalma alapján automatikusan szabályozzák a locsolást, így energiát és vizet takarítanak meg, miközben a kert mindig ápolt marad. Emellett léteznek távolról vezérelhető kültéri világítási rendszerek, okos kapunyitók, biztonsági kamerák, robotfűnyírók is, illetve akik rendelkeznek kert medencével náluk tökéletes lehetőség egy medencevezérlő rendszer, mellyel lehet állítani a vízhőmérsékletet, vegyszeradagolást, vagy a szűrőberendezés működését.

Végül, az okos otthonok hosszú távon pénzt takaríthatnak meg. Bár az okosotthoni készülékek és eszközök ára magasabb lehet, a megtakarítások, amelyeket az energiafogyasztás csökkentése és a hosszabb élettartam nyújthat, valamint az általuk megspórolt idő hosszú távon megtérülhetnek. [3]



4. ábra Az okosotthonok előnyeit bemutató ábra

1.3 Hátrányok, veszélyek

Az okosotthonok használatával kapcsolatosan az előnyök mellett biztonsági kockázatok és hátrányok is léteznek, amelyeket érdemes figyelembe venni, amikor ilyen infrastruktúrát szeretnénk kiépíteni.

Az egyik ilyen veszély az adatvédelem. Az okoseszközök – például a kamerák vagy mikrofonokkal ellátott hangszórók – folyamatosan adatokat gyűjtenek és továbbítanak, amelyek gyakran érzékeny, személyes információkat tartalmaznak., amelyek magánéleti kérdéseket érintenek. Az adatvédelem hiánya esetén az érzékeny adatokhoz való hozzáférés illetéktelen személyek kezébe kerülhet, ami a felhasználók magánéleti jogainak súlyos megsértéséhez vezethet.

További veszélyforrást jelent a kibertámadások lehetősége. Az okosotthonok eszközei gyakran kapcsolódnak az internethez, ami azt jelenti, hogy távolról is vezérelhetők. Ha a biztonsági protokollok nem megfelelőek vagy könnyen feltörhetők, akkor a támadók hozzáférhetnek az otthon eszközeihez és képesek lehetnek azokat manipulálni vagy ellenőrzésük alá vonni.

Egy 2021-es statisztika szerint, hetente több, mint 12000 hacker támadás érte az ilyen eszközökkel ellátott otthonokat, azonban ez az adat azóta folyamatosan növekedik.

Az okosotthonok másik jelentős hátránya az ár. Az eszközök és rendszerek ára általában magasabb, mint a hagyományos otthoni készülékeké vagy rendszereké. Ez azt jelenti, hogy az okosotthonok kiépítése és karbantartása magasabb költséggel járhat, ami nem mindenki számára elérhető.

Továbbá az okosotthonok használatához szükséges digitális készségek hiánya is nehézséget okozhat bizonyos felhasználói csoportok számára. Az idősebb generációk, illetve azok, akik kevésbé jártasak a modern technológiai megoldásokban, kihívásként élhetik meg az eszközök kezelését és karbantartását. Különösen igaz ez olyan személyek esetében, akik valamilyen speciális betegséggel élnek, számukra a felhasználóbarát kialakítás és a megfelelő oktatás kiemelten fontos.

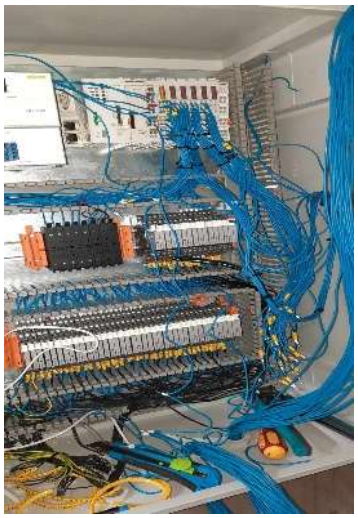
Összefoglalva, az okosotthonok használata számos előnnyel járhat, de figyelembe kell venni a biztonsági kockázatokat, az árakat és a készségek hiányát is. Az okosotthonok terjedése azonban továbbra is növekszik, és a jövőben várhatóan még több innovációval és fejlesztéssel fognak rendelkezni. [4]

2. Tervezéstől a megvalósításig

2.1 Szempontok, melyeket már a ház alapjainál figyelembe kell venni

Ha valaki az építkezés során szeretné az otthonát okosotthonná fejleszteni, akkor több szempontot is figyelembe kell vennie. Az alábbiakban megemlítek néhány fontos szempontot:

- Kábelezés: Az okosotthonokban nagyon fontos a megfelelő kábelezés. Az okos eszközök nagy része ugyanis nem csak a Wi-Fi hálózaton keresztül kommunikál, hanem kábelre is szükség lehet. Ezért fontos, hogy az építkezés során megfelelően kábelezzük az otthonunkat.
- Hálózat: Az okosotthonokban az eszközök sokszor nagy mennyiségű adatot küldenek és fogadnak, ezért fontos, hogy a hálózatunk megfelelő sebességgel és kapacitással rendelkezzen. Érdemes tehát megfelelő Wi-Fi routert és szélessávú internetkapcsolatot választani.
- Okos eszközök: Az okosotthonokban az eszközöknek kommunikálniuk kell egymással, ezért fontos, hogy kompatibilisek legyenek egymással. Az építkezés során érdemes olyan okos eszközöket választani, amelyek között könnyen lehet integrálni az újabb eszközöket is.
- Központi vezérlés: A központi vezérlés nagyon fontos, mivel ezáltal lehet az összes eszközt egy helyen kezelni. Ezért érdemes a tervezési fázisban már kialakítani egy központi vezérlőpultot, ahol az összes okos eszközt lehet kezelni.



5. ábra Kábelezés a szekrényen belül: saját kép, kert teljes okos öntözőrendszer vezérlése

- Biztonság: Fontos, hogy az okos eszközök ne legyenek kiszolgáltatva a hackereknek, ezért érdemes olyan eszközöket választani, amelyek biztonságosak és folyamatosan frissítik a szoftverüket.
- Energiahatékonyság: Az okosotthonokban az energiatakarékosság és az energiahatékonyság kiemelten fontos. Az építkezés során érdemes figyelni a megfelelő szigetelésre, az energiatakarékos ablakokra, a LED-es világításra és az okos energiatakarékos eszközök használatára. [5]

2.2 Hálózat kiépítése

Az okosotthonok esetében az internetes kapcsolat elengedhetetlen a különböző funkciók működtetéséhez. Az otthoni hálózat általában vezetékes és vezeték nélküli (Wi-Fi) eszközökből áll, amelyek összekapcsolják a különböző okos eszközöket és a felhasználókat.

6. ábra Egy okosotthon eszközeinek lehetséges összeköttetései

A Wi-Fi hálózat a leggyakrabban használt kapcsolati forma, mivel egyszerű és kényelmes. A Wi-Fi router a hálózat központi eszköze, amely általában a lakás középső részén helyezkedik el, hogy az összes okos eszköz elérje a jelet. A Wi-Fi hálózat azonban korlátozott hatótávolsággal rendelkezik, és gyakran szenved a jel interferenciájától.

Az Ethernet kábelek is használhatók az okosotthonokban, hogy a hálózat stabilabb és biztonságosabb legyen. Az Ethernet kábelek közvetlenül csatlakoztatják az okos eszközöket a routerhez, és általában magasabb sebességet és megbízhatóságot kínálnak, mint a Wi-Fi.

A Bluetooth is népszerű kapcsolati forma. Ez a vezeték nélküli technológia rövid hatótávolsággal rendelkezik, és általában a kisebb eszközök, például okos zárak vagy okos hangszórók csatlakoztatására használják.

A Z-Wave, a Thread és a Zigbee olyan vezeték nélküli kommunikációs protokollok, amelyeket kifejezetten okosotthon-rendszerekhez fejlesztettek ki. Ezek a technológiák lehetővé teszik az eszközök közötti hatékony adatcserét, miközben lényegesen alacsonyabb energiafogyasztással működnek, mint például a Wi-Fi vagy a Bluetooth. Ennek köszönhetően az ilyen protokollokat

használó eszközök – például érzékelők, kapcsolók vagy termosztátok – hosszabb üzemidőt biztosítanak elemes működés mellett. Ráadásul a mind a három technológia Mesh-hálózat kialakítású. A mesh hálózat egy olyan hálózati struktúra, ahol az eszközök nemcsak a központi egységgel, hanem egymással is képesek kommunikálni. Ez azt jelenti, hogy az adatokat több útvonalon is továbbíthatják, így stabilabb, megbízhatóbb lefedettséget biztosít, különösen nagyobb otthonokban vagy olyan helyeken, ahol a hagyományos jel könnyen megszakad. [6]

Összességében, az okos otthonok számos hálózati kapcsolati formát használhatnak. Minden kapcsolati forma előnyökkel és korlátokkal rendelkezik, és a megfelelő kiválasztása az otthon méretétől, a hálózat stabilitásától és egyéb változó tényezőktől függ.

2.3 A ZigBee, Z-Wave, Thread bemutatása

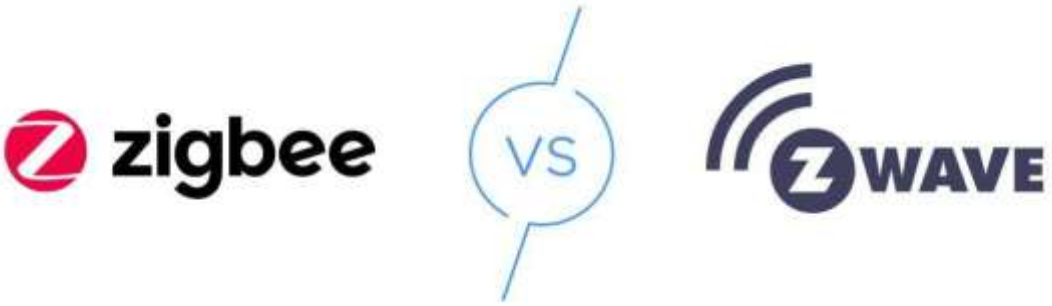
A ZigBee egy vezeték nélküli hálózati protokoll, amelyet kifejezetten a szenzorok és az eszközök kis adatátviteli igényeihez terveztek. A protokoll gyakran alkalmazott a szenzorok, kapcsolók, mozgásérzékelők, intelligens világítási rendszerek, fűtési rendszerek, zárak és egyéb eszközök vezérlésére és kapcsolatban tartására az okosotthonokban.

A ZigBee alacsony energiafogyasztású és egyszerűen kezelhető, ami lehetővé teszi a hosszú élettartamú, autonóm eszközök használatát az okosotthonokban. Az eszközök könnyen telepíthetők és beüzemelhetők, és az egész rendszer jól skálázható a nagyobb otthonokhoz vagy épületekhez is.

Egy mesh hálózatot alkot, amelyben minden eszköz kapcsolatban áll az adó-vevő egységek között, így a kommunikáció mindig megtörténik, még akkor is, ha egy eszköz meghibásodik vagy eltűnik a hálózatból. Emiatt a ZigBee hálózatok meglehetősen megbízhatóak és biztonságosak.

Az okosotthonokban a ZigBee rendszer általában egy központi hubból vagy vezérlőegységből vezérli az összes eszközt. A hub egyfelől lehetővé teszi az eszközök közötti kommunikációt, másrészt pedig lehetővé teszi a felhasználó számára az eszközök távoli vezérlését, valamint a rendszer állapotának ellenőrzését a telefonjáról vagy a számítógépéről.

Összességében a ZigBee egy nagyon hatékony és megbízható hálózati protokoll az okosotthonokban, amely lehetővé teszi az eszközök egyszerű és hatékony kezelését, és hosszú élettartamú, autonóm működést biztosít az eszközök számára.



7. ábra Kép a Zigbee és a Z-Wave összehasonlításáról

A Z-Wave egy vezeték nélküli kommunikációs protokoll, amelyet elsősorban az okosotthon eszközök kommunikációjára használnak. Az első Z-Wave termékek 2004-ben jelentek meg, azóta pedig a protokoll egyre népszerűbbé vált az okosotthon piacán.

A Z-Wave protokoll működése hasonló a ZigBee-hez. A Z-Wave hálózat is felépül egy központi eszközből (pl. egy okosotthon vezérlőközpont), amely kommunikál a hálózat többi eszközével. Az eszközök a hálózaton keresztül kommunikálnak egymással, és így lehetővé teszik az okosotthonok számára, hogy az eszközök egymással és a felhasználóval kommunikáljanak.

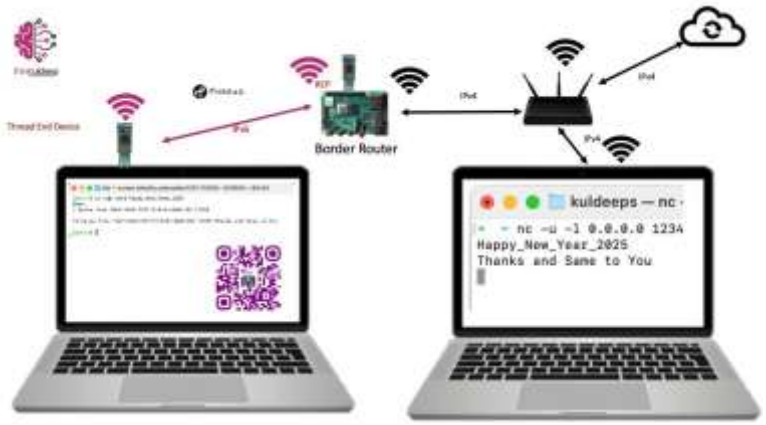
A Z-Wave azonban biztonságosabb protokoll, mint a ZigBee. Az eszközöknek minden kommunikációjuk során egyedi titkosítási kulcsot kell használniuk, amely csak a hálózat tagjainak ismert. Ez a kulcs biztosítja, hogy csak az engedélyezett eszközök kommunikálhassanak a hálózaton keresztül, és védelmet nyújt a külső támadásokkal szemben.

A Z-Wave protokoll további előnye, hogy a kommunikációja nagyon stabil és megbízható, és az eszközök jelentős távolságra is képesek kommunikálni egymással. Emellett a Z-Wave hálózat kialakítása is rendkívül egyszerű, és a telepítése sem igényel nagyobb szaktudást.

Összességében elmondható, hogy a Z-Wave protokoll egy biztonságos és megbízható vezeték nélküli kommunikációs megoldás az okos otthonok számára. Az eszközök közötti kommunikáció stabilitása és a könnyű telepítés lehetővé teszi az egyszerűbb és hatékonyabb okosotthoni élményt a felhasználók számára.

A Thread egy modern, IPv6-alapú vezeték nélküli protokoll, amelyet az okosotthon-eszközök közötti gyors, biztonságos és megbízható kommunikációra fejlesztettek ki. Eredetileg a Google (Nest), Apple, Amazon és más technológiai nagyvállalatok által létrehozott Thread Group dolgozta ki, hogy megoldják a korábbi protokollok, például a Wi-Fi, Bluetooth vagy Zigbee – korlátait.

A Thread egyik legfontosabb jellemzője, hogy mesh hálózatot hoz létre: minden eszköz nemcsak kommunikál, hanem adatokat is továbbít más eszközök között, így a hálózat lefedettsége és stabilitása nagymértékben nő. Emellett, mivel nincs szükség központi hubra, a



8. ábra Kép a Thread protokollról

rendszer rugalmasan bővíthető, és nem dől össze egyetlen eszköz meghibásodása esetén.

A Thread kifejezetten alacsony energiafogyasztásra lett optimalizálva, így ideális akkumulátorral működő érzékelőkhöz, kapcsolókhoz, redőnyvezérlőkhöz és más kis teljesítményű eszközökhöz. Ráadásul, mivel IPv6 protokollt használ, minden eszköz egyedi IP-címmel rendelkezik, ami megkönnyíti az internetes integrációt és a skálázhatóságot.

A Thread különösen jelentős szerepet kapott a Matter szabványban, amelynek egyik alaptechnológiája. Emiatt a Thread várhatóan a jövő egyik legelterjedtebb kommunikációs protokollja lesz az okosotthonokban.

A Zigbee előnye a széles gyártói támogatás és a magas eszközszám egy hálózatban, azonban mivel a Wi-Fi-vel azonos frekvencián működik, előfordulhat interferencia. A Z-Wave kevesebb eszközt támogat, viszont stabilabb jelet biztosít, mivel eltérő, kevésbé zsúfolt frekvenciát használ – ez különösen előnyös lehet nagyobb otthonokban. A Thread a legújabb technológia, amely IP-alapú, energiatakarékos és jövőbiztos megoldást kínál, különösen a Matter szabvány révén, amely hosszú távon a gyártók közötti együttműködés alapja lesz. Míg a Zigbee és Z-Wave jól bevált rendszerek, a Thread a legalkalmasabb választás lehet azok számára, akik egy nyitott, modern és rugalmas okosotthon-infrastruktúrát szeretnének kiépíteni. [7] [8]

Jellemző:	Zigbee	Z-Wave	Thread
Hálózat típus:	Mesh	Mesh	Mesh
Nyílt/Zárt:	Nyílt szabvány	Zárt szabvány (de ipari szabvány	Nyílt szabvány
Hatótávolság:	~10-20 m / eszköz	~30-100 m / eszköz	~10-20 m / eszköz
Támogatott eszközök száma:	~65 000 / hálózat	~232 / hálózat	~250+ (gyártótól függően)
Interferencia érzékenység:	Közepes (2.4 GHz, mint Wi-Fi)	Alacsony (külön frekvencia)	Közepes (2.4 GHz)
Energiafogyasztás:	Alacsony	Alacsony	Nagyon alacsony
IPv6 támogatás:	Nem	Nem	Igen
Matter kompatibilitás:	Korlátozott vagy nem	Nem jellemző	Igen (alaprétegként)
Fő előny:	Széles gyártói támogatás	Jó hatótáv, stabil működés	Jövőbiztos, internetképes, Matter-alapú
Fő hátrány:	Interferencia a Wi-Fi-vel	Kevesebb eszköz, zárt rendszer	Még kevés eszköz támogatja

9. ábra Összehasonlító táblázat a Zigbee-ről, Z-Wave-ről és a Threadről

2.4 Az okosotthonok kiépítésének akadályai

Napjainkban az otthonaink korszerűsítése egyre népszerűbbé válik, ugyanakkor számos akadályba beleütközhetnek azok, akik szeretnének okosotthont kialakítani. Az alábbiakban bemutatnék néhányat azok közül a fő akadályok közül, amelyekkel az emberek találkozhatnak egy okosotthon kiépítése során:

Központi irányítás hiánya: Az okosotthonok esetében az eszközök és rendszerek több platformon keresztül kommunikálnak egymással, ami azt jelenti, hogy az egyik rendszeren keresztül nem minden eszközt lehet irányítani. Az egyik probléma az lehet, hogy a felhasználóknak nehéz lehet az eszközök közötti összehangolás és kommunikáció megszervezése.

Ár: A rendszerek kiépítései nagy költségekkel járhatnak, különösen, ha az ember magas minőségi és funkcionális eszközöket szeretne használni.

Biztonsági aggályok: Az okosotthoni rendszerek használata során az adatokat és a biztonságot illetően sok aggály merülhet fel, különösen a magas szintű integráció és az adatok tárolása miatt.

Kompatibilitási problémák: A szükséges eszközök és rendszerek nem mindig kompatibilisek egymással, ami megnehezítheti azok dolgát, akik szeretnék az otthonukat okossá tenni. Az egyes eszközök gyártói eltérő protokollokat és kommunikációs szabványokat alkalmazhatnak, ami kompatibilitási problémákhoz vezethet.

Technikai ismeretek hiánya: Az okosotthonok kialakítása során számos technikai készség és ismeret szükséges. Azok számára, akiknek nincsenek ezek a készségeik és ismereteik, az okosotthonok kiépítése bonyolultnak tűnhet, vagy komoly nehézségekbe ütközhetnek a rendszer működtetése során.

Alkalmazkodás: Az embereknek alkalmazkodniuk kell az okosotthon rendszerekhez, ami időt és energiát igényelhet. Meg kell tanulniuk az eszközök használatát és azokat szinkronizálniuk kell a mindennapi rutinjukkal, ami némi időt és figyelmet igényelhet, különösen az idősebb generációk vagy a technológiában kevésbé jártas felhasználók számára.

Internet-kapcsolat: Ezen rendszerek széles körű internetkapcsolatot igényelnek a megfelelő működéshez. Az internetkapcsolatnak stabilnak és megbízhatónak kell lennie, hogy az eszközök rendeltetésszerűen működjenek, ezért azoknak, akiknek gyenge vagy instabil internetkapcsolatuk van, ez is lehet akadály az okosotthonok kiépítése során.

Karbantartás és frissítések: Az eszközök rendszeres karbantartást és frissítést igényelnek. Ezek elmulasztása azonban megnövelheti az eszközök hibájának vagy meghibásodásának kockázatát. [9]

3. Eszközök, szolgáltatások bemutatása

3.1 Intelligens asszisztensek

Az intelligens asszisztensek olyan alkalmazások, amelyek segítségével felhasználóik kommunikálhatnak a számítógépekkel, okostelefonokkal vagy akár az okosotthonokkal. Ezek az alkalmazások képesek értelmezni az emberi beszédet vagy írást, és megfelelő választ vagy cselekvést ajánlani a felhasználónak.

Az intelligens asszisztensek népszerűsége az utóbbi években meredeken növekedett, köszönhetően a fejlett technológiáknak, mint például a gépi tanulásnak és a természetes nyelvfeldolgozásnak. Ezek az alkalmazások sokféle területen hasznosak lehetnek, beleértve az okostelefonokat, az otthoni automatizálást és a személyi asszisztenseket.

Az otthoni automatizálásban az intelligens asszisztensek képesek összekapcsolni az okosotthon eszközöket, mint például az okos világítás, okos fűtés, okos zárak, okos biztonsági rendszerek és más okos eszközök. Az asszisztensek lehetővé teszik a felhasználóknak, hogy hangutasításokat adjanak az otthoni eszközöknek, például, hogy kapcsolják be vagy ki a világítást, állítsák be a hőmérsékletet, nyissanak vagy zárjanak ajtókat, indítsanak zenét, esetleg filmet, ellenőrizzék az otthoni biztonsági rendszert, vagy éppen segítsenek a főzésben. [10]

Az okosotthon asszisztensek közül a legnépszerűbbek a következők:

- Amazon Alexa
- Google Home
- Apple HomeKit
- Samsung Bixby

10. ábra Kép az okos otthon asszisztensekről

Az alábbi fejezetekben szeretném részletesen bemutatni néhány szolgáltató által kínált megoldást, az előnyöket, illetve hátrányokat, továbbá, hogy milyen jelentős különbségek, eltérések vannak közöttük.

3.2 Apple HomeKit

Az Apple HomeKit először az iOS 8 rendszerrel 2014-ben került bemutatásra. Ez volt az első alkalom, amikor az Apple hivatalosan is bemutatta az okosotthoni rendszerek integrációját az iOS rendszerbe. Azóta az Apple HomeKit integrációja számos okos otthoni eszközön elérhetővé vált, és az Apple folyamatosan fejleszti a platformot a még jobb és egyszerűbb használat érdekében.

Az Apple HomeKit egy olyan okosotthon platform, amely lehetővé teszi az Apple eszközök tulajdonosai számára, hogy irányítsák és automatizálják otthonukat. Az HomeKit integrálva van az Apple operációs rendszereibe, mint az iOS, az iPadOS és a watchOS, így a felhasználók akár az okostelefonjukon, akár az Apple Watch-on keresztül is vezérelhetik az otthonukat.

A HomeKit-eszközök az otthoni Wi-Fi hálózaton keresztül kommunikálnak az Apple eszközökkel, és a platform egy egységes felhasználói felületen keresztül kezeli az összes csatlakoztatott eszközt. A HomeKit segítségével az okosotthon tulajdonosok számos dolgot tehetnek, például be- és kikapcsolhatják a világítást, állíthatják a hőmérsékletet, nyitják és zárják az ajtókat és az ablakokat, ellenőrizhetik a biztonsági rendszert és még sok mást.

Az Apple HomeKit használata során az egyik nagy előny az Apple-tól megszokott szigorú biztonsági szabványok. Az HomeKit-eszközöket kriptográfiával védik, és csak azok a felhasználók, akik engedélyt kapnak, tudnak hozzáférni az eszközökhöz.

Az Apple HomeKit-hez számos eszköz érhető el, például világítás- és fűtésszabályozók, biztonsági kamerák, zárak és kapuk, mozgásérzékelők, víz- és tűzérzékelők és még sok más. A HomeKit-eszközöket az Apple alkalmazásokon keresztül lehet konfigurálni és vezérelni, vagy akár hangutasításokkal Siri segítségével is irányíthatjuk őket. – Ezeket a funkciókat az „Otthon” alkalmazásban lehet például kezelni.

Az Apple új stratégiája három fő pillérre épül: az Apple Intelligence mesterséges intelligencia platformra, a homeOS operációs rendszerre és a Matter szabvány szélesebb körű támogatására. Az Apple Intelligence célja, hogy a Siri intelligensebbé váljon, képes legyen komplex parancsok végrehajtására és alkalmazások közötti műveletek kezelésére. A homeOS egy új operációs

rendszer, amely egyesíti az Apple különböző hardvereszközeit, és egységes platformot biztosít az okosotthon eszközök számára.

Az egyik legnagyobb előnye a kiemelkedő adatvédelem és biztonság, amely az Apple rendszerek sajátossága. A HomeKit-eszközök kommunikációja titkosított, és csak a jogosult felhasználók férhetnek hozzá az otthon eszközeihez, így az adatok védelme kiemelten biztosított.

Az Apple az elmúlt időszakban számos újítást jelentett be, amelyek közül néhány már most is elérhető. Ilyenek például a: robotporszívók támogatása, érintésmentes ajtónyitás és vendég hozzáférések kezelése, megjelent az energiafogyasztások követhetősége. A közeljövőben (2025 második felében) elérhetőek lesznek a saját Apple kamerák. [11]

Összegezve, az Apple HomeKit lehetővé teszi az okosotthon tulajdonosok számára, hogy egyszerűen és biztonságosan irányítsák és automatizálják otthonukat az Apple eszközeik segítségével.

11. ábra Az ábrán az Apple HomeKit látható

3.3 Amazon Alexa

Az Amazon Alexa az Egyesült Államokban 2014-ben jelent meg, kezdetben az Amazon Echo nevű okos hangszórón keresztül. Azóta az Alexa funkciók elérhetőek az Echo készülékeken kívül számos más okos otthon eszközön is, és számos országban elérhetővé váltak. Az Alexa használata kiterjedt az otthoni automatizálás mellett a zenelejátszási, információ- és vásárlási funkciókra is.

Az Alexa alapvetően egy hangfelismerő és értelmező szoftver, amely képes az emberi beszéd megértésére és a kívánt tevékenységek elvégzésére. Fontos továbbá, hogy az Alexa képes több hangprofil kezelésére is, vagyis felismeri a háztartás különböző tagjainak hangját, így személyre szabott válaszokat adhat, például külön naptári bejegyzéseket, üzeneteket vagy zenelejátszási preferenciákat kezel. Ez különösen hasznos többfelhasználós háztartásokban, ahol mindenki mást vár el a digitális asszisztenstől.

Az Alexa által támogatott okosotthon eszközök közé tartoznak okos lámpák, okos zárak, okos kamerák, okos termosztátok, okos konnektorok és sok más eszköz. Az Alexa segítségével ezeket az eszközöket hangvezérléssel lehet irányítani.

Az Alexa használatához szükséges egy Alexa-kompatibilis eszköz, például az Amazon Echo vagy a Dot. Ezek az eszközök mikrofonokat tartalmaznak, amelyek lehetővé teszik a felhasználók számára, hogy hangparancsokat adjanak az Alexának. Az Echo és a Dot kétirányú hangkommunikációra is képes, ami azt jelenti, hogy az Alexa visszajelezhet a felhasználónak.

Az Alexa alkalmazásban a felhasználók beállíthatják az okos otthon eszközeiket, vezérelhetik azokat, ellenőrizhetik azok állapotát és létrehozhatnak automatizálási szabályokat is. Az Alexa az okosotthon eszközök mellett képes az időjárás-előrejelzések, a hírek, a sporteredmények és még sok más információ megjelenítésére is.

Az Alexa felhasználók számára további előny, hogy az Amazon folyamatosan bővíti az Alexa funkcionalitását és integrálja az eszközöket egyre több szolgáltatással, így az Alexa használata egyre rugalmasabbá és sokoldalúbbá válik. [12]

12. ábra Az ábrán Amazon Alexa látható

3.4 Google Home

A Google Home egy olyan intelligens asszisztens, amelyet a Google fejlesztett ki az otthoni automatizálás és az okosotthonok kezelése érdekében.

A Google Home első generációja 2016-ban jelent meg az Egyesült Államokban. Azóta a termékcsalád többi tagja, például a Google Home Mini, a Google Home Max és a Google Nest Hub is megjelent. Azóta számos új funkcióval és lehetőséggel bővült a Google Home, amely azóta Google Nest Home néven is ismert.

A Google Home eszközök vezérlése egyszerű és intuitív. A felhasználók csak a "Hey Google" vagy "OK Google" parancsot kell mondaniuk, majd megadniuk a kívánt utasítást. Például a felhasználók bekapcsolhatják vagy kikapcsolhatják a világítást, szabályozhatják a hőmérsékletet, vagy értesítéseket kérhetnek az okos otthoni eszközök állapotáról.

A Google Home eszközök rendelkeznek egy sor érzékelővel, beleértve a hangfelismerő és a hangfeldolgozó rendszert is. Ez lehetővé teszi, hogy a Google Home eszközök pontosan felismerjék a felhasználók hangját, még zajos környezetben is. A hangfelismerő rendszer felismeri a beszéd intonációját, a szótöveket és a nyelvtani szabályokat, hogy pontosan értelmezze a felhasználó utasításait. A Google Home hasonlóan az Alexa-hoz képes több hangprofilt kezelni, így különbséget tud tenni a háztartás tagjai között. Ez azt jelenti, hogy külön naptárakat, emlékeztetőket, Spotify-fiókokat stb. tud kezelni felhasználónként.

A Google Home eszközök az otthoni automatizálás és az okos otthonok kezelése mellett a különböző okos készülékek integrálására is képesek. A Google Home támogatja a Google Assistantet, amely számos készüléket támogat, például okostelefonokat, táblagépeket, okosórákat, okosautókat és még sok mást. A Google Home/Nest eszközök nagy előnye, hogy

szorosan integráltak a Google szolgáltatásaival: Gmail, Google Calendar, YouTube, Google Maps stb. Ez lehetővé teszi, hogy a felhasználók például naptárbejegyzéseket kérjenek le, útvonalat terveztessenek vagy videót játsszanak le YouTube-ról.

A Google Home eszközök könnyen csatlakoztathatóak más okosotthon eszközökhöz, mint például az okos zárak, okos világítás, okos hangszórók és még sok más. A Google Home lehetővé teszi a felhasználók számára, hogy integrálják az okosotthon eszközöket az egységes vezérlőpulthoz, ami egyszerűsíti az otthonuk vezérlését.

A Google Home lehetőséget ad arra, hogy a hangfelvételeket törölni lehessen, valamint azt is be lehet állítani, hogy a mikrofon ne figyeljen (fizikai gombbal vagy hangparanccsal). Ez fontos lehet adatvédelmi szempontból. [12]

13. ábra Az Ábrán a google home látható

3.5 Samsung SmartThings

A SmartThings platformot eredetileg 2012-ben alapította az amerikai SmartThings, Inc., majd 2014-ben a Samsung felvásárolta, és azóta is folyamatosan fejleszti. A rendszer célja, hogy egyetlen, egységes felületen keresztül lehetővé tegye a felhasználók számára otthonuk automatizálását és vezérlését. A SmartThings Hub központi egységként szolgál, amely Wi-Fi, Ethernet és Bluetooth kapcsolaton keresztül kommunikál a különböző okoseszközökkel.

Az alkalmazás a felhasználók számára lehetővé teszi, hogy beállítsák a különböző automatizálási szabályokat és feltételeket, amelyek lehetővé teszik az okosotthon eszközök automatikus működését. Például, ha a felhasználó hazaérkezik, az alkalmazás észleli a felhasználó telefonjának helyét, és bekapcsolja a lámpákat vagy a klímát.

A SmartThings-nek számos integrált szolgáltatása van, amelyek lehetővé teszik a felhasználók számára, hogy egyszerűen integrálják más okosotthon platformokkal, például a Google Asszisztenssel és az Amazon Alexával. Ez azt jelenti, hogy a felhasználók a SmartThings alkalmazásból vezérelhetik azokat a készülékeket, amelyek más platformokkal integrálódtak.

A SmartThings vezérlő központját és eszközeit könnyű beállítani és használni, és a platform széles körű kompatibilitással rendelkezik, így a felhasználók számos eszközzel használhatják a rendszert.

2025-ben a Samsung jelentős újításokat vezetett be a SmartThings platformon, amelyek középpontjában a mesterséges intelligencia (AI) áll. Az új "Home AI" funkció lehetővé teszi, hogy az otthonunk tanuljon a mindennapi szokásainkból, és ennek megfelelően automatikusan alkalmazkodjon, például a világítás, hőmérséklet vagy zenelejátszás terén. A biztonság terén is történtek fejlesztések: a Samsung és az Arlo együttműködésének köszönhetően a felhasználók mostantól kétirányú hangkommunikációt folytathatnak a kamerákon keresztül, valamint AI-alapú objektumfelismerést használhatnak a biztonsági értesítések testreszabására. Végül, a Samsung bejelentette a SmartThings Pro verziót, amely kifejezetten vállalkozások, szállodák és más intézmények számára készült, lehetővé téve a világítás, biztonság és más rendszerek központi kezelését.

Összességében a Samsung SmartThings egy hatékony és felhasználóbarát okosotthon platform, amely lehetővé teszi a felhasználók számára, hogy egyszerűen vezéreljék az otthonukat, és számos eszközzel integrálódik, hogy a lehető legnagyobb rugalmasságot nyújtsa a felhasználóknak. [13][14]

14. ábra Az ábrán a Samsung intelligens asszisztens látható

3.6 Biztonsági berendezések: zárak, kamerák, riasztók

Az okosotthonok egyik legfontosabb szempontja a biztonság. Az okos zárral, biztonsági kamerákkal és riasztórendszerekkel a tulajdonosok nagyobb biztonságban érezhetik magukat és könnyedén ellenőrizhetik otthonukat bármikor, bárhonnan.

Az okos zárak lehetővé teszik a tulajdonosok számára, hogy okostelefonjukkal vagy táblagépükkel távolról zárják, vagy nyissák az ajtót, illetve nyomon kövessék a zár állapotát. Az okos záraknak két fő típusa van: a vezeték nélküli és a hálózati zárak. Mindkét típusnak számos előnye van az általános kulcsos zárhoz képest.

A vezeték nélküli zárak működéséhez általában Bluetooth kapcsolatot használnak, amely lehetővé teszi a mobiltelefon és a zár közötti kommunikációt. Az ilyen típusú zárak általában elemekkel működnek, így nem igényelnek áramforrást, és a telepítés is egyszerű. A vezeték nélküli zárakat általában az ajtó belsejébe helyezik, így a kulcs elvesztése esetén a külső oldalról is nyitható marad az ajtó. Az ilyen zárak vezérlése általában egy alkalmazáson keresztül történik, amely lehetővé teszi az ajtó állapotának ellenőrzését, valamint a felhasználók hozzáférésének kezelését.

A hálózati zárak az internetkapcsolatot használják a kommunikációhoz, és általában a Wi-Fi-n vagy a Z-Wave-en keresztül kapcsolódnak az otthoni hálózathoz. Az ilyen típusú zárakat általában az ajtó külső oldalára helyezik, és áramforrásra van szükségük. Az ilyen zárak általában további funkciókkal rendelkeznek, mint például az érintőképernyős vezérlő, az érintőképernyős billentyűzet, az ujjlenyomat-olvasó és a videokamera. Ezek a funkciók növelik az otthonbiztonságot, és lehetővé teszik a felhasználók hozzáférési jogainak pontosabb kezelését. [15]

15. ábra A képen okos zár látható

Az okos kamerák lehetővé teszik a felhasználók számára, hogy valós időben élő videofelvételeket nézzenek meg, és értesítéseket kapjanak, ha a kamera érzékel valamilyen mozgást.

Az okos kamerák számos hasznos funkcióval rendelkeznek, amelyek növelik az otthoni biztonságot és kényelmet. Az éjjellátó képesség lehetővé teszi, hogy a kamera sötétben is tiszta képet rögzítsen, gyakran infravörös technológiát használva. A mozgásérzékelés funkció segítségével a rendszer képes észlelni a mozgást, és automatikusan értesítést küld a felhasználónak. A beépített mikrofon révén a kamerák hangokat is rögzítenek, így a felhasználók hallhatják, mi zajlik otthonukban. Sok eszköz hangszóróval is fel van szerelve,

amely lehetővé teszi a kétirányú kommunikációt – így a kamera közelében tartózkodók beszélhetnek is egymással.

16. ábra Az ábrán biztonsági kamera látható

Fontos megjegyezni, hogy az okos kamerák is sérülékenyek lehetnek a biztonsági fenyegetésekkel szemben, ezért megfelelő biztonsági intézkedéseket kell tenni annak érdekében, hogy megvédjék a kamerákat és az otthonokat a hackerek és más potenciális támadók ellen. [16]

Az okosotthon biztonsági rendszerei általában intelligens asszisztensekkel vannak összekapcsolva, például az Amazon Alexával, a Google Home-mal vagy az Apple HomeKittel, ezáltal lehetővé teszik a tulajdonosok számára, hogy hangutasításokat adjanak, illetve figyelmeztetéseket kapjanak a rendszerekkel kapcsolatos eseményekről. Továbbá a biztonsági rendszerek felügyeleti szolgáltatásokkal is rendelkezhetnek, amelyek automatikusan értesítik a rendőrséget vagy a tűzoltókat, ha az otthonban probléma merül fel.

Az okosotthonok biztonsági rendszerei tehát sokkal többet kínálnak, mint a hagyományos biztonsági eszközök. Az okos zárak, kamerák, riasztók és biztonsági rendszerek egyszerűen használhatóak, távolról vezérelhetőek és intelligens asszisztensekkel összekapcsolhatóak, amelyekkel a tulajdonosok nagyobb biztonságban érezhetik magukat otthonukban.

3.7 Néhány okos háztartási gép

Az okos háztartási gépek olyan eszközök, melyek segítségével távolról lehet vezérelni és ellenőrizzni az otthonunkban található különböző készülékeket, mint például a hűtőszekrény, a mosógép, a porszívó, és a légkondicionáló. Az okos háztartási gépek többféle módon kommunikálhatnak, például WiFi-n, Bluetooth-on, Zigbee-n és Z-Wave-n keresztül.

Az okos hűtőszekrények olyan funkciókkal vannak ellátva, melyekkel távolról lehet ellenőrizni a hűtőszekrényünk állapotát, valamint, be lehet állítani a hőmérsékletet is. Néhány ilyen hűtő képes monitorozni a benne található készleteket, melynek segítségével a felhasználók előre tervezhetik a bevásárlásokat, vagy éppen az élelmiszerkészletüket ellenőrizhetik.

17. ábra Az ábrán okos hűtőszekrény látható

Az okos mosógépek szintén rendelkeznek távoli vezérléses funkciókkal, ilyen például az, hogy távolról be lehet állítani a mosási ciklust, és akár időzítővel is el lehet látni azokat, hogy automatikusan be- és kikapcsoljanak, amikor szükség van rájuk. Vannak olyan okos mosógépek, amelyek képesek a tanulásra, és a mosási szokásokat is figyelembe véve, automatikusan beállítják a megfelelő mosási ciklust.

18. ábra A képen okos mosógép látható

Az okos légkondicionálók lehetővé teszik, hogy távolról vezéreljük és programozzuk az otthonunkban lévő klímaberendezéseket. Így akár még munkában vagy utazás közben is bekapcsolhatjuk a légkondit, hogy amikor hazaérünk, kellemes hőmérséklet fogadjon minket.

Ezen felül számos más funkcióval is rendelkeznek, amelyek tovább javítják a kényelmet és a hatékonyságot. Például az érzékelők segítségével képesek felmérni a szobában lévő

hőmérsékletet és nedvességet, és automatikusan szabályozzák a légkondi működését ennek megfelelően. Emellett egyes okos légkondicionálók képesek az energiafogyasztás monitorozására is, így lehetővé teszik a takarékosabb használatot.

Az okos légkondicionálók szintén különböző protokollokat használnak a kommunikációra, mint például a Wi-Fi vagy a Bluetooth, így szükség van megfelelő hálózati beállításokra és biztonsági intézkedésekre is a használatuk során. A gyártók általában biztonsági ajánlásokat és frissítéseket is nyújtanak, amelyek segítenek az eszközök biztonságosabbá tételében.

19. ábra A képen okos légkondicionáló látható

Az okos porszívók az otthoni takarítást teszik egyszerűbbé és hatékonyabbá, mivel automatikusan tisztítják a padlókat, és egyes modellek képesek navigálni a helyiségek között. Az okos porszívók általában Wi-Fi vagy Bluetooth protokollt használnak a kommunikációra, és az internetkapcsolat lehetővé teszi a távoli vezérlést a mobilalkalmazások használatával.

Az okos porszívók érzékelők segítségével takarítják a padlót, mivel képesek felismerni a padló típusát, a szennyeződést és az akadályokat. Az érzékelőkkel ellátott okos porszívók képesek automatikusan átváltani a padlótípusok között, és a szennyeződések érzékelésekor megnövelni a teljesítményüket a hatékonyabb takarítás érdekében.

Egyes modelleknél lehetőség van hangutasításokkal történő vezérlésre is, így nem szükséges a készülékhez való közvetlen hozzáférés. Ezenkívül képesek megtanulni az otthonunkat és az elrendezést, így az idővel hatékonyabban takarítanak. [17]

20. ábra Az ábrán okos robotporszívó látható

3.8 Néhány okosotthoni eszköz költsége

Az okosotthon kialakításának költségei jelentősen függnek az otthon méretétől, az automatizálni kívánt rendszerek számától és típusától, valamint az alkalmazott technológiáktól. A kiadások két fő kategóriába sorolhatók: az installációs költségek és a hardver-szoftver eszközök beszerzési árai.

Az installációs költségek magukban foglalják az okosotthon rendszerének tervezését, telepítését, konfigurálását és integrálását. Egy átlagos, körülbelül 100 négyzetméteres ház esetében az okosítás költsége 2–5 millió forint között mozoghat, a választott technológiától és a rendszer bonyolultságától függően. Ez az összeg tartalmazhatja a vezetékrendszerek, kapcsolók, szenzorok, intelligens eszközök és a szükséges infrastruktúra kiépítését, valamint a rendszer beüzemelését és tesztelését.

Az okos eszközök és rendszerek árai változóak, attól függően, hogy milyen funkciókkal és minőségi szinttel rendelkeznek. Néhány példa az okosotthon eszközök árára:

- **Okos világítás rendszerek**: Az okos lámpák és égők ára általában 5.000 és 40.000 forint között változik darabonként, a minőségtől és funkcionalitástól függően.
- **Okos termosztátok**: Az okos termosztátok ára 40.000 és 100.000 forint között mozoghat, a funkciók és a márka függvényében.
- **Okos zárak**: Egy megbízható okos zár ára nagyjából 100.000 és 200.000 forint között mozog.
- **Okos hűtőszekrények**: Az okos hűtőszekrények ára 200.000 forinttól akár több millió forintig terjedhet, a térfogat és a kínált szolgáltatások függvényében.

- **Okos redőnyök**: Az okos redőnyök ára 50.000 és 150.000 forint között mozoghat, a mérettől és a vezérlési lehetőségektől függően.
- **Okos biztonsági kamerák**: Az okos biztonsági kamerák ára 20.000 és 100.000 forint között változhat, a felbontás, a látószög és az éjjellátó képességek függvényében.
- **Okos vízérzékelők**: Az okos vízérzékelők ára 10.000 és 30.000 forint között mozoghat, a funkcionalitástól és a márkától függően.

Az okosotthon technológiák folyamatosan fejlődnek, és számos új trend és fejlesztés jelenik meg a piacon. Ezek közé tartozik az intelligens vízgazdálkodás, amely lehetővé teszi a vízfogyasztás optimalizálását és a szivárgások azonnali észlelését, valamint az otthoni energiatárolás, amely segít az áramkimaradások kezelésében és az energiahatékonyság növelésében. Emellett a mesterséges intelligencia és az automatizálás egyre nagyobb szerepet kap az otthonok kényelmének, biztonságának és fenntarthatóságának növelésében.

Az okosotthon kialakításának költségei jelentősen változhatnak az egyéni igények, az otthon mérete és a választott technológiák függvényében. Az alapvető rendszerek telepítése néhány százezer forinttól indulhat, míg a teljes körű, prémium megoldások akár több millió forintba is kerülhetnek. Fontos megjegyezni, hogy az okosotthon rendszerek nemcsak a kényelmet és a biztonságot növelik, hanem hosszú távon energiamegtakarítást is eredményezhetnek, így a beruházás megtérülhet az évek során.[18]

4. Okosotthonok jövője

Az okosotthonok jövője szorosan összefonódik a mesterséges intelligencia (MI) és a big data technológiák fejlődésével. A jövőben az MI alapú rendszerek nemcsak végrehajtják a felhasználók parancsait, hanem képesek lesznek előre megjósolni a lakók szokásait és igényeit is. Például egy MI rendszer automatikusan beállítja a hőmérsékletet vagy a világítást a megszokott napi rutin alapján, akár anélkül, hogy a felhasználónak bármit tennie kellene.

A big data technológiák lehetővé teszik, hogy az okosotthon eszközök óriási mennyiségű adatot gyűjtsenek a felhasználók viselkedéséről, energiafogyasztásáról vagy éppen a biztonsági mintázatokról. Ezeket az adatokat az MI elemzi, és ennek alapján optimalizálja az otthon működését, így nemcsak kényelmesebbé, hanem energiatakarékosabbá is válik az életvitel.

A fejlesztések egyik iránya a prediktív karbantartás, ahol az MI előre jelzi az eszközök meghibásodását a szokásos működésük alapján, így megelőzhetőek a váratlan problémák. Emellett egyre hangsúlyosabb lesz az adatbiztonság és az etikus adatkezelés kérdése is, hiszen a személyes adatok tömeges gyűjtése komoly felelősséget ró a fejlesztőkre.

A jövő okosotthonai egyre inkább hálózatba kapcsolódnak – nemcsak a házon belül, hanem más otthonokkal vagy városi rendszerekkel is –, így a „smart home” fogalma átalakul „smart city” irányba. Összességében az okosotthon nemcsak a kényelmet, hanem a tudatosabb, fenntarthatóbb életmódot is szolgálni fogja a következő években.[19]

5. Összegzés

Az okosotthonok kiépítése egyre népszerűbb az emberek körében, akik szeretnék kihasználni a modern technológia előnyeit a mindennapi életük során. Ezek a rendszerek lehetővé teszik az otthoni eszközök távoli vezérlését és felügyeletét, és javítják az otthon kényelmét, biztonságát és hatékonyságát.

Azonban, az okos otthonok kiépítése során számos akadály merülhet fel, például a magas bekerülési költségek, az eszközök összekapcsolásának bonyolultsága, az adatvédelmi aggályok stb...

Fontos azonban megjegyezni, hogy ezek az akadályok általában megoldhatók. Az okosotthoni rendszerek előnyei meghaladják az ezzel járó nehézségeket, és a befektetés hosszú távon megtérülhet. Az okosotthonok kiépítése továbbá előnyöket kínálhatnak a környezetre is, például a fogyasztás csökkentésével, ami az energiahatékonyság javítását jelenti.

Összefoglalva, az okosotthonok kiépítése nem csak a jelen, hanem a jövő is, és a technológia fejlődésével egyre több embernek válik elérhetővé ez a lehetőség. Ahhoz azonban, hogy az ezek az ökoszisztémák valóban hatékonyan működjenek, fontos a megfelelő tervezés és az eszközök összekapcsolása, kompatibilitása, valamint a karbantartás és frissítések rendszeres elvégzése. Az okosotthonok kiépítése azonban még mindig egy új terület, és az embereknek folyamatosan kell tanulniuk és fejleszteniük a technológiai ismereteiket, hogy az otthonaikban lévő okos eszközök teljes mértékben kihasználhassák a modern technológia előnyeit.

Személyes véleményem szerint, hazánkban is sokkal jobban kéne népszerűsíteni az okosotthonokat, és azok előnyeit. Számos nagyvállalatot be lehetne vonni ilyen témákban, hogy minél több emberhez eljussanak ezek az információk.

Források, Hivatkozások

[1] https://hu.wikipedia.org/wiki/Okosotthon

[2] https://lakasgeneral.com/2023/04/05/milyen-tipusu-adatokat-gyujtenek-az-intelligens-otthoni-rendszerek/

[3] https://lakasgeneral.com/2024/03/13/okosotthonokkal-kapcsolatos-eszkozok-es-fogalmak/

[4] https://www.plc-program.hu/blog/okos-otthon-automatizalas

[5] https://www.oott.hu/okos-otthon-kiepitese/

[6] https://smartbuild.hu/okosotthon-megoldasok/

[7] https://www.nachi.org/problems-smart-home-tech.htm

[8] https://www.matteralpha.com/explainer/zigbee-z-wave-or-thread-what-to-know-before-buying-your-next-smart-home-device

[9] https://tudastar.ingatlan.com/tippek/hogyan-valik-egyre-elerhetobbe-az-okosotthontechnologia/

[10] https://rencanaringgit.com/hu/mi-az-intelligens-digit%C3%A1lis-asszisztens/M

[11] https://9to5mac.com/2024/10/15/apple-has-a-new-smart-home-device-and-strategy-coming-in-2025-per report/#:~:text=There%20are%20new%20home%20devices%20and%20a%20fresh,major%20new%20smart%20home%20push%20starting%20in%202025.

[12] https://www.makeuseof.com/amazon-alexa-vs-google-home-vs-apple-homekit-best-smarthome-system/

[13] https://www.samsung.com/hu/smartthings/app/?msockid=2012b24cb79d6cef15c5a6c5b6806d48

[14] https://blog.smartthings.com/roundups/samsung-smartthings-introduces-new-ai-features-at-unpacked/?utm_source=chatgpt.com

[15] https://legrand.hu/szakemberek/cikkek/okos-tanacsok-otthonra/biztonsag-es-okosotthon

[16] https://www.origo.hu/techbazis/2024/05/okos-kamera-okosotthon

[17] https://www.mediamarkt.hu/hu/category/okos-haztartasi-eszkozok-695516.html

[18] A költségeket számos webáruház aktuális ajánlatai alapján néztem, nem választottam sehol konkrét termékeket.

[19] https://www.unite.ai/hu/A-mesters%C3%A9ges-intelligencia-az-okosotthonok-k%C3%B6vetkez%C5%91-l%C3%A9p%C3%A9se/

Egyes bekezdéseknél az OpenAI programját használtam kiegészítésnél: https://chat.openai.com

Ábrajegyzék

[1] https://www.okosotthonok.com/hu/blog-hu-hu/11-az-okosotthon-tortenete

[2] https://www.otthonokesmegoldasok.hu/tipp-2/igy-lesz-tokeletes-a-jovo-otthona/

[3] https://www.bitsathy.ac.in/the-transformative-role-of-ai-and-iot-in-smart-homes/

[4] https://twitter.com/HogarControls/status/1209504096744546304

[5] Saját kép

[6] https://www.researchgate.net/figure/SHSec-based-smart-homenetwork_fig1_328490414

[7] https://www.security.org/home-security-systems/z-wave-vs-zigbee/

[8] https://medium.com/iotpractices/understanding-the-thread-protocol-and-network-4b94111884e3

[9] Táblázat a ZigBee és Z-Wave és Thread technikai adatairól, magyarra fordítva: https://www.mouser.es/blog/zigbee-vs-z-wave-whats-the-difference

[10] https://www.homekitauthority.com/matter-1-0-released-and-what-does-it-mean-for-homekit/

[11] https://micasaconapple.com/que-es-homekit-de-apple-y-como-funciona/

[12] https://amvstore.com.uy/catalogo/asistente-virtual-amazon-echo-dot-alexa-5ta-gen-bt-wifi-sea-blue_6791_6791

[13] https://golivexplore.com/google-home-mini-review-top-features/

[14] https://www.samsungmobilepress.com/feature-stories/samsung-smartthings-unveils-new-interface-offering-customers-a-more-dynamic-connected-home-experience/

[15] https://kinatech.hu/hirek/karacsonyi-akcioban-rendelhetoek-a-legujabb-welock-okos-zarak

[16] https://tudastar.ingatlan.com/tippek/kamera-otthonra/

[17] https://foodyny.hu/a-nagybetus-etel/4111-okokonyha-okoseszkoz-mestersegesintelligencia-hutoszekreny

[18] https://www.samsung.com/au/washers-and-dryers/smart-washing-machine-dryer/

[19] https://cielowigle.com/blog/smart-ac-benefits-and-features/

[20] https://allegro.hu/termek/ba168cc0-481d-4e65-af84-09022c7231cd?offerId=&utm_source=mall.hu

2.5. Talajnedvesség-vezérelt IoT locsolórendszer ESP8266-tal Pálmási Ákos

IPAR 4.0 technológiák

GKNB_INTM087

2024/2025/2

Talajnedvesség-vezérelt IoT locsolórendszer ESP8266-tal

Pálmási Ákos

[redacted]

Gazdaságinformatikus BSc

Tartalomjegyzék

Bevezetés **2**

1. Célkitűzés **2**

2. Alkalmazott technológiák és eszközök **2**

3. Rendszerterv és architektúra **2**

3.1 Hardverkomponensek 2

3.2 Interakciók 2

4. Megvalósítás **3**

4.1 Rendszer működése 3

4.2 Webes interfész 3

5. Tesztelés **3**

6. Eredmények, jövőbeli fejlesztések **3**

6.1 Eredmények 3

6.2 Jövőbeli fejlesztések 3

7. Forráskód **4**

Bevezetés

A projekt célja egy ESP8266 mikrovezérlőre épülő automatikus locsolórendszer megvalósítása, amely a talajnedvesség mérése alapján dönt az öntözés szükségességéről. A rendszer beépített Wi-Fi hotspotként működik, és egy valós idejű, dinamikusan frissülő webes felületet biztosít a felhasználónak a rendszerállapot megfigyelésére.

1. Célkitűzés

A cél egy egyszerű, de megbízható öntözőautomatika kialakítása, amely képes:

- A talaj nedvességi szintjének valós idejű mérésére,
- Automatikusan működtetni a szivattyút a mért érték alapján,
- Webes felületet biztosítani a felhasználónak az adatok megtekintésére.

2. Alkalmazott technológiák és eszközök

- **Mikrovezérlő:** ESP8266 NodeMCU V3
- **Szenzor:** Kapacitív talajnedvesség-érzékelő (analóg)
- **Aktuátor:** 1-csatornás 5V-os relémodul
- **Webes technológiák:** HTML, JavaScript (AJAX fetch)
- **Fejlesztői környezet:** Arduino IDE
- **Kommunikáció:** Wi-Fi (ESP saját AP módban)

3. Rendszerterv és architektúra

3.1 Hardverkomponensek

- ESP8266: Wi-Fi kapcsolat, adatfeldolgozás, vezérlés.
- Talajnedvesség-érzékelő: Analóg érték alapján történő nedvesség-érzékelés.
- Relémodul: Kapcsolja a vízpumpát a meghatározott nedvesség-értéktől függően.

3.2 Interakciók

- Automatikus öntözés a talaj szárazsága esetén.
- Valós idejű felhasználói visszajelzés: HTML oldal JavaScript segítségével frissíti a megjelenített értékeket.

4. Megvalósítás

4.1 Rendszer működése

- A talajnedvesség-érzékelő folyamatosan méri az értéket
- Ha az érték < 20 (száraz), akkor aktiválódik a relé, ami a pumpát vezérli
- A rendszer Wi-Fi AP módban saját hálózatot hoz létre
- A felhasználó ellenőrizheti a talaj nedvességtartalmát, illetve a locsolás állapotát a webes felületen

4.2 Webes interfész

Valós idejű visszajelzés a következő elemek megjelenítésével:

- Nedvességi érték
- Locsolás állapota

5. Tesztelés

Bemenet	**Elvárt eredmény**	**Tényleges eredmény**
Nedvesség < 20	Relé kapcsol, pumpa elindul	Relé kapcsolt, pumpa elindult
Nedvesség > 20	Relé kikapcsol, pumpa leáll	Relé kikapcsolt, pumpa leállt
Weboldal elérése	Elérhető weboldal, frissülő adatok	Megjelenik a felület, az értékek frissülnek

6. Eredmények, jövőbeli fejlesztések

6.1 Eredmények

- A rendszer megbízhatóan és stabilan működik
- A webes felület működik és valós adatokkal szolgál.
- A vezérlési logika egyszerű, de hatékony.

6.2 Jövőbeli fejlesztések

- Időzített öntözési funkció bevezetése.
- Mikrovezérlő cseréje ESP32-re
- Deep Sleep mód alkalmazása az energiahatékonyság érdekében.
- Távoli elérés lehetővé tétele STA módban Wi-Fi-n keresztül.
- Több öntözési zóna támogatása több relé- és szenzorkimenettel.
- Mobilalkalmazás fejlesztése az adatok lekérésére és vezérlésre.

7. Forráskód

```
#include <ESP8266WiFi.h>
#include <ESP8266WebServer.h>

#define SENSOR_PIN A0          // Talajnedvesség-érzékelő (analóg)
#define RELAY_PIN  D2          // Szivattyú vezérlés (relé: aktív HIGH)
#define THRESHOLD  20          // Nedvességküszöb
#define WATER_TIME 10000       // Locsolás időtartama (ms) → 10 s
#define SAMPLE_DELAY 2000      // Mintavétel gyakorisága (ms) – 2 s

ESP8266WebServer server(80);

bool watering = false;               // éppen locsol-e?
unsigned long waterStart = 0;        // locsolás kezdete

String htmlPage() {
  String html =
    "<!DOCTYPE html><html><head><meta charset='UTF-
8'><title>SmartWater</title>"
    "<script>"
    "function frissit(){fetch('/data').then(r=>r.json()).then(d=>{"
    "document.getElementById('moisture').innerText=d.moisture;"
    "document.getElementById('status').innerText=d.status;});}"
    "setInterval(frissit,2000);window.onload=frissit;"
    "</script></head><body>"
    "<h1>SmartWater - Locsolórendszer</h1>"
    "<p><strong>Nedvesség érték:</strong> <span id='moisture'>...</span></p>"
    "<p><strong>Állapot:</strong> <span id='status'>...</span></p>"
    "</body></html>";
  return html;
}

void handleData() {
  int m = analogRead(SENSOR_PIN);
  String st = watering ? "LOCSOLÁS FOLYAMATBAN"
                       : (m > THRESHOLD ? "RENDBEN - nem locsol" : "SZÁRAZ -
várható locsolás");
  String json = "{\"moisture\":" + String(m) + ",\"status\":\"" + st + "\"}";
  server.send(200, "application/json", json);
}

void handleRoot() { server.send(200, "text/html", htmlPage()); }

void setup() {
  Serial.begin(9600);
  pinMode(SENSOR_PIN, INPUT);
  pinMode(RELAY_PIN, OUTPUT);
```

```
  digitalWrite(RELAY_PIN, LOW);          // relé OFF

  WiFi.softAPConfig(IPAddress(192,168,4,1),
                    IPAddress(192,168,4,1),
                    IPAddress(255,255,255,0));
  WiFi.softAP("SmartWater", "jelszo");

  Serial.print("AP IP: "); Serial.println(WiFi.softAPIP());

  server.on("/",  handleRoot);
  server.on("/data", handleData);
  server.begin();
  Serial.println("Webszerver elindult");
}

void loop() {
  server.handleClient();

  int moisture = analogRead(SENSOR_PIN);
  Serial.print("Nedvesség: "); Serial.println(moisture);

  // Ha éppen nem locsolunk és túl száraz → indítjuk
  if (!watering && moisture <= THRESHOLD) {
    digitalWrite(RELAY_PIN, HIGH);   // relé ON
    watering   = true;
    waterStart = millis();
    Serial.println("Locsolás indult (10 s)...");
  }

  // Ha locsolunk, ellenőrizzük, letelt-e a 10 s
  if (watering && millis() - waterStart >= WATER_TIME) {
    digitalWrite(RELAY_PIN, LOW);    // relé OFF
    watering = false;
    Serial.println("Locsolás leállítva.");
  }

  delay(SAMPLE_DELAY);               // 2 s-enként új mérés
}
```

2.6. A Bluetooth fejlődése, architektúrája, újszerű alkalmazásai beágyazott rendszereken

IPAR 4.0 TECHNOLÓGIÁK

A Bluetooth fejlődése, architektúrája, újszerű alkalmazásai beágyazott rendszereken

Kasza Dominik Dániel

[redacted]

(GKNB_INTM087)

2024/2025/2

Abstract:

Bluetooth technology has undergone substantial evolution, particularly in the areas of energy efficiency, data transmission speed, and communication reliability. This thesis begins with a historical overview of the technology, covering the initial versions (Bluetooth 1.0 to 2.1), the introduction of Bluetooth Low Energy (BLE) with version 4.0, and the enhancements introduced in the 5.x series, such as extended range, higher throughput, and improved robustness.

The work proceeds with an in-depth examination of the Bluetooth architecture, detailing the protocol stack, network topologies including piconet and scatternet, and the roles of central and peripheral devices in BLE communication. Furthermore, various Bluetooth profiles (e.g., GATT, A2DP, HFP) are presented, along with their relevance in industrial and embedded system applications.

Particular emphasis is placed on the integration of Bluetooth technology into embedded platforms. The study explores BLE capabilities of popular microcontrollers (e.g., ESP32, nRF52), firmware-level implementation strategies, and the use of Bluetooth software stacks in environments such as Zephyr RTOS and Arduino.

Emerging applications—including industrial sensor networks, smart home devices, healthcare monitoring systems, and BLE beacons—are also discussed, highlighting novel human–machine and machine–machine (M2M) interaction models. Finally, the role of Bluetooth Mesh networking is analyzed in the context of scalable Internet of Things (IoT) architectures.

Tartalom

Abstract: 2

Bevezetés: 5

A Bluetooth technológia történeti áttekintése 5

Bluetooth 1.0–2.1: Kezdeti alkalmazások és technológiai korlátok 6

Bluetooth 3.0–4.0: High Speed és Low Energy paradigmaváltás 6

Bluetooth 5.x: Hatótávolság, sebesség, megbízhatóság fejlesztése 7

A Bluetooth architektúra és protokoll stack áttekintése 7

Protokoll stack felépítése 7

Bluetooth profilok és alkalmazási lehetőségeik 8

GATT – Generic Attribute Profile 8

A2DP – Advanced Audio Distribution Profile 9

HFP – Hands-Free Profile 9

Bluetooth architektúra és hálózati modellek 10

Protokoll stack felépítése 10

Hálózati modellek: piconet és scatternet 11

Központi és perifériás szerepkörök a Bluetooth LE-ben 11

Bluetooth profilok és ipari alkalmazások 11

Bluetooth profilok áttekintése 12

Ipari alkalmazások és Bluetooth profilok 12

Profilok implementálása beágyazott rendszerekben 12

Bluetooth integrációja beágyazott rendszerekbe 12

Mikrokontroller platformok Bluetooth LE támogatással 12

Bluetooth stack-ek és fejlesztői környezetek 13

Hardveres és szoftveres integráció kihívásai 13

Bluetooth alkalmazása ipari környezetekben 14

Ipari szenzorhálózatok és adatgyűjtés 14

Mobil ipari gépek és eszközök közötti kommunikáció 14

Bluetooth Mesh szerepe ipari automatizálásban 14

Egészségügyi alkalmazások és személyes monitorozás 15

Viselhető eszközök és egészségmonitorozás 15

BLE szerepe orvosi eszközök szabványosításában 15

Hosszú távú megfigyelés és telemedicina 16

BLE beacon technológia és kontextusérzékeny alkalmazások 17

A BLE beacon működési elve 17

Beltéri pozicionálás és navigáció 17

Interaktív és kontextusérzékeny szolgáltatások 17
Bluetooth Mesh hálózatok és szerepük IoT rendszerekben 18
Bluetooth Mesh architektúra 18
Előnyök és kihívások az IoT rendszerekben 18
Alkalmazási példák ipari és otthoni környezetben 18
Mikrokontrollerek és fejlesztőplatformok Bluetooth LE támogatással 19
Fejlesztői eszközök és keretrendszerek 19
Hardverintegráció és energiaoptimalizálás 19
Bluetooth stack-ek és szoftveres implementációk beágyazott rendszerekhez 20
Bluetooth stack-ek felépítése és működése 20
Nyílt forráskódú stack-ek és SDK-k 20
Stack-integráció a fejlesztési folyamatban 20
Bluetooth Mesh hálózat és szerepe az IoT rendszerek skálázásában 21
Bluetooth Mesh architektúra és működés 21
Mesh-kompatibilis eszközök és fejlesztői platformok 21
Mesh alkalmazások ipari és okosrendszerekben 21
A Bluetooth technológia jövője és fejlesztési irányai 22
Bluetooth 5.3 és a következő generációs fejlesztések 22
Jövőbeli alkalmazási területek 22
Integráció mesterséges intelligenciával és prediktív funkciókkal 23
Források: 23

Bevezetés:

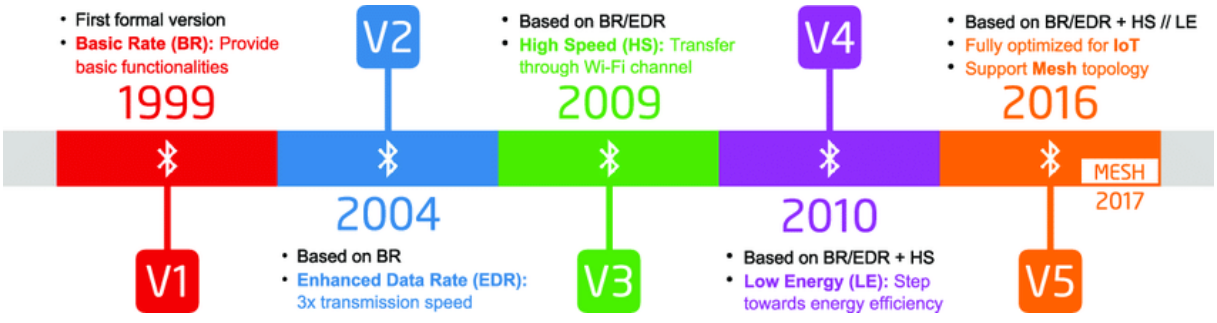
A vezeték nélküli kommunikáció napjaink egyik legmeghatározóbb technológiai területévé vált, amely kulcsszerepet játszik az okoseszközök, beágyazott rendszerek és ipari automatizálási megoldások fejlődésében. Ezen belül a Bluetooth technológia az egyik legismertebb és legelterjedtebb szabvány, amely eredetileg rövid hatótávú, alacsony sávszélességű adatátvitelre készült, mára azonban komplex, nagy megbízhatóságú és energiahatékony kommunikációs megoldássá vált, különösen a Bluetooth Low Energy (BLE) megjelenésével.

A Bluetooth technológia fejlődése lehetővé tette annak széles körű alkalmazását a beágyazott rendszerekben, az okosotthonok vezérlésétől kezdve az ipari érzékelőhálózatokon át az orvosi eszközökig. A BLE előnyei – mint az alacsony energiafogyasztás, a gyors csatlakozási idő és a skálázhatóság – ideálissá teszik a technológiát olyan rendszerekhez, ahol a folyamatos, mégis erőforrás-takarékos adatkapcsolat alapvető követelmény.

A dolgozat célja a Bluetooth technológia fejlődésének és architektúrájának áttekintése, valamint annak bemutatása, hogy miként integrálható hatékonyan a modern beágyazott rendszerekbe. A munka kiemelten foglalkozik az újabb verziók nyújtotta lehetőségekkel, a különféle mikrokontroller platformok támogatásával, valamint azokkal az újszerű alkalmazási területekkel, amelyekben a Bluetooth technológia alapvető szerepet játszik a gép-gép és ember-gép közötti interakcióban.

A Bluetooth technológia történeti áttekintése

A Bluetooth technológia 1994-ben indult útjára az Ericsson kezdeményezésére, azzal a céllal, hogy egy vezeték nélküli, alacsony energiafogyasztású alternatívát kínáljon a rövid hatótávú eszközkapcsolatokra. A technológia nevét Harald „Bluetooth” Gormsson dán királyról kapta, aki történelmi szerepéről híres: különböző skandináv törzseket egyesített – épp úgy, ahogy a Bluetooth célja is a különféle digitális eszközök közötti egységes kommunikáció biztosítása. A Bluetooth technológia azóta számos generáción ment keresztül, mindegyik jelentős technikai előrelépést hozott a sávszélesség, energiahatékonyság, hatótávolság és megbízhatóság terén. A következőkben bemutatjuk a főbb verziók fejlődését.



Bluetooth 1.0–2.1: Kezdeti alkalmazások és technológiai korlátok

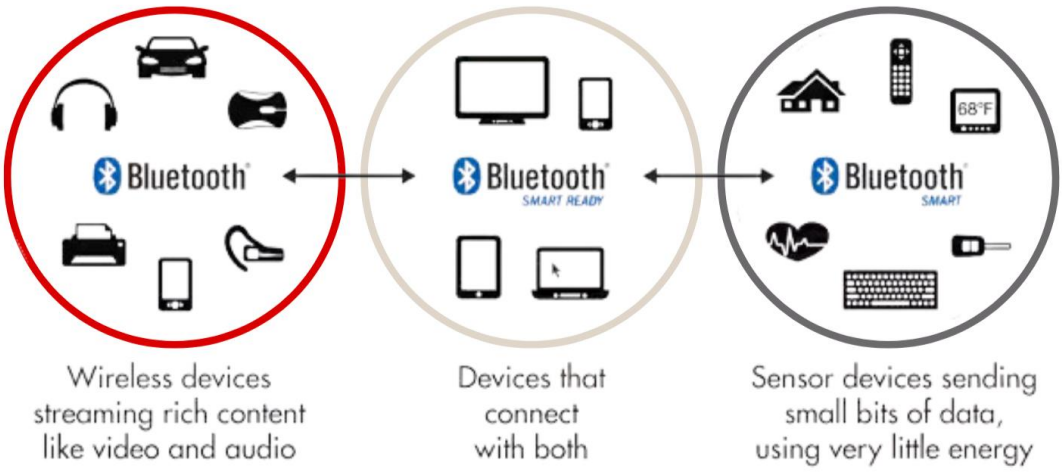
A Bluetooth első verziói (1.0 és 1.1) az alapvető vezeték nélküli kommunikációs célokat szolgálták, jellemzően mobiltelefonok, headsetek és számítógépek közötti adatcserére. A maximális adatátviteli sebesség 721 kbit/s volt, a hatótávolság pedig nagyjából 10 méter. A technológia ugyan működőképes volt, de megbízhatósági problémákkal és nehézkes eszközpárosítással küzdött.

A 2.0 és 2.1 verziók már jelentős fejlesztéseket hoztak. A **2.0** verzió bevezette az *Enhanced Data Rate (EDR)* képességet, amely akár 3 Mbit/s sebességet is lehetővé tett, ezáltal gyorsabb adatátvitelt és kevesebb energiaveszteséget biztosítva. A **2.1** verzió egyik legfontosabb újítása a *Secure Simple Pairing (SSP)* bevezetése volt, amely nagymértékben egyszerűsítette és biztonságosabbá tette az eszközök közötti kapcsolat létrehozását.

Bluetooth 3.0–4.0: High Speed és Low Energy paradigmaváltás

A **Bluetooth 3.0+HS** verzió 2009-ben jelent meg, amely ugyan maga nem hozott új fizikai réteget, de lehetővé tette, hogy a Bluetooth kapcsolat mellett a nagysebességű adatátvitelre a Wi-Fi technológiát használja. Ez „High Speed” módban akár 24 Mbit/s adatátvitelt tett lehetővé, de ehhez két különféle rádiós interfész használatára volt szükség.

A valódi paradigmaváltást azonban a **Bluetooth 4.0** megjelenése jelentette 2010-ben, amely bevezette a *Bluetooth Low Energy (BLE)* technológiát. A BLE célja nem a nagy adatsebesség, hanem a minimális energiafogyasztás volt, ami különösen alkalmassá tette akkumulátoros, kis teljesítményű eszközök – például viselhető okoseszközök, szenzorok, orvostechnikai berendezések – számára. A BLE révén a Bluetooth már nem csupán hangátvitelre és fájlmegosztásra, hanem érzékelőhálózatok és IoT-megoldások alaptechnológiájává is vált.



Bluetooth 5.x: Hatótávolság, sebesség, megbízhatóság fejlesztése

A **Bluetooth 5.0** 2016-ban került bevezetésre, és több olyan fejlesztést tartalmazott, amelyek a BLE platformot tovább erősítették. A legfontosabb újítások közé tartozik a:

- négyszeres hatótávolság (akár 200 méter nyílt térben),
- kétszeres adatsebesség (2 Mbit/s),
- és nyolcszoros üzenetkapacitás a reklámcsatornákon.

A **Bluetooth 5.1** és **5.2** verziók új lehetőségeket teremtettek, például **irányalapú helymeghatározással (Angle of Arrival, AoA)**, valamint a *LE Audio* technológia bevezetésével, amely jobb hangminőséget és több eszköz egyidejű támogatását tette lehetővé. Emellett a 5.2-es verzió bevezette az *Isochronous Channels* nevű koncepciót, amely lehetővé teszi a hangadatok szinkronizált átvitelét – ez különösen fontos az okos hallókészülékek és vezeték nélküli fülhallgatók számára.

A Bluetooth 5.x széria tehát már nem csak fejlődés, hanem valódi átalakulás: az egyszerű „vezeték nélküli kábel” szerepből az IoT ökoszisztéma kulcstechnológiájává vált.

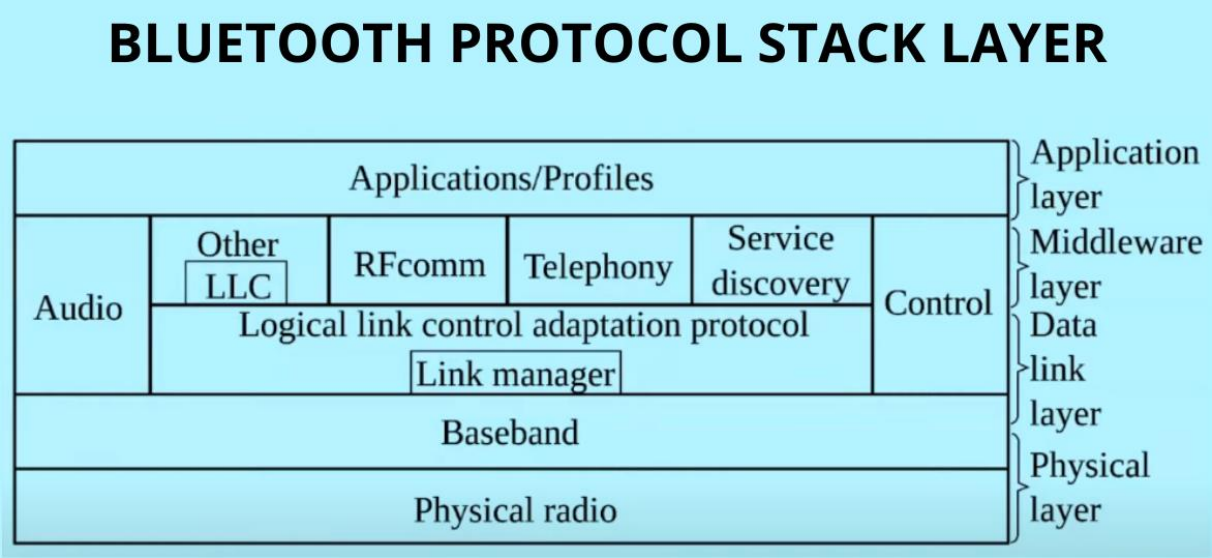
A Bluetooth architektúra és protokoll stack áttekintése

A Bluetooth technológia működésének megértéséhez elengedhetetlen a protokoll stack és az architektúra részletes vizsgálata. Ez a rétegzett felépítés biztosítja a kommunikáció megbízhatóságát, energiahatékonyságát és kompatibilitását különböző eszközök között. Az alábbi alcímek részletesen tárgyalják a Bluetooth architektúrájának főbb elemeit és működési elveit.

Protokoll stack felépítése

A Bluetooth protokoll stack több rétegből áll, amelyek egymásra épülnek, és különböző funkciókat látnak el:

- **Alacsony szintű rádiós réteg (Radio Layer):** Ez kezeli a fizikai rádiójelet, az adó- és vevőfunkciókat, valamint a frekvenciaszórást (FHSS), ami a zavarok elkerülésében segít.
- **Bázisvezérlő és hozzáférési réteg (Baseband and Link Layer):** Ebben a rétegben történik a fizikai linkek kiépítése, a csomagok időzítése, hibakezelés, titkosítás és az energiatakarékos üzemmódok kezelése.
- **Host réteg:** A magasabb szintű protokollok futnak itt, például L2CAP (Logical Link Control and Adaptation Protocol), amely az adatcsomagok továbbítását és multiplexelését végzi.
- **Szolgáltatási réteg:** Ez foglalja magában a profilokat és szolgáltatásokat, mint például GATT (Generic Attribute Profile) a Bluetooth Low Energy-ben, amely szabványosított interfészeket biztosít különböző alkalmazások számára.



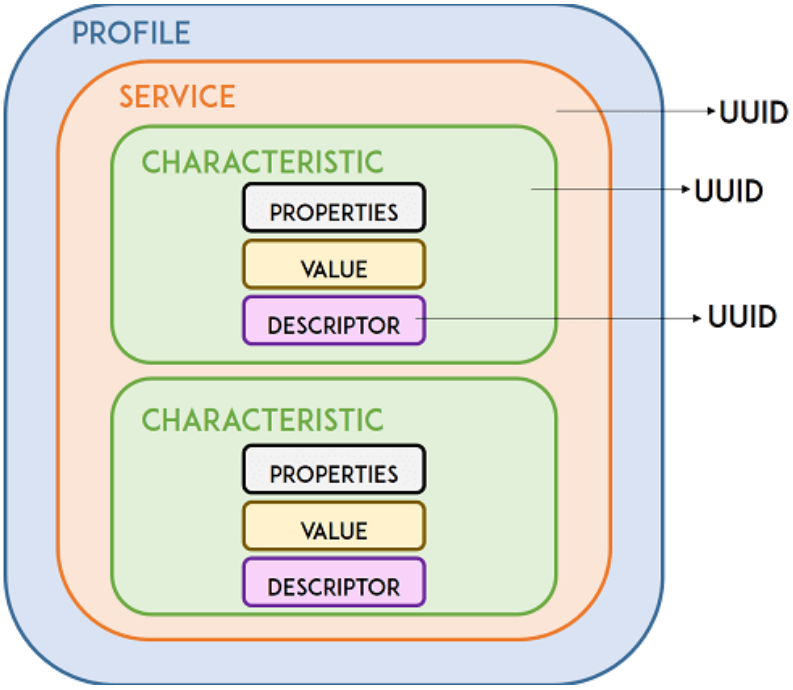
Bluetooth profilok és alkalmazási lehetőségeik

A Bluetooth profilok a technológia specifikus használati esetekre szabott szabványosított protokollok és szolgáltatások összességei, amelyek biztosítják az interoperabilitást különböző eszközök és alkalmazások között. Az ipari és beágyazott rendszerek számára különösen fontos a megfelelő profilok kiválasztása és alkalmazása, hogy optimális működést és kompatibilitást érjenek el.

GATT – Generic Attribute Profile

A GATT profil a Bluetooth Low Energy (LE) egyik alapköve, amely az adatok szerkezetét és cseréjét szabályozza. Különösen fontos a szenzorok, orvosi eszközök és egyéb IoT komponensek esetén.

- **Adatszerkezet és szolgáltatások:** A GATT hierarchikus modellje alapján az eszközök szolgáltatásokat (services) és attribútumokat (characteristics) kínálnak, amelyek lekérdezhetők vagy módosíthatók a kliens eszközök által.
- **Alkalmazási területek:** Egészségügyi monitorozás (pl. pulzusmérők, vérnyomásmérők), ipari szenzorok adatgyűjtése, okosotthon eszközök (pl. világítás, termosztát) irányítása.



A2DP – Advanced Audio Distribution Profile

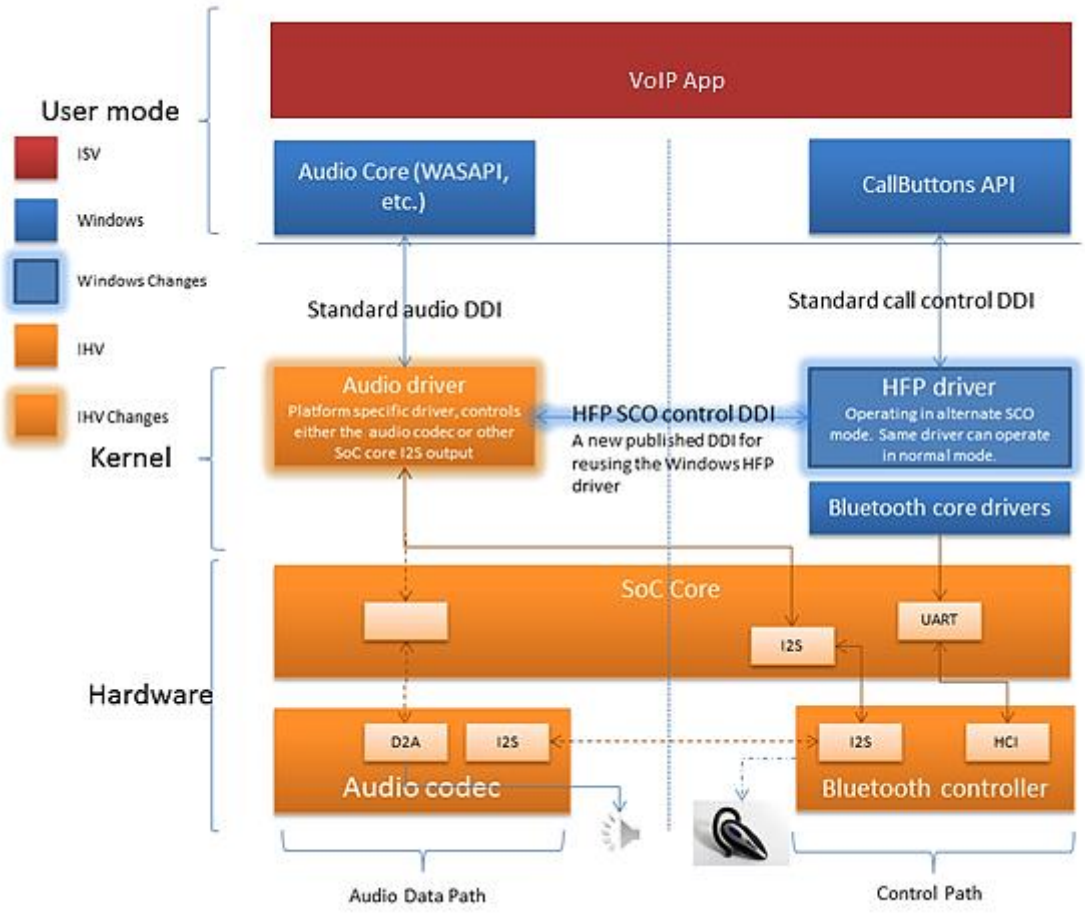
Az A2DP profil a Bluetooth audioátvitelének szabványa, amely lehetővé teszi nagy minőségű sztereó hang továbbítását vezeték nélküli eszközök között.

- **Hangátvitel technikai jellemzői:** Támogatja az SBC (Subband Codec) és más fejlettebb kodekeket (pl. aptX), amelyek az adatátvitel minőségét és késleltetését befolyásolják.
- **Ipari alkalmazások:** Bár elsősorban fogyasztói elektronikai eszközökben elterjedt (pl. vezeték nélküli fejhallgatók, hangszórók), ipari környezetben például hangutasítások vagy riasztások vezeték nélküli továbbítására is használható.

HFP – Hands-Free Profile

A HFP profil a Bluetooth telefonkihangosító eszközök kommunikációját teszi lehetővé, amely ipari környezetben is releváns lehet, például vezeték nélküli kommunikációban gépek vagy járművek között.

- **Kommunikációs protokoll:** Biztosítja a hívások kezelését, hangátvitelt, és a vezérlő parancsokat, például hangerő szabályozást.
- **Beágyazott rendszerek szerepe:** Alkalmazható ipari járművekben, robotikai rendszerekben vagy más olyan területeken, ahol a vezeték nélküli hangkommunikáció növeli a hatékonyságot és a biztonságot.



Bluetooth architektúra és hálózati modellek

A Bluetooth technológia sikerének alapja annak jól kidolgozott architektúrája és hálózati modellje, amelyek lehetővé teszik a különböző eszközök közötti megbízható és energiatakarékos kommunikációt. Ezek megértése kulcsfontosságú a beágyazott rendszerekben való alkalmazás szempontjából.

Protokoll stack felépítése

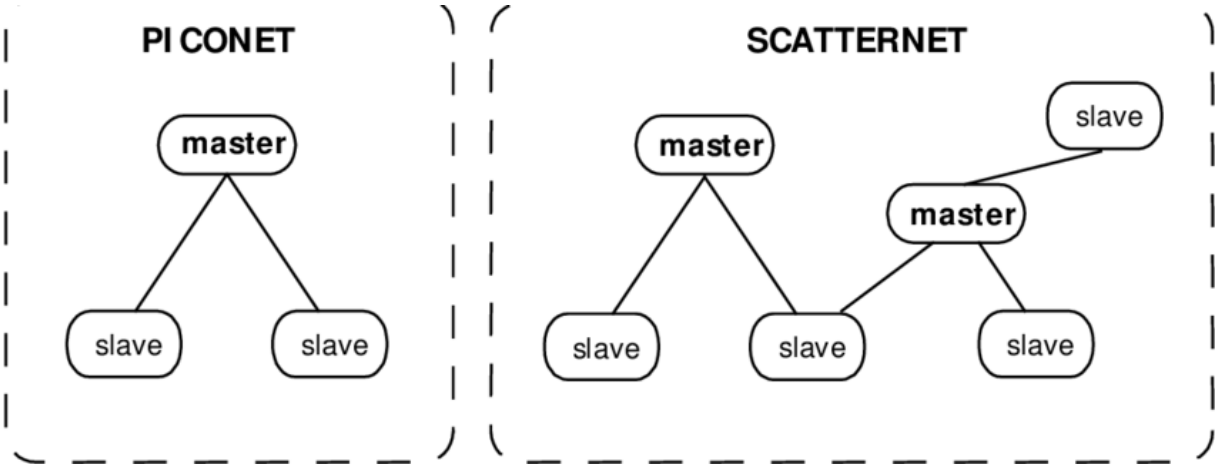
A Bluetooth protokoll stack egy réteges architektúrát követ, amelyben minden réteg külön funkciót lát el az adatátvitel biztonságának és hatékonyságának biztosítására.

- **Alaprétegek:** A fizikai réteg (PHY) és az adatkapcsolati réteg (Link Layer) felelősek az adatok vezeték nélküli továbbításáért és a kapcsolat fenntartásáért.
- **Magasabb szintű protokollok:** A Host Controller Interface (HCI), Logical Link Control and Adaptation Protocol (L2CAP), valamint a Generic Attribute Profile (GATT) és más profilok vezérlik az adatok szerkezetét és kommunikációját.
- **Biztonsági rétegek:** Titkosítás, hitelesítés és párosítási mechanizmusok szerepe a megbízható és biztonságos adatátvitelben.

Hálózati modellek: piconet és scatternet

A Bluetooth hálózati modellje a kis hatótávolságú, alacsony energiaigényű eszközök hatékony összekapcsolását szolgálja.

- **Piconet:** Egy központi (master) és akár 7 perifériás (slave) eszközből álló hálózat, amely az alapvető kommunikációs egységet képezi. Az időosztásos multiplexelés révén működik.
- **Scatternet:** Több piconet összekapcsolódásával kialakuló hálózat, ahol egy eszköz akár több piconet-ben is részt vehet áthidaló (bridge) szerepben. Ez növeli a hálózat rugalmasságát és méretét.
- **Alkalmazási lehetőségek:** Ipari környezetben scatternetekkel nagyobb, összetettebb szenzorhálózatok és kommunikációs struktúrák valósíthatók meg.



Központi és perifériás szerepkörök a Bluetooth LE-ben

A Bluetooth Low Energy kommunikáció a központi (central) és perifériás (peripheral) szerepek világos elhatárolásán alapul, amely fontos a hálózat energiahatékonysága szempontjából.

- **Perifériás eszközök:** Ezek általában alacsony energiafogyasztású szenzorok vagy egyszerűbb végpontok, amelyek adatokat gyűjtenek és továbbítanak.
- **Központi eszközök:** Ezek kezelik a hálózatot, felépítik a kapcsolatokat, gyűjtik és feldolgozzák az adatokat. Például okostelefonok vagy ipari vezérlők.
- **Energiagazdálkodási stratégiák:** Az alacsony fogyasztású működés biztosítása érdekében a perifériák rövid kapcsolatokat tartanak fenn, és készenléti állapotba kapcsolnak.

Bluetooth profilok és ipari alkalmazások

A Bluetooth profilok a technológia alkalmazási területeinek szabványosított kommunikációs szabályait határozzák meg, lehetővé téve a különféle eszközök közötti interoperabilitást. Az ipari és beágyazott rendszerek esetében különösen fontos a megfelelő profilok kiválasztása és alkalmazása a hatékony és biztonságos működés érdekében.

Bluetooth profilok áttekintése

- **GATT (Generic Attribute Profile):** Az egyik legfontosabb Bluetooth LE profil, amely az eszközök közötti adatcserét strukturálja, főként szenzoradatok és vezérlőparancsok továbbítására.
- **A2DP (Advanced Audio Distribution Profile):** Hangátvitelhez használt profil, mely ipari kommunikációban ritkábban, de speciális multimédiás megoldásoknál előfordulhat.
- **HFP (Hands-Free Profile):** Telefonos kihangosító rendszerekben használt, ipari környezetben ritkábban alkalmazott profil.
- **Egyéb profilok:** HID (Human Interface Device) például ipari kezelőpanel eszközökön, SPP (Serial Port Profile) régebbi, soros kommunikációra alapuló alkalmazásokhoz.

Ipari alkalmazások és Bluetooth profilok

- **Szenzornetworkök és adatgyűjtés:** A GATT profil segítségével szenzorokból származó adatokat gyűjtenek be, például hőmérséklet, páratartalom vagy gépi állapotinformációk monitorozására.
- **Ipari vezérlőrendszerek:** Bluetooth kapcsolaton keresztül történő vezérlés és diagnosztika, például gépek, robotok vagy beágyazott vezérlők között.
- **Egészségügyi és biztonsági eszközök:** Munkahelyi egészségügyi monitorok, védőeszközök, amelyek Bluetooth kapcsolaton keresztül továbbítanak adatokat központi rendszereknek.
- **Kollaboratív robotika:** Az ember-robot együttműködés megkönnyítésére szolgáló kommunikáció, ahol a Bluetooth profilok szerepet játszanak a gyors és megbízható adatcsere biztosításában.

Profilok implementálása beágyazott rendszerekben

- **Firmware és stack támogatás:** A különböző Bluetooth profilok implementálása az adott mikrokontroller vagy rendszer szoftveres környezetében (például Zephyr RTOS, Nordic SDK).
- **Kompatibilitás és szabványosítás:** A profilok helyes implementálásával biztosítható a különböző gyártók eszközeinek interoperabilitása és a későbbi bővíthetőség.
- **Biztonsági megfontolások:** A profilok biztonsági beállításainak kezelése, például titkosítás és hitelesítés, különösen ipari környezetben kritikus a megbízható működés érdekében.

Bluetooth integrációja beágyazott rendszerekbe

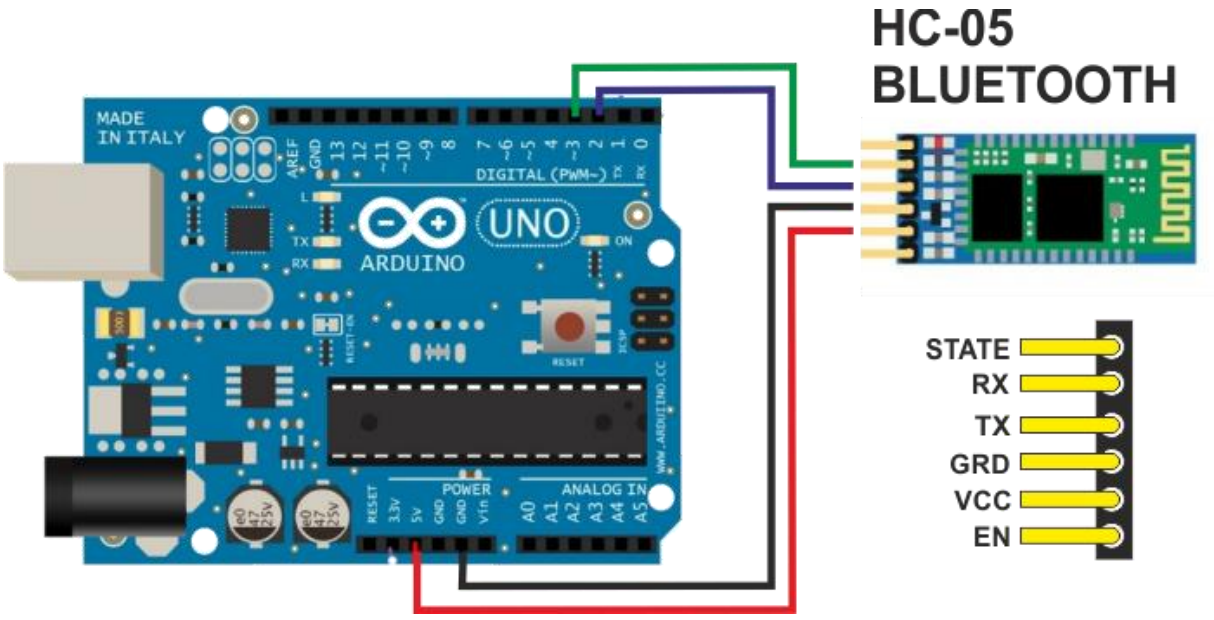
A Bluetooth technológia beágyazott rendszerekbe való integrálása kulcsfontosságú a modern IoT és ipari automatizálási megoldásokban. Az alacsony energiafogyasztású, megbízható és szabványos kommunikációs lehetőségek révén a Bluetooth különösen alkalmas mikrovezérlős környezetekben történő alkalmazásra.

Mikrokontroller platformok Bluetooth LE támogatással

- **ESP32:** Az Espressif népszerű kétmagos mikrokontrollere beépített Bluetooth Classic és BLE támogatással rendelkezik. Az Arduino és ESP-IDF környezetekben is könnyen programozható, így kiváló választás prototípusokhoz és kis fogyasztású eszközökhöz.
- **nRF52 család:** A Nordic Semiconductor nRF52 sorozata rendkívül elterjedt BLE-alapú eszközök fejlesztésére, kiváló energiahatékonysággal, kiterjedt SDK támogatással és Zephyr RTOS kompatibilitással.
- **STM32WB:** Az STMicroelectronics által fejlesztett mikrokontrollerek szintén támogatják a Bluetooth LE kommunikációt, különösen ipari és orvosi alkalmazásokban használatosak, mivel beépített rádiós egységet kínálnak.

Bluetooth stack-ek és fejlesztői környezetek

- **Zephyr RTOS:** Nyílt forráskódú, valós idejű operációs rendszer, amely kiváló BLE támogatással rendelkezik, főként ipari és IoT fejlesztésekhez. Számos platformot (pl. nRF, STM32) támogat, és modularitása révén optimalizálható.
- **Arduino környezet:** Kezdők és gyors prototípuskészítők körében népszerű, az ESP32 Bluetooth funkciói egyszerűen programozhatók az Arduino könyvtárak segítségével. Bár korlátozottabb, de gyorsan tesztelhető és demonstrálható vele a BLE kommunikáció.
- **Nordic SDK és SoftDevice:** A Nordic félvezető platformokhoz dedikált Bluetooth stack, amely pontosan szabályozott funkcionalitást kínál, stabil és biztonságos kommunikációt tesz lehetővé.
- **BlueZ Linux stack:** Fejlettebb beágyazott rendszerek (pl. Raspberry Pi, Linux-alapú edge eszközök) esetén használatos, teljes értékű Bluetooth stack, amely mind BLE, mind Classic támogatást kínál.



Hardveres és szoftveres integráció kihívásai

- **Energiagazdálkodás:** A beágyazott rendszerekben kritikus fontosságú az energiafogyasztás optimalizálása, amelyet megfelelő ütemezéssel, alvó módokkal és adatcsere optimalizálással lehet biztosítani.

- **Memória- és processzorkorlátok:** A BLE stack-ek futtatása komoly kihívást jelenthet kis memória- és számítási kapacitású eszközökön, különösen ha több szerepkört vagy párhuzamos kapcsolatot kell kezelni.
- **Interoperabilitás és kompatibilitás:** Az ipari környezetekben különböző gyártók eszközeinek együttműködése szükséges, amit a szabványos profilok helyes implementációja és a BLE stack megbízhatósága biztosít.

Bluetooth alkalmazása ipari környezetekben

A Bluetooth technológia egyre nagyobb teret hódít az ipari környezetekben is, ahol megbízható, szabványosított és vezeték nélküli kommunikációra van szükség alacsony energiafogyasztás mellett. A BLE (Bluetooth Low Energy) különösen előnyös szenzorhálózatokban, állapotfigyelésben és mobil gépek közötti kapcsolatokban.

Ipari szenzorhálózatok és adatgyűjtés

- **Vezeték nélküli érzékelők integrációja:** A Bluetooth LE ideális szenzorcsomópontok kiépítésére, mivel kis energiafogyasztás mellett képes periodikus vagy eseményalapú adatátvitelre. Tipikus alkalmazások: hőmérséklet-, páratartalom-, rezgés- és nyomásérzékelés.
- **Edge computing és adat előfeldolgozás:** Az ipari BLE eszközök gyakran képesek helyben előfeldolgozni az adatokat, csökkentve az átvitt adat mennyiségét, ezzel optimalizálva a hálózati forgalmat és az energiafelhasználást.
- **Prediktív karbantartás támogatása:** A folyamatos szenzoradat-gyűjtés és elemzés révén lehetővé válik a gépek állapotának előrejelzése és a nem tervezett leállások csökkentése.

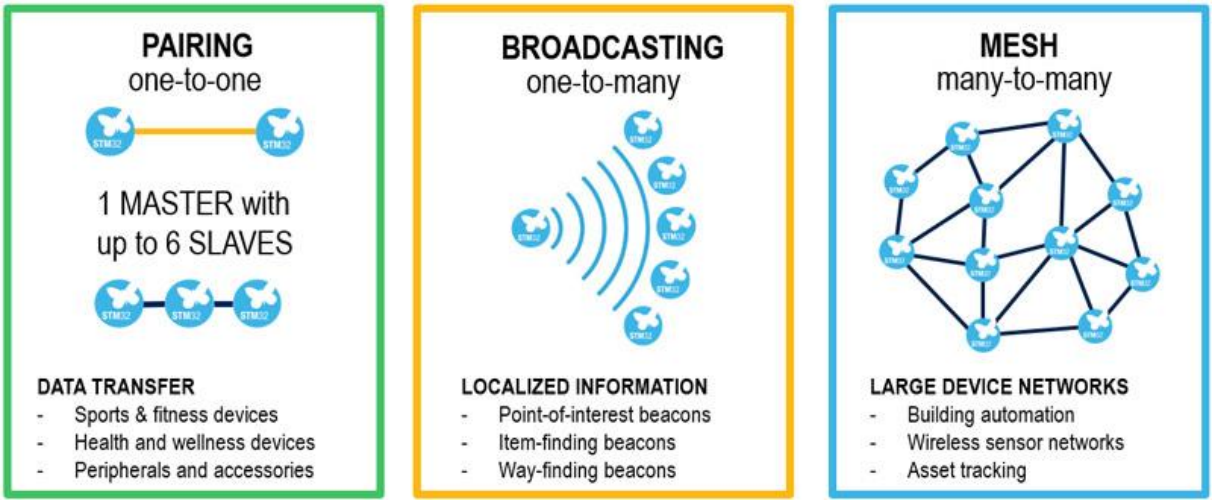
Mobil ipari gépek és eszközök közötti kommunikáció

- **Bluetooth alapú eszközazonosítás:** Ipari mobilgépek (pl. AGV-k, robotkarok) Bluetooth-on keresztül képesek azonosítani egymást és a környezetükben lévő objektumokat, lehetővé téve a dinamikus munkafolyamat-szervezést.
- **Adatcsere és szinkronizáció:** Bluetooth lehetőséget biztosít gépek közötti közvetlen adatcserére (például diagnosztikai adatok vagy munkautasítások továbbítása), akár infrastruktúra nélküli környezetben is.
- **Biztonságos párosítás és hitelesítés:** Ipari alkalmazásokban elengedhetetlen a kapcsolat biztonsága – a Bluetooth LE támogatja a titkosított kommunikációt, kulcsmenedzsmentet és eszköz-hitelesítést.

Bluetooth Mesh szerepe ipari automatizálásban

- **Skálázható kommunikációs topológia:** A Bluetooth Mesh hálózati architektúra lehetővé teszi, hogy akár több száz eszköz kommunikáljon egymással egy irányított hálózatban, ezzel biztosítva a gyárak vagy raktárak teljes lefedettségét.
- **Többcsomópontos adatforgalom:** A Mesh architektúrában minden node továbbíthat adatot mások számára, így a hálózat redundáns, és ellenállóbb a lokális hibákkal szemben.

- **Alkalmazási példák:** Világítási rendszerek automatizálása, szenzoradatok hálózati gyűjtése, gyártósori állapotfigyelés, okos táblák és kijelzők hálózati szinkronizálása.



Egészségügyi alkalmazások és személyes monitorozás

A Bluetooth, különösen a Bluetooth Low Energy (BLE) verzió, meghatározó szerepet játszik a modern egészségügyi eszközök és személyes monitorozó rendszerek fejlesztésében. A kis energiafogyasztás, biztonságos adatátvitel és a szabványosított profilok lehetővé teszik hordozható és viselhető eszközök hatékony használatát.

Viselhető eszközök és egészségmonitorozás

- **Fitnesz és életmód eszközök:** Olyan BLE-alapú eszközök, mint az okosórák és fitneszkarpántok képesek monitorozni a pulzusszámot, alvásmintát, napi aktivitást, lépésszámot és kalóriaégetést. Ezek az adatok szinkronizálhatók mobilalkalmazásokkal vagy felhőalapú platformokkal.
- **Klinikai monitorozás otthon:** Vércukorszint-mérők, vérnyomásmérők és EKG eszközök is integrálhatók Bluetooth segítségével, így a betegek adatokat továbbíthatnak orvosuknak vagy családtagjaiknak anélkül, hogy elhagynák otthonukat.
- **Adatbiztonsági szempontok:** Az orvosi adatok érzékeny volta miatt kulcsfontosságú a titkosított Bluetooth kommunikáció, különösen a GATT protokollon történő adatátvitel esetén.

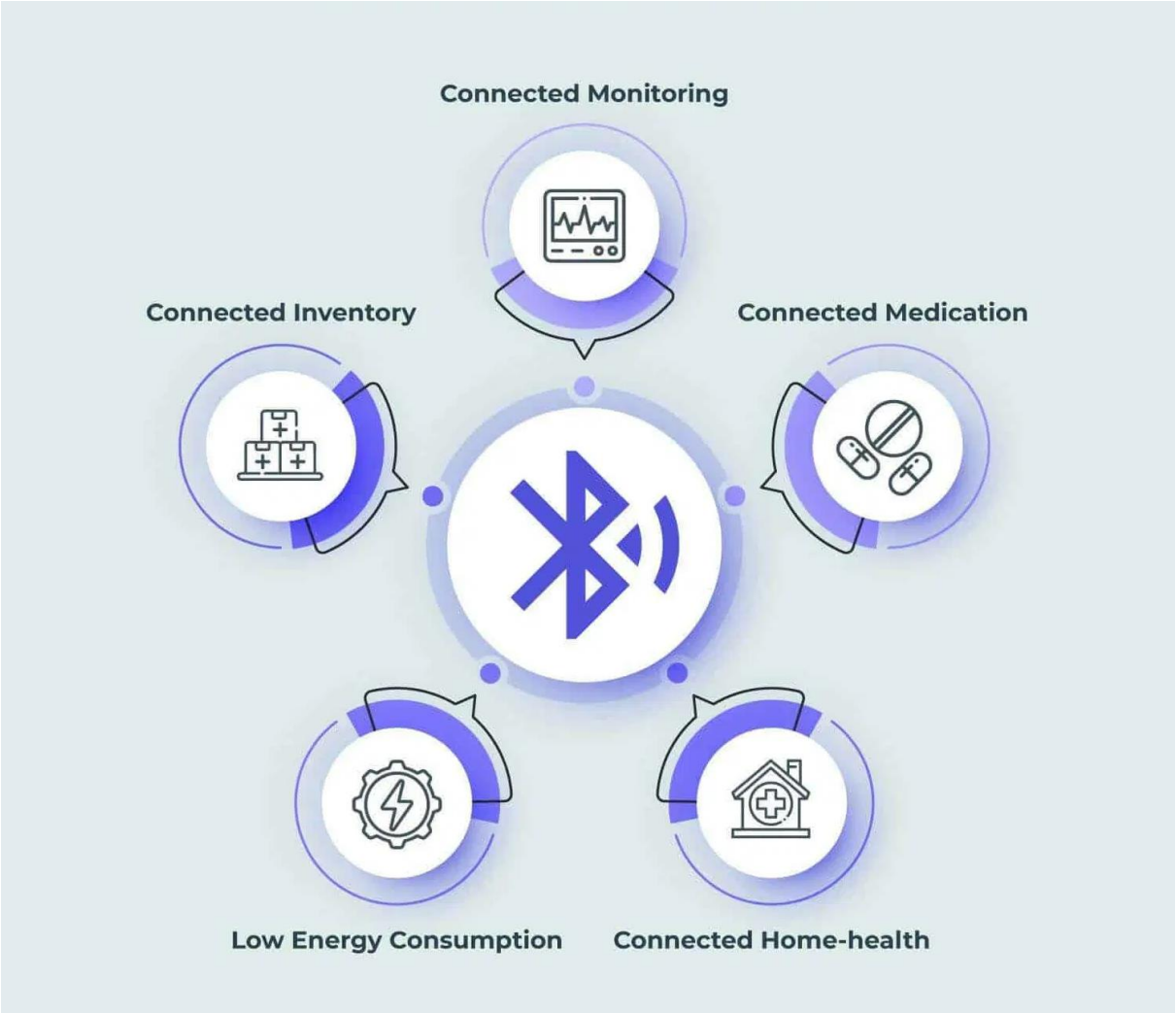
BLE szerepe orvosi eszközök szabványosításában

- **Bluetooth Health Device Profile (HDP):** A BLE-ben kialakított HDP profil szabványosított interfészt biztosít orvosi eszközök számára, amely lehetővé teszi interoperábilis működésüket különböző gyártók megoldásaival.
- **IEEE 11073 szabványcsalád:** A BLE együttműködik az IEEE 11073-as szabványokkal, amelyek az orvosi eszközök adatstruktúráit és kommunikációs protokolljait határozzák meg. Ez megkönnyíti a különböző egészségügyi rendszerek közötti adatcserét.

- **Egészségügyi alkalmazások és mobil integráció:** A BLE révén egyszerűen integrálhatók orvosi eszközök mobiltelefonokkal, így a páciens-adatok valós időben elérhetők és analizálhatók egy központi alkalmazás segítségével.

Hosszú távú megfigyelés és telemedicina

- **Kórházon kívüli ellátás támogatása:** A Bluetooth segítségével megvalósítható távoli monitorozás jelentősen tehermentesítheti a kórházi rendszereket, különösen krónikus betegek esetében.
- **Rendszeres adatküldés és riasztás:** A BLE képes folyamatos adatgyűjtésre és meghatározott küszöbértékek túllépése esetén riasztások küldésére, ezáltal növelve a páciens biztonságát.
- **Interoperabilitás egészségügyi platformokkal:** A BLE technológia lehetővé teszi, hogy a különböző gyártók által készített eszközök egységes platformra integrálódjanak (pl. Apple Health, Google Fit, vagy intézményi EHR-rendszerek).



BLE beacon technológia és kontextusérzékeny alkalmazások

A Bluetooth Low Energy (BLE) beacon-ök kis hatótávolságú adók, amelyek periodikusan sugároznak egyedi azonosítókat. Ezek az adók kontextusérzékeny alkalmazásokhoz, beltéri pozicionáláshoz, információterjesztéshez és interaktív szolgáltatásokhoz nyújtanak megbízható alapot. Előnyük a kis energiafogyasztás, alacsony költség és széleskörű platformtámogatás.

A BLE beacon működési elve

- **Adatküldés – egyirányú kommunikáció:** A beacon eszközök tipikusan csak egyirányú kommunikációt folytatnak, folyamatosan sugározzák az azonosítójukat (UUID, major, minor értékek), amelyet a környező eszközök (okostelefonok, tabletek) képesek érzékelni.
- **Időzített jelek és detektálás:** Az eszközök 100–1000 ms-onként sugároznak, észlelésükkor pedig a fogadó fél kontextusfüggő tartalmat jeleníthet meg vagy eseményt indíthat el.
- **Távolságbecslés (proximity):** A beacon jelek jelerőssége (RSSI) alapján becsülhető a felhasználó távolsága, amivel különböző reakciók válthatók ki (pl. közel, közepes, távoli zónák kezelése).

Beltéri pozicionálás és navigáció

- **GPS alternatívája zárt térben:** A BLE beacon technológia megbízható beltéri pozicionálást tesz lehetővé, ahol a GPS jel nem érhető el, például irodaházakban, bevásárlóközpontokban, repülőtereken vagy gyárakban.
- **Háromszögelés és pozíciószámítás:** Több beacon eszköz együttes használatával (trilateráció) lehetséges meghatározni a pontos felhasználói pozíciót, külön szoftveres algoritmusok segítségével.
- **Navigációs rendszerek kialakítása:** A technológia segítségével személyre szabott útvonalvezetés biztosítható épületen belül, például kórházakban a különböző osztályok között, vagy múzeumokban a látogatói útvonal mentén.

Interaktív és kontextusérzékeny szolgáltatások

- **Célzott tartalomszolgáltatás:** Üzletekben, múzeumokban vagy kiállításokon a beacon érzékelése után automatikusan megjeleníthetők promóciók, audioguide információk vagy termékleírások.
- **Okosvárosi alkalmazások:** Városi környezetben BLE beacon segítségével automatizált közlekedési információk, parkolási lehetőségek vagy közeli szolgáltatások jeleníthetők meg mobilkészüléken.
- **Biztonsági és jogosultsági rendszerek:** A technológia beléptető rendszerekben is használható, ahol a beacon érzékelése jogosultságot adhat egy adott helyiségbe való belépésre, például okosirodákban vagy ipari környezetekben.

Bluetooth Mesh hálózatok és szerepük IoT rendszerekben

A Bluetooth Mesh hálózatok lehetővé teszik a Bluetooth technológia skálázható, többcsomópontos hálózati alkalmazását, ahol az eszközök nemcsak kommunikálnak egymással, hanem továbbítják is az adatokat. Ez különösen fontos olyan IoT (Internet of Things) környezetekben, ahol nagy számú eszköz közötti megbízható és energiatakarékos adatcsere szükséges.

Bluetooth Mesh architektúra

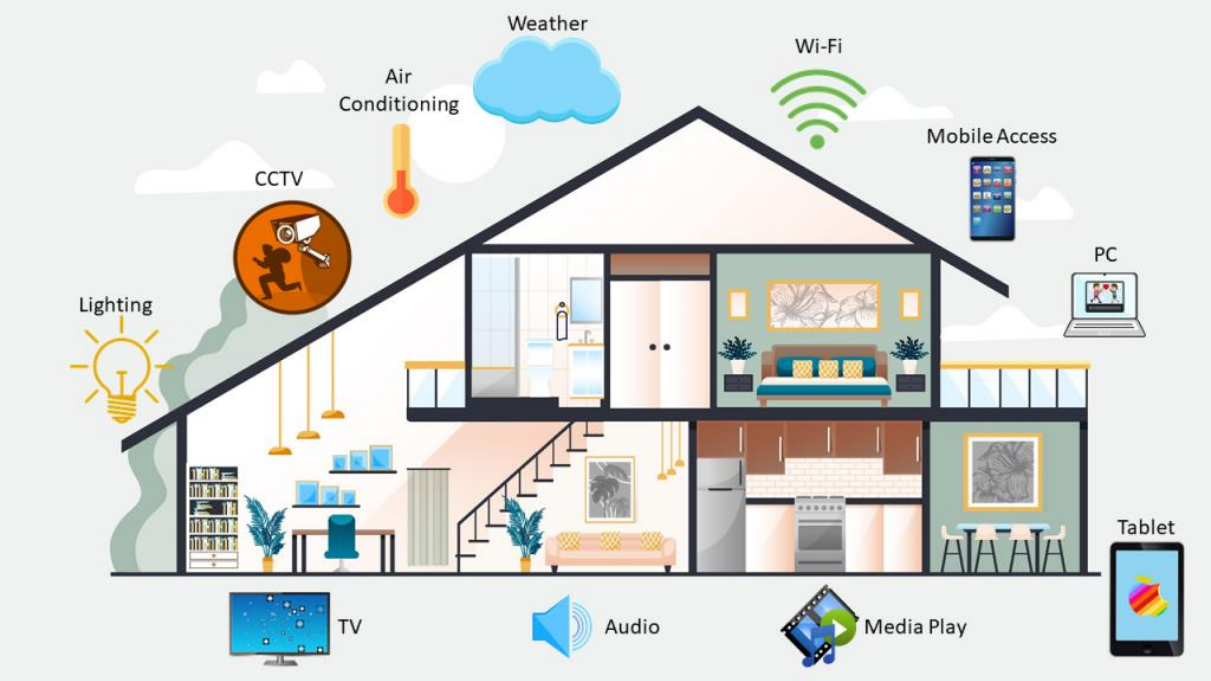
- **Flooding alapú kommunikáció:** A Bluetooth Mesh nem egy hagyományos point-to-point vagy star topológiát használ, hanem üzenetszórásra épülő technológiát, amely biztosítja az adatok megbízható célba juttatását.
- **Relay, Proxy és Friend node-ok:** A hálózat különböző szerepkörökre bontja a csomópontokat – például a Relay továbbítja az üzeneteket, a Proxy a nem-mesh eszközökkel való kapcsolatot biztosítja, a Friend pedig alacsony fogyasztású node-ok számára puffereli az adatokat.
- **Publikálás/feliratkozás modell:** Az eszközök ún. modellek és csoportok alapján kommunikálnak – például egy lámpa „feliratkozik” egy mozgásérzékelő „publikálására”, így elkerülhető a közvetlen címzés.

Előnyök és kihívások az IoT rendszerekben

- **Skálázhatóság és robusztusság:** A Mesh topológia könnyen bővíthető több száz vagy akár ezer eszközre, így kiválóan alkalmazható ipari automatizálásban, okosvárosokban vagy épületmenedzsment rendszerekben.
- **Energiagazdálkodás és teljesítmény:** Bár a Bluetooth LE energiatakarékos, a mesh működés esetén a relay node-ok energiaigénye nőhet – ezért kulcsfontosságú a szerepkörök megfelelő kiosztása.
- **Hálózati késleltetés és torlódás:** Nagy méretű hálózatokban a „flooding” miatt megnőhet a válaszidő, ami intelligens ütemezést vagy csomagszűrést igényel a hatékony működés érdekében.

Alkalmazási példák ipari és otthoni környezetben

- **Okos világítás:** A Mesh hálózatok tökéletesen alkalmasak okos világítási rendszerekben, ahol a kapcsolók, érzékelők és világítótestek egymással együttműködve reagálnak a jelenlétre, fényviszonyokra vagy időzítésekre.
- **Épületautomatizálás:** Hőmérséklet-, páratartalom- és mozgásérzékelők összehangolása Bluetooth Mesh segítségével lehetővé teszi az energiahatékony működtetést és a komfortnövelést.
- **Ipari felügyeleti rendszerek:** Szenzorhálózatok kiépítésére is alkalmas, például gépállapot-monitorozásra, ahol a node-ok továbbítják az adatokat a központi elemző rendszerek felé.



Mikrokontrollerek és fejlesztőplatformok Bluetooth LE támogatással

A Bluetooth Low Energy (BLE) alkalmazása beágyazott rendszerekben szorosan kapcsolódik a megfelelő mikrokontroller és fejlesztőkörnyezet kiválasztásához. Az elmúlt években több gyártó is integrálta a BLE támogatást saját termékeibe, megkönnyítve az alacsony fogyasztású, vezeték nélküli rendszerek fejlesztését.

Fejlesztői eszközök és keretrendszerek

- **Arduino és PlatformIO:** Ezek a fejlesztői környezetek egyszerű, gyors prototípusfejlesztést tesznek lehetővé, támogatva az olyan modulokat, mint ESP32 vagy nRF52. A BLE könyvtárak széles választéka elérhető ezekhez.
- **Zephyr RTOS:** Egy nyílt forráskódú, real-time operációs rendszer, amely kiemelkedő BLE stack integrációt biztosít (pl. Bluetooth Mesh támogatással), különösen az ipari alkalmazások számára.
- **nRF Connect SDK:** Nordic saját fejlesztőkörnyezete, amely magas szintű eszköztámogatással és BLE-profil implementációkkal segíti a fejlesztést.

Hardverintegráció és energiaoptimalizálás

- **Energiagazdálkodási technikák:** Alvó módok, interrupt-alapú ébresztések és rádiómodul vezérlés segítik a mikrokontrollerek energiafogyasztásának minimalizálását BLE kommunikáció során.
- **Perifériák kezelése BLE-vel:** Szenzorok, aktuátorok és egyéb beágyazott eszközök integrálása BLE-n keresztül megkívánja a perifériák és a kommunikációs réteg összehangolt működését.

- **PCB-tervezési szempontok:** Antennatervezés, elektromágneses zavarvédelem és tápellátási stabilitás kulcsfontosságú a BLE-s eszközök megbízható működéséhez.

Bluetooth stack-ek és szoftveres implementációk beágyazott rendszerekhez

A Bluetooth funkcionalitás implementálása nemcsak a hardveres támogatást, hanem egy megfelelő szoftveres stack meglétét is igényli, amely biztosítja a protokollrétegek működését, a kapcsolatkezelést és az adatátvitelt. A különböző fejlesztési környezetek más-más lehetőségeket kínálnak a BLE-funkciók kezelésére.

Bluetooth stack-ek felépítése és működése

- **Bluetooth klasszikus vs. Bluetooth LE stack:** A két rendszer eltérő protokollrétegekkel és működési logikával rendelkezik. A BLE esetében a GATT és ATT protokollok dominálnak, míg a klasszikus Bluetooth inkább streaming (pl. hangátvitel) célokra használható.
- **Funkcionális rétegek:** A BLE stack jellemző rétegei közé tartozik a L2CAP (Logical Link Control and Adaptation Protocol), az ATT (Attribute Protocol), a GATT (Generic Attribute Profile) és a GAP (Generic Access Profile).
- **Memória- és energiaigény:** A stack komplexitása befolyásolja a rendszer erőforrás-igényét. Kisebb mikrokontrollerek esetén előnyösebb a kompakt, optimalizált BLE stack-ek alkalmazása.

Nyílt forráskódú stack-ek és SDK-k

- **Zephyr RTOS Bluetooth stack:** A Zephyr projekt beépített BLE stack-kel rendelkezik, amely támogatja a GATT szerver/kliens szerepköröket, valamint a Bluetooth Mesh protokollt. Kiváló választás ipari vagy skálázható IoT-megoldásokhoz.
- **Arduino BLE könyvtárak:** Az Arduino platformon több BLE-könyvtár is elérhető (pl. NimBLE, ArduinoBLE), amelyek egyszerű API-kat kínálnak ESP32 vagy nRF52 eszközökhöz.
- **Apache Mynewt NimBLE:** Egy könnyű, nyílt forráskódú BLE stack, amely különösen kis energiafogyasztású eszközökre optimalizált, és támogatja az újabb BLE 5.x funkciókat is.

Stack-integráció a fejlesztési folyamatban

- **Konfiguráció és testreszabás:** A BLE stack-ek beállítása a kívánt profilok (pl. GATT szolgáltatások) és szerepkörök (pl. central/peripheral) szerint történik. Az SDK-k rendszerint példaprojektekkel és konfigurációs fájlokkal segítik a folyamatot.
- **Hibakeresés és validálás:** A BLE kommunikáció tesztelése során fontos az eszközök közötti kapcsolat stabilitásának, szolgáltatásainak és adatcseréjének vizsgálata – például snifferekkel, mobilalkalmazásokkal (pl. nRF Connect) vagy szimulátorokkal.

- **Firmware-frissítés BLE-n keresztül (DFU):** Bizonyos fejlesztőplatformok lehetővé teszik az OTA (Over-The-Air) firmware frissítést BLE-n keresztül, ami különösen hasznos IoT eszközöknél, ahol a fizikai hozzáférés korlátozott.

Bluetooth Mesh hálózat és szerepe az IoT rendszerek skálázásában

A Bluetooth Mesh technológia kiterjeszti a klasszikus Bluetooth LE korlátait, és lehetővé teszi nagyméretű, decentralizált kommunikációs hálózatok létrehozását. A Mesh-hálózat különösen előnyös az ipari automatizálásban, épületmenedzsment rendszerekben, okosvilágítási megoldásokban és más IoT-szcenáriókban, ahol több száz vagy akár ezer csomópont stabil összekapcsolására van szükség.

Bluetooth Mesh architektúra és működés

- **Hálózati topológia:** A Mesh hálózat többcsomópontos, egyenrangú (peer-to-peer) struktúrát alkalmaz, ahol az információt több „ugráson” keresztül továbbítják a végpontokhoz. A relay és proxy csomópontok segítik a hálózat kiterjesztését.
- **Publikáció-feliratkozás modell:** A Mesh nem klasszikus kliens-szerver modellt használ, hanem egy „publish-subscribe” modellt, amelyben a csomópontok témákra (pl. világításvezérlés) iratkoznak fel.
- **Biztonsági megfontolások:** A Mesh hálózatok titkosítva működnek, külön hálózati és alkalmazási kulcsokat használva a támadások elleni védekezés érdekében.

Mesh-kompatibilis eszközök és fejlesztői platformok

- **nRF52 sorozatú SoC-k:** Az egyik legismertebb és leginkább támogatott Bluetooth Mesh fejlesztési platform. A Nordic SDK-n keresztül teljes Mesh-stack érhető el.
- **Silicon Labs megoldásai:** A Simplicity Studio környezet és az EFR32 eszközök teljes támogatást nyújtanak a Mesh protokollhoz.
- **ESP32 támogatás:** Noha az ESP32 alapvetően nem natív Mesh-re készült, bizonyos fejlesztői közösségek dolgoznak nem hivatalos Bluetooth Mesh stack implementációkon ESP32-re.

Mesh alkalmazások ipari és okosrendszerekben

- **Okosvilágítási rendszerek:** A Mesh hálózat lehetővé teszi LED-lámpák központ nélküli vezérlését nagy épületekben, automatikus világításmenedzsmenttel.
- **Épületautomatizálás:** A Mesh ideális hőmérséklet-szabályozás, redőnyvezérlés, beléptetés és más funkciók decentralizált vezérlésére.
- **Ipari IoT (IIoT):** Szenzorhálózatok, gépek közti kommunikáció és karbantartási értesítések továbbítása skálázható és megbízható módon valósítható meg Mesh technológiával.

A Bluetooth technológia jövője és fejlesztési irányai

A Bluetooth folyamatosan fejlődő technológia, amely igazodik az ipari és fogyasztói igényekhez. A következő generációs fejlesztések középpontjában az adatbiztonság, alacsony késleltetés, megnövelt hatótáv, és IoT-kompatibilitás áll. Az új Bluetooth specifikációk célja, hogy a technológia alkalmas legyen a jövő intelligens rendszereinek kiszolgálására, legyen szó egészségügyről, iparról vagy közlekedésről.

Bluetooth 5.3 és a következő generációs fejlesztések

- **Alacsonyabb energiafogyasztás intelligens algoritmusokkal:** Az 5.3 verzió újításai közé tartozik az alacsonyabb energiahasználat az Adaptive Frequency Hopping (AFH) és az Enhanced Attribute Protocol (EATT) révén, amely jobb üzenetkezelést és párhuzamos adatkapcsolatokat tesz lehetővé.
- **Isochronous Channel és LE Audio:** A LE Audio bevezetése lehetővé teszi a jobb minőségű, energiatakarékos audió adatátvitelt, különösen fontos például hallókészülékek vagy több hangszóró szinkronizálása esetén.
- **Periodikus hirdetések és irányított reklám (PAwR):** Ezek a fejlesztések javítják a hatékonyságot tömeges eszközkommunikáció esetén, például okosvárosokban vagy ipari monitorozó hálózatokban.

Jövőbeli alkalmazási területek

- **Egészségügyi rendszerek:** A Bluetooth továbbra is kulcsszerepet tölt be viselhető eszközök és egészségügyi szenzorok kommunikációjában – a folyamatos adatgyűjtés és a távoli betegmegfigyelés területén.

- **Járműipar:** A BLE használható például kulcs nélküli autónyitásra (digital key), infotainment rendszerekhez és jármű-érzékelők kommunikációjára.
- **Precíziós mezőgazdaság:** Bluetooth alapú szenzorok alkalmazhatók talajnedvesség-, hőmérséklet- és tápanyagszint-méréshez, drónalapú adatgyűjtéssel kombinálva.

Integráció mesterséges intelligenciával és prediktív funkciókkal

- **Edge AI + Bluetooth:** Az alacsony fogyasztású Bluetooth chip-ek és az edge computing kombinációja lehetővé teszi, hogy a szenzoradatokat lokálisan elemezzék, csak a fontos eredményeket küldve tovább.
- **Prediktív karbantartás BLE alapokon:** Ipari eszközökbe beépített Bluetooth szenzorok segítségével a rendszer képes előre jelezni a meghibásodásokat gépi tanulás alkalmazásával.
- **Okosváros architektúrák:** A BLE beacon technológia révén pontos beltéri navigáció és dinamikus forgalomirányítás is megvalósítható nagy léptékben.

Források:

Getting Started with ESP32 Bluetooth Low Energy (BLE) on Arduino IDE, https://randomnerdtutorials.com/esp32-bluetooth-low-energy-ble-arduino-ide

Bluetooth SIG. (n.d.). *Bluetooth Technology Overview. ,* https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology

Bluetooth SIG. (n.d.). *Bluetooth Core Specification Documents. ,* https://www.bluetooth.com/specifications/bluetooth-core-specification/

MathWorks. (n.d.). *Bluetooth Protocol Stack. ,* https://www.mathworks.com/help/bluetooth/ug/bluetooth-protocol-stack.html

Arduino. (n.d.). *Arduino BLE Library Reference. ,* https://www.arduino.cc/en/Reference/ArduinoBLE

Apple Inc. (n.d.). *iBeacon Specification. ,* https://developer.apple.com/ibeacon/

Bluetooth Wikipedia, https://hu.wikipedia.org/wiki/Bluetooth

Bluetooth Architecture from Scratch, https://www.tarlogic.com/blog/bluetooth-architecture-from-scratch/

Bluetooth SIG. (n.d.). *Bluetooth* Part A. Architecture. , https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/architecture,-mixing,-and-conventions/architecture.html

Espressif ESP32 Bluetooth Architecture. , https://www.espressif.com/sites/default/files/documentation/esp32_bluetooth_architecture_en.pdf

Bluetooth SIG. (n.d.). *Bluetooth 5.3 Technology Overview*. , https://www.bluetooth.com/specifications/specs/core-specification-5-3/

nRF5 SDK - Nordic Semiconductor , https://www.nordicsemi.com/Products/Development-software/nRF5-SDK

Bluetooth mesh networking, https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/mesh/mesh-faq/ , https://www.bluetooth.com/wp-content/uploads/2019/03/Mesh-Technology-Overview.pdf

TIME – What is Bluetooth? , https://time.com/3672820/you-asked-what-is-bluetooth/

Lebara UK – Demystifying Bluetooth, https://blog.lebara.co.uk/demystifying-bluetooth-technology-a-beginners-guide-to-wireless-connectivity/

Intel – What is Bluetooth Technology? , https://www.intel.com/content/www/us/en/products/docs/wireless/what-is-bluetooth.html

Tech Pep - Exploring the Best Uses for Bluetooth in Everyday Life, https://www.technologypep.com/best-uses-for-bluetooth.html

Moxly – What can you create with bluetooth? , https://www.moxly.io/blog/exploring-the-possibilities-what-can-you-create-with-bluetooth

2.7. Védelem biztosítása az automatizált ipari termelésben

Védelem biztosítása az automatizált ipari termelésben

Kerekes Erik Gábor

Gazdaságinformatikus Bsc, kerekeserik684@mail.com

A védelem biztosítása az ipari automatizálásban egy kifejezetten fontos téma, ha Ipar 4.0-ról van szó. A dolgozat célja, hogy bemutassa a fontosabb védelmi eszközöket és módszereket, amelyek segítségével biztosítható a rendelkezésre állás, integritás és a bizalmasság. A feladat első részében bemutatásra kerül, hogy valójában hogyan is alakult ki az automatizált ipari infrastruktúra, majd ezen infrastruktúra részletezése következik. A továbbiakban az ipari automatizálást védelmi szemszögből vizsgálja meg a dolgozat. A titkosítási technológiák kerülnek bemutatásra, amely során részletezésre kerülnek a szimmetrikus, aszimmetrikus és a hibrid titkosítási megoldások, illetve ezen titkosítások alkalmazásaira is fény derül az ipari automatizálás kontextusában. A továbbiakban bemutatásra kerülnek a digitális aláírás, hozzáférés-kezelés és autentikációs mechanizmusok, amelyek biztosítják a felhasználók azonosítását és a jogosulatlan hozzáférés megelőzését. A kétfaktoros és többfaktoros autentikációs rendszerek is szerepet kapnak, hiszen manapság számos területen bizonyultak hasznosnak, és ez az iparban sincs másképp. A behatolásérzékelő és -megelőző rendszerek, mint az IDS és IPS, illetve a tűzfalak és a proxyk védelmi megoldásai is részletes bemutatásra kerülnek.

A dolgozat második felében pedig a különböző biztonsági algoritmusok és protokollok elemzésére kerül sor, hiszen ezen megoldások segítségével biztosítható a megfelelő védelem és a valós idejű védelem. Ezáltal az AES, a Diffie-Hellman kulcscsere és a TLS protokollok kerülnek bemutatásra.

A dolgozat utolsó részében két haladó védelmi megoldás kerül tárgyalás alá, amelyek a Zero Trust modell és az SD-CPS. A Zero Trust modell segítségével a hozzáférés kezelés, míg az SD-CPS rendszerrel a rendelkezésre állás biztosítható. Az említett két védelmi mechanizmus előnyei a modern ipari termelésben elengedhetetlenek a folyamatos termelés érdekében, hiszen egy-egy kiesés jelentős pénzkieséseket eredményezhet.

Kulcsszavak: ipari automatizálás, Ipar 4.0, kiberbiztonság, titkosítás, szimmetrikus titkosítás, aszimmetrikus titkosítás, digitális aláírás, hozzáférés-kezelés, autentikáció, kétfaktoros azonosítás, IDS, IPS, tűzfal, proxy, AES, Diffie-Hellman, TLS, Zero Trust, SD-CPS, M2M

1. BEVEZETÉS

Az ipari automatizálás kiemelt szerepet tölt be az Ipar 4.0-ban, amelyben a kiberfizikai rendszerek (CPS) jelentős szerepet töltenek be. Ez azonban egy hosszú fejlődési folyamat eredményeként alakult ki. A 18. század elején a gyártóipar többsége mechanikai rendszereket alkalmazott a gyártósorokon. A 20. század elején a gyártóipar rendkívül nagy mennyiségű termelést indított el a globális piaci kereslet növekedése miatt. A mechanikai rendszerek már nem tudták kiszolgálni ezt a megnövekedett keresletet az elvárt mennyiségben és minőségben.

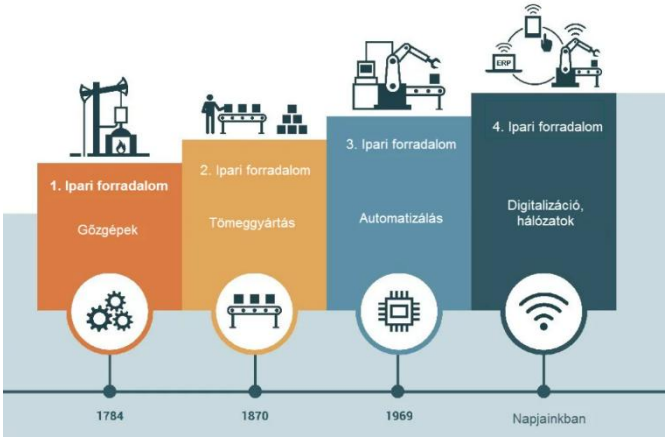
A probléma megoldására bevezették az elektronikai és információs technológiák alkalmazását. Az új technológiának köszönhetően már képesek voltak nagy mennyiségű adatot tárolni, illetve automatizáltan utasításokat kiadni az egyes gyártósoroknak. A következő ábrán az egyes ipari forradalmak jellemző gyártási technológiái szemléltethetők. (1. ábra)

Az ipari forradalmak olyan átmeneti folyamatokat foglalnak magukban, amelyek során a technológiák fejlődése a mechatronikától egészen a kiberfizikai rendszerekig (CPS) ívelt. A mechatronika, mint fogalom, az elektromos, elektronikai, vezérlési és számítástechnikai mérnöki tudományok integrációját jelenti. Ezen technológiák ismerete magas szaktudást igényelt, ami magas költségekhez, illetve a különböző szaktudományok közötti hiányos megértéshez vezetett.

Az említett problémák leküzdése érdekében a 20. században bevezették a CPS-t. A technológia általában három fő elemből épül fel: ezek az érzékelők, a beavatkozók (más néven aktuátorok), valamint a vezérlők. Működésük segít csökkenteni az üzemeltetési költségeket, és optimalizálja az adatfeldolgozási időt.

Az automatizálás fontossága kiemelt szerepet kapott a megnövekedett termelési igényeknek köszönhetően. A CPS-rendszerek szoros kapcsolatban állnak a fizikai világgal, ezért jelentős célpontjai lehetnek a különböző kibertámadásoknak. Ezen rendszerek valós idejű adatfeldolgozást és automatizált döntéshozatalt végeznek, amelyek kibertámadás esetén jelentős károkat okozhatnak. Ezek a károk érinthetik mind a digitális, mind a fizikai teret. Például egy sikeres támadás egy teljes gyártósor leállását is eredményezheti.

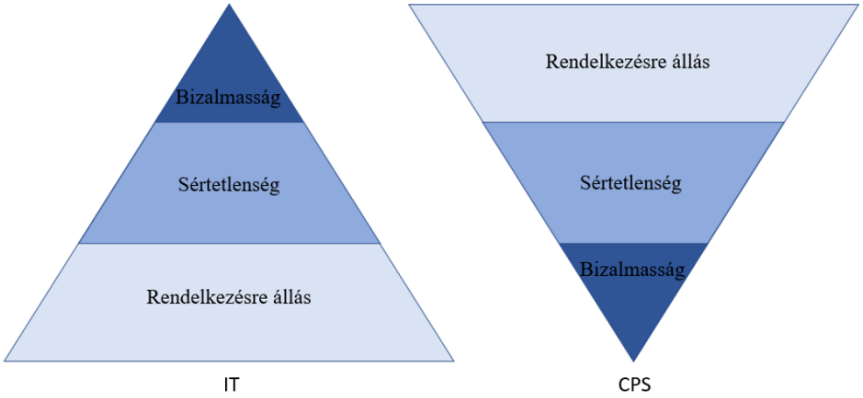
Az automatizált gyártást támogató CPS-rendszerek védelme összetett kihívást jelent, amely magában foglalja a kriptográfiai technikákat, a hálózati védekezési stratégiákat és a fejlett biztonsági algoritmusok alkalmazását. [1]



1. ábra: Ipari forradalmak technológiai alakulása grafikusan ábrázolva.
(https://blog.eplm.hu/4-ipari-forradalom/)

2. A VÉDEKEZÉS ESZKÖZEI ÉS MÓDSZEREI

A hagyományos IT-rendszerekhez képest a CPS-rendszerek területe viszonylag új, technológiai és védelmi szempontból pedig kevésbé fejlett. Az általános informatikai rendszerek elsősorban adatfeldolgozási és kommunikációs feladatokat látnak el, ezzel szemben a CPS-rendszerek a fizikai és a digitális világ közötti hidat képezik.



2. ábra Biztonsági prioritás az IT-ban és a CPS-ben.
(Saját szerkesztésű ábra.)

Tulajdonságaik közé tartozik az érzékelés, feldolgozás, döntéshozatal és beavatkozás, ezek révén kiemelkedően fontos szerepet töltenek be a modern ipari automatizálásban.

Továbbá, míg a hagyományos IT-biztonságban az adatbizalmasság az elsődleges szempont, vagyis annak megakadályozása, hogy illetéktelenek hozzáférjenek a bizalmas információkhoz, addig a CPS-rendszerek esetében a rendelkezésre állás élvez prioritást. Ez különösen fontos az ipari automatizálásban, ahol a termelés mennyisége és minősége nagymértékben függ a rendszerek folyamatos működésétől. (2. ábra)

Kiemelten fontos foglalkozni e rendszerek támadhatóságával, mivel egy esetleges kibertámadás komoly kockázatot jelenthet nemcsak a digitális térre, hanem a fizikai világra is, a különböző vezérlőkön keresztül.

Az iparban alkalmazott CPS-komponensek életciklusa jelentősen hosszabb, mint a hagyományos IT-eszközöké, míg utóbbiak jellemzően 3–5 évig használatosak, a CPS-komponensek akár 15–30 évig is működhetnek. Ez a hosszabb élettartam számos biztonsági kihívást hordoz magában. Ilyen lehet például az elavult szoftverek használata, amelyekre már nem érkezik frissítés ezek pedig súlyos biztonsági réseket rejthetnek.

A folyamatos használat, amelyet ezek a rendszerek az ipari automatizálás során produkálnak, jelentős karbantartási kihívásokat eredményez. Mivel gyakran a hét minden napján, megszakítás nélkül üzemelnek, az infrastruktúrájuk nem lett a gyakori frissítésekre optimalizálva. [2]

2.1. Titkosítás

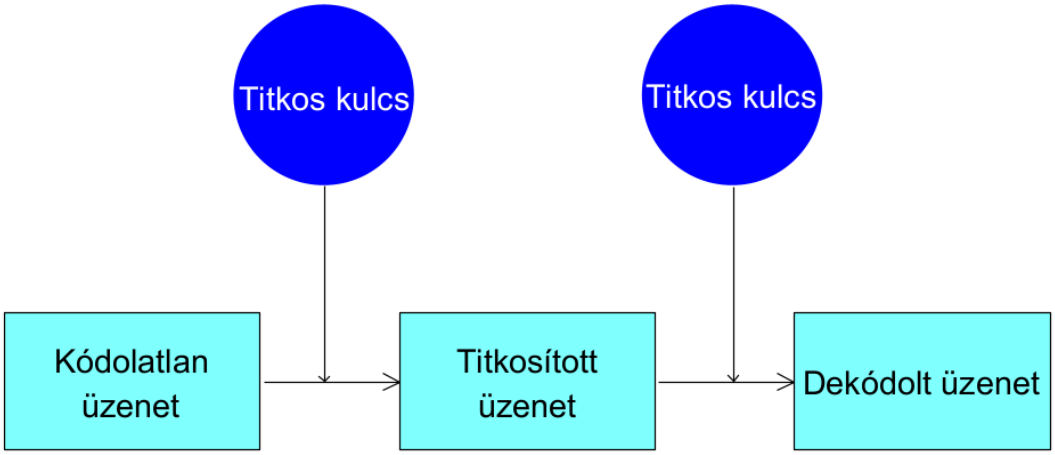
Az ipari automatizálásban alkalmazott CPS-rendszerek egyik alappillére az adatok biztonságos kezelése az egyes komponensek között. Mivel ezek a rendszerek sok esetben valós idejű adatkommunikációt folytatnak az elemek között legyen szó a szenzorok és a vezérlőegységek, vagy a vezérlőegységek és a beavatkozók közötti adatáramlásról, az információk megfelelő titkosítása kiemelten fontos. A titkosítás lehetővé teszi, hogy egy esetleges adatforgalmi lehallgatás során a kibertámadók ne tudják értelmezni az üzeneteket, így biztosítva, hogy kizárólag az arra jogosult felek férhessenek hozzá az adatokhoz.

2.1.1. Szimmetrikus titkosítás

A szimmetrikus titkosítás vagy más néven az egykulcsos titkosítás a mai titkosítási metódusok közül az egyik legrégebbi, ezáltal a legelterjedtebb is. A módszer kifejezetten egyszerű mechanizmust követ, mivel egy darab titkos kulcs található meg az üzenet titkosítását szolgálva. (3. ábra)

A módszer népszerűségét az egyszerűsége, illetve a gyorsasága eredményezte. Ebből kifolyólag jelentősen alacsony számítási teljesítményt igényel, amely kifejezetten hasznos tud lenni a valós idejű adatforgalom esetén, ahol rendkívül nagy mennyiségű adatot kell valós időben titkosítani és továbbítani. Ezért az ipari automatizálásban jelentős számban alkalmazott metódus például egy PLC (Programmable Logic Controller) és egy HMI (Human-Machine Interface) közötti adatforgalom esetében. Viszont a titkosítás egyszerűségéből az is adódik, hogy egy darab kulcs szolgál a titkosításra és a dekódolásra is. A titkos kulcs megfelelő kezelése kifejezetten magas odafigyelést igényel, mivel a kulcs birtokában bárki számára olvashatóvá válik a titkosított adatforgalom.

Az egyik legelterjedtebb egykulcsos titkosítási algoritmus az AES (Advanced Encryption Standard). A mai kor tudásának megfelelően ez az egyik legbiztonságosabb titkosítási módszer, amely egyúttal széles körben használatos CPS rendszerek esetén.



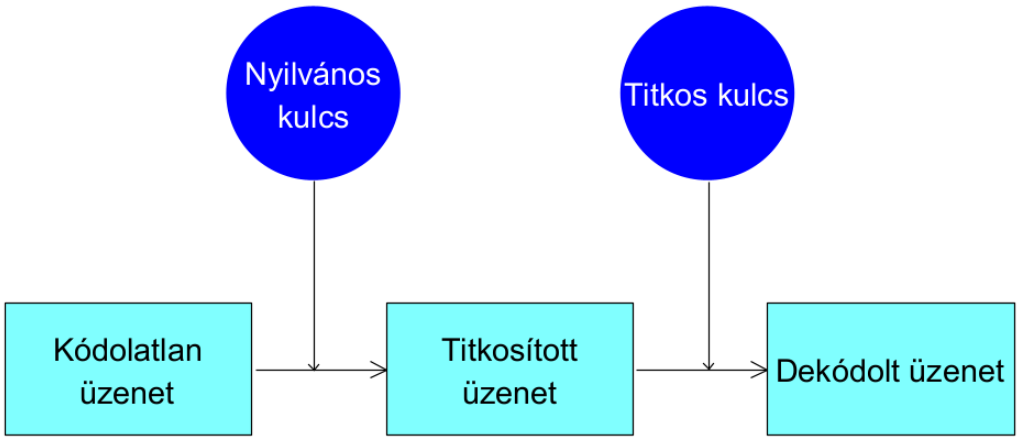
3. ábra: Szimmetrikus titkosítási elv működése.
(http://old.sztaki.hu/~sztibor/eszigno/sztaki-titk/sld002.htm - Alapján saját szerkesztésű ábra.)

2.1.2. Aszimmetrikus titkosítás

Az aszimmetrikus titkosítás vagy más néven a nyilvános kulcsú titkosítás a mai kriptográfia egyik alapköve. A módszer lényegi működése az, hogy két darab kulccsal titkosít, az egyik kulcs a nyilvános kulcs, amely bárki számára elérhető. Ezen kulccsal történik a titkosítás is, azonban az üzenetnek a dekódolása már a titkos kulccsal történik, amelyet csak a címzett ismer. (4. ábra) Ezért, ha valamely behatoló számára sikerül fognia a kommunikációt, az még nem azt jelenti, hogy képes is a tartalmát értelmezni a nyilvános kulcs birtokában.

A metódus lényegi működése alapján az már következtethető, hogy ez egy biztonságosabb módszernek bizonyul. Viszont ennek ára is van, mivel jelentősen magasabb számítási igénnyel rendelkezik a szimmetrikus titkosítással szemben. Ebből kifolyólag az ipari automatizálás területén főként csak az olyan területen használatos, ahol körülményes lenne a szimmetrikus titkosítás használata, ezért főként az eszközök hitelesítésére, azonosítására és a szimmetrikus kulcsok továbbítására használják.

A legelterjedtebb algoritmus, amely az aszimmetrikus titkosítás családjába tartozik, az RSA (Rivest, Shamir, Adleman). A módszer a matematikai faktorizáción alapul, valamint az ECC (Elliptic Curve Cryptography), amely az elliptikus görbék matematikáját használja. Az ECC használata előnyös, mivel alacsonyabb számítási igényekkel rendelkezik, ezáltal jól használható egyes CPS-komponensek között. [3]



4. ábra: Aszimmetrikus titkosítási elv működése
(https://www.okta.com/au/identity-101/asymmetric-encryption/ - Alapján saját szerkesztésű ábra.)

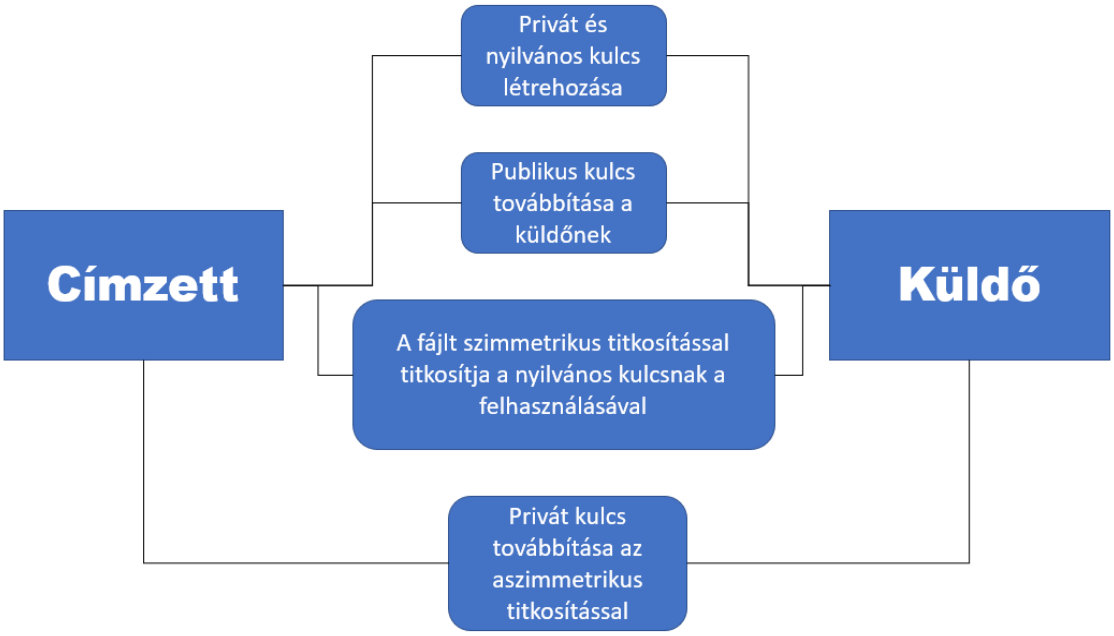
2.1.3. Hibrid titkosítás

Az imént tárgyalt két titkosítási metódus mindegyike rendelkezik előnyökkel és hátrányokkal egyaránt. A szimmetrikus titkosítás előnye, hogy rendkívül alacsony számítási teljesítményt igényel, ebből adódóan viszonylag gyors is, azonban a titkosítási kulcs megosztása nem túl gördülékeny. Ezzel szemben az aszimmetrikus titkosítás esetében megoldott a kulcscsere problémája a titkos kulcs használatával, viszont a számítási igény jelentősen magasabb, ami korlátozza használhatóságát az ipari automatizálás területén.

Erre a problémára fejlesztették ki a hibrid titkosítási módszert, amely ötvözi a szimmetrikus és az aszimmetrikus titkosítás előnyeit. A hibrid titkosítás során a titkosítás folyamata úgy zajlik, hogy az aszimmetrikus titkosítást például egy vezérlő és egy szenzor közötti kommunikáció során csak a kulcscsere idejéig alkalmazzák. A titkos kulcs sikeres megosztása után a rendszer áttér szimmetrikus titkosításra az alacsony számítási igény és a gyorsaság érdekében. (5. ábra)

Az ipari automatizálásban a hibrid titkosítás egyik alkalmazási módja például az, amikor távoli hozzáférés során firmware- vagy szoftverfrissítést kell végrehajtani. E folyamatok manipulációja külső beavatkozás révén jelentős gyártási károkat vagy kieséseket okozhat.

A hibrid titkosítási családba tartozik például a TLS (Transport Layer Security), valamint az elődje az SSL (Secure Socket Layer). Ezen protokollok a CPS területén például a felhőalapú vezérlés, diagnosztika vagy a rendszerfrissítések esetén fordulnak elő. [4]



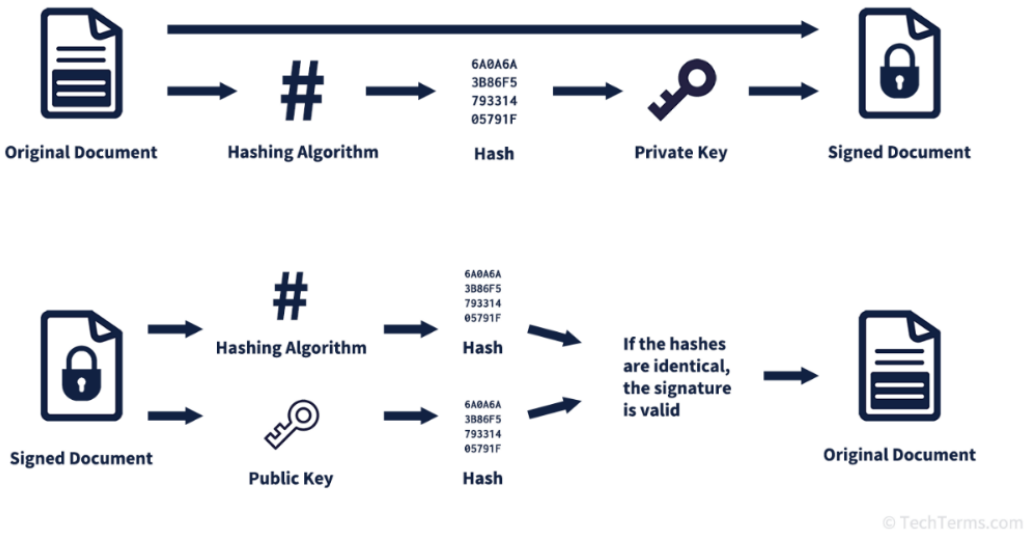
5. ábra: Hibrid titkosítási elv működése
(https://techblogs.42gears.com/hybrid-cryptography/ – Alapján saját szerkesztésű ábra.)

2.2. Digitális aláírás

A digitális aláírás kiemelten fontos szerepet játszik az automatizált kiberfizikai rendszerek védelmében, mivel biztosítja az üzenetek hitelességét, integritását, valamint az aláíró személyazonosságát. Számos területen alkalmazzák a CPS rendszereken belül, legyen szó adatkommunikációról, szoftverfrissítésről, vezérlésről vagy eszközhitelesítésről.

Ez a kriptográfiai módszer aszimmetrikus algoritmusokra épül, és a PKI (Public Key Infrastructure) rendszerekkel kombinálva biztosítja a biztonságos kulcskezelést és a digitális tanúsítványok megbízható kezelését. A módszer működésének lényege, hogy csak az ismert eszközök vagy felhasználók tudjanak kommunikálni a rendszerrel. Például egy SCADA szerver csak akkor fogad adatot az RTU-tól vagy a szenzortól, ha ezek tanúsítványa hiteles.

A digitális aláírás viszonylag egyszerű működési mechanizmussal rendelkezik. A küldő a továbbítandó üzenetből vagy parancsból egyedi hash értéket hoz létre (például SHA-256 segítségével), amelyet saját privát kulcsával titkosít – így jön létre a digitális aláírás. Ezután az üzenetet és az aláírást továbbítja a címzettnek. A fogadó fél az üzenet alapján újra kiszámítja a hash értéket, majd a kapott aláírást a küldő nyilvános kulcsával visszafejti. Ha a két hash érték megegyezik, az üzenet hitelesnek és sértetlennek tekinthető. [5] (6. ábra)



6. ábra: Digitális aláírás működési folyamatának a grafikus szemléltetése.
(https://techterms.com/definition/digitalsignature)

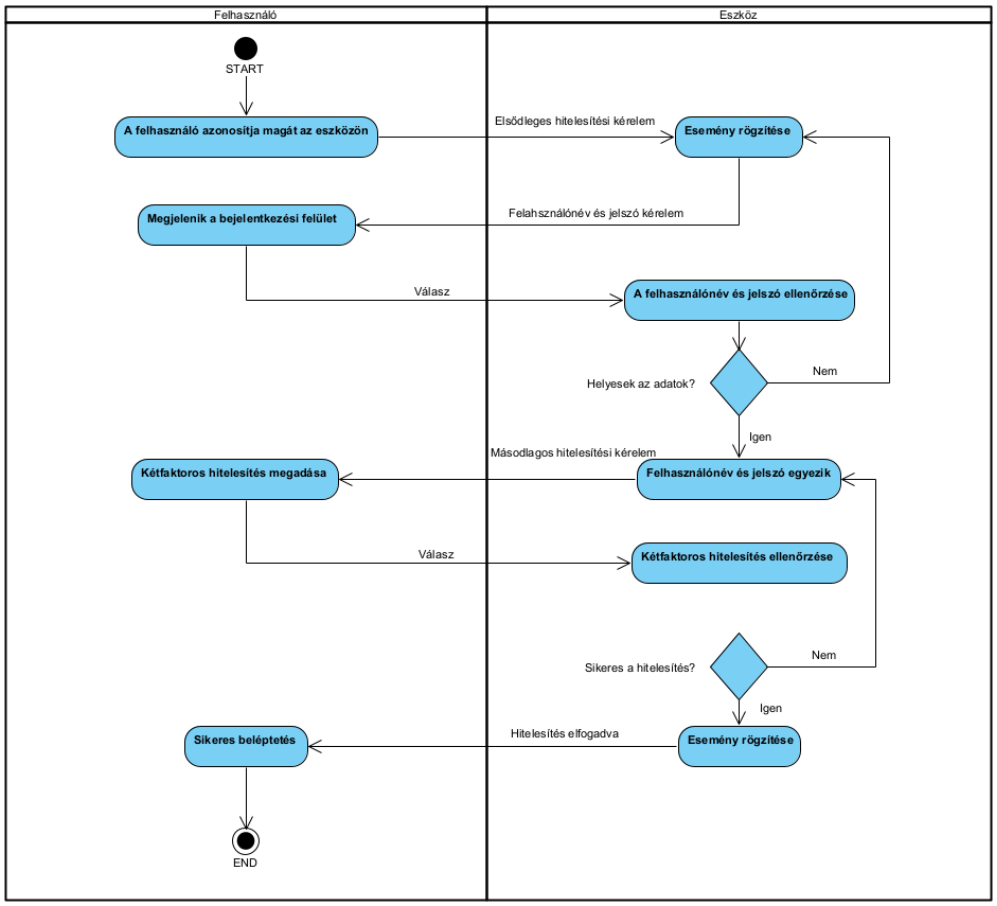
2.3. Hozzáférés-kezelés és autentikáció

Az ipari automatizálásban a CPS-komponensek között kifejezetten fontos szerepet kap a hozzáférés-kezelés és az autentikáció, hiszen ezen rendszerek valós idejű adatfeldolgozással operálnak. Ebből adódóan jelentős károk keletkezhetnek egy manipuláció során. Erre a problémára a különböző szerepkörökből adódóan szükségesek az óvintézkedések.

2.3.1. A kétfaktoros (2FA) autentikáció

Az ipari automatizált rendszerek modernizációjából, illetve az őket körülvevő számítástechnikai rendszerek összetettségéből adódóan az autentikáció kifejezetten magas figyelmet igényel, hiszen ezzel párhuzamosan a különböző támadási technikák is fejlődtek. Ezen védelmi rendszerek az ipari automatizálásban a brute-force vagy a credential stuffing jellegű támadásokat hivatottak megelőzni. Az autentikációk közül két darabot különböztetünk meg, amelyek a kétfaktoros és a többfaktoros autentikáció.

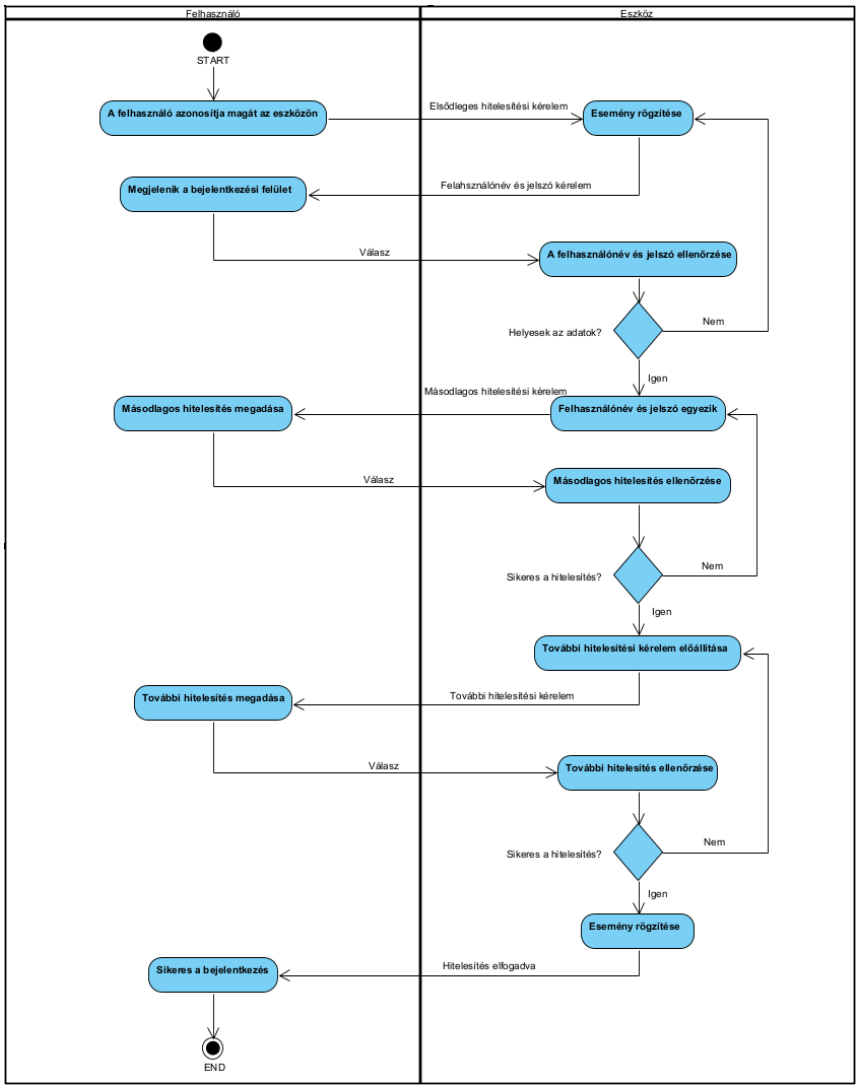
A kétfaktoros autentikáció (Two-Factor Authentication) egy olyan védelmi eljárás, amely két védelmi kaput állít a rendszer belépéséhez. Az első számú védelmi kapu lehet valamilyen jelszó vagy PIN-kód, amelyet állandóként kezelünk, illetve tartalmaz egy másodlagos védelmi kaput is, ahol valamilyen változó értéket vagy biometrikus azonosítást alkalmazunk. A változó érték lehet egy token vagy egy egyszer használatos kód, a biometrikus azonosítás alatt azt értjük, amikor arc-, ujj- vagy hangalapú azonosítás által hitelesítjük magunkat. (7. ábra) Az elv kifejezetten hatékony egy jelszószivárgást követően is, a dupla védelmi kapus megoldás miatt. Az iparban főként karbantartás során használatos a kétfaktoros autentikáció. [6]



7. ábra: Kétfaktoros hitelesítés, ahogy egy felhasználó egy adott eszközön szeretne bejelentkezni.
(Saját szerkesztésű ábra.)

2.3.2. Többfaktoros autentikáció (MFA)

A többfaktoros autentikáció (Multi-Factor Authentication) a 2FA továbbfejlesztett változata. Ezen autentikáció során nem csak kettő védelmi kaput állít a rendszer a bejelentkező fél számára, hanem gyakorlatban ez kettőnél több. A magas védelmi szint mellett, amit az elv biztosít kifejezetten hasznos egyes vezérlőrendszerek estében, amely lehet például SCADA. A védelmi kapuk feloldása során gyakran megeshet, hogy szükséges egy szokványos jelszó, egy változó token, illetve valamilyen biometrikus azonosítás a belépés sikeres elvégzéséhez. (8. ábra) Ezen kapuk felállítása után jelentősen csökkennek a támadók behatolási sikereinek az aránya.



8. ábra: Többfaktoros hitelesítés, ahogy egy felhasználó bejelentkezik egy eszközön keresztül.
(Saját szerkesztésű ábra.)

2.3.3. Hozzáférés-kezelés típusai

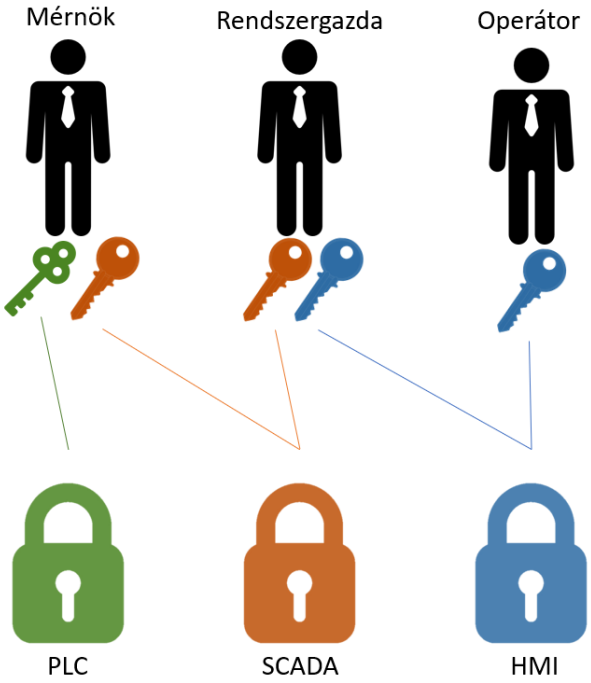
A hozzáférés-kezelés biztosítása a CPS rendszerekben szerep-alapú (Role-Based Access Control), illetve attribútum-alapú (Attribute-Based Access Control) szabályokkal történik. Segítségükkel a különböző felhasználók és eszközök csak a számukra jogosult erőforrásokhoz férhessenek hozzá, ezzel csökkentve a rendszerbe történő jogosulatlan belépést.

2.3.4. Szerepkör-alapú hozzáférés-kezelés (RBAC)

A szerepkör-alapú hozzáférés-kezelés egy átlátható és skálázható technikának örvend, hiszen segítségével nem közvetlenül kell meghatározni a felhasználókhoz tartozó jogosultságokat, hanem szerepkörönként. Ezen szerepkörök különböző csoportokra bonthatók fel például rendszergazda, mérnök vagy operátor. (9.ábra) Ezáltal egy átláthatóbb

és strukturáltabb hozzáférés-kezelést kapunk, amellyel jelentősen egyszerűsödik az ipari rendszereken belüli jogosultságkezelés.

A modell segítségével valamennyi szerepkörhöz a lehető legalacsonyabb jogosultsági szintet lehet rendelni, amely a feladatkör ellátásához szükséges. Továbbá nem csak az átláthatóságot és a skálázhatóságot hivatott elvégezni, hanem egy támadó a sikeresen feltört felhasználói fiók birtokában sem képes jelentős módosításokat elvégezni az ipari rendszeren belül.

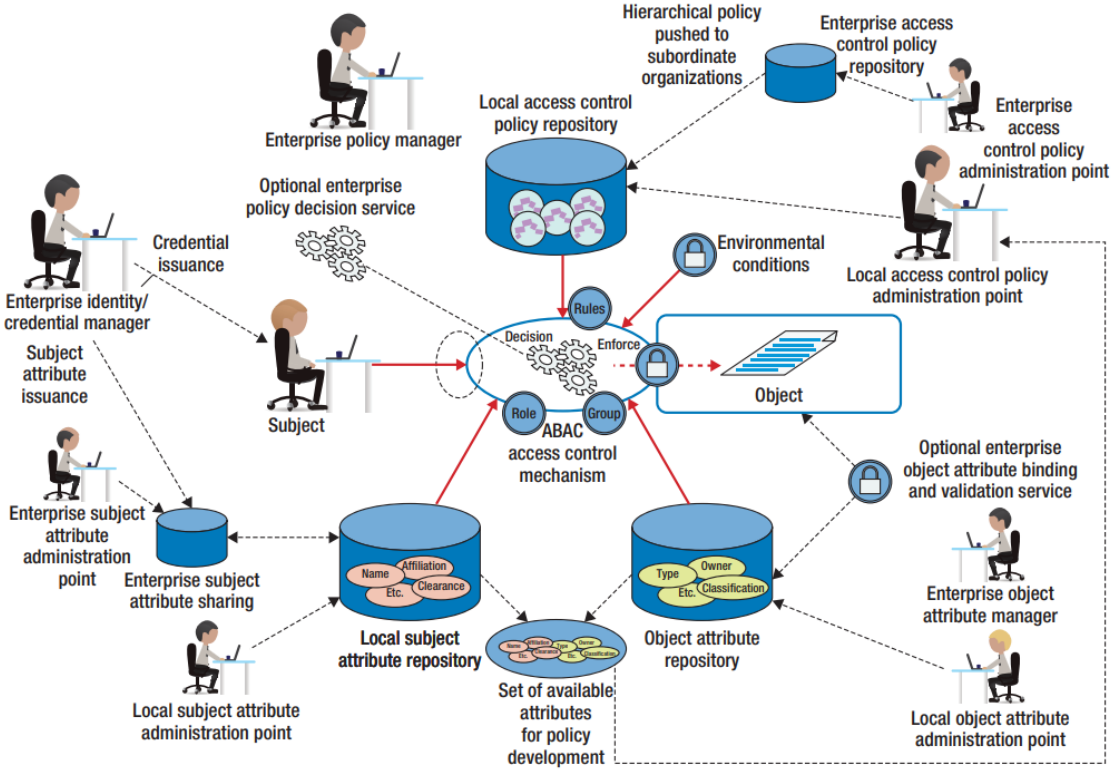


9. ábra: Szerepkör-alapú hozzáférés-kezelés egy példája a CPS-ben.
(Saját szerkesztésű ábra.)

2.3.5. Attribútum-alapú hozzáférés-kezelés (ABAC)

Az attribútum-alapú hozzáférés-kezelés egy fejlettebb és komplexebb működési mechanizmussal rendelkezik, hiszen a hozzáférés jogosultságát úgymond felülvizsgálja. A vizsgálat során nagyító alá helyezi a különböző attribútumokat. Ezen attribútumok közé tartozik a jogosultsági szint, a környezeti és az erőforrási attribútumok. A környezeti attribútum alatt a tevékenységekhez köthető időpontot, helyszínt és a hálózati állapotot vizsgálja, amelyek az elért értékek esetén sikertelen bejelentkezést eredményeznek. Az erőforrás attribútum alatt az eszköz típusát, verziószámát és állapotát vizsgálja, amely egy ipari rendszeren kívüli eszköz esetén eltérő lehet.

A modell lehetővé teszi az előre meghatározott viselkedési sémákhoz illő vizsgálatot, amely segítségével egy külső beavatkozó a biztonsági kulcsok birtokában sem képes a rendszerbe behatolni. [7] (10.ábra)



10. ábra: Attribútum-alapú hozzáférés-kezelés.
(https://www.researchgate.net/publication/361495251_A_Critical_Comparative_Study_and_Characterisation_of_Access_Control_Model)

2.4. A behatolásérzékelő és -megelőző rendszerek (IDS/IPS)

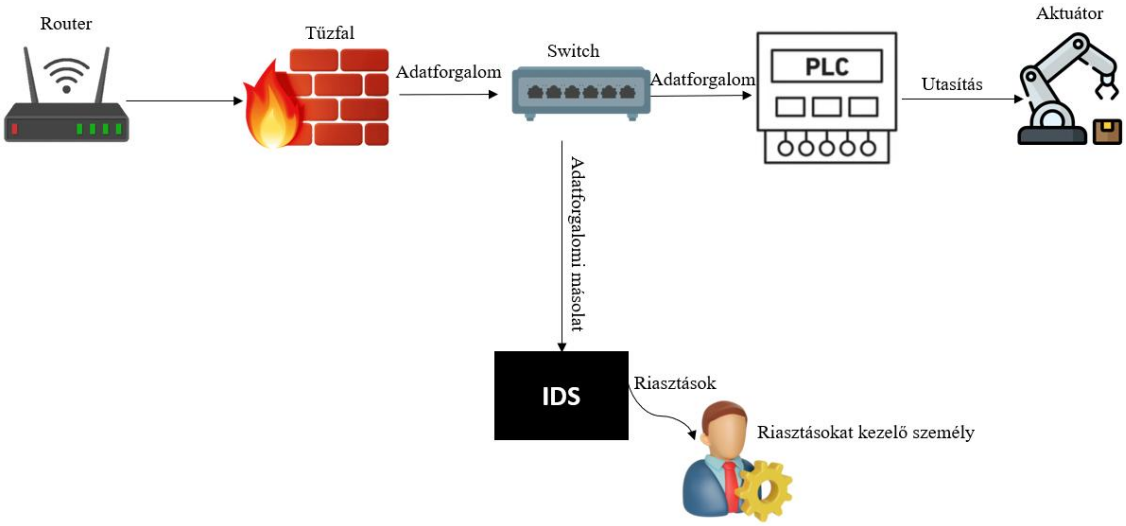
Az ipari automatizálás területén a behatolásérzékelő és behatolásmegelőző rendszerek kifejezetten fontos szerepet töltenek be, hiszen ezen rendszerek gyakran megállás nélküli működést biztosítanak, amely során egy esetleges kibertámadás kritikus következményekkel járhat.

Az ipari automatizálásban a komponensek hálózatba kapcsoltan működnek, ami biztosítja a valós idejű kommunikációt. Ezen kommunikáció adatforgalma a rendszer egy kifejezetten sérülékeny pontja, hiszen közvetlenül befolyásolhatja a gyártási tényezőket.

2.4.1. Behatolásérzékelő rendszer (IDS)

A behatolásérzékelő rendszer (IDS – Intrusion Detection System) egy olyan hálózatvédelmi megoldás, amely az adatforgalmat elemzi valós időben. Az elemzés során kifejezetten keresi a hálózati behatolási kísérleteket, ismeretlen protokollhasználatot vagy szabálytalan forgalmi mintákat. Ugyanakkor a rendszer sikeres észlelés esetén csupán jelezni képes az illetékes személynek, aki általában a rendszerüzemeltető vagy a kibervédelmi szakember. A jelzést követően a szakemberek feladata a manuális beavatkozás.

A metódus képes hardveres, illetve szoftveres módon is üzemelni, és a hálózat részeként van integrálva. Működése lehet in-line és passzív módú. In-line módban közvetlenül a hálózat részeként működik, ezáltal az adatforgalom az IDS-en keresztül kerül továbbításra. Passzív üzemmódban az adatforgalomról egyszerűen csak egy másolat készül, amit az IDS elemez a különböző gyanús támadási próbálkozások felderítése érdekében.



11. ábra: Behatolásérzékelő rendszer in-line üzemmódban való elvnek a működése.
(Saját szerkesztésű ábra.)

Az IDS kifejezetten hatékony megoldásnak bizonyul a PLC-k és a SCADA rendszerek esetében. Ezek a rendszerek ugyanis különösen érzékenyek a késleltetésre, amely különböző anomáliákhoz vezethet. Mivel az IDS képes passzív üzemmódban is működni, az egyes támadási próbálkozásokat vagy szokatlan működési mintákat képes jelezni anélkül, hogy a rendszer stabilitását befolyásolná. (11. ábra)

2.4.2. Behatolásmegelőző rendszer (IPS)

A behatolásmegelőző rendszer (IPS – Intrusion Prevention System) egy hálózatvédelmi megoldás, amely valós időben elemzi az adatforgalmat. Az IPS minden olyan tulajdonsággal rendelkezik, amelyre az IDS képes, továbbá lehetőséget biztosít valós idejű blokkolásra és beavatkozásra is. Szükség esetén képes a hálózati forgalmi szabályok módosítására a további támadások megelőzése érdekében.

Az ipari rendszerekben ez a védelmi metódus főként a PLC- és SCADA-rendszereknél figyelhető meg. Ezen eszközök kompromittálása esetén egy támadó jelentős károkat okozhat. A rendszer in-line módban működik, mivel így képes közvetlenül megakadályozni például egy rosszindulatú kód vagy ismeretlen protokoll használatát. Fontos azonban megjegyezni, hogy ezen ipari rendszerek működésére nem lehet negatív hatással az IPS használata, mivel az ipari automatizált rendszerek kifejezetten érzékenyek a késleltetésre. [2] (12. ábra)

12. ábra: Behatolásmegelőző rendszer elvének a működése.
(Saját szerkesztésű ábra.)

2.4.3. Szabály-alapú észlelés

A szabályalapú észlelés (signature-based detection) az egyik legszélesebb körben alkalmazott védelmi megoldás az IDS- és IPS-rendszerek esetén. A működési elve kifejezetten egyszerű, mivel előre betáplált támadási módszereket keres a rendszer működése közben. Ezek lehetnek szokatlan protokollok, portok, IP-címek vagy forgalmi minták.

Az ipari automatizálásban az elv működése kifejezetten hatékony, mivel a PLC- és SCADA-rendszerek adatforgalma rendszerint ritkán változik. Ezért a változó értékek kiszűrése szabályalapú észleléssel viszonylag egyszerű.

Fontos azonban megjegyezni, hogy a módszer a múltbéli eseményekre épül, ezért egyes új támadási technikák ellen nem a leghatékonyabb megoldás. A szabályrendszer definiálása és a támadási technikák felvitele a rendszerbe manuálisan történik, amely szintén az elv egyik hátrányaként sorolható fel.

2.4.4. Anomália-alapú észlelés

Az anomáliaalapú észlelés (anomaly-based detection) a szabályalapú észlelés korszerűbb megoldása, mivel itt már nagyrészt nem manuálisan történik a támadási pontok betáplálása. Működése során a rendszer először betanulja azt az adatforgalmat, amelyet a későbbiekben valós idejű elemzéssel vizsgál, majd az ettől eltérő értékek esetén avatkozik be.

Az ipari rendszerek esetében ez az elv kifejezetten hatékony, mivel az adatforgalom nagy eséllyel mindig hasonló. Ezáltal a rendszer könnyedén betanulja a viselkedési normákat, majd képes azok alapján beavatkozni.

A magas önállóságból következik, hogy egyes esetekben a rendszer téves riasztásokat adhat. Ezek az állapotok főként a karbantartási időszakokra jellemzők, amikor a rendszer viselkedése megváltozik.

Továbbá a működése nagyban hasonlít a gépi tanulásra, mivel csak hatalmas mennyiségű adat elemzése után képes felismerni az ettől eltérő értékeket.

2.5. Tűzfalak és proxyk védelmi szerepe

A tűzfalak és a proxyk által nyújtott védelmi pajzs elengedhetetlen az iparban használt automatizálási rendszerek mellett, mivel ezeknek a rendszereknek a biztonsága és megbízhatósága kiemelt fontosságú. Számos ipari automatizálási megoldás a legmodernebb technológiákat alkalmazza, ezáltal a különböző védelmi rendszerek bevezetése jelentős kihívást jelenthet a szakemberek számára.

2.5.1. Tűzfal

A tűzfalak alapvető építőkövei a CPS-rendszerek védelmi mechanizmusainak. Különféle szabályok alkalmazhatók, amelyek segítségével a hálózati forgalmat szűrni és korlátozni lehet. Fő céljuk a kiberfizikai rendszerek hálózatának védelme. A tűzfalak témakörében több típust is megkülönböztethetünk funkciójuk alapján; ezek irányulhatnak a hálózati forgalom szűrésére, a hozzáférés korlátozására, illetve a külső és belső hálózat szegmentálására.

A hálózati forgalom szűrésére olyan megoldásokat alkalmaznak, amelyek az áramló adatokat különböző paraméterek alapján szűrik. Ezen szűrések segítségével szabályozható például az egyes eszközök közötti adatforgalom. Ilyen eset lehet például a PLC-k és a vezérlőrendszerek közötti kommunikáció lebonyolítása.

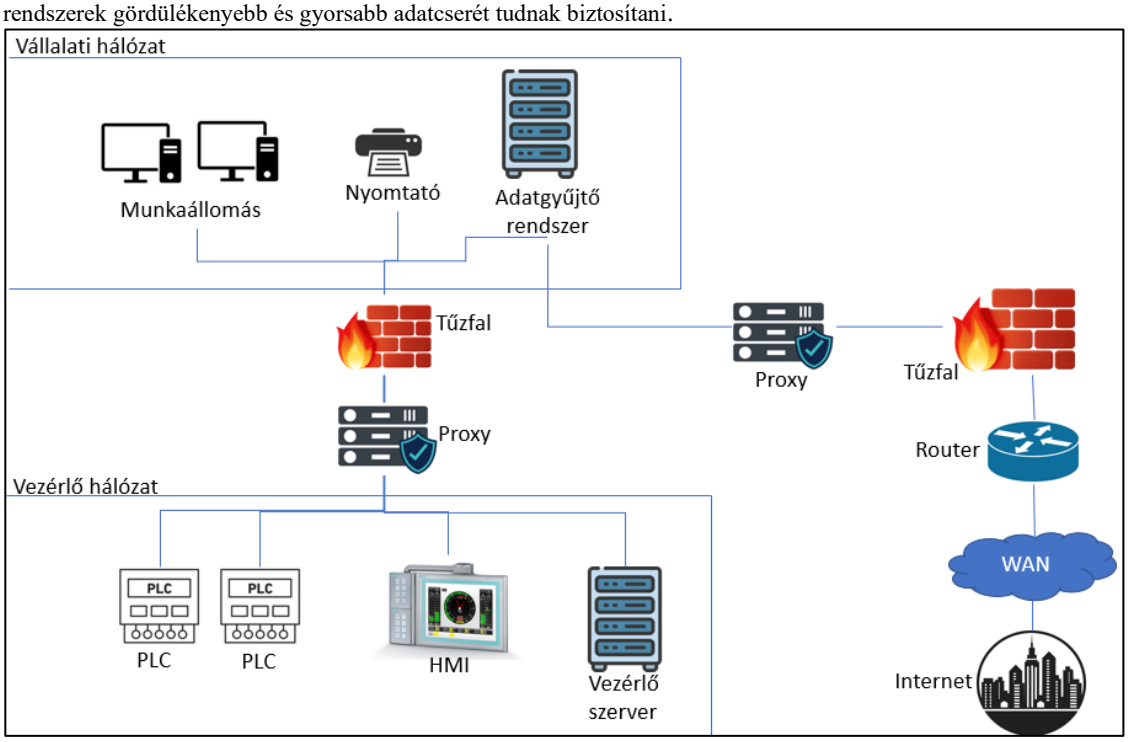
A hozzáférés korlátozása szintén a tűzfalak feladatai közé tartozik, hiszen ezek védelmet nyújtanak az ipari rendszerek komponenseihez való illetéktelen hozzáféréssel szemben.

Az iparban használt automatizált rendszerek esetében gyakran elkülönítik a belső és külső hálózatokat. A megoldás lényege, hogy egy esetleges behatolás esetén csak egy adott hálózati szegmens váljon érintetté, ne pedig az egész rendszer.

2.5.2. *Proxy*

A proxy szerverek közreműködésével biztonságosabb adatforgalom valósítható meg a CPS-rendszerek számára, mivel ezek a belső hálózat és az internet közé ékelődnek. Segítségükkel biztosítható az anonimitás, hiszen elrejtik az egyes IP-címeket, így azok nehezen visszakereshetők.

A proxy szerverek a teljesítményoptimalizálásban is szerepet játszanak, mivel az ismétlődő kéréseket eltárolják, ezáltal csökkentik a hálózat terhelését és a válaszidőt. Ennek köszönhetően az iparban használt kommunikációs rendszerek gördülékenyebb és gyorsabb adatcserét tudnak biztosítani.



13. ábra: A tűzfal és a proxy szerver elhelyezkedése egy ipari hálózatban.
(Saját szerkesztésű ábra.)

3. BIZTONSÁGI ALGORITMUSOK

Manapság az ipari automatizált rendszerek használata jelentősen megnőtt, amivel párhuzamosan nőtt azoknak az adatoknak a mennyisége is, amelyeket ezek a rendszerek feldolgoznak. Az adatok védelme kiemelt jelentőséggel bír, hiszen a szenzorok, vezérlők és aktuátorok között jelentős mennyiségű érzékeny adat kerül továbbításra.

Ezek az adatok sok esetben nyilvános hálózatokon keresztül kerülnek továbbításra, ami komoly biztonsági rést jelenthet a rendszerben. Ezt a rést hivatottak betömni a különféle titkosítási algoritmusok. Segítségükkel biztosítható a bizalmasság, az integritás és a hitelesség elve – ezek a védelem három alappillérét képezik. [8]

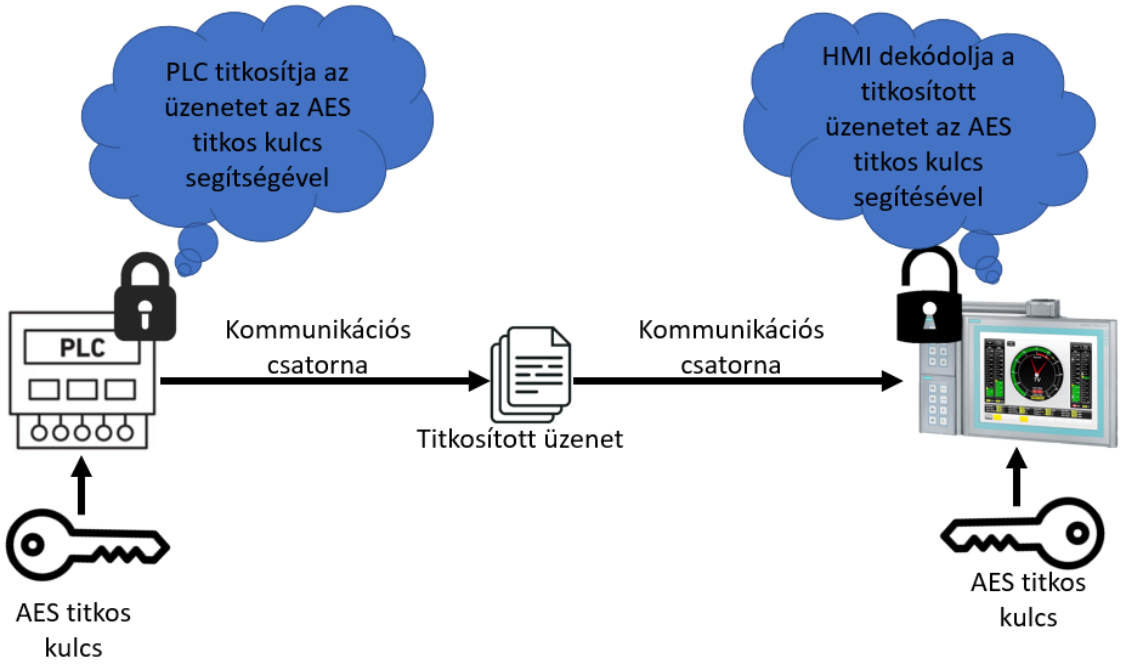
3.1. AES (Advanced Encryption Standard)

Az AES egy széles körben alkalmazott titkosítási algoritmus az ipari automatizálás területén, mivel az autentikáció, az adatbizalmasság és az adatintegritás biztosítását szolgálja. Az algoritmust elsősorban ipari vezérlőrendszerekben alkalmazzák, például PLC-kben vagy SCADA rendszerekben. Ezen rendszerek adatforgalmának titkosítása

elengedhetetlen, hiszen a kommunikáció során jelentős mennyiségű bizalmas vezérlési adat kerül továbbításra, amelyek manipulálása kritikus hatással lehet a rendszer működésére.

Az AES a szimmetrikus titkosítási módszerekhez tartozik, mivel egyetlen kulcs segítségével titkosítja és dekódolja az adatforgalmat. Az algoritmus képes 128, 192 és 256 bites titkosításra, és ebből következően a 256 bites titkosítás az egyik legbiztonságosabb a felsoroltak közül. Az ipari automatizálás területén a 256 bites AES titkosítási algoritmus a legelterjedtebb. Az algoritmus működése 14 lépéses műveletsorozatból épül fel, amely során az adatok összekeverése, elosztása és a titkos kulccsal való kapcsolat létrehozása történik. (14. ábra)

Az algoritmus kifejezetten hatékony, mivel alacsony számítási teljesítményt igényel. Az ipari rendszerekben az egyes komponensek között jellemzően alacsony számítási kapacitás figyelhető meg. Ez az alacsony számítási teljesítmény önmagában nem okozna problémát, mivel bizonyos idő elteltével az adatok titkosítása sikeresen végrehajtható lenne. Azonban ezen rendszerek hatékonyságából és működési mechanizmusából adódóan a valós idejű adatkapcsolatokhoz elengedhetetlen a gyors titkosítás. Ezért egy viszonylag alacsony számítási teljesítményt igénylő algoritmus szükséges, melyet az AES biztosít. [4]



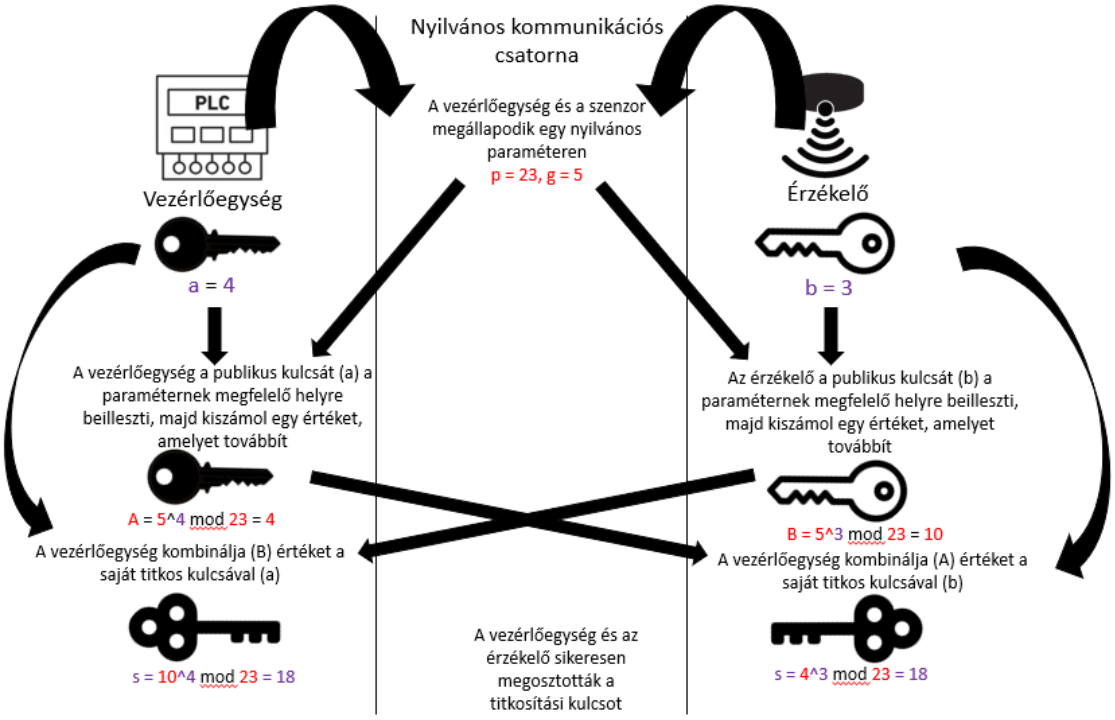
14. ábra: AES titkosítási algoritmus elv működése.
(Saját szerkesztésű ábra.)

3.2. Diffie-Hellman

Manapság az ipari automatizálásban a PLC-k, SCADA rendszerek vagy IoT eszközök közötti adatkommunikáció titkosításában kiemelten fontos szerepet játszik a Diffie-Hellman kulcscsere algoritmus. Segítségével két kommunikálni kívánó fél képes titkosítási kulcsot generálni, még akkor is, ha nem rendelkeznek előzetes titkosítással (15. ábra), ami kifejezetten fontos a Man-in-the-Middle támadásokkal szemben. Ezzel biztosítva van az érzékeny vezérlőjelek és adatcsomagok biztonságos továbbítása.

Az algoritmus továbbá képes a titkosításon túl a hitelesítést is biztosítani a rendszerek számára. Ezen hitelesítés révén a kommunikálni kívánó felek megbizonyosodhatnak a másik fél azonosságáról. Ez kifejezetten fontos, hiszen

számos olyan folyamat figyelhető meg a mai modern ipari automatizálásban, ahol az automatikus döntéshozatal történik. Ezen döntéshozatalhoz tartozó információk hamisítása különösen magas fokú figyelmet igényel a biztonságos és folyamatos működés érdekében. [9]



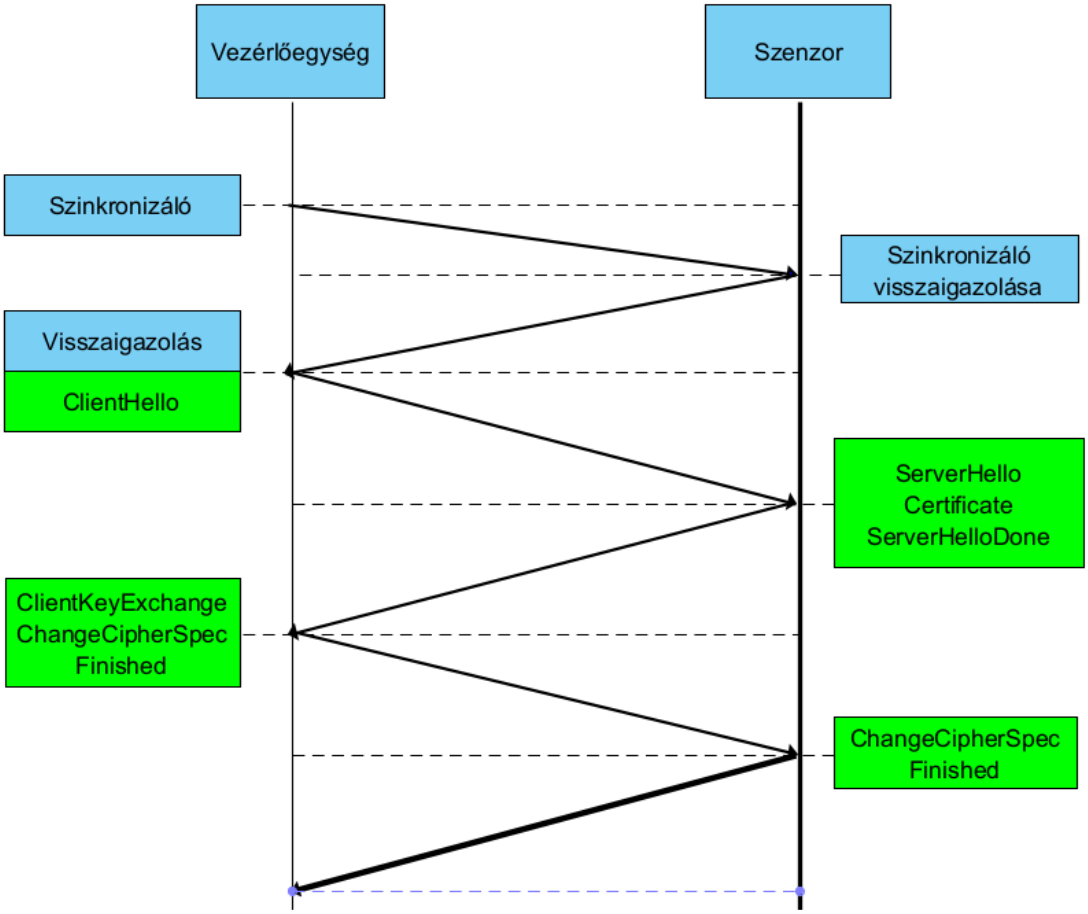
15. ábra: Diffie-Hellman kulcscsere algoritmus elv működése.
(https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange – Alapján saját szerkesztésű ábra.)

3.3. Szállítási rétegbeli biztonsági protokoll (Transport Layer Security)

A szállítási rétegbeli biztonsági protokoll (TLS) kifejezetten fontos funkcionalitást biztosít az ipari hálózatokban történő adatátvitel során. Biztosítja az adatbizalmasságot, hitelesítést és integritást két kommunikáló fél között, ami az ipari automatizálásban például egy vezérlőrendszert és egy ipari szenzort jelenthet. A protokoll két fő rétegből áll: a TLS Record és a TLS Handshake rétegekből. A TLS Record protokoll biztosítja az adatok titkosságát és sértetlenségét, míg a TLS Handshake protokoll a berendezések és központi vezérlőegységek közötti kölcsönös hitelesítést, valamint a titkosítási kulcsok egyeztetését végzi el.

A TLS az ipari automatizálás területén két további protokollal rendelkezik. Ezen protokollok a TLS Alert és a TLS Change Cipher Spec. A TLS Change Cipher Spec protokoll a titkosítási beállítások módosítását kezeli, míg a TLS Alert protokoll az esetleges biztonsági hibák felbukkanásának elemzésére szolgál.

Miután a Handshake protokoll sikeresen lejátszódott, biztonságos kommunikációs csatorna jön létre a két komponens között. Ezen a csatornán továbbított ipari vezérlők adatai, szenzorinformációi vagy naplózási eseményei a TLS Record réteg alá kerülnek. [10] (16. ábra)



16. ábra: TLS Handshake elv működése.
(Saját szerkesztésű ábra.)

4. HALADÓ BIZTONSÁGTECHNIKAI MÓDSZEREK

A távközlés, az ipari adatátviteli hálózatok és a gépek közötti kommunikáció (M2M) folyamatos növekedése és integrációja új ipari védelmi architektúrákat hoz létre, amelyek a funkcionalitáson és a rugalmasságon túl védelmi hiányosságokat is eredményeznek. Itt kifejezetten az ipari vezérlőrendszerek internetes integrációja jelent számos biztonsági kihívást; ezen esetekre fejlesztették ki a különböző haladó védelmi mechanizmusokat. Ezek a védelmi módszerek valós időben reagálnak a környezeti változásokra, ami kifejezetten hatékony tud lenni. Ezen rendszerekről elmondható, hogy dinamikusan konfigurálhatók, ami növeli a védelem minőségét, viszont nagyobb kockázatot is jelenthet. A hagyományos „periméteralapú” védelmi megoldások már nem elegendőek a nyitott, elosztott, illetve gyakran távoli hozzáférésű rendszerek védelméhez. [11]

4.1. Zero Trust modell

Az ipari automatizálás világában, ahol a kibertámadásokra érzékeny infrastruktúrák és rendszerek működnek, kifejezetten fontos a kiberbiztonság. A különböző gyártósoroktól kezdve az automatizált logisztikai rendszereken át a SCADA hálózatokig, a kibertámadásokra érzékeny és összetett rendszerek védelme egyre nagyobb kihívást jelent.

Ezen rendszerek védelme érdekében önmagában nem elegendő a peremvédelem, amely csupán a külső kapcsolatokat védi. Az olyan védelem, amely minden egyes komponensre, kommunikációra és hozzáférésre kiterjed, a zero-trust modell alkalmazásával érhető el. (17. ábra)

A zero-trust modell fő kiindulása az, hogy alapjaiban változtatja meg az eszközök közötti kommunikációt és hozzáférhetőséget. A hagyományos modellek feltételezik a megbízhatóságot, míg a zero-trust modell semmilyen körülmények között nem vallja azt. Ebből kifolyólag minden hozzáférési próbálkozást ellenőriz.

A modell öt alapelvre épül, amelyek biztosítják az ipari automatizálás területén a komponensek közötti bizalmasságot.

Az első alapelv a CPS rendszereken belül a gépek, érzékelők, vezérlők, szoftverek és hálózati eszközök automatizált kommunikációját tekinti potenciális támadási felületnek. A zero-trust modell úgy tekinti ezeket a kommunikációkat, mintha azok egy támadás során kerülnének végrehajtásra. Ezért a sikeres hitelesítés nélkül ezen kapcsolatok működésképtelenek.

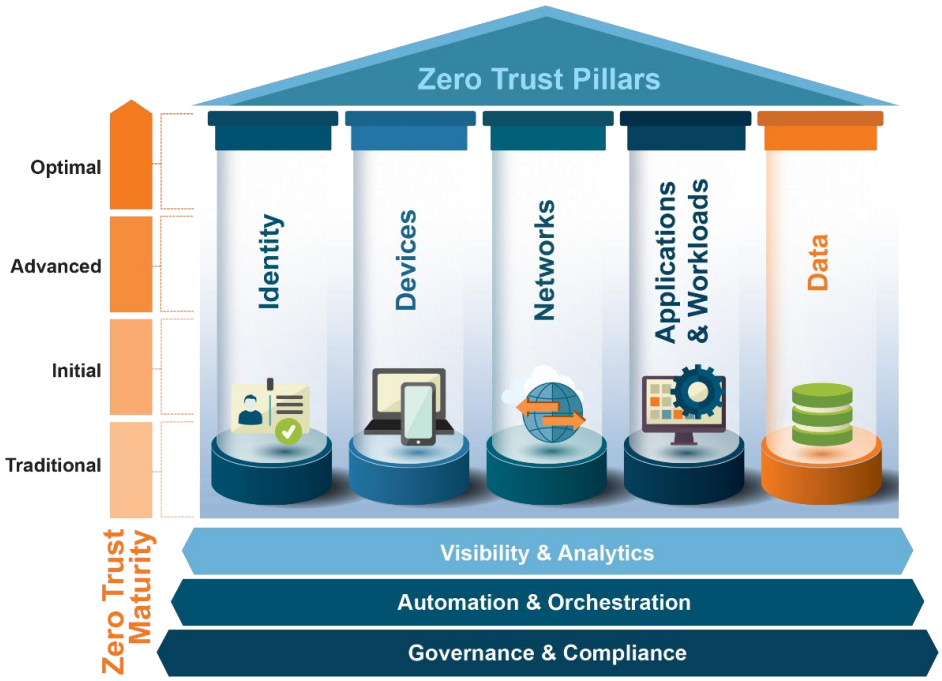
A második alapelv, hogy a CPS rendszerekben minden egyes kommunikációs csatornát, adatátvitelt és felhasználói folyamatot folyamatos ellenőrzés alatt kell tartani. Mivel a rendszer számos komponensből áll, amelyek különböző jogosultságokkal rendelkeznek, ezeken a jogosultságokon alapulva minden komponenst a szükséges legkisebb jogosultsági jogkörrel kell üzemeltetni.

A harmadik alapelv azt foglalja magába, hogy a belső hálózatban szereplő eszközöket sem lehet megbízhatónak tekinteni, hiszen egy belső támadás jelentős károkat okozhat a rendszer működésében. A zero-trust modell azt vallja, hogy minden hálózati kapcsolatot, szenzort, vezérlőt és minden más kommunikációt külső hálózatként kell kezelni.

A negyedik alapelv lényege, hogy a rendszer valós időben reagáljon a különböző eseményekre, legyen az egy komponens hibás működése vagy egy jogosulatlan hozzáférési kísérlet bizalmas információk megszerzése érdekében. Az ipari automatizálás területén különösen nagy figyelmet igényel, hiszen a fizikai eszközök szoros kapcsolati működéséből adódóan egy változás kritikus hatással lehet a rendszer működésére.

Az ötödik és egyben utolsó elv az analitikai eszközök és a gépi tanulás alkalmazását taglalja a CPS rendszerek biztonsága érdekében. Ezen eszközök segítségével valós idejű elemzések, következtetések és beavatkozások valósíthatók meg. Emellett segíti az anomáliák és a szokatlan működési minták felismerését. [12]

A zero-trust modell alkalmazása elengedhetetlen az ipari automatizálás területén, hiszen ezen rendszerek közvetlenül elemzik és avatkoznak be egyes folyamatokba. A felsorolt alapelvek segítségével minimalizálható a kockázatok és támadások sikeressége, illetve jelentősen növelhető a rendszer biztonsága.



17. ábra: Zero Trust modell 5 alappillére.
(https://www.linkedin.com/pulse/quick-case-study-zero-trust-architecture-chuck-mackey--nbt4e)

4.2. SD-CPS szerepe a biztonságban

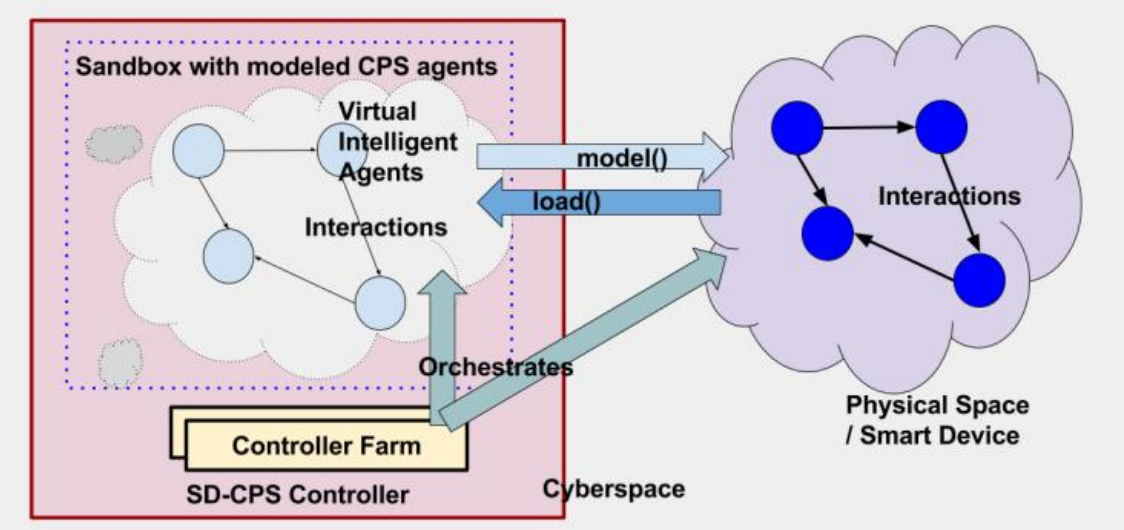
Az SD-CPS (Software-Defined Cyber-Physical Systems) egy kifejezetten fontos technológia az ipari automatizálásban, hiszen számos érzékelő, vezérlő és aktuátor található meg a rendszerben. Ezen rendszer rendelkezésre állását kifejezetten hatékonyan biztosítja, illetve a stabilitásból kifolyólag a biztonság is megemlítendő szempont, hiszen az egyes védelmi rendszerek működését is alátámasztja.

A rendszer rendelkezik egy modellezési homokozóval (Modeling Sandbox) (18.ábra), amely egy ipari automatizált rendszer esetében kifejezetten fontos. Segítségével az egyes rendszerbeállításokra lehetőséget biztosít arra, hogy egy elkülönített tesztkörnyezetben szimulálni lehessen az éles működést. Ezen beállítások lehetnek például parancsok vagy vezérlési folyamatok. Ezzel jelentősen megnöveli az éles rendszer stabilitását, amely egyben növeli a védelmi rendszerek rendelkezésre állását is, ezáltal egy biztonságosabb és megbízhatóbb működést biztosít.

Továbbá rendelkezik a rendszer egy központosított felügyelettel is, amely például képes az egyes érzékelők és vezérlők közötti adatforgalmat elemezni. Ha a rendszer talál egy szokatlan viselkedési normát vagy valamilyen normál értéktől való eltérést, akkor a jelzésen túl képes beavatkozni is.

A már korábban tárgyalt CPS rendszerek alacsony számítási teljesítményét illetően a rendszer képes folyamatos elemzést végezni, amely során figyeli az egyes komponensek kihasználtságát. Ha egy eszköz jelentősen túllépte azt a határt, amelyen túl teljesítménybeli romlások következhetnek be, vagy ha egy védelmi rendszer lassulna be, akkor képes parancsok segítségével közbeavatkozni.

A rendszer magas felügyeletéből adódóan minden kommunikációs folyamat naplózásra kerül, ennek segítségével egy esetleges hiba vagy leállás visszakövethető. Ez a tulajdonság kifejezetten fontos, mivel az ipari rendszerekben a fő szempont a rendelkezésre állás és a minőségi gyártás megőrzése. [13]



18. ábra: SD-CPS modellezési homokozó elv működése.
(https://www.researchgate.net/publication/329249724_SD-CPS_software-defined_cyber-physical_systems_Taming_the_challenges_of_CPS_with_workflows_at_the_edge)

5. ÖSSZEGZÉS

Az ipari automatizálás területén manapság a kibervédelem nem egy opcionális, hanem egy elhagyhatatlan terület. A megfelelő védelem felállítása elengedhetetlen az ipari rendszerek zavartalan működése érdekében. A korábban tárgyalt védelmi mechanizmusok, a titkosítás különböző formái, hozzáférés-kezelés, behatolásérzékelés és a Zero Trust modell létrejötte mind azt mutatja, hogy egy rendkívül magas szakértelmet igénylő területről van szó, hiszen ezen technikák megfelelő alkalmazása kihívást jelenthet.

A számos védelmi algoritmus és biztonsági protokoll szerepe jelentősen hozzájárul az ipari rendszerek zavartalan működéséhez. A szimmetrikus, az aszimmetrikus, illetve a hibrid titkosítási eljárások segítségével biztosítható az adatvédelem, autentikáció és az attribútum-alapú hozzáférés-kezelés, amely az emberi hibalehetőségek valószínűségét jelentősen csökkenti.

Kiemelt figyelmet érdemel az SD-CPS és a Zero Trust modell, hiszen segítségükkel egy dinamikus védelmi vonal biztosítható az ipari rendszerek számára. A jövőben valószínűleg ezen komplex védelmi megoldások jelenthetik a megoldást az egyre csak fejlődő kibertámadások ellen.

IRODALOMJEGYZÉK

[1] Juliza Jamaludin and Jemmy Mohd Rohani. 2018. Cyber-physical system (CPS): State of the art. In Proceedings of the 2018 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube). IEEE, 1–5. https://doi.org/10.1109/ICECUBE.2018.8610996

[2] Hynek Noll. 2024. IDS/IPS řešení pro kyberfyzikální systémy s využitím ML. Master's thesis. Czech Technical University in Prague, Computing and Information Centre. http://hdl.handle.net/10467/115634

[3] Muneer Bani Yassein, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini and Yaser Khamayseh. 2017. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of the 2017 International Conference on Engineering & Technology (ICET). IEEE, 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215

[4] Noura Aleisa. 2015. A comparison of the 3DES and AES encryption standards. International Journal of Security and Its Applications. 9, 7 (2015), 241–246. https://doi.org/10.14257/ijsia.2015.9.7.21

[5] Leonardo Babun, Hidayet Aksu and A. Seluck Uluagac. 2021. CPS device-class identification via behavioral fingerprinting: From theory to practice. IEEE Transactions on Information Forensics and Security. 16 (2021), 2413–2428. https://doi.org/10.1109/TIFS.2021.3054968

[6] Laura Vegh. 2018. Cyber-physical systems security through multi-factor authentication and data analytics. In Proceedings of the 2018 IEEE International Conference on Industrial Technology (ICIT). IEEE, 1369–1374. https://doi.org/10.1109/ICIT.2018.8352379

[7] Vincent C. Hu, D. Richard Kuhn, David F. Ferraiolo and Jeffrey Voas. 2015. Attribute-based access control. Computer. 48, 2 (2015), 85–88. https://doi.org/10.1109/MC.2015.33

[8] Tunbosun Oyewale Oladoyinbo, Oluseun Babatunde Oladoyinbo and Adeyemo Isiaka Akinkunmi. 2024. The importance of data encryption algorithm in data security. IOSR Journal of Mobile Computing and Application. 11, 2 (2024), 10–16. https://www.iosrjournals.org/iosr-jmca/papers/Vol11-Issue2/Ser-1/B11021016.pdf

[9] Yusfrizal Yusfrizal, Abdul Meizar, Helmi Kurniawan and Fhery Agustin. 2018. Key management using combination of Diffie–Hellman key exchange with AES encryption. In Proceedings of the 2018 6th International Conference on Cyber and IT Service Management (CITSM). IEEE, 1–6. https://doi.org/10.1109/CITSM.2018.8674278

[10] M. Portmann and A. Seneviratne. 2001. Selective security for TLS. In Proceedings of the Ninth IEEE International Conference on Networks (ICON 2001). IEEE, 216–221. https://doi.org/10.1109/ICON.2001.962343

[11] M. Merabti, Q. Shi and R. Oppliger. 2000. Advanced security techniques for network protection. Computer Communications. 23, 17 (2000), 1581–1583. https://doi.org/10.1016/S0140-3664(00)00243-7

[12] Saqib Hasan, Isaac Amundson and David Hardin. 2024. Zero-trust design and assurance patterns for cyber–physical systems. Journal of Systems Architecture. 155 (2024), 103261. https://doi.org/10.1016/j.sysarc.2024.103261

[13] Pradeeban Kathiravelu and Luís Veiga. 2017. SD-CPS: Taming the challenges of cyber-physical systems with a software-defined approach. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS). IEEE, 6–13. https://doi.org/10.1109/SDS.2017.7939133

2.8. Az 5G internet jellemzése , és haszna az iparban, a

Az 5G internet jellemzése , és haszna az iparban, a 6G internet lehetősége

Féléves feladat: Ipar4.0 tantárgyból

Győrvári Márton Bulcsú, [redacted], gyorvari.marton@gmail.com
Mérnökinformatikus, BSc, nappali

Készítés dátuma: 2025.05.14. World formátumban

Tartalomjegyzék:

Az 5G internet jellemzése , és haszna az iparban, a 6G internet lehetősége..... 1
Bevezetés..... 3

Az 5G technológia jellemzése 4
5G technológia haszna az iparban 6
Ipar 4.0 és 5G – az okosgyártás alapja 6
Rugalmas és skálázható gyártás 6
IoT és 5G – tömeges eszközkapcsolat 7
Logisztika és önvezető rendszerek 7
Távkarbantartás és kiterjesztett valóság (AR) 7
A Vezetéknélküli Technológia Előnyei az Ipar 4.0-ban 7
1. A Vezetéknélküli Technológia Általános Előnyei 7
Költségmegtakarítás: 7
Nagyobb Hatékonyság: 8
Méretezhetőség és Rugalmasság: 8
Jobb Együttműködés: 8
Könnyebb Hálózatkezelés: 9
3. Rugalmasság a Vezetéknélküli Technológiával 9
Méretezhetőség és Alkalmazkodóképesség: 9
Támogatás Különböző Munkavégzési Irányelvekhez és Környezetekhez: 9
Rugalmasság az Ipari Automatizálásban: 10
4. Karbantartás és Vezetéknélküli Technológia 10
Csökkentett Kábelezési és Karbantartási Költségek: 10
Prediktív Karbantartás Vezetéknélküli Szenzorokkal: 10
Távoli Felügyelet és Diagnosztika: 11
Gyorsabb Reagálás a Problémákra: 11
5. Távoli Vezérlés Előnyei a Vezetéknélküli Technológiával 11
Nagyobb Mozgásszabadság: 11
Hatékonyabb Munkavégzés: 12
Nagyobb Működési Biztonság 12
Testreszabhatóság és Kényelem: 12
Nagyobb Hatótávolság és Megbízhatóság 12
Nincs Szükség Közvetlen Rálátásra (RF Távirányítók): 13
6. Munkabiztonság Növekedése a Vezetéknélküli Technológiával az Ipar 4.0-ban 13
Veszélyek és Munkavállalói Helyzet Valós Idejű Felügyelete: 13

Veszélyes Feladatok Automatizálása: ... 13
Jobb Működési Láthatóság és Vészhelyzeti Reagálás: ... 14
7. A Hatékonyság Növekedése a Vezetéknélküli Technológiával az Ipar 4.0-ban ... 14
Valós Idejű Automatizálás és Felügyelet: ... 14
Jobb Adatcsere és Elemzés: ... 14
Fejlett Technológiák Támogatása: ... 15
Optimalizált Erőforrás-felhasználás és Csökkentett Hulladék: ... 15
Ábra 2: Vezetékes vs. Vezetéknélküli Hálózatok az Iparban ... 15
8.Ipari alkalmazási területek ... 16
• Gyártás és automatizálás ... 16
• Raktározás és logisztika ... 16
• Energiaipar ... 17
• Mezőgazdaság ... 17
6G technológia lehetőségei és jövőképe ... 17
Bevezetés – Miért van szükség a 6G-re? ... 17
A 6G céljai és jellemzői ... 17
Új technológiák a 6G-ben ... 17
Ipari és társadalmi alkalmazások ... 18
Kutatási trendek és globális fejlesztések ... 18
Ábra 3, elemzése: 6G technológia lehetőségei ... 19
A 6G társadalmi és gazdasági hatásai ... 20
A 6G társadalmi és gazdasági hatásai ... 20
Kitekintés a jövőbe – Mikorra várható a 6G bevezetése, és mit jelenthet ez a mindennapi életben? ... 21
Befejezés: ... 22
Források: ... 24

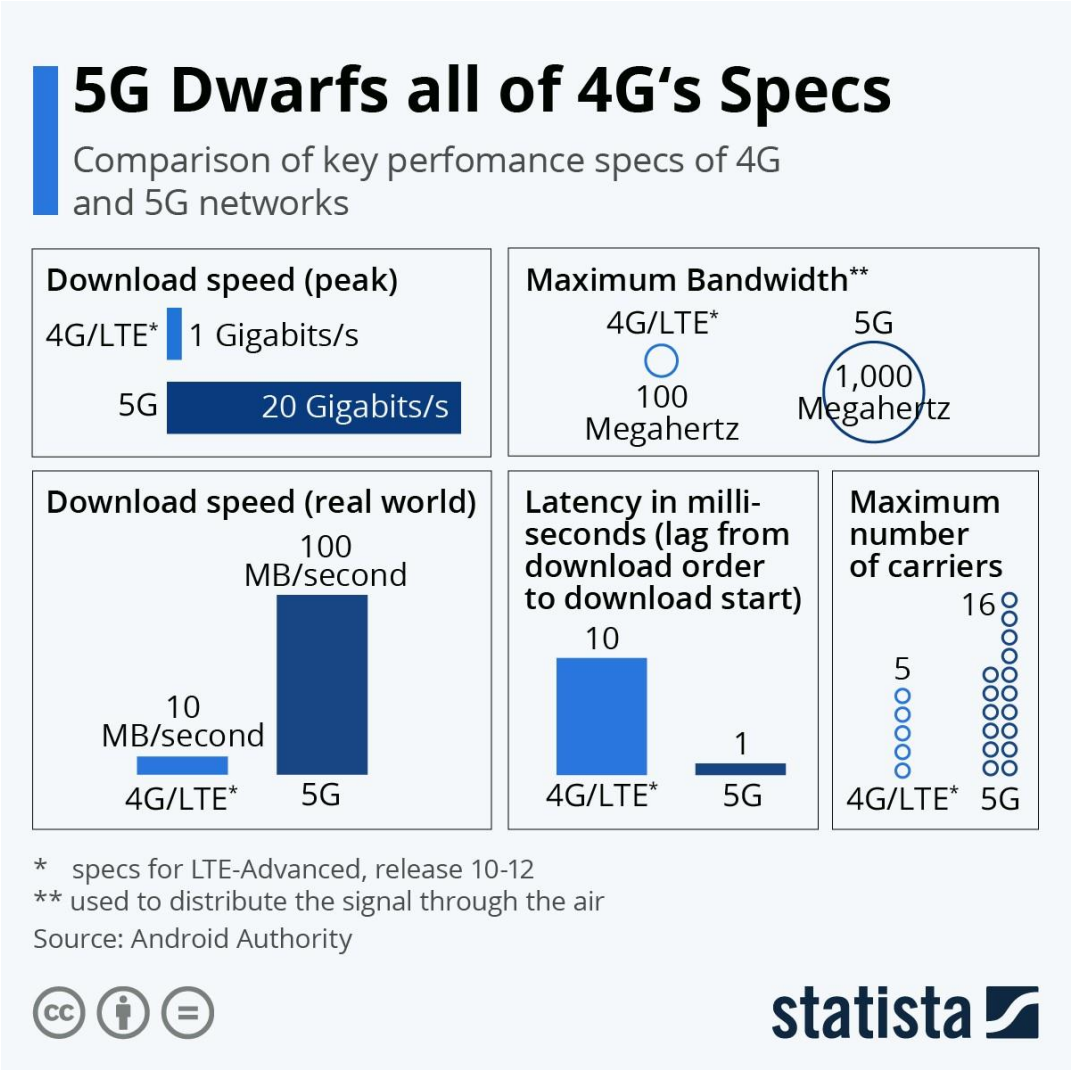
Bevezetés

A kommunikációs technológia rohamos fejlődése az elmúlt évtizedekben alapjaiban változtatta meg a mindennapi életünket és a gazdaság működését. Az 5G, azaz az ötödik generációs mobilhálózat nem csupán gyorsabb adatátvitelt jelent, hanem egy új korszak nyitányát is az ipari digitalizáció terén. Az ipar 4.0 és a dolgok internete (IoT) elterjedése olyan infrastruktúrát

igényel, amely képes kiszolgálni a valós idejű kommunikáció, a nagyfokú automatizáció és a gépek közötti adatcserék komplex igényeit – mindezt megbízhatóan, nagy sávszélességgel és minimális késleltetéssel. Az 5G technológia ezen követelményekre ad választ, lehetővé téve az okosgyárak, autonóm robotrendszerek és távoli irányítású eszközök biztonságos működését.
Ugyanakkor a technológiai fejlődés nem áll meg az 5G-nél. Már most aktívan zajlanak a 6G hálózatok kutatásai, amelyek a jövő hálózatainak új dimenzióit ígérik. Az előzetes tervek szerint a 6G nemcsak a sebesség és kapacitás szempontjából jelent majd előrelépést, hanem mélyebben integrálódik a mesterséges intelligenciával, és képes lesz olyan innovatív alkalmazások támogatására, mint a holografikus kommunikáció vagy a teljesen önálló járművek működtetése.
A dolgozat célja az 5G és a fejlődő 6G technológia részletes bemutatása, különös tekintettel azok ipari alkalmazásaira, valamint arra, hogyan alakítják át ezek a fejlesztések a termelés, logisztika és kommunikáció jövőjét.

Az 5G technológia jellemzése

Az 5G, azaz az ötödik generációs mobilhálózat a korábbi mobiltechnológiákhoz képest alapvető minőségi ugrást jelent. Míg a 4G (LTE) elsődlegesen az emberek közötti kommunikáció gyorsítását célozta meg – például a mobilinternet és videostreaming felgyorsításával –, az 5G-t már a gépek közötti kommunikáció, az ipari automatizáció és a valós idejű adatfeldolgozás igényei szerint tervezték. A cél nem csupán a gyorsabb kapcsolat, hanem egy intelligensebb, megbízhatóbb és szélesebb körűen alkalmazható hálózat megteremtése.
Az 5G egyik legfontosabb technikai jellemzője a **rendkívül alacsony késleltetés** – ideális esetben akár 1 milliszekundum –, amely elengedhetetlen a valós idejű működéshez, például önvezető járművek vagy távműtétek esetében. A másik kulcstulajdonság a **nagy adatátviteli sebesség**, amely elérheti a 10 Gbps-t is, ez közel százszorosa lehet a 4G átlagos sebességének. Emellett az 5G támogatja az **óriási eszköztömörséget**, azaz egyszerre akár **egymillió eszköz** is csatlakozhat egyetlen négyzetkilométeren belül – ez különösen fontos az okosvárosokban és gyárakban, ahol szenzorok, kamerák, robotok és más IoT-eszközök hálózatba kapcsolása történik.



1. ábra: Az 5G és 4G technológiák főbb jellemzőinek összehasonlítása.

Forrás: Statista (https://www.statista.com/chart/17506/5g-and-4g-comparison/)

Az 1. ábrán jól látható, hogy az 5G technológia az adatátviteli sebesség, a késleltetés és az eszközsűrűség tekintetében is messze túlszárnyalja a 4G-t, lehetővé téve új típusú alkalmazások például: önvezető járművek vagy ipari automatizált rendszerek elterjedését.

Az 5G hálózat három fő alkalmazási területet különít el, amelyeket eltérő technikai prioritások szerint optimalizáltak:

1. **eMBB (enhanced Mobile Broadband)** – Főként a nagy sávszélességű adatátvitelt igénylő alkalmazásokhoz, például 4K/8K videók, AR/VR (kiterjesztett és virtuális valóság) és nagysebességű mobilinternethez.
2. **URLLC (Ultra-Reliable Low Latency Communications)** – Kritikus fontosságú, minimális késleltetést és rendkívüli megbízhatóságot igénylő alkalmazásokhoz, mint az ipari automatizálás, egészségügyi robotika vagy önvezető autók.

3. **mMTC (massive Machine-Type Communications)** – Nagy számú, kis adatforgalmú IoT-eszköz csatlakoztatására szolgál, például okosmérők, szenzorhálózatok és mezőgazdasági alkalmazások.

A technológiai fejlődést lehetővé tevő háttérrendszer is jelentősen átalakult. Az 5G **új frekvenciatartományokat** használ, beleértve a milliméteres hullámokat (mmWave), amelyek nagyobb adatátviteli kapacitást biztosítanak, ám kisebb lefedettségi távolsággal – ez új típusú hálózatépítést igényel sűrűbb bázisállomás-elhelyezéssel. Az 5G-ben alkalmazott **hálózatszeletelés (network slicing)** révén pedig a szolgáltatók képesek testreszabott, elkülönített hálózati "szeleteket" biztosítani az eltérő igényű felhasználók számára, például egy gyár, egy kórház vagy egy önvezető járműflotta részére.

Az 5G nem csak a mobilkommunikáció újabb állomása, hanem egy **alaptechnológia**, amely a jövő digitális gazdaságának és iparának alappillére lesz. Alkalmazási területei túlnyúlnak a fogyasztói felhasználáson: az egészségügytől kezdve a mezőgazdaságon át a közlekedésig és az energetikai szektorig mindenhol fontos szerepet kap. Az iparban pedig különösen nagy hatással van a gyártás hatékonyságára, az energiafelhasználás optimalizálására, és a döntések gyorsaságára – mindezt a valós idejű, megbízható kommunikáció révén.

5G technológia haszna az iparban

Az 5G technológia nem pusztán a mobilhálózatok következő generációja, hanem egy komplex digitális infrastruktúra, amely új dimenziókat nyit meg az ipari alkalmazásokban. A nagy adatátviteli sebesség, az alacsony késleltetés és a hálózati szeletelés révén az 5G lehetővé teszi az intelligens gyárak, önvezető járművek, robotizált rendszerek és a valós idejű monitorozás széleskörű elterjedését.

Ipar 4.0 és 5G – az okosgyártás alapja

Az ipari digitalizáció – más néven Ipar 4.0 – egyik kulcseleme a gépek és rendszerek közötti folyamatos, valós idejű adatkommunikáció. Az 5G lehetővé teszi, hogy a gyártósorok eszközei – robotkarok, szenzorok, kamerák – vezeték nélküli módon kapcsolódjanak a központi vezérlőrendszerhez. Ez csökkenti a kábeles infrastruktúra kiépítésének költségeit, és nagyfokú rugalmasságot biztosít a gyártási folyamatok újratervezéséhez.

Az 5G egyik legfontosabb előnye, hogy **akár 1 ms alatti késleltetést** biztosíthat, így lehetővé válik az olyan időkritikus alkalmazások futtatása is, mint a valós idejű gépi látás, hibafelismerés vagy prediktív karbantartás [Ericsson, 2022].

Rugalmas és skálázható gyártás

A korábbi vezetékes vagy Wi-Fi-alapú ipari rendszerek gyakran nehézkesek voltak, ha új gépeket kellett integrálni vagy át kellett rendezni a gyártósorokat. Az 5G által biztosított **privát**

hálózatok lehetővé teszik, hogy a vállalatok saját, dedikált 5G hálózatot működtessenek zárt térben – például egy üzemcsarnokban –, amely optimalizált a saját igényeikhez.
Ez az autonóm, lokálisan irányított rendszer gyors bevezetést és skálázhatóságot biztosít. Az olyan gyártóóriások, mint a Bosch vagy a Siemens már több tesztüzemet is indítottak Európában, amelyekben privát 5G-hálózat működik [Bosch, 2021].

IoT és 5G – tömeges eszközkapcsolat

Az 5G úgy lett tervezve, hogy **egyetlen négyzetkilométeren akár egymillió eszköz** is csatlakozhasson a hálózatra (mMTC – massive Machine Type Communications). Ez rendkívül fontos az ipari IoT (IIoT) rendszerek szempontjából, ahol szenzorok ezrei monitorozzák a hőmérsékletet, páratartalmat, gépállapotokat és más paramétereket.
A szenzoradatok valós idejű elemzése lehetővé teszi a hibák korai felismerését, az automatizált beavatkozást és az energiahatékonyság növelését. Ezáltal az 5G nemcsak az üzemi hatékonyságot, hanem a fenntarthatóságot is segíti.

Logisztika és önvezető rendszerek

A logisztikai ágazat is jelentős átalakulás előtt áll az 5G révén. Raktárakban és ipari parkokban **önvezető járművek** és drónok használhatók áruszállításra, nyomon követésre, valamint térképezésre. Mindez az 5G valós idejű adatátviteli képességein alapul. Egy jól működő rendszerrel csökkenhetnek a késések, optimalizálható az árumozgatás, és nőhet az üzleti reakcióidő.
A DHL, a világ egyik vezető logisztikai vállalata, már tesztelte az 5G-alapú autonóm járműveket németországi raktáraiban [DHL, 2021].

Távkarbantartás és kiterjesztett valóság (AR)

Az 5G lehetővé teszi a **kiterjesztett valóság (AR)** alkalmazását ipari környezetben is, például távoli karbantartás vagy technikusi támogatás céljából. Egy távoli szakértő AR-szemüvegen keresztül valós időben láthatja, mit csinál egy operátor, és azonnali utasításokat adhat. Az alacsony késleltetés és a nagy sávszélesség kritikus ennek megvalósításához.
Ez különösen hasznos lehet globális cégek számára, ahol egy-egy szakterület szakértője nem tud fizikailag minden telephelyen jelen lenni.

A Vezetéknélküli Technológia Előnyei az Ipar 4.0-ban

1. A Vezetéknélküli Technológia Általános Előnyei

A vezetéknélküli technológia bevezetése számos előnnyel jár a különböző üzleti környezetekben.
Költségmegtakarítás: A vezetéknélküli rendszerek bevezetése jelentős költségmegtakarítást eredményezhet a hagyományos vezetékes hálózatokhoz képest. Elhagyható a kiterjedt

kábelezés és a kapcsolódó telepítési költségek, ami különösen előnyös lehet régebbi vagy nagy épületekben működő vállalkozások számára. Emellett a kevesebb fizikai alkatrész miatt csökkennek a folyamatos karbantartási költségek. A méretezhető megoldások hosszú távú megtakarítást biztosítanak, mivel a vállalkozás növekedésével párhuzamosan bővíthetők a hálózatok jelentős infrastrukturális átalakítások nélkül. Ipari környezetben a vezetéknélküli bevezetések akár 20-30%-os költségcsökkenést is eredményezhetnek az egyszerű konfigurációkban. A fizikai infrastruktúra csökkentése alacsonyabb erőforrás-felhasználást és potenciálisan kisebb ökológiai lábnyomot is jelent.

Nagyobb Hatékonyság: A vezetéknélküli hálózatok lehetővé teszik az alkalmazottak számára, hogy az irodán belül bárhonnan csatlakozzanak, javítva a termelékenységet és az együttműködést. Azáltal, hogy az alkalmazottak szabadon mozoghatnak a munkaterületen, miközben továbbra is hozzáférhetnek a kritikus rendszerekhez és adatokhoz, a munkafolyamatok egyszerűsödnek és csökken az állásidő. A jobb adatkommunikáció gyorsabb információátvitelt eredményez a vállalkozásokon belül, valamint partnereikkel és ügyfeleikkel. Az ipari műveletekben a valós idejű automatizálás és felügyelet révén mérhető hatékonyságnövekedés érhető el.

Méretezhetőség és Rugalmasság: Az új felhasználók, eszközök és technológiák zökkenőmentesen integrálhatók a hálózatba jelentős fennakadások nélkül. A vezetéknélküli hálózatok képesek alkalmazkodni a változó üzleti igényekhez, biztosítva a folyamatos és hatékony működést. Az eszközök könnyen hozzáadhatók vagy eltávolíthatók a hálózatból további kábelek vagy vezetékek nélkül. Ez különösen fontos a növekvő vállalkozások számára, amelyeknek gyorsan és hatékonyan kell bővíteniük hálózati infrastruktúrájukat. A vezetéknélküli hálózatok biztosítják azt a rugalmasságot és méretezhetőséget, amelyre a vállalkozásoknak szükségük van a növekedéshez és a változó technológiai környezethez való alkalmazkodáshoz anélkül, hogy jelentős költségeket vagy a vezetékes infrastruktúrával kapcsolatos működési zavarokat okoznának. A vezetéknélküli technológia ezt a rugalmasságot kínálja, lehetővé téve a vállalkozások számára, hogy zökkenőmentesen bővítsék működésüket és integrálják az új technológiákat.

Jobb Együttműködés: A vezetéknélküli hálózatok megkönnyítik az alkalmazottak számára, hogy kapcsolatba lépjenek egymással és valós időben osszák meg az információkat, függetlenül a helyszíntől. A vezetéknélküli hálózatok elősegítik az együttműködőbb munkakörnyezetet azáltal, hogy megszüntetik a földrajzi korlátokat és azonnali hozzáférést biztosítanak a kommunikációs és együttműködési eszközökhöz, ezáltal javítva a csapatmunkát és az innovációt.

Könnyebb Hálózatkezelés: A vezetéknélküli hálózatok általában egyszerűbben konfigurálhatók, felügyelhetők és karbantarthatók, mint a hagyományos vezetékes rendszerek. Csökken a kézi beavatkozás szükségessége, felszabadítva a belső informatikai erőforrásokat más fontos feladatokra. A vezetéknélküli hálózat kezelése gyakran kevésbé összetett, mint egy vezetékes hálózaté, köszönhetően a fejlett kezelőeszközöknek és a fizikai beavatkozás csökkentett szükségességének, ami hatékonyabb informatikai működést eredményez.

3. Rugalmasság a Vezetéknélküli Technológiával

A vezetéknélküli technológia számos területen növeli a rugalmasságot az üzleti és ipari műveletekben.

Egyszerű Telepítés és Bevezetés: A telepítés sokkal gyorsabb, mint a hagyományos vezetékes hálózatoknál, kevesebb hardverigénnyel és kevesebb kábelezéssel. Csökkenti az állásidőt és a fennakadásokat a beállítás során, ideális megoldás azoknak a vállalkozásoknak, amelyek kevés idő áll rendelkezésükre a rendszerek kiépítésére. A vezetékes hálózatok telepítésével járó bonyolultságok és költségek jelentős akadályt jelenthetnek a technológia bevezetésében. A vezetéknélküli technológia egyszerűsíti ezt a folyamatot, lehetővé téve a gyorsabb és kevésbé zavaró telepítéseket.

Méretezhetőség és Alkalmazkodóképesség: Az eszközök könnyen hozzáadhatók vagy eltávolíthatók a hálózatból további kábelek vagy vezetékek nélkül. A vállalkozás növekedésével a hálózat könnyen méretezhető új felhasználók és eszközök befogadására bonyolult kábelezési beállítások nélkül. Rendkívül rugalmas, lehetővé téve a módosításokat, amelyek révén a vállalkozás hatékonyan alkalmazkodhat a változó igényekhez. Támogatja az ideiglenes vagy pop-up helyszíneket a vezetéknélküli infrastruktúra egyszerű telepítésével. A vezetéknélküli hálózatok kiemelkedő méretezhetőséget és alkalmazkodóképességet kínálnak, lehetővé téve a vállalkozások számára, hogy könnyen bővítsék hálózati kapacitásukat és módosítsák infrastruktúrájukat. a változó igényekre reagálva a fizikai kábelezés korlátai nélkül.

Támogatás Különböző Munkavégzési Irányelvekhez és Környezetekhez: Támogatja a hibrid munkavégzési irányelveket, lehetővé téve az alkalmazottak számára, hogy különböző helyszínekről dolgozzanak. Megkönnyíti a "hot desking"-et a helyszűkében lévő irodákban azáltal, hogy az alkalmazottak bármelyik szabad munkaállomásról csatlakozhatnak. Lehetővé

teszi az irodák gyors átalakítását átkábelezés nélkül. A vezetéknélküli technológia kulcsszerepet játszik a rugalmas munkavégzési formák támogatásában és a munkaterület-kihasználtság optimalizálásában azáltal, hogy zökkenőmentes kapcsolatot biztosít a fizikai helytől függetlenül az irodán belül és azon kívül. A rugalmasabb munkamodellek felé történő elmozdulás olyan technológiát igényel, amely támogatja a kapcsolódást és a termelékenységet különböző környezetekben.

Rugalmasság az Ipari Automatizálásban: Lehetővé teszi a gépek és a kezelők könnyebb áthelyezését költséges átkábelezés nélkül, ami elengedhetetlen a moduláris termelési környezetekben. Megkönnyíti az új technológiák egyszerű integrálását kiterjedt kábelezés nélkül, egyszerűsítve az automatizálási folyamatokat. Támogatja a kábelekkel nem kötött robotok és automatizált rendszerek telepítését és vezérlését. Ipari környezetben a vezetéknélküli technológia rugalmassága alkalmazkodóbb termelősorokat, az automatizálás egyszerűbb integrációját és a gyorsan változó gyártási igényekhez igazodó elrendezések gyors átalakítását jelenti. A modern gyártás dinamikus természete olyan termelési rendszereket igényel, amelyek könnyen adaptálhatók és átalakíthatók. A vezetéknélküli technológia biztosítja a szükséges rugalmasságot ennek eléréséhez.

4. Karbantartás és Vezetéknélküli Technológia

A vezetéknélküli technológia hatással van a karbantartási folyamatokra és javítja azokat.

Csökkentett Kábelezési és Karbantartási Költségek: Megszünteti a kiterjedt kábelezés szükségességét, csökkentve a telepítéssel és a folyamatos fizikai karbantartással kapcsolatos költségeket. Kevesebb fizikai alkatrész van kitéve a kopásnak, ami alacsonyabb javítási gyakoriságot és költségeket eredményez. Elkerülhetők az irodai átkábelezéssel kapcsolatos költségek a bővítések vagy átalakítások során. és kevesebb potenciális meghibásodási pontot jelent a vezetékes rendszerekhez képest. A fizikai kábelek sérülékenyek, kopásra és elhasználódásra hajlamosak, rendszeres ellenőrzést és karbantartást igényelnek. A vezetéknélküli hálózatok minimalizálják ezt a fizikai infrastruktúrát, ami csökkentett karbantartási igényeket és költségeket eredményez.

Prediktív Karbantartás Vezetéknélküli Szenzorokkal: A vezetéknélküli szenzorok lehetővé teszik a gépek és rendszerek folyamatos felügyeletét, megkönnyítve a prediktív karbantartást és a valós idejű beállításokat. A szenzorok vezeték nélkül továbbíthatnak kritikus adatokat, például hőmérsékletet, vibrációt és sebességet a központi vezérlőrendszerekbe elemzés céljából. Lehetővé teszi a rendszeres, proaktív eszközellenőrzéseket, segítve az előre nem látható javítási problémák és az állásidő elkerülését. Csökkenti a kábelezéssel és a kézi

adatgyűjtéssel kapcsolatos költségeket, mivel a folyamat automatizálttá válik. Előre jelezheti a mechanikai problémákat, mielőtt kritikus állapotba kerülnének, lehetővé téve a proaktív karbantartást és megakadályozva a költséges megszakításokat. A vezeték nélküli szenzorok integrálása lehetővé teszi potenciális problémák korai felismerését, a csökkentett állásidőt és az optimalizált karbantartási ütemterveket A vezeték nélküli szenzorok valós idejű adatokat biztosítanak, amelyek lehetővé teszik az állapotfüggő karbantartást, optimalizálva az erőforrás-elosztást és minimalizálva a zavarokat.

Távoli Felügyelet és Diagnosztika: A vezetéknélküli szenzorok felügyelhetik a berendezéseket veszélyes vagy nehezen megközelíthető helyeken, az adatokat közvetlenül a felügyeleti rendszerekbe továbbítva szakértői elemzés céljából. Lehetővé teszi az elszigetelt műveletek távoli felügyeletét, csökkentve a gyakori fizikai ellenőrzések szükségességét. A távoli felügyeleti képességek javítják a biztonságot azáltal, hogy minimalizálják a személyzet veszélyes környezetben való tartózkodását, és növelik a hatékonyságot azáltal, hogy lehetővé teszik a szakértők számára a problémák diagnosztizálását és megoldását bárhonnan.

Gyorsabb Reagálás a Problémákra: A vezetéknélküli szenzorok azonnali riasztásokat indíthatnak el, ha egy gép működése elér egy előre meghatározott határt, azonnali hozzáférést biztosítva az elemzőknek a gép állapotadataihoz. Lehetővé teszi a valós idejű elemzést és a gyorsabb reagálást a potenciális problémákra az eszközkezelő szoftveren keresztül. A kapcsolat lehetővé teszi a kezelők számára, hogy jelezzék az olyan problémákat, mint az ütközések vagy a kiömlések, azonnal leállítva a munkát és lehetővé téve a gyorsabb reagálást. A vezeték nélküli kommunikáció valós idejű jellege lehetővé teszi a berendezések meghibásodásainak vagy biztonsági eseményeinek gyorsabb észlelését és reagálását, minimalizálva a potenciális károkat és az állásidőt. Az azonnali riasztások és a valós idejű adathozzáférés lehetővé teszik a gyorsabb döntéshozatalt és beavatkozást, ami kulcsfontosságú annak megakadályozásában, hogy a kisebb problémák súlyosabbá vagy biztonsági kockázatokká váljanak.

5. Távoli Vezérlés Előnyei a Vezetéknélküli Technológiával

A vezeték nélküli technológia használata a távoli vezérléshez számos előnnyel jár az ipari és más alkalmazásokban.

Nagyobb Mozgásszabadság: Lehetővé teszi a készülékek vagy gépek vezérlését zavaró kábelek nélkül, nagyobb mozgásszabadságot biztosítva. A kezelőket nem korlátozza a kábel

maximális hossza, ami növeli a rugalmasságot a munkaterületen. A felhasználók a vezeték nélküli hálózat hatótávolságán belül bárhonnan elérhetik és vezérelhetik a hálózatot, nem kötődnek Ethernet-kábelhez. A vezeték nélküli távvezérlés felszabadítja a kezelőket a vezetékes kapcsolatok "fizikai korlátait" alól, nagyobb mobilitást és rugalmasságot biztosítva a gépek és folyamatok kommunikációjában. A vezeték nélküli technológia áttöri ezeket a korlátokat, dinamikusabb és alkalmazkodóbb munkafolyamatokat és környezeteket teremtve.

Hatékonyabb Munkavégzés: A vezérlés a kezelő keze ügyében van, bárhol is tartózkodjon, lehetővé téve a gép vagy eszköz bármilyen körülmények közötti működtetését. Időt takarít meg és lehetővé teszi, hogy ugyanannyi idő alatt több munkát végezzenek el. Bizonyos esetekben kevesebb emberre van szükség a gépek vezérléséhez a távvezérlés segítségével. A vezeték nélküli távvezérlés egyszerűsíti a munkafolyamatokat és növeli a hatékonyságot azáltal, hogy lehetővé teszi a szakemberek számára a berendezések távoli vezérlését, potenciálisan csökkentve a több személyzet szükségességét és optimalizálva a feladatok végrehajtását.

Nagyobb Működési Biztonság: A gépek távoli vezérlése jobb áttekintést nyújt a műveletről, lehetővé téve a gyorsabb reagálást vészhelyzetekben. Lehetővé teszi robotok küldését veszélyes környezetekbe, miközben a szakember biztonságos helyen marad. Csökkenti a balesetek kockázatát azáltal, hogy minimalizálja a kezelő veszélyes környezetnek való kitettségét. A vezeték nélküli távvezérlés jelentősen növeli a működési biztonságot azáltal, hogy lehetővé teszi a szakemberek számára a gépek biztonságos távolságból történő vezérlését, távol a potenciális veszélyektől és veszélyes környezetektől.

Testreszabhatóság és Kényelem: Az ipari távvezérlők igény szerint testre szabhatok és konfigurálhatók, beleértve a gombok funkcionalitását és a visszajelző kijelzőket. Az ergonómikus és felhasználóközpontú kialakítás javítja a kezelő kényelmét a hosszú műszakok során. Kevesebb fáradtságot okoz, mint a hagyományos, kézi gépműködtetés. A vezeték nélküli távvezérlők a konkrét működési igényekhez igazíthatók, és a kezelő kényelmét szem előtt tartva tervezhetők, ami javítja a használhatóságot és csökkenti a kezelő fáradtságát.
Nagyobb Hatótávolság és Megbízhatóság: A vezeték nélküli távvezérlő berendezések nagy hatótávolságú kommunikációs képességekkel rendelkezhetnek, egyesesetekben akár több kilométerrel is. Megbízható és előre jelezhető valós idejű kommunikációt kínál a folyamatirányításhoz és a minőségbiztosításhoz. Különböző frekvenciasávokon működik, minimalizálva a más vezeték nélküli eszközök okozta interferencia kockázatát. A vezeték nélküli távvezérlő rendszerek kiterjesztett működési hatótávolságot és megbízható

kommunikációt kínálnak, biztosítva a gépek következetes vezérlését még jelentős távolságokon vagy potenciális interferenciával rendelkező környezetekben is. A berendezések jelentős távolságból történő vezérlésének képessége kibővíti a távvezérlés alkalmazási lehetőségeit, míg a megbízható kommunikáció elengedhetetlen a pontos és biztonságos működés biztosításához.

Nincs Szükség Közvetlen Rálátásra (RF Távirányítók): Az RF távirányítók rádióhullámokat használnak, amelyek falakon és más akadályokon is áthatolhatnak, ellentétben az infravörös távirányítókkal. Lehetővé teszi a készülékek vezérlését különböző helyiségekből vagy akár egy épületen kívülről is, páratlan kényelmet kínálva. A rádiófrekvenciás alapú vezeték nélküli távvezérlők nagyobb rugalmasságot és kényelmet kínálnak azáltal, hogy megszüntetik a távirányító és a készülék közötti közvetlen rálátás szükségességét. Ez a funkció kibővíti a távirányítók használhatóságát különböző beállításokban, ahol a fizikai akadályok akadályozhatják az infravörös alapú távirányítók jelét.

6. Munkabiztonság Növekedése a Vezetéknélküli Technológiával az Ipar 4.0-ban

A vezeték nélküli technológiák hozzájárulnak a biztonságosabb munkakörnyezet kialakításához a modern ipari létesítményekben.

Veszélyek és Munkavállalói Helyzet Valós Idejű Felügyelete: Az intelligens szenzorhálózatok és a viselhető eszközök figyelemmel kísérhetik a munkavállalók helyzetét a munkahelyi veszélyekhez viszonyítva, valós idejű riasztásokat lehetővé téve. A biztonságkritikus berendezéseken elhelyezett szenzorok adatokat szolgáltathatnak a karbantartási ütemtervekhez, megelőzve a berendezések meghibásodását. A viselhető szenzorok nyomon követhetik a magas kockázatú környezetben dolgozó munkavállalók fiziológiai adatait. A vezeték nélküli technológia lehetővé teszi a környezeti veszélyek és a munkavállalói állapot folyamatos felügyeletét, megkönnyítve a proaktív biztonsági intézkedéseket és az időben történő beavatkozásokat. A potenciális veszélyekre és a munkavállalók jólétére vonatkozó valós idejű adatok lehetővé teszik a veszélyes helyzetekre való azonnali reagálást és a balesetek megelőzését, mielőtt bekövetkeznének.

Veszélyes Feladatok Automatizálása: A távirányítású berendezések veszélyes környezetben használhatók, megszüntetve a szakemberek közvetlen érintkezésének szükségességét a működő gépekkel. A robotok és az autonóm járművek potenciálisan veszélyes feladatokat végezhetnek el, növelve a személyzet biztonságát. A drónok biztonsági ellenőrzéseket végezhetnek veszélyes vagy távoli területeken, csökkentve a munkavállalók kockázatát. A

vezeték nélküli technológia megkönnyíti a veszélyes feladatok automatizálását és távoli működtetését, jelentősen csökkentve a munkavállalók potenciális kockázatoknak való kitettségét. Azáltal, hogy a gépek olyan feladatokat végezhetnek el, amelyek veszélyesek az emberekre, a vezeték nélküli technológia közvetlenül hozzájárul a biztonságosabb munkakörnyezet kialakításához.

Jobb Működési Láthatóság és Vészhelyzeti Reagálás: A gyártási folyamatok valós idejű frissítései segíthetnek megelőzni a baleseteket, például a veszélyes vegyi anyagok kibocsátását. A viselhető szenzorok értékes kapcsolatot biztosítanak a kollégákkal és a mentőszemélyzettel, ha az alkalmazottak nehezen megközelíthető helyeken tartózkodnak. A vezeték nélküli hálózatokon keresztül működő video- és hangtechnológia lehetővé teheti a kommunikációt válsághelyzetekben. A vezeték nélküli rendszerek azonnali riasztásokat tesznek lehetővé gázszivárgás, túlmelegedés vagy berendezés meghibásodása esetén. A vezeték nélküli kapcsolat növeli a működési láthatóságot, és lehetővé teszi a gyorsabb és összehangoltabb vészhelyzeti reagálást, minimalizálva a balesetek hatását és biztosítva a munkavállalók biztonságát.

7. A Hatékonyság Növekedése a Vezetéknélküli Technológiával az Ipar 4.0-ban

A vezeték nélküli technológia számos módon növeli a hatékonyságot az Ipar 4.0-ban.
Valós Idejű Automatizálás és Felügyelet: A vezeték nélküli hálózatok lehetővé teszik a gépek és rendszerek folyamatos felügyeletét, megkönnyítve a prediktív karbantartást és a valós idejű beállításokat. Az IoT szenzorok az olyan vezeték nélküli technológiákkal, mint az 5G és a Wi-Fi 6, megkönnyítik a kis adatcsomagok valós idejű továbbítását, növelve a gyártási folyamatok rugalmasságát és hatékonyságát. A csatlakoztatott eszközökről származó valós idejű adatok lehetővé teszik a vállalatok számára, hogy felgyorsítsák gyártási kezdeményezéseiket, csökkentsék költségeiket és javítsák teljesítményüket. A vezeték nélküli technológia alapvető fontosságú a valós idejű automatizálás és felügyelet megvalósításához az Ipar 4.0-ban, biztosítva a szükséges infrastruktúrát az adatközpontú döntéshozatalhoz és a folyamatok optimalizálásához. Az ipari környezet különböző pontjairól származó adatok valós idejű gyűjtésének és elemzésének képessége kulcsfontosságú a termelési folyamatok optimalizálásához, az állásidő csökkentéséhez és az általános hatékonyság javításához.

Jobb Adatcsere és Elemzés: A vezeték nélküli technológia segíti az adatok ponttól pontig történő továbbítását, ami kulcsfontosságú az Ipar 4.0 intelligens gyárakra vonatkozó célkitűzésének eléréséhez. Lehetővé teszi a zökkenőmentes kommunikációt ember, gép,

rendszer és szenzor között, megkönnyítve a valós idejű adatcserét és a betekintést. A vezeték nélküli hálózatok támogatják a szenzorokról származó hatalmas mennyiségű adat gyűjtését és elemzését, segítve a gyártókat a munkafolyamatok optimalizálásában és a berendezések terhelésének szabályozásában. A vezeték nélküli hálózatok biztosítják az Ipar 4.0-ban szükséges kiterjedt adatcseréhez szükséges gerinchálózatot, lehetővé téve a fejlett analitikát és az informált döntéshozatalt, amelyek a hatékonyság javulását eredményezik. Az intelligens gyárakban keletkező hatalmas mennyiségű adatot hatékonyan kell gyűjteni és elemezni ahhoz, hogy értékes betekintést nyerjünk. A vezeték nélküli technológia biztosítja ennek az átfogó adatcserének a lehetőségét.

Fejlett Technológiák Támogatása: A vezeték nélküli infrastruktúra, különösen az 5G és a Wi-Fi 6/6E, támogatja a fejlett alkalmazásokat, például a mesterséges intelligenciát, a gépi tanulást, a robotikát és a virtuális valóságot, amelyek hozzájárulnak a hatékonyság növeléséhez. Lehetővé teszi a digitális ikrek használatát a termelési folyamatok optimalizálására és a távoli technikai segítségnyújtást a kiterjesztett valóság (AR) révén. Megkönnyíti az IoT és az intelligens ipari rendszerek integrálását a valós idejű felügyelet, a diagnosztika és az adatközpontú döntéshozatal érdekében. A vezeték nélküli technológia kulcsfontosságú a fejlett Ipar 4.0 technológiák telepítéséhez és felhasználásához, amelyek közvetlenül hozzájárulnak a jelentős hatékonyságnövekedéshez az automatizálás, az optimalizálás és a jobb döntéshozatal révén.

Optimalizált Erőforrás-felhasználás és Csökkentett Hulladék: A valós idejű felügyelet képes észlelni az anomáliákat vagy a potenciális veszélyeket, megkönnyítve az azonnali intézkedést a munkaerő biztonságának és az erőforrások felhasználásának optimalizálása érdekében. A vezeték nélküli szenzorokból származó adatközpontú betekintés segíthet optimalizálni az energiafogyasztást és csökkenteni a hulladékot. A prediktív karbantartás csökkenti az állásidőt és biztosítja, hogy a gépek optimális szinten működjenek, ami jobb termelékenységet és nagyobb nyereséget eredményez. A vezeték nélküli technológia hozzájárul a hatékonyság növeléséhez azáltal, hogy lehetővé teszi az erőforrások jobb kezelését, a hulladék csökkentését és a gépek teljesítményének optimalizálását valós idejű adatok és prediktív képességek révén. A hatékony erőforrás-felhasználás és a hulladékcsökkentés az Ipar 4.0 kulcsfontosságú céljai, és a vezeték nélküli technológia biztosítja az eszközöket ezek eléréséhez a jobb felügyelet és vezérlés révén.

Ábra 2: Vezetékes vs. Vezetéknélküli Hálózatok az Iparban

Szempontok	Vezetékes hálózat	Vezetéknélküli hálózat

Késleltetés (latency)	Nagyon alacsony, jellemzően <1 ms	Alacsony (5G: <1 ms), de érzékeny lehet interferenciára
Megbízhatóság	Kiemelkedő, stabil kapcsolat	Nagyon jó, de környezeti tényezők (fém, falak) zavarhatják
Telepítési költség	Magas (kábelezés, infrastruktúra kiépítése)	Alacsonyabb, gyorsan telepíthető
Rugalmasság	Alacsony – eszközök helyhez kötöttek	Magas – eszközök könnyen áthelyezhetők, gyártósor újrarendezhető
Skálázhatóság	Korlátozott, fizikai bővítést igényel	Magas – új eszközök gyorsan integrálhatók
Karbantartás	Kábelek elhasználódása miatt rendszeres beavatkozást igényel	Kevesebb fizikai probléma, de szoftveres frissítések szükségesek
Mobilitás támogatása	Nem támogatott – eszközök fix pozícióban	Teljes mobilitás – AGV, robotkar, szenzorok mozgás közben is működnek
Adatbiztonság	Fizikailag védett, nehezebb lehallgatni	Titkosítás szükséges, támadhatóbb lehet (pl. zavarás, hozzáférés)
Sebesség / sávszélesség	Magas (Ethernet: akár 10 Gbps+)	5G és Wi-Fi 6 esetén szintén magas, de megosztott
Általános használat	Régi gyárakban elterjedt, jól bevált	Modern gyárakban és okosüzemekben terjedőben

Ábra2 Összegzés:

- Vezetékes hálózatok megbízhatóbbak és ideálisak kritikus, fix rendszerekhez (pl. adatbázis szerverek, vezérlőegységek).
- Vezetéknélküli technológiák (különösen 5G, Wi-Fi 6) kiemelten alkalmasak rugalmas, adaptív és mobil ipari megoldásokhoz, amire az Ipar 4.0 törekszik.

8.Ipari alkalmazási területek

• Gyártás és automatizálás

Az ipari automatizálás fő haszonélvezője a vezeték nélküli kommunikációnak. Az 5G révén a robotok, CNC gépek és szállítórendszerek szinkronizáltan és valós időben működhetnek.

• Raktározás és logisztika

Automata járművek (AGV-k), drónok és valós idejű készletkövető rendszerek működtethetők stabil vezeték nélküli hálózaton. Ez gyorsabb, pontosabb logisztikát és költségcsökkentést eredményez.

• ***Energiaipar***

A vezeték nélküli technológia lehetővé teszi az **elérhetetlen vagy veszélyes környezetekben** (pl. olajfúró tornyok, atomreaktorok) történő adatgyűjtést és távfelügyeletet.

• ***Mezőgazdaság***

A precíziós gazdálkodás egyik alappillére a vezeték nélküli hálózat. Drónok, talajérzékelők, öntöző- és betakarítórendszerek kommunikálnak egymással és a központi irányító egységgel.

6G technológia lehetőségei és jövőképe

Bevezetés – Miért van szükség a 6G-re?

A mobilkommunikáció fejlődése minden évtizedben új technológiai ugrást hoz: a 4G elhozta a mobilinternet korszakát, az 5G lehetővé tette az ipari automatizálást és az IoT robbanásszerű terjedését. A 6G – várhatóan 2030 körül – ezt a fejlődési ívet folytatja, de már nem pusztán gyorsabb adatátvitelt ígér. A cél egy olyan **intelligens, érzékelőkkel teli, önszerveződő digitális környezet** kialakítása, amely a fizikai és digitális világot egyetlen rendszerként kezeli [1].

A 6G céljai és jellemzői

A 6G nem csupán az 5G továbbfejlesztett változata, hanem egy új hálózati paradigma, amely olyan jellemzőkkel bír majd, mint:

- **1 Tbps (terabit/másodperc) adatátviteli sebesség**,
- **0,1 ms körüli késleltetés**,
- **ultra-sűrű eszközkapcsolat (10 millió eszköz/km²)**,
- **100%-os elérhetőség és megbízhatóság**,
- **beépített mesterséges intelligencia és gépi tanulás** az irányításba [2].

A 6G-ben a kommunikációs infrastruktúra már nemcsak adattovábbító rendszer lesz, hanem **valós idejű érzékelő és prediktív döntéshozó rendszer** is egyben.

Új technológiák a 6G-ben

A 6G alapját olyan fejlett technológiák adják, amelyek jelenleg még kutatási fázisban vannak:

- **Terahertzes frekvenciasávok** (100 GHz – 1 THz), amelyek sokkal nagyobb sávszélességet biztosítanak, de kisebb hatótávval.

- **AI-alapú hálózatvezérlés**, ahol a rendszer önállóan optimalizálja a forgalmat, erőforrásokat, és válaszidőt.
- **Reconfigurable Intelligent Surfaces (RIS)** – új típusú antennarendszerek, melyek fizikailag irányítják a rádióhullámokat.
- **Holografikus kommunikáció** – teljes térbeli jelenlét élménye valós idejű kapcsolat során [3].

Ipari és társadalmi alkalmazások

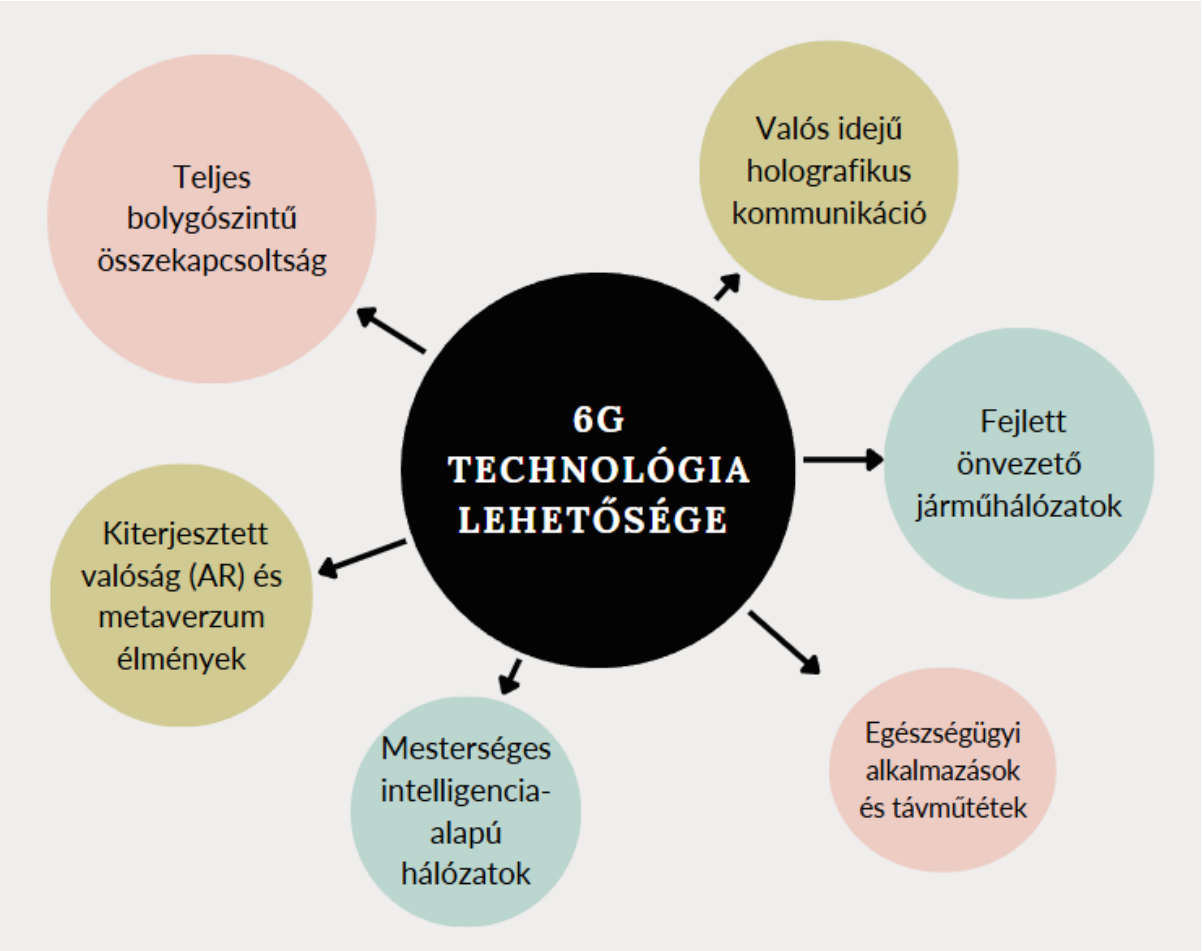
A 6G különösen az alábbi területeken hozhat forradalmi változást:

- **Precíziós ipar és automatizálás** – pl. gépek közti döntéshozás, önálló gyártósorok.
- **Egészségügy** – távműtétek, mesterséges intelligenciával támogatott diagnosztika.
- **Okosvárosok** – valós idejű közlekedésirányítás, energiafelhasználás optimalizálása.
- **Agrárium** – drónok, földradarok, gépi tanulással vezérelt ültetési és betakarítási rendszerek.

Kutatási trendek és globális fejlesztések

Több ország és vállalat már most komoly erőforrásokat fektet a 6G fejlesztésébe:

- **EU – Hexa-X és Hexa-X-II program**: célja az európai 6G architektúra kialakítása.
- **USA – NextG Alliance**: a 6G stratégiai kutatások koordinálása amerikai szereplők között.
- **Dél-Korea – Samsung és LG**: cél, hogy 2028-ra kereskedelmi 6G szolgáltatást indítsanak.
- **Kína – 6G műholdak tesztelése** már 2020 óta folyik [4].



Ábra 3, elemzése: 6G technológia lehetőségei

A 6G technológia, amelynek bevezetése várhatóan 2030 körül történik meg, a jelenlegi 5G hálózatokhoz képest jelentős előrelépést ígér mind sebesség, mind késleltetés terén. A 6G hálózatok célja, hogy akár 1 Tbps adatátviteli sebességet és mikrosekundumos késleltetést biztosítsanak, lehetővé téve olyan alkalmazásokat, amelyek a valós idejű adatfeldolgozást és azonnali reakciót igényelnek [1].

Holografikus kommunikáció

A 6G egyik legígéretesebb alkalmazása a valós idejű holografikus kommunikáció. Ez lehetővé teszi, hogy a felhasználók háromdimenziós, valósághű képeken keresztül kommunikáljanak egymással, mintha fizikailag is egy térben lennének. Ez forradalmasíthatja az orvosi konzultációkat, az oktatást és az üzleti megbeszéléseket [2].

Önvezető járművek és intelligens közlekedés

A 6G hálózatok ultra-alacsony késleltetése és magas megbízhatósága kulcsfontosságú az önvezető járművek és az intelligens közlekedési rendszerek számára. A járművek valós időben kommunikálhatnak egymással és az infrastruktúrával, elősegítve a balesetek megelőzését és a forgalom optimalizálását [1].

Távorvoslás és robotizált sebészet
A 6G lehetővé teszi a távoli orvosi beavatkozásokat, például robotizált sebészeti műtéteket, ahol a sebész több ezer kilométer távolságból irányíthatja a műtéti eszközöket valós időben. Ez különösen hasznos lehet olyan területeken, ahol nincs közvetlen hozzáférés szakorvosokhoz [3].

Mesterséges intelligencia által vezérelt hálózatok
A 6G hálózatok integrálják a mesterséges intelligenciát a hálózatkezelésbe, lehetővé téve az önoptimalizáló rendszerek kialakítását. Ez azt jelenti, hogy a hálózat képes lesz valós időben alkalmazkodni a forgalmi mintákhoz, előre jelezni a hibákat és automatikusan optimalizálni a teljesítményt [4].

Globális lefedettség és digitális egyenlőség
A 6G célja, hogy globális lefedettséget biztosítson, beleértve a távoli és vidéki területeket is. Ez műholdas és lézeralapú kommunikációs technológiák integrálásával valósulhat meg, elősegítve a digitális egyenlőség megteremtését világszerte [5].

Kiterjesztett valóság és metaverzum
A 6G hálózatok támogatják a kiterjesztett valóság (AR), virtuális valóság (VR) és kevert valóság (MR) alkalmazásokat, amelyek zökkenőmentes és valósághű élményeket nyújtanak. Ez új lehetőségeket teremt az oktatásban, a szórakoztatásban és a távoli együttműködésben [6].

A 6G technológia tehát nem csupán a jelenlegi hálózatok továbbfejlesztése, hanem egy új, intelligens és összekapcsolt világ alapja lehet, amely számos iparágat és társadalmi területet forradalmasíthat.

A 6G társadalmi és gazdasági hatásai

A 6G nem csupán a kommunikációs sebesség további növelését jelenti, hanem a digitális világ új szintjét, ahol a fizikai valóság és a kibertér határai elmosódnak. Ez a technológia a jövő ipari, gazdasági és társadalmi rendszereinek alapját képezheti. Bár az alkalmazások többsége még fejlesztés alatt áll, a kutatás és beruházás üteme alapján kijelenthető: a 6G lesz a digitális transzformáció következő motorja.

A 6G társadalmi és gazdasági hatásai

A 6G technológia – azaz a hatodik generációs mobilhálózat – nemcsak műszaki szempontból jelent majd előrelépést, hanem alapvető hatást gyakorolhat a társadalmi és gazdasági rendszerekre is. A gyorsabb adatátviteli sebesség, a közel zéró késleltetés, valamint az extrém hálózati sűrűség olyan új alkalmazásokat tesz lehetővé, amelyek alapjaiban formálhatják át a munka világát, a társadalmi egyenlőtlenségek dinamikáját, valamint az adatvédelem és szabályozás jövőjét [1][2].

Az egyik legjelentősebb hatás a munkapiac átalakulása lehet. A 6G révén új iparágak és munkakörök jelenhetnek meg, különösen a mesterséges intelligencia, a robotika, az adatelemzés és a kiberbiztonság területén [3]. A nagy sávszélesség és alacsony késleltetés

lehetővé teszi a távoli munkavégzés olyan szintjét, amely már nemcsak az irodai munkára korlátozódik, hanem a gyártás, az egészségügy, sőt a valós idejű távoli beavatkozások (pl. sebészet vagy gépek távkarbantartása) terén is alkalmazható lesz [4]. Ez elősegítheti a munkavállalók földrajzi függetlenedését, ami hosszú távon a globális munkaerőpiac újraformálódásához vezethet. Ugyanakkor a technológiai fejlődés kiszoríthat bizonyos munkaköröket, főként az alacsony képzettséget igénylő fizikai és rutinszerű munkák terén, ami társadalmi feszültségekhez vezethet, ha nem társul megfelelő átképzési és oktatási stratégiákkal [3][5].

Szorosan kapcsolódik ide a digitális szakadék problémája, amelyet a 6G akár tovább is mélyíthet. Míg a fejlett országok és technológiai központok képesek lesznek gyorsan alkalmazni és kihasználni a 6G előnyeit, addig a fejlődő régiókban még az 5G-hez való hozzáférés is gyakran korlátozott [6]. Ez az egyenlőtlenség súlyos következményekkel járhat, különösen az oktatás, az egészségügy és a gazdasági fejlődés területén. Ha bizonyos társadalmi csoportok vagy országok nem férnek hozzá a legújabb kommunikációs technológiákhoz, az hosszú távon fokozhatja az esélyegyenlőtlenséget és elmélyítheti a társadalmi kirekesztettséget [6][7].

A 6G emellett komoly adatbiztonsági és szabályozási kihívásokat is magában hordoz. Az új generációs hálózatok extrém mennyiségű adatot generálnak, amelyek közül sok érzékeny információkat tartalmaz – például egészségügyi, helymeghatározási vagy személyazonosító adatokat [8]. A mesterséges intelligencia által vezérelt rendszerek, az önvezető járművek, az intelligens városok és az ipari automatizálás mind olyan környezetek, ahol a hálózatra kapcsolt eszközök valós időben cserélnek adatokat. Az adatvédelem és a kiberbiztonság tehát kritikus tényezővé válik, különösen olyan helyzetekben, ahol az információk megsértése nemcsak személyes, hanem akár nemzetbiztonsági kockázatot is jelenthet [8][9]. Ennek megfelelően sürgető igény mutatkozik a globális szintű szabályozásra, amely lefedi az adatkezelés etikai és jogi kérdéseit, és biztosítja a felhasználók védelmét a technológiai fejlődés közepette is [10].

Végső soron a 6G nem csupán egy újabb generációs mobilhálózat, hanem egy komplex társadalmi-gazdasági áttörés előfutára. A benne rejlő lehetőségek hatalmasak, de kihívásai is jelentősek. Csak akkor aknázható ki teljes mértékben a technológia előnye, ha a társadalmi egyenlőtlenségek csökkentésére, az oktatásra, az átképzésre és a szabályozás fejlesztésére egyaránt kellő figyelmet fordítunk.

Kitekintés a jövőbe – Mikorra várható a 6G bevezetése, és mit jelenthet ez a mindennapi életben?

A 6G technológia – amely az 5G utáni következő generációs mobilhálózat – jelenleg még fejlesztés alatt áll, de a világ technológiai nagyhatalmai már intenzíven dolgoznak rajta. A várakozások szerint az első kereskedelmi 6G hálózatok bevezetése valószínűleg 2030 körül kezdődhet meg, míg a kísérleti rendszerek már 2028–2029 között megjelenhetnek [1][2]. A globális szabványosítási folyamat – melyet többek között a 3GPP és az ITU irányít – jelenleg a kutatási fázisnál tart, ahol már körvonalazódnak a főbb technológiai irányok, például a THz frekvenciatartomány használata, a mesterséges intelligenciával támogatott hálózatmenedzsment, valamint az ún. „holografikus kommunikáció” koncepciója [3].

A 6G nem csupán technológiai előrelépés, hanem egy paradigmaváltás is a digitális életben. Míg az 5G elsősorban a dolgok internete (IoT), az ipari automatizálás és az önvezető járművek számára jelentett ugrásszerű fejlődést, addig a 6G a valóság és a virtuális tér közötti határok további elmosódását vetíti előre. A mindennapi életben ez azt jelentheti, hogy például valós idejű holografikus hívások, immerszív kiterjesztett valóság (XR) élmények, vagy intelligens városok hálózata válnak elérhetővé [4].

A lakossági felhasználók számára a 6G olyan szolgáltatásokat nyújthat, mint a valós idejű gépi fordítás szemüvegbe integrált AR segítségével, vagy a távsebészeti beavatkozásokhoz való hozzáférés a világ bármely pontjáról. Oktatási területen pedig a tanulók holografikus avatarokon keresztül élhetnek át kísérleteket vagy történelmi eseményeket, amelyek eddig csak elméletben voltak taníthatók. A mesterséges intelligenciával támogatott 6G-hálózatok képesek lesznek dinamikusan optimalizálni a kapcsolatokat, így a hálózati torlódások vagy leállások még nagy terhelés esetén is minimálisra csökkennek [5].

Fontos azonban megjegyezni, hogy a 6G tömeges elterjedése – különösen a fejletlenebb régiókban – komoly társadalmi és infrastrukturális kihívásokat vet fel. Az előző generációk tapasztalatai alapján valószínű, hogy az új technológia először a gazdaságilag erősebb országokban jelenik meg, míg a globális hozzáférés fokozatosan alakul majd ki az évtized második felében [6].

Összefoglalva, a 6G nemcsak gyorsabb adatkapcsolatot jelent, hanem egy új digitális korszak alapját képezi, amely a kommunikációt, az oktatást, az egészségügyet és az ipart is új szintre emelheti – amennyiben sikerül a hozzáférés egyenlőségét és a biztonságos felhasználást is biztosítani.

Befejezés:

Az 5G technológia térhódítása jelentős fordulópontot jelentett az ipar fejlődésében. Az Ipar 4.0 szellemiségének megfelelően az okosgyártás és az adatvezérelt termelés csakis ilyen fejlett kommunikációs hálózatokon keresztül valósulhat meg. Az 5G lehetővé teszi a rugalmas és skálázható gyártási rendszerek kialakítását, ahol a különböző gépek, robotok, szenzorok és vezérlőrendszerek valós időben képesek kommunikálni egymással. A nagy sávszélesség, az alacsony késleltetés és a megnövelt kapcsolódási kapacitás révén az IoT-eszközök milliói kapcsolódhatnak össze, új távlatokat nyitva a tömeges eszközkapcsolatok és az adatelemzés terén.
Az ipari logisztikában az 5G kulcsszerepet játszik az önvezető járművek és autonóm rendszerek biztonságos és hatékony működtetésében. Ugyancsak forradalmi változást hoz a távkarbantartás és a kiterjesztett valóság alkalmazása, ahol távoli szakemberek avatkozhatnak be gyártási folyamatokba vizuális és haptikus visszacsatolás segítségével. Ezek az újítások nemcsak a termelékenységet fokozzák, hanem hozzájárulnak a munkahelyi biztonság és a fenntarthatóság javításához is.

A vezetéknélküli technológia ipari alkalmazása jelentős előnyöket biztosít a vállalatok számára. Az infrastruktúra telepítése és újraszervezése sokkal gyorsabb és költséghatékonyabb, mint a hagyományos vezetékes rendszerek esetében. A rendszer rugalmasságából adódóan a termelési folyamatok könnyen átalakíthatók, optimalizálhatók, és új munkafolyamatok is könnyedén integrálhatók. A vezeték nélküli rendszerek révén a karbantartás is hatékonyabbá válik, mivel az eszközök és gépek állapota folyamatosan figyelhető, így a hibák már a kialakulásuk előtt előrejelezhetők. A távoli vezérlés további előnyt jelent, hiszen a gyártósorok, robotkarok vagy akár teljes üzemegységek irányítása távolról is megvalósítható, ami különösen válsághelyzetek vagy nehezen hozzáférhető telephelyek esetén kulcsfontosságú. A munkabiztonság is nő, mivel a veszélyes feladatokat automatizált eszközök végezhetik el, az emberi jelenlét szükségességének csökkenésével párhuzamosan. Mindezek eredményeként a hatékonyság is ugrásszerűen nő, hiszen az emberi hibák csökkennek, a folyamatok pedig optimalizálhatóvá válnak a valós idejű adatok és a mesterséges intelligencia által.

A 6G technológia még inkább kitágítja az eddig ismert lehetőségek határait. Ez az új generációs hálózat nem csupán a jelenlegi sebességi és késleltetési korlátokat törli el, hanem teljesen új paradigmát kínál: intelligens, érzékelőkkel átszőtt környezetek jöhetnek létre, ahol az adatcsere nemcsak gyors, hanem értelmezett is. A 6G céljai között szerepel a szub-milliszekundumos késleltetés, az extrém sűrű kapcsolat, valamint a gépi intelligencia és kommunikáció egységes integrációja. A kvantumkommunikáció, a mesterséges intelligencia-alapú hálózati menedzsment, valamint a holografikus adatátvitel mind olyan technológiák, amelyek a 6G alapját képezik majd.

Az ipari és társadalmi alkalmazások spektruma ezzel tovább bővül. Az iparban a 6G lehetővé teszi a teljesen autonóm gyártási környezeteket, ahol a döntéshozatal is a gépekre bízható, míg a társadalmi szférában a kiterjesztett valóság, a valós idejű fordítás és az intelligens városok új szintre emelkednek. A kutatások jelenleg is intenzíven folynak világszerte, és az első 6G-hálózatok bevezetését 2030 környékére prognosztizálják. A technológiai fejlődés mellett azonban egyre hangsúlyosabbá válik a társadalmi és gazdasági hatások vizsgálata is. A munkapiac átalakulása, az új készségek iránti igény, valamint a digitális szakadék problémája komoly kérdéseket vet fel a jövő fenntarthatóságával kapcsolatban. Emellett az adatbiztonság és az etikus szabályozás kérdése is középpontba kerül: minél több adat kerül valós időben áramoltatásra és feldolgozásra, annál nagyobb a visszaélések vagy technológiai függőség kockázata.
A 6G tehát nem csupán a kommunikáció jövője, hanem társadalmi, gazdasági és kulturális változások katalizátora is lehet. Mindennapi életünket gyökeresen átalakíthatja: az intelligens otthonok, járművek, egészségügyi rendszerek és munkahelyek már nem távoli víziók, hanem közeli realitások. A kitekintés a jövőbe világossá teszi, hogy a 6G-vel egy új digitális korszak küszöbén állunk, amelynek kihívásaira és lehetőségeire egyaránt fel kell készülnünk.

Források:

A Vezetéknélküli Technológia Előnyei az Ipar 4.0-ban:
https://questsys.com/ceo-blog/wireless-networking-benefits-enhance-business-efficiency-and-mobility/
https://www.plantengineering.com/wireless-technology-benefits-for-manufacturing/
5G technológia haszna az iparban:
[1] Nokia Bell Labs – „Transforming the 6G vision to action” https://www.nokia.com/asset/214027
[2] Hexa-X – „Expanded 6G vision, use cases and societal values” https://hexa-x.eu/wp-content/uploads/2021/05/Hexa-X_D1.2.pdf
[3] Samsung Research – „AI-Native & Sustainable Communication” https://cdn.codeground.org/nsr/downloads/researchareas/Samsung_6G_Vision_2025.pdf
[4] IEEE Spectrum – *6G Development Around the Globe* https://spectrum.ieee.org/6g-technology

A 6G társadalmi és gazdasági hatásai:
[1] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," IEEE Access, vol. 7, pp. 78729–78757, 2019.
Elérhető: https://doi.org/10.1109/ACCESS.2019.2921522
[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 34, no. 3, pp. 134–142, 2020.
Elérhető: https://doi.org/10.1109/MNET.001.1900287
[3] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015.
Elérhető: https://doi.org/10.1109/ACCESS.2015.2461602
[4] M. Giordani et al., "Toward 6G networks: Use cases and technologies," IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, Mar. 2020.
Elérhető: https://doi.org/10.1109/MCOM.001.1900411
[5] PwC, “Will robots really steal our jobs?,” PricewaterhouseCoopers, 2018.
Elérhető: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html
[6] International Telecommunication Union (ITU), “Measuring digital development: Facts and figures 2022,” 2022
Elérhető: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
[7] R. van Dijk et al., "Digital divide: Impact of access and skills on inequality," Journal of Information Technology, vol. 35, no. 4, pp. 317–330, 2020.
Elérhető: https://doi.org/10.1177/0268396220912746
[8] L. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28–41, Sep. 2019.
Elérhető: https://doi.org/10.1109/MVT.2019.2921208

[9] ENISA, “Threat landscape for 5G networks and beyond,” European Union Agency for Cybersecurity, 2022.
Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks-and-beyond
[10] OECD, “Data governance in the age of AI and 6G,” Organisation for Economic Co-operation and Development, 2021.
Elérhető: https://www.oecd.org/digital/data-governance-in-the-age-of-ai-and-6g.html
Kitekintés a jövőbe – Mikorra várható a 6G bevezetése, és mit jelenthet ez a mindennapi életben?

[1] M. Latva-aho és K. Leppänen (szerk.), „Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence”, 6G Flagship, University of Oulu, 2019. Elérhető: https://www.6gflagship.com/key-drivers-and-research-challenges-for-6g-ubiquitous-wireless-intelligence/
[2] ITU-R, “IMT Vision for 2030 and beyond,” International Telecommunication Union, 2022. Elérhető: https://www.itu.int/en/ITU-R/study-groups/rsg5/Pages/default.aspx
[3] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," IEEE Access, vol. 7, pp. 78729–78757, 2019.
Elérhető: https://doi.org/10.1109/ACCESS.2019.2921522
[4] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, Mar. 2020.
Elérhető: https://doi.org/10.1109/MCOM.001.1900411
[5] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 34, no. 3, pp. 134–142, 2020.
Elérhető: https://doi.org/10.1109/MNET.001.1900287
[6] GSMA Intelligence, “The Mobile Economy 2023,” GSMA, 2023. Elérhető: https://www.gsma.com/mobileeconomy/

2.9. Business analytics az ipari termelésben Kocsis Ákos Gazdaságinformatkus Bsc, akoskocsis2005@gmail.com

Business analytics az ipari termelésben

Kocsis Ákos [redacted]

Gazdaságinformatkus Bsc, akoskocsis2005@gmail.com

1. Bevezetés

A mesterséges intelligencia (MI) és a prediktív analitika napjainkban egyre fontosabb szerepet töltenek be az ipari termelésben, különösen az üzleti döntéshozatal támogatásában. Az Ipar 4.0 és a digitális transzformáció előretörésével a vállalatok számára elengedhetetlenné vált az adatok hatékony felhasználása a versenyképesség megőrzése érdekében.

A mesterséges intelligencia, különösen a gépi tanulás és a prediktív modellezés révén, lehetőséget biztosít a vállalatok számára, hogy az adatokból rejtett összefüggéseket tárjanak fel, előre jelezzék a jövőbeli eseményeket, és ezáltal megalapozottabb döntéseket hozzanak. Ez különösen fontos az ipari környezetben, ahol a termelési folyamatok optimalizálása, a karbantartási igények előrejelzése és a minőségbiztosítás kulcsfontosságú tényezők. [1], [6]

A dolgozat célja, hogy bemutassa, hogyan épül fel egy prediktív analitikai modell, milyen adatforrásokra van szükség, és hogyan integrálhatóak ezek a megoldások a vállalati üzleti intelligencia rendszerekbe, mint például az SAP vagy a Power BI. Emellett kitér a mesterséges intelligencia alkalmazásának előnyeire és kihívásaira az ipari döntéshozatalban.

A dolgozat felépítése a következő: először bemutatásra kerül a mesterséges intelligencia és a prediktív analitika elméleti háttere, majd részletesen tárgyalásra kerül a prediktív analitikai modellek felépítése és működése. Ezt követően a BI rendszerekbe való integráció lehetőségei kerülnek bemutatásra, végül pedig az MI-alapú döntéstámogatás előnyei és korlátai kerülnek elemzésre. [2], [4]

2. Elméleti háttér

2.1 Mesterséges intelligencia és gépi tanulás

Az MI rendszerek egyik legfontosabb építőköve a gépi tanulás (machine learning, ML). A gépi tanulás lényege, hogy a számítógép algoritmusok segítségével képes mintákat felismerni az adatokban, és ezekből általánosítható szabályokat alkotni. Ezek a szabályok teszik lehetővé, hogy a rendszer később új, ismeretlen adatokon is megfelelő következtetéseket vonjon le. Például egy prediktív karbantartási rendszer megtanulhatja, hogy milyen szenzorminták előzik meg egy gép meghibásodását, és ez alapján előre jelezheti a jövőbeli hibákat. [11]

A gépi tanulásnak három fő típusa van: [11]

1. **Felügyelt tanulás (supervised learning)**: Ebben az esetben a rendszer tanításához szükség van egy előre címkézett adathalmazra. Az algoritmus megtanulja az inputok és az outputok közötti kapcsolatot, majd képes lesz új inputokhoz predikciót rendelni. Ilyen például egy minőségellenőrzési rendszer, amely képeken ismeri fel a hibás termékeket.
2. **Felügyelet nélküli tanulás (unsupervised learning)**: Itt az adathalmaz nem tartalmaz előre definiált címkéket, az algoritmusnak magának kell felfedeznie a struktúrákat, mintákat az adatokban. Ez hasznos lehet például a gyártási folyamatok klaszterezésére, vagy új anomáliák felismerésére.
3. **Megerősítéses tanulás (reinforcement learning)**: Ebben a tanulási módszerben az algoritmus egy környezettel lép interakcióba, és a kapott jutalmak vagy büntetések alapján tanulja meg a helyes cselekvések sorozatát. Az iparban ez például robotok mozgásának optimalizálására vagy gyártósorok dinamikus vezérlésére használható.

A gépi tanulás különféle algoritmusok széles skáláját alkalmazza, például döntési fákat, neurális hálózatokat, szupport vektor gépeket és mély tanulási modelleket. A választott algoritmus függ az adathalmaz típusától, az előrejelzési feladat komplexitásától és a szükséges pontosságtól. [11]

A mesterséges intelligencia szerepe az ipari termelésben [1], [6]

Az ipari termelésben az MI alkalmazása számos előnnyel jár. Az egyik legfontosabb előnye az **automatizálás**: lehetővé teszi, hogy olyan feladatokat automatizáljunk, amelyek korábban emberi erőforrást igényeltek. Például a vizuális ellenőrző rendszerek gépi látással és mély tanulási algoritmusokkal képesek felismerni a hibákat a termékeken, sokkal gyorsabban és pontosabban, mint az emberi szem.

Egy másik kulcsfontosságú terület a **prediktív karbantartás**, amely a szenzoradatok elemzésével előre jelzi a berendezések meghibásodását, így csökkentve a váratlan leállások kockázatát. Emellett az MI segíthet az **ellátási lánc optimalizálásában**, az **energiafogyasztás csökkentésében**, valamint az **ügyfélrendelések pontosabb előrejelzésében**.

Egy átfogó elemzés szerint az MI alkalmazása az ipari termelésben akár 20-30%-os költségmegtakarítást és 10-15%-os termelékenységnövekedést is eredményezhet.

2.2 Prediktív analitika

A prediktív analitika az adatelemzés egy fejlett ága, amely statisztikai modellezést, gépi tanulást és adatbányászati technikákat alkalmaz annak érdekében, hogy előrejelzéseket készítsen jövőbeli eseményekről. Nem csupán leíró vagy diagnosztikai analízisről van szó, hanem proaktív megközelítésről: azt próbáljuk megjósolni, hogy mi fog történni, és esetenként azt is, hogy miért. [2], [4]

A prediktív analitika szerepe az ipari termelésben:

Az ipari termelésben a prediktív analitika egyre fontosabbá válik a következő okok miatt:

- **Berendezések állapotának előrejelzése**: A gépek szenzoraiból származó adatokat elemezve előre megjósolható, mikor várható egy alkatrész meghibásodása. Ez lehetővé teszi az ütemezett karbantartást, csökkentve az állásidőt és a váratlan leállásokat.
- **Minőségbiztosítás támogatása**: Az adatok elemzése révén azonosíthatók azok a folyamatparaméterek, amelyek a hibás termékekhez vezetnek, így beavatkozás történhet még a hiba kialakulása előtt.
- **Kereslet-előrejelzés**: A piac és a vásárlói szokások előrejelzése segíti az alapanyagok beszerzését, a gyártási ütemezést és a raktározást.
- **Folyamatoptimalizálás**: A termelési adatok alapján javíthatók a folyamatparaméterek, hogy a lehető legkevesebb energia- és alapanyag-felhasználással a legmagasabb termelékenységet érjék el.
- **Ellátási lánc kezelése**: Az ellátási lánc eseményeinek előrejelzésével csökkenthető a késések és készlethiányok kockázata.

A prediktív analitika kulcselemei:

A prediktív analitikai folyamat általában a következő lépésekből áll: [2], [4]

1. **Célok meghatározása**
   Az első lépés annak meghatározása, hogy milyen problémát szeretnénk megoldani, vagy milyen döntési helyzetet szeretnénk támogatni. Az iparban ez

lehet a karbantartási igények előrejelzése, selejtes termékek arányának csökkentése, vagy a gépüzemidő optimalizálása.

2. Adatgyűjtés és adatforrások integrálása
   A prediktív analitika sikere nagymértékben függ az adatok minőségétől és elérhetőségétől. Ipari környezetben számos adatforrás áll rendelkezésre:
   - Szenzoradatok (pl. hőmérséklet, rezgés, nyomás)
   - PLC (programmable logic controller) logok
   - Gyártósori eseménynaplók
   - ERP-rendszerekből (pl. SAP) származó adatok [9]
   - Kézi bevitelek és minőségellenőrzési jegyzőkönyvek
3. **Adattisztítás és előkészítés**
   A nyers adatok gyakran zajosak, hiányosak vagy redundánsak. Az adattisztítás során eltávolítják az irreleváns adatokat, kitöltik a hiányzó értékeket, és normalizálják az adatokat a modellezéshez.
4. **Jellemzők kiválasztása és létrehozása (feature engineering)**
   Az adatmodellezés hatékonyságát nagyban befolyásolja, hogy milyen inputváltozókat választunk ki. Például a rezgésadatokból számíthatunk statisztikai mutatókat (átlag, szórás), frekvenciaanalízist végezhetünk, vagy kombinált mutatókat hozhatunk létre.
5. Modellezés
   Ebben a lépésben különféle statisztikai és gépi tanulási módszereket alkalmaznak. A leggyakoribb algoritmusok: [11]
   - Regressziós modellek
   - Döntési fák és random forest
   - Neurális hálózatok és mély tanulás
   - Támogatott vektor gépek (SVM)
   - Boosting-algoritmusok (pl. XGBoost)
6. **Modellek értékelése és validálása**
   Az elkészített modellt tesztelni kell korábban nem látott adatokon, hogy megbizonyosodjunk a pontosságáról, robusztusságáról és általánosíthatóságáról. Tipikus mérőszámok: RMSE, MAE, ROC-AUC.
7. Üzembe helyezés és folyamatos monitorozás
   A jóváhagyott modellt integrálni kell az üzleti vagy ipari környezetbe, ahol valós

időben fut, és előrejelzéseket készít. Fontos a modell teljesítményének folyamatos nyomon követése és újratanítása, ha változnak a körülmények. [3]

Adatforrások részletezése

Az ipari prediktív analitika adatforrásai különösen összetettek és heterogének: [2], [4]

- **Strukturált adatok**: ERP- és MES-rendszerekből származó numerikus, táblázatos adatok (pl. termelési volumen, üzemidő, leállások okai).
- **Idősoros adatok**: Szenzorokból származó folyamatos mérések, amelyek kulcsfontosságúak az időfüggő minták felismerésében.
- **Kép- és hangadatok**: Gépi látás vagy akusztikus diagnosztika alkalmazása esetén képi és hangfájlokat is elemezhet a rendszer.
- **Nem strukturált adatok**: Karbantartási jegyzőkönyvek, üzemeltetési naplók szöveges formában, melyek természetes nyelvfeldolgozással (NLP) feldolgozhatók.

2.2.1 Prediktív analitika és mesterséges intelligencia kapcsolata [2], [4]

A prediktív analitika és a mesterséges intelligencia (MI) szorosan összefonódó területek. Míg a prediktív analitika alapvetően statisztikai modellezést és gépi tanulást alkalmaz, az MI tágabb keretet biztosít, amely magában foglalja a gépi tanulás, a természetes nyelvfeldolgozás, a számítógépes látás és egyéb intelligens technológiák használatát.

MI szerepe a prediktív modellekben

Az MI a következő módokon erősíti a prediktív analitikát:

- Öntanuló rendszerek: A gépi tanulási algoritmusok képesek idővel javulni, ahogy egyre több adat áll rendelkezésre. [11]
- **Komplex mintázatok felismerése**: Az MI képes összetett, nemlineáris összefüggések felismerésére, amelyeket hagyományos statisztikai módszerekkel nehéz lenne modellezni.
- **Automatizált feature engineering**: Bizonyos MI-alapú eszközök automatikusan képesek az adatokból releváns jellemzőket generálni, csökkentve az emberi szakértelem szükségességét.
- Valós idejű elemzés: A modern MI-alapú prediktív analitikai rendszerek képesek valós idejű adatfolyamokat feldolgozni, és azonnali előrejelzéseket adni.

2.2.2 Prediktív analitika gyakorlati kihívásai az iparban

Bár a prediktív analitika hatalmas lehetőségeket kínál, az ipari bevezetése során számos kihívással kell szembenézni:

Adatminőségi problémák [3], [5]

- Hiányzó adatok: A szenzorok hibája, adatvesztés vagy emberi mulasztás miatt.
- Zajos adatok: A gépi érzékelők által mért adatok tartalmazhatnak mérési hibákat vagy kiugró értékeket.
- Nem standardizált adatstruktúrák: Különböző forrásokból származó adatok eltérő formátuma miatt integrációs nehézségek léphetnek fel.

Technológiai kihívások

- **Infrastruktúra**: Nagy mennyiségű adat tárolásához és elemzéséhez robusztus IT-infrastruktúra szükséges.
- **Valós idejű feldolgozás**: Nem minden ipari környezet képes biztosítani az adatfolyamok azonnali feldolgozását.

Szervezeti kihívások

- **Adatvezérelt kultúra hiánya**: A vállalatok egy részénél az adat alapú döntéshozatal nem része a vállalati kultúrának.
- Szakértelem hiánya: A prediktív analitika bevezetéséhez adatkutatókra, adatmérnökökre és üzleti elemzőkre van szükség.

2.2.4 Prediktív analitika integrációja üzleti intelligencia rendszerekbe

A prediktív analitika csak akkor tud valódi üzleti értéket teremteni, ha az eredményei eljutnak a döntéshozókhoz, és beépülnek a napi üzleti folyamatokba. Ehhez szükség van az üzleti intelligencia (BI) rendszerekkel való integrációra. [2], [4]

Integráció módjai:

- SAP integráció: Az SAP Predictive Analytics modul segítségével az előrejelzési modellek beágyazhatók az SAP ERP-rendszerbe, lehetővé téve az automatizált riportokat és előrejelzéseket a meglévő munkafolyamatokban. [9]
- Power BI integráció: A Microsoft Power BI natívan támogatja a Python és R szkripteket, amelyekkel prediktív modellek hívhatók meg. A Power BI adatvizualizációval kombinálva interaktív dashboardokat lehet készíteni, ahol a felhasználók valós időben követhetik a predikciókat. [10]

2.3 Üzleti döntéshozatal támogatása prediktív analitikával

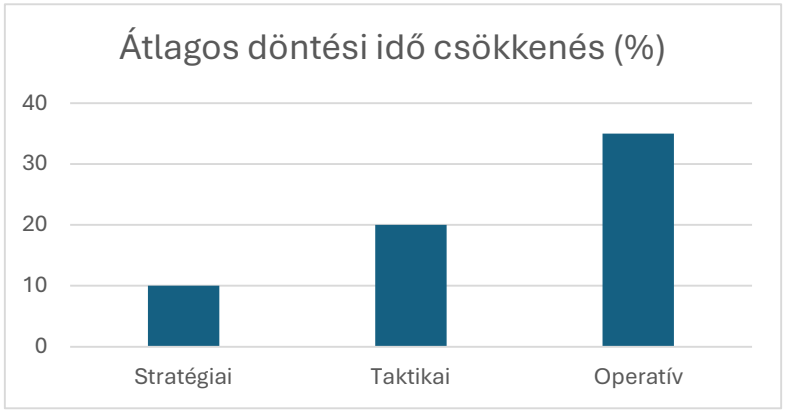
A modern ipari környezetben a döntéshozatal egyre inkább adatvezérelté válik. A prediktív analitika célja nem csupán előrejelzések készítése, hanem az is, hogy ezek az előrejelzések támogassák és javítsák az üzleti döntéseket.

Ez a fejezet bemutatja, hogyan alkalmazható a prediktív analitika az ipari vállalatok döntéshozatali folyamataiban, milyen típusú döntések támogathatók vele, és hogyan illeszkedik az analitikai eredmények hasznosítása a vállalati üzleti intelligencia rendszerébe. [2], [4]

2.3.1 Döntéshozatali szintek és prediktív analitika szerepe

A vállalati döntéshozatal három fő szinten történik:

1. **Stratégiai döntések** – hosszú távú, a vállalat egészére kiható döntések (pl. új gyárépítés, beruházások).
2. **Taktikai döntések** – középtávú, egyes részlegekre, folyamatokra vonatkozó döntések (pl. kapacitásbővítés, termelési terv módosítása).
3. **Operatív döntések** – napi szintű működési döntések (pl. gépek leállítása karbantartásra, rendelés átsorolása).



Döntési idő, forrás: [1]

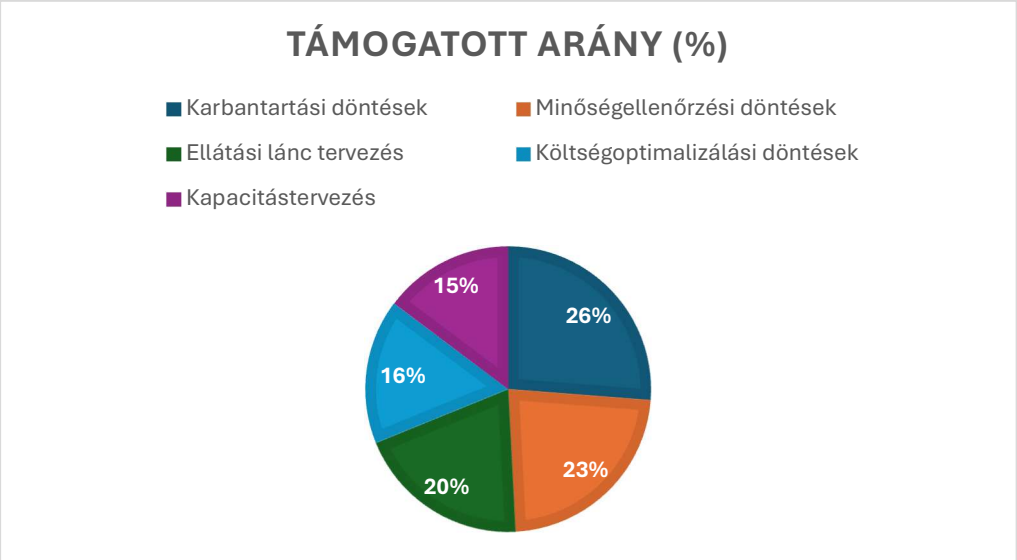
A prediktív analitika bevezetése jelentősen csökkenti az üzleti döntéshozatalhoz szükséges időt. Különösen az operatív szinten figyelhető meg drámai, akár 35%-os gyorsulás.

2.3.2 Milyen típusú döntések támogathatók?

A prediktív analitika az alábbi ipari döntéseket segíti elő:

- **Karbantartási döntések**: mikor kell egy gépet leállítani javításra → prediktív karbantartási modell alapján.
- **Minőségellenőrzési döntések**: mely gyártási tételek esélyesek hibásnak → minőségprediktív modell alapján.
- **Ellátási lánc döntések**: mikor kell alapanyagot rendelni → kereslet előrejelző modell alapján.
- **Költségoptimalizálási döntések**: mely folyamatlépéseknél lehet költséget csökkenteni → költség-prediktív modellek elemzésével.

- **Kapacitástervezési döntések**: mekkora termelési kapacitásra lesz szükség → kapacitás-előrejelző modellek használatával.



Döntéstipusok, forrás: [2]

Ez az ábra azt mutatja, hogy mely ipari döntéshozatali típusoknál alkalmazzák leggyakrabban a prediktív analitikát. A leggyakrabban támogatott terület a karbantartás, de jelentős arányban támogatja a minőségellenőrzést és az ellátási láncot is.

2.3.3 Prediktív analitika és döntéstámogatás folyamata [2], [4]

A döntéstámogatás **adatvezérelt folyamata** általában a következő lépéseken keresztül valósul meg:

1. **Adatgyűjtés** – szenzorokból, ERP-rendszerből, logisztikai adatokból.
2. **Adattisztítás és előkészítés** – zajok, hiányzó adatok kezelése.
3. Modellezés – gépi tanulási algoritmusok alkalmazása (pl. regresszió, döntési fa, neurális hálózat). [11]
4. **Modellek validációja** – pontosság, megbízhatóság tesztelése.
5. Előrejelzések integrálása BI-rendszerekbe – pl. SAP, Power BI. [10]
6. **Vizualizáció és interpretáció** – dashboardok, jelentések készítése.
7. **Döntéshozatal támogatása** – az eredmények felhasználása konkrét döntésekhez.

2.3.4 Üzleti intelligencia rendszerek szerepe a döntéstámogatásban

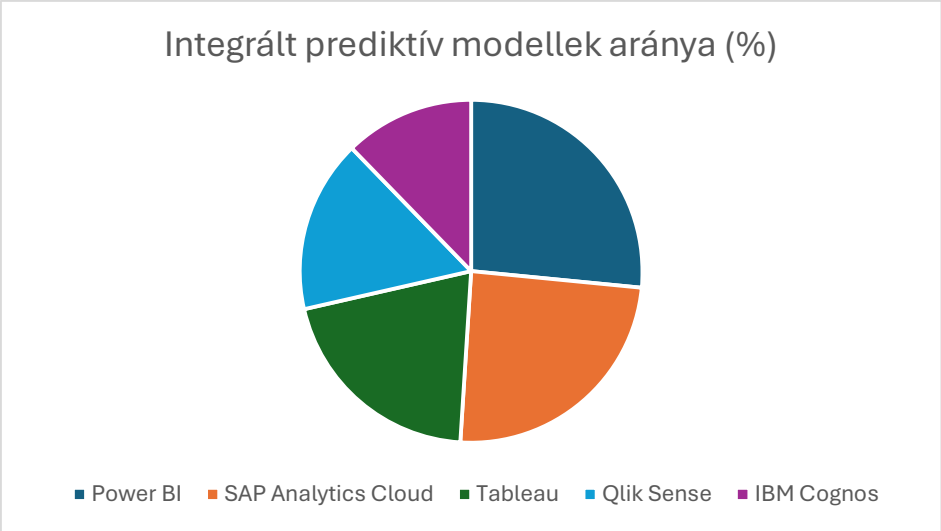
A prediktív analitikai modellek önmagukban nem elegendőek; az előrejelzéseknek el kell jutniuk a döntéshozókhoz érthető, hasznosítható formában. Ezt szolgálják az üzleti intelligencia (BI) rendszerek.

Példák integrációra:

- SAP BI: a prediktív modellek eredményei SAP HANA adatbázisban tárolhatók, majd a SAP Analytics Cloud-ban vizualizálhatók. [9]
- Power BI: Python vagy R integrációval előrejelzések hívhatók meg, interaktív dashboardon jelenítve meg. [10]
- Tableau: gépi tanulási modellek eredményei Tableau Serveren keresztül érhetők el. [11]

Miért fontos a BI-integráció?

- Központi adatszolgáltatás biztosítása.
- Egységes adatértelmezés.
- Valós idejű riportolás és riasztások.
- Döntéshozói hozzáférés bárhonnan (web, mobil).



BI-rendszerek, forrás: [10]

Ez az ábra különböző üzleti intelligencia platformokat hasonlít össze aszerint, hogy milyen arányban integrálnak prediktív analitikai modelleket. A legnagyobb integrációs arány a Power BI és SAP rendszerekben figyelhető meg.

3. A prediktív analitikai modell felépítése és folyamata

A prediktív analitika célja az ipari termelésben az, hogy a rendelkezésre álló adatok alapján előre jelezze a jövőbeli eseményeket, trendeket vagy problémákat. Ennek érdekében olyan modelleket kell kialakítani, amelyek a történelmi és valós idejű adatok feldolgozásával képesek felismerni az összefüggéseket és előrejelzéseket készíteni. A modellépítési folyamat több egymásra épülő lépésből áll, amelyek mindegyike kulcsszerepet játszik a végső eredmény megbízhatóságában és pontosságában. [2], [4]

3.1 Az adatforrások szerepe

A prediktív modellek alapja az adat. Az ipari környezetben számos különféle forrásból származnak adatok, amelyek együttesen adnak átfogó képet a folyamatokról és működésről. Az adatok sokfélesége lehetővé teszi a modellek gazdagítását és pontosítását.

A leggyakrabban használt adatforrások a következők:

- **Szenzorok által gyűjtött adatok (IoT):** Ezek az érzékelők a gépek működéséről, állapotáról, például hőmérsékletről, rezgésről, nyomásról vagy áramfelvételről szolgáltatnak adatokat, rendszerint időbélyeggel ellátva.
- **ERP-rendszerekből származó információk:** A vállalatirányítási rendszerek rögzítik a gyártással, készletezéssel, beszerzéssel és egyéb üzleti folyamatokkal kapcsolatos adatokat, amelyek segíthetnek feltárni a termelésben rejlő mintázatokat.
- **CRM-rendszerek adatai:** Az ügyfélkapcsolati adatok elemzésével következtetni lehet a kereslet alakulására, a termékek iránti érdeklődésre és az ügyfél-elégedettségre.
- **SCM-rendszerek információi:** Az ellátási lánc adatai (beszállítók, szállítási idők, logisztika) a gyártási tervek optimalizálásában nyújtanak alapot.

Ezek az adatforrások együttesen alkotják a modell tanításához szükséges adathalmazt, amelyet gyakran adatpiacok (data lake), adattárházak vagy integrált rendszerek segítségével gyűjtenek össze.

3.2 Az adatelőkészítés és adatminőség biztosítása

A nyers adatokat ritkán lehet közvetlenül modellépítésre felhasználni, ezért kiemelt jelentősége van az előkészítésnek. Az adatok tisztítása és feldolgozása nélkülözhetetlen ahhoz, hogy a prediktív modellezés pontos és megbízható eredményeket adjon.

Az előkészítési folyamat lépései:

- Hiányzó értékek kezelése: Az üres adatok pótlása statisztikai vagy gépi tanulási módszerekkel történhet, például mediánnal, regresszióval vagy más predikciós technikákkal. [11]
- **Kiugró adatok azonosítása:** Az anomáliák kiszűrése történhet IQR, z-score vagy vizuális elemzési módszerekkel, hogy ne torzítsák a modellt.
- Normalizálás, standardizálás: Az eltérő mértékegységek és skálák összehangolása elengedhetetlen, hogy a gépi tanulási algoritmusok megfelelő súlyozással kezeljék az egyes jellemzőket. [11]

- **Időbeli szinkronizáció:** Az időbélyeges adatok összehangolása interpolációval, aggregációval vagy resampling technikákkal történik.
- **Új jellemzők létrehozása:** Az adatelemzés során új változók képzése, például mozgóátlagok, deriváltak, idősoros trendek segíthetnek gazdagítani az adathalmazt.

Az adattisztítás és előkészítés alapvető feltétele annak, hogy a modell stabil és prediktív képességekkel rendelkező legyen.

3.3 Modellépítési lépések

A modellépítés folyamata során a cél a releváns jellemzők és a legmegfelelőbb algoritmus megtalálása, majd a modell tanítása és kiértékelése.

3.3.1 Jellemzők kiválasztása

A jellemzők (feature-ök) közötti kapcsolat feltárása és a legfontosabbak kiválasztása a modell egyszerűsítését és teljesítményének növelését szolgálja. Ehhez különféle technikák állnak rendelkezésre: [3]

- Korrelációs vizsgálat
- Mutual information számítás
- Recursive Feature Elimination
- Feature importance mutatók döntési fákból
- Dimenziócsökkentés (pl. PCA)

A felesleges vagy redundáns jellemzők eltávolításával csökkenthető az overfitting kockázata és javítható a predikció pontossága.

3.3.2 Algoritmus kiválasztása

A választott algoritmus nagyban befolyásolja a modell előrejelzési képességét. Az algoritmus megválasztása az adatok típusától és a megoldandó feladattól függ.

Lehetséges módszerek:

- **Osztályozás:** Random Forest, Support Vector Machine, XGBoost
- **Regresszió:** Ridge, Lasso, Gradient Boosting
- **Idősoros előrejelzés:** ARIMA, SARIMA, Prophet, LSTM neurális hálózat

A döntés során mérlegelni kell a számítási erőforrásokat, a tanítási időt és az interpretálhatóságot.

3.3.3 Modell tanítása és validálása

A modell tanításához az adatokat rendszerint edző és tesztkészletre osztják. A validálás célja, hogy a modell általánosíthatóságát ellenőrizzék, és elkerüljék a túlilleszkedést.

Gyakori megoldások:

- Train-test split (pl. 80-20 arány)
- K-keresztvalidáció
- Paraméterhangolás (grid search, random search, Bayesian optimization)

A teljesítményt értékelő metrikák a feladattól függenek, például pontosság, F1-score, MSE, RMSE vagy R^2.

3.4 Teljesítményértékelés és finomhangolás

A modell teljesítményének növelése érdekében iteratív módon kell finomhangolni az egyes lépéseket. A javítás lehetséges irányai: [3]

- Irreleváns jellemzők eltávolítása
- Új adatforrások bevonása
- Paraméteroptimalizálás
- Ensemble technikák (bagging, boosting)

A cél, hogy a modell stabil, általánosítható és magas prediktív pontosságú legyen, miközben elkerülhető a túlilleszkedés.

4. A prediktív analitikai megoldások integrációja az üzleti intelligencia rendszerekbe

A prediktív analitikai modellek önmagukban nem elegendőek az ipari termelés és a vállalati döntéshozatal támogatásához. Ahhoz, hogy az elemzésekből származó előrejelzések és felismerések a gyakorlatban is hasznosuljanak, integrálni kell őket a meglévő üzleti intelligencia (BI) rendszerekbe. Az integráció célja, hogy a döntéshozók és az operatív munkatársak a megszokott felületeken, valós időben férjenek hozzá az előrejelzésekhez, riasztásokhoz és elemzésekhez. [2], [4]

4.1 Az integráció szükségessége és előnyei

A prediktív analitika és a BI-rendszerek összekapcsolása számos előnnyel jár: **Egységes adatforrások:** Az üzleti és gyártási adatok közös platformra kerülnek, így átfogó képet adnak a vállalat működéséről.

- **Valós idejű döntéstámogatás:** Az előrejelzések közvetlenül megjelenhetnek a vezetői dashboardokon, interaktív riportokban.
- **Automatizált riasztások és workflow-k:** A prediktív modellek által detektált anomáliák automatikusan folyamatokat indíthatnak (pl. karbantartási feladatok ütemezése).
- **Könnyebb interpretáció:** A modellek eredményei vizuálisan, a BI-eszközökön keresztül jobban értelmezhetők.

4.2 Integrációs módszerek

A prediktív modellek és BI-rendszerek integrációjára több technikai megoldás létezik, melyek a vállalati IT-infrastruktúra és a felhasznált technológiák függvényében választhatók ki.

4.2.1 API-alapú integráció

A modern analitikai platformok (pl. Python alapú modellek, Azure Machine Learning, AWS SageMaker) **REST API-kon** keresztül szolgáltatják a modell előrejelzéseit. Ezek az API-k könnyen csatlakoztathatók a BI-eszközökhöz, például:

- Power BI: A Power Query vagy az Azure kapcsolat révén közvetlenül képes API-hívásokkal adatokat betölteni. [10]
- SAP Analytics Cloud: Webszolgáltatásokat integrálva importálhatja a prediktív outputokat. [9]

Ez a megközelítés **valós idejű vagy közel valós idejű frissítést** tesz lehetővé.

4.2.2 Adattárházi integráció

Alternatív megoldás, hogy az előrejelzéseket **adattárházba (data warehouse)** töltik vissza, amelyből a BI-eszköz olvassa az adatokat. Ez a módszer stabil, jól kontrollált környezetet biztosít, főként akkor előnyös, ha **történeti elemzések és trendkövetés** is szükséges.

- A modell előrejelzéseit batch folyamatokban tölthetik be egy **SQL-alapú adattárházba**.
- A BI-rendszer ezután standard adatkapcsolaton keresztül jeleníti meg az eredményeket.

4.2.3 Beépített analitikai modulok

Egyes BI-platformok már tartalmaznak beépített gépi tanulási és prediktív analitikai funkciókat. Például:

- Power BI: Azure Machine Learning integráció, AutoML-funkciók [10]

- SAP: Predictive Analytics Library, SAP HANA beépített ML-motor [9]

Ebben az esetben a modellek közvetlenül a BI-környezetben taníthatók és futtathatók, ezáltal **csökkentve a külön rendszerek közötti adatmozgatás szükségességét**.

4.3 Az integráció kihívásai

A prediktív analitika és BI-rendszerek integrálása technológiai és szervezeti szempontból egyaránt kihívásokat jelenthet:

- Adatminőség és adatkonzisztencia fenntartása: A különböző rendszerek eltérő adatstruktúrái és formátumai harmonizációt igényelnek. [3], [5]
- **Valós idejű adatfrissítés biztosítása:** Nagy mennyiségű adatnál a késleltetés minimalizálása kulcsfontosságú.
- **Felhasználói interpretáció támogatása:** A modell előrejelzéseinek magyarázata (explainability) szükséges ahhoz, hogy a döntéshozók bízzanak az eredményekben.
- **Biztonsági és adatvédelmi megfelelés:** Az érzékeny adatok áramlása szigorú IT-biztonsági előírásokat igényel.

5. A prediktív analitikai modellek teljesítményének értékelése és finomhangolása

A prediktív analitikai modellek létrehozása nem ér véget a modell betanításával. Az elkészült modellek teljesítményét alaposan értékelni és szükség esetén finomhangolni kell annak érdekében, hogy megbízható, pontos előrejelzéseket biztosítsanak. Ez a lépés kulcsfontosságú az ipari környezetben, ahol a hibás előrejelzések jelentős üzleti vagy gyártási kockázatot hordozhatnak. [2], [4]

5.1 Teljesítménymérési módszerek

A modell teljesítményének kiértékelésére különböző statisztikai és gépi tanulási metrikák állnak rendelkezésre, amelyek a predikciók pontosságát, stabilitását és általánosíthatóságát mérik. A választott metrika típusát az előrejelzési feladat jellege határozza meg: [11]

- **Regressziós problémák esetén:**
    - **Mean Absolute Error (MAE):** Az előrejelzések és a tényleges értékek közötti abszolút eltérés átlaga.
    - **Root Mean Squared Error (RMSE):** Az eltérések négyzetes átlaga, amely érzékenyebb a nagyobb hibákra.
    - **R^2 (determination coefficient):** A magyarázott variancia aránya, ami megmutatja, mennyire illeszkedik a modell az adatokhoz.
- **Osztályozási problémák esetén:**
    - **Pontosság (Accuracy):** A helyesen besorolt esetek aránya.
    - **Precízió (Precision) és Recall:** A pozitív osztályokra vonatkozó helyes előrejelzések aránya.
    - **F1-score:** A precízió és recall harmonikus átlaga.
    - **ROC-AUC:** Az osztályozó teljesítményének összefoglalása különböző küszöbértékek mentén.

Ezeket a metrikákat **tesztadatokon** kell értékelni, melyeket a modell betanításakor nem látott, hogy elkerüljük az overfittinget.

5.2 Validációs módszerek

A teljesítménymérés során kulcsfontosságú a megfelelő **validációs stratégia** megválasztása, mely biztosítja a modell általánosíthatóságát:

- **Holdout validáció:** Az adathalmaz egy részét elkülönítjük tesztelésre (pl. 70-30% megosztás).
- **K-keresztvalidáció (k-fold cross-validation):** Az adatot k egyenlő részre osztjuk, és minden rész külön tesztadatként szerepel egyszer, miközben a többi a tanításhoz használatos.
- **Stratified k-fold cross-validation:** Kiegyensúlyozott keresztvalidáció osztályeloszlások megtartásával, osztályozási problémáknál ajánlott.

A validáció révén felderíthetők az **adatfüggő torzítások, a túlilleszkedés (overfitting) és az alulilleszkedés (underfitting)** problémái.

5.3 Modell finomhangolása (tuning)

A teljesítménymérés és validáció után a modellek finomhangolására kerül sor, hogy a legjobb eredményt érjük el. A tuning célja a modell **hiperparamétereinek optimalizálása**:

- **Grid Search:** Egy előre definiált hiperparaméter-rács mentén próbál ki minden kombinációt.
- **Random Search:** A paraméterteret véletlenszerűen mintázza, hatékony nagy keresési területeken.
- **Bayesian Optimization:** Korábbi eredményekből tanulva, valószínűségi modellekkel választja ki a következő kipróbálandó paramétert.

A hiperparaméterek közé tartozhatnak például a **tanulási ráta (learning rate), regulációs együtthatók (regularization coefficients), döntési fák mélysége (tree depth), vagy neurális hálók rétegeinek száma (number of layers)**.

5.4 Modell-robosztusság és interpretáció

Egy ipari környezetben nem elég, ha egy modell pusztán pontos – fontos, hogy **robosztus és megbízható** legyen változó körülmények között is. A robosztusságot szimulációkkal, érzékenységvizsgálatokkal lehet ellenőrizni:

- **Feature Importance Analysis:** Megmutatja, mely bemeneti jellemzők a leginkább meghatározóak az előrejelzés szempontjából.
- **Partial Dependence Plots:** A változók és a predikció közötti kapcsolat vizualizálása.
- **SHAP (SHapley Additive exPlanations):** Egyre népszerűbb módszer a predikciók magyarázhatóságának biztosítására.

A magyarázhatóság kritikus, hiszen az üzleti döntéshozók **bizalmat és átláthatóságot** várnak el a modellektől.

5.5 Modell frissítése és életciklus-kezelés

A prediktív modellek nem statikusak: idővel **adatdrift** és **kontextusváltozások** miatt teljesítményük romolhat. Ezért elengedhetetlen egy **modell monitoring és retraining folyamat** kialakítása:

- **Automatizált teljesítmény-figyelés:** Kulcsmutatók rendszeres ellenőrzése.
- **Trigger alapú újratanítás:** Előre definiált teljesítményküszöbök átlépése esetén a modell automatikus újratanítása friss adatokkal.
- **Modell verziókezelés:** Különböző modellverziók tárolása, dokumentálása a követhetőség érdekében.

6. A mesterséges intelligencia és prediktív analitika jövője az iparban

Az ipar digitalizációja és automatizációja nemcsak jelenleg zajlik intenzíven, hanem a következő években még dinamikusabb fejlődés várható. A mesterséges intelligencia (MI) és a prediktív analitika területén tapasztalható technológiai előrelépések már most új lehetőségeket kínálnak a gyártóvállalatok számára, és átalakítják az üzleti döntéshozatal mechanizmusait. Ebben a fejezetben a legfontosabb trendeket, fejlődési irányokat és várható hatásokat vesszük sorra.

6.1 Mesterséges intelligencia a teljes gyártási ökoszisztémában

A mesterséges intelligencia az ipari környezetben fokozatosan elmozdul a szűk alkalmazási területektől (pl. hibadetektálás, gépi látás) egy átfogóbb, rendszerszintű szerep felé. Várható, hogy: [1], [6]

- Az MI **önoptimalizáló gyártósorokat** működtet, amelyek képesek valós időben módosítani paramétereiket.
- A **folyamatalapú tanulás** révén a rendszerek nemcsak reagálnak a változásokra, hanem előre képesek alkalmazkodni az új gyártási környezethez.
- A gyártási adatok nem szigetszerűen, hanem **egységes adatplatformon** keresztül fognak hasznosulni, megteremtve a teljes üzleti környezet integrált látását.

6.2 Üzleti döntéstámogatás fejlődése

A jövő analitikai rendszerei nem csupán adatokat szolgáltatnak, hanem egyre inkább **döntéshozatalt támogató tanácsadóként** működnek. Ennek főbb irányai:

- **Augmented analytics**: a rendszerek természetes nyelvi lekérdezésekre képesek válaszolni (pl. „Miért esett vissza a termelés tegnap?”), és javaslatokat is tesznek.

- **Szcenárió-alapú döntéshozatal**: több lehetséges üzleti kimenetel modellezése és értékelése különböző döntési utak mentén.
- Kognitív automatizáció: a döntések egy része teljesen automatizálttá válik a gépi tanulás és a szabályalapú rendszerek kombinációjával. [11]

6.3 Prediktív és preskriptív analitika összefonódása

Míg a prediktív analitika a jövő eseményeinek előrejelzésére koncentrál, a preskriptív analitika egy lépéssel tovább megy: azt is megmutatja, mit tegyünk a kívánt eredmény eléréséhez.

A két terület jövőbeni integrációja lehetővé teszi:

- **Optimalizált beavatkozások javaslatát** (pl. gyártási ütemezés, készletszintek módosítása)
- **Automatikus döntés-végrehajtást** az adott üzleti szabályrendszer alapján
- **Simulációk futtatását**, melyek vizsgálják a különféle döntések hosszú távú hatásait

6.4 Technológiai trendek, amelyek befolyásolják a fejlődést

A jövő analitikai rendszereinek fejlődését több technológiai újítás is katalizálja:

- **Edge computing**: az adatok helyi feldolgozása csökkenti a válaszidőt, kritikus az ipari alkalmazásoknál.
- **Digital twin technológia**: a fizikai rendszerek digitális másai lehetővé teszik a gyártási folyamatok valós idejű szimulációját.
- **IoT 2.0**: fejlettebb, intelligens szenzorhálózatok, amelyek képesek önálló döntések meghozatalára és tanulásra.

7. Következtetések és zárógondolatok

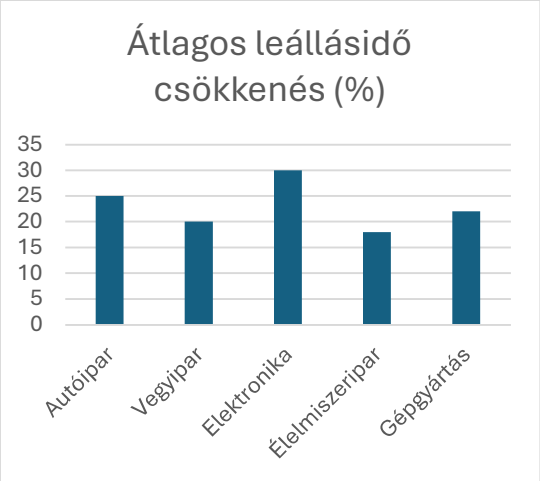
A dolgozat során részletesen megvizsgáltuk, hogyan támogatja a mesterséges intelligencia (MI) és a prediktív analitika az ipari termelésben történő üzleti döntéshozatalt. A tárgyalt elméleti és gyakorlati aspektusok alapján világosan kirajzolódik, hogy a vállalatok számára a prediktív analitikai eszközök bevezetése már nem csupán versenyelőnyt jelent, hanem egyre inkább alapfeltétele az ipar 4.0 környezethez való alkalmazkodásnak. [2], [4]

A modellépítési folyamat, az adatforrások strukturálása és a vállalati üzleti intelligencia rendszerekkel való integráció mind kritikus pontok a sikeres MI-alapú analitikai rendszer létrehozásához. Az is világossá vált, hogy a prediktív modellek nem önálló célként, hanem egy komplex döntéstámogató keretrendszer részeként működnek hatékonyan.

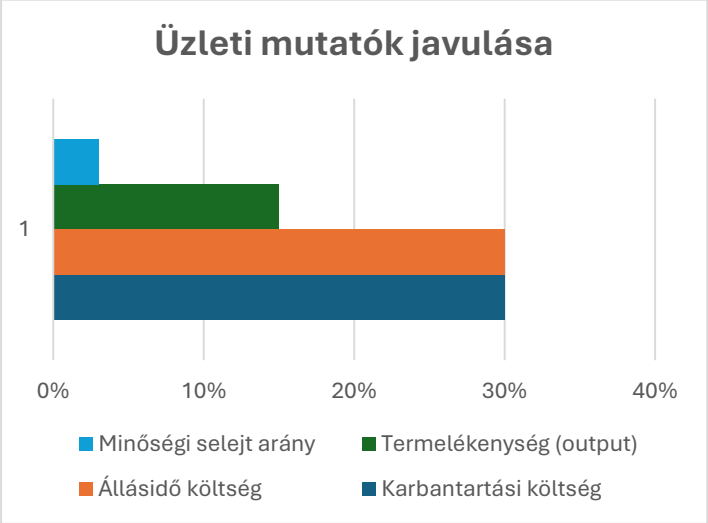
Főbb következtetések:

- Az adatok minősége, előkészítése és konzisztenciája meghatározza a prediktív modellek hasznosságát.
- Az üzleti döntéshozatal támogatása akkor működik hatékonyan, ha az elemzési eredmények közérthető és jól vizualizált formában jutnak el a döntéshozókhoz. [14]
- A prediktív analitika akkor éri el valódi potenciálját, ha integrálva van az ERP, SCM és CRM rendszerek működésébe.

Az előző fejezetekben bemutattuk a prediktív analitika működését, alkalmazási lehetőségeit és szerepét a döntéstámogatásban. Mindezek elméleti áttekintése után érdemes megvizsgálni a technológia gyakorlati, számszerűsíthető hatásait is. A következő ábrák szemléltetik, hogy a prediktív analitika milyen mértékben képes javítani az ipari vállalatok üzleti teljesítményét, különös tekintettel a költségek csökkentésére, a termelékenység növelésére, valamint a leállási idők rövidítésére.



leállásidő, forrás: [7]



uzleti mutatok, forrás: [7]

Zárógondolat:

Az MI és a prediktív analitika alkalmazása az ipari termelésben nem csupán technológiai, hanem szervezeti és stratégiai kérdés is. A jövő gyárai azok lesznek, amelyek képesek adatvezérelt módon működni, és az adatokat nem csak visszatekintő elemzésre, hanem proaktív, jövőbe mutató döntések meghozatalára is használják. Ehhez elengedhetetlen az MI technológiák integrálása a mindennapi működésbe, valamint a döntéshozatal átalakítása egy agilisabb, adatközpontú irányba.

Források:

A forrásokat összegyűjtötte és feldolgozta a **ChatGPT**

[1] T. Davenport and J. G. Harris, *Competing on Analytics: The New Science of Winning*, Boston, MA: Harvard Business School Press, 2007.

[2] E. Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*, 2nd ed., Hoboken, NJ: Wiley, 2016.

[3] G. Shmueli and O. Koppius, "Predictive analytics in information systems research," *MIS Quarterly*, vol. 35, no. 3, pp. 553–572, 2011.

[4] M. Kuhn and K. Johnson, *Applied Predictive Modeling*, New York, NY: Springer, 2013.

[5] B. Marr, Data Strategy: How to Profit from a World of Big Data, Analytics and the Internet of Things, 2nd ed., London: Kogan Page, 2021.

[6] M. Provost and T. Fawcett, *Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking*, Sebastopol, CA: O'Reilly Media, 2013.

[7] McKinsey & Company, "The age of analytics: Competing in a data-driven world," Dec. 2016. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world

[8] Gartner, "Top Trends in Data and Analytics for 2022," 2022. [Online]. Available: https://www.gartner.com/en/articles/top-trends-in-data-and-analytics-for-2022

[9] SAP, "Predictive Analytics – Integration with SAP ERP and SAP BW," SAP Help Portal. [Online]. Available: https://help.sap.com

[10] Microsoft, "Power BI documentation," [Online]. Available: https://learn.microsoft.com/en-us/power-bi/

[11] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, Cambridge, MA: MIT Press, 2016.

[12] J. W. Tukey, *Exploratory Data Analysis*, Reading, MA: Addison-Wesley, 1977.

[13] J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," in *Communications of the ACM*, vol. 51, no. 1, pp. 107–113, Jan. 2008.

[14] D. J. Power, "Decision Support Systems: A Historical Overview," *Handbook on Decision Support Systems*, Springer, pp. 121–140, 2008.

2.10. Önvezető járművek, okos tömegközlekedés és városi stratégiák, drónok és autonóm légi közlekedés a városokban

Önvezető járművek, okos tömegközlekedés és városi stratégiák, drónok és autonóm légi közlekedés a városokban

Csicsmann Kevin Hunor

Mérnökinformatikus BSC, kevinhun112@gmail.com

1. Bevezetés

A 21. század közlekedési rendszerei radikális átalakuláson mennek keresztül, amit a technológiai fejlődés, a mesterséges intelligencia, a fenntarthatósági törekvések és a városok folyamatos növekedése együttesen hajt előre. A városi mobilitás kihívásai – mint például a forgalmi torlódások, a környezetszennyezés, az energiahatékonyság hiánya és az infrastruktúra túlterheltsége – napjainkra sürgető szükségessé tették az intelligens, integrált és autonóm rendszerek alkalmazását. A közlekedés digitalizációja nem csupán kényelmi fejlesztés, hanem stratégiai válasz a klímaválságra, a demográfiai nyomásra és a gazdasági fenntarthatóság kérdéseire is.

Ez a dolgozat az intelligens közlekedési megoldások különféle aspektusait vizsgálja, különös tekintettel az önvezető járművekre, az okos tömegközlekedési rendszerekre, a városi mobilitásmenedzsment stratégiáira, valamint a drónok és autonóm légi járművek szerepére. A cél az, hogy átfogó képet adjunk arról, hogyan integrálhatóak ezek az új technológiák egy hatékony, fenntartható és biztonságos városi közlekedési ökoszisztémába.

A kutatás során részletesen bemutatjuk a háttértechnológiákat – például a mesterséges intelligencián alapuló vezérlőrendszereket, szenzorikus rendszereket (mint a LIDAR, RADAR, kameraalapú és ultrahangos érzékelők), a V2V (vehicle-to-vehicle) és V2X (vehicle-to-everything) kommunikációs protokollokat –, valamint a különféle szoftverarchitektúrákat, amelyek lehetővé teszik az autonóm működést és a rendszerintegrációt. Ugyanakkor hangsúlyt fektetünk az ADAS (Advanced Driver Assistance Systems) technológiák szerepére, amelyek átmenetet képeznek a kézi irányítás és a teljes autonómia között, fokozva a biztonságot és csökkentve az emberi hibákból eredő balesetek számát.

A dolgozat célja nem csupán a jelenlegi trendek és megoldások bemutatása, hanem azok kontextusba helyezése egy tágabb várostervezési, társadalmi és etikai keretrendszerben. Mivel az intelligens közlekedés nem technikai szigetként működik, hanem komplex rendszerek és szereplők (állampolgárok, önkormányzatok, közlekedési vállalatok, szoftverfejlesztők) együttműködésének eredményeként, elengedhetetlen ezeknek a szempontoknak a részletes tárgyalása is. A társadalmi elfogadottság, a hozzáférhetőség, az adatvédelem és az etikai döntéshozatal mind olyan kérdések, amelyek az autonóm közlekedés jövőjét meghatározzák.

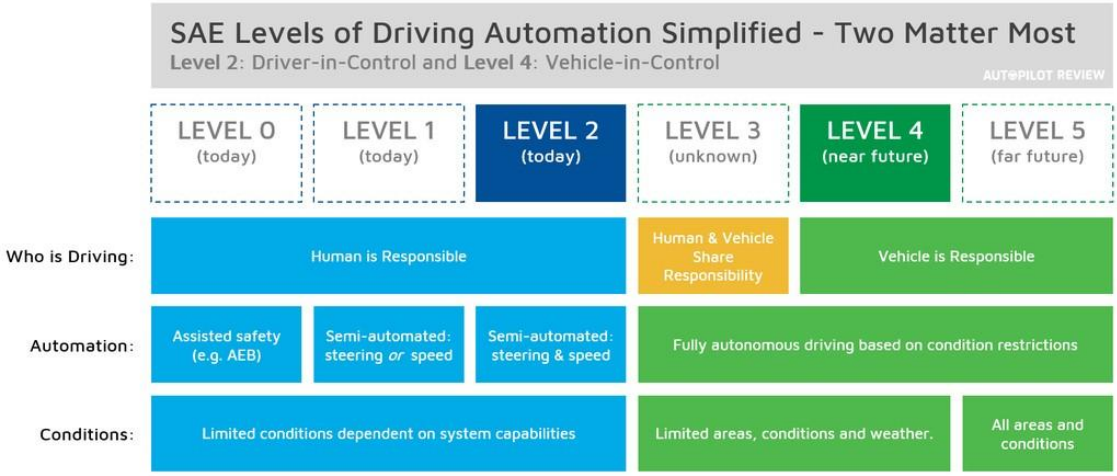
A dolgozat végigvezet az elméleti alapokon, gyakorlati példákon keresztül bemutatva a világ különböző pontjain már működő megoldásokat – legyen szó Szingapúr drón-alapú csomagszállításáról, Helsinki okos buszhálózatáról vagy Kalifornia önvezető flottáiról. A cél, hogy a dolgozat olvasója teljes képet kapjon arról, miként válik a jövő mobilitása napjaink valóságává – és milyen kérdésekre kell még válaszolnunk, mielőtt az intelligens közlekedés széles körben elterjedhetne.

2. Önvezető járművek: technológiai háttér és működés

2.1 Bevezetés az autonóm járművek világába

Az önvezető járművek már nem a távoli jövő sci-fi víziói, hanem egyre inkább a jelen és a közeljövő meghatározó szereplői a közlekedésben. Ezek a járművek képesek emberi beavatkozás nélkül érzékelni a környezetüket, döntéseket hozni és biztonságosan közlekedni a városi vagy közúti forgalomban. A mögöttes technológia összetett szenzorrendszerek, algoritmusok, mesterséges intelligencia és valós idejű adatfeldolgozás együtteséből áll.

Az autonóm járműveket az SAE (Society of Automotive Engineers) besorolása alapján hat különböző szintre osztjuk (0-tól 5-ig), ahol a 0-szint teljesen emberi vezérlést jelent, míg az 5. szint teljesen autonóm működést, amely során az emberi beavatkozásra egyáltalán nincs szükség. A mai járművek többsége a 2-es vagy 3-as szintet képviseli, ahol az autó képes például sávtartásra, követési távolság tartására, de a sofőrnek továbbra is figyelemmel kell kísérnie az utat.



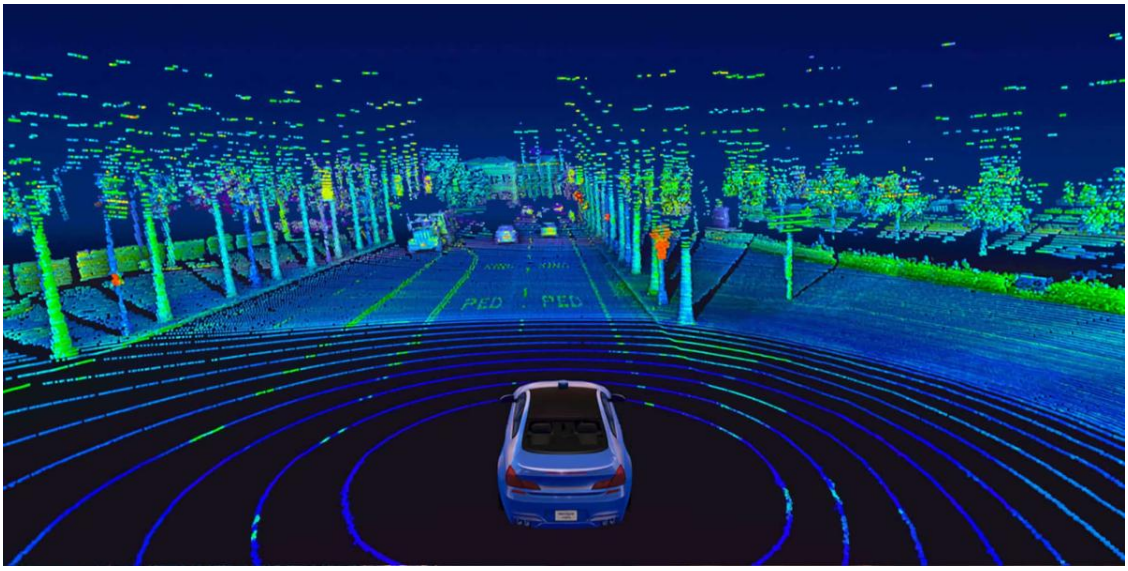
1. ábra: SAE autonómiaskála szemléltetése 0-tól 5-ig, a “SAE Self-Driving Levels 0 to 5 for Automation – What They Mean” cikkéből [Publikus forrás] (autopilotreview.com/self-driving-cars-sae-levels/)

2.2 Szenzorok és észlelés: a jármű „érzékszervei”

Az önvezető autók működésének egyik alapfeltétele a környezet pontos érzékelése. Ehhez többféle szenzor kombinációjára van szükség:

- LIDAR (Light Detection and Ranging): lézeralapú távolságmérés, amely 3D-s térképet hoz létre a jármű környezetéről.
- Radar: rádióhullámokat használ távolság és sebesség mérésére, különösen hasznos rossz látási viszonyok között.
- Ultrahangos szenzorok: elsősorban parkolásnál, rövid távú manőverezésnél használják.
- Kamerarendszerek: vizuális információkat gyűjtenek a sávok, jelzőlámpák, táblák és gyalogosok azonosítására.

Ezeket a szenzorokat úgynevezett sensor fusion (szenzorfúziós) rendszerek kapcsolják össze, amelynek célja az eltérő forrásokból származó adatok egységes és megbízható környezeti modellezése. Az adatok feldolgozását mesterséges intelligencián alapuló algoritmusok végzik, amelyek képesek felismerni objektumokat, értelmezni közlekedési helyzeteket és előre jelezni a többi közlekedő mozgását.



2. ábra LiDAR techológia működési illusztrációja a “Mi az a LiDAR technológia és hogyan működik?” cikkéből [Publikus forrás] (bytech.hu/lidar/)

2.3 ADAS rendszerek: az autonómia előszobája

A fejlett vezetéstámogató rendszerek (ADAS – Advanced Driver Assistance Systems) a teljes autonómia felé vezető átmenet kulcselemei. Ezek az intelligens funkciók már ma is jelen vannak sok járműben, és fokozatosan bővülnek:

- Automatikus vészfékezés
- Adaptív tempomat
- Sávtartó automatika
- Holttérfigyelés
- Fáradtságérzékelés

Az ADAS rendszerek célja, hogy fokozzák a biztonságot, csökkentsék az emberi hibákból eredő balesetek számát, és előkészítsék a sofőröket a jövő autonóm technológiáira. Fontos hangsúlyozni, hogy ezek a rendszerek még nem helyettesítik a sofőrt, de jelentősen képesek csökkenteni a kockázatokat – és közben folyamatosan adatokat is gyűjtenek a későbbi autonóm modellek számára.

2.4 V2X kommunikáció: az összekapcsolt járművek világa

Az önvezető járművek biztonságos működéséhez nem elég a környezet észlelése: szükség van arra is, hogy a jármű kommunikáljon más járművekkel (V2V – vehicle-to-vehicle), az infrastruktúrával (V2I – vehicle-to-infrastructure), valamint a gyalogosokkal és okoseszközökkel is (V2X – vehicle-to-everything). Ez az összekapcsoltság lehetővé teszi:

- a balesetek korai előrejelzését,
- a torlódások csökkentését,
- az intelligens útvonaltervezést,
- és a forgalom adaptív szabályozását.

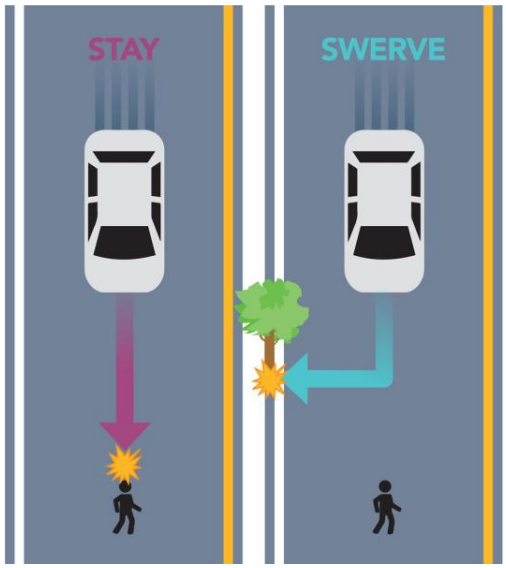
A V2X technológiák olyan hálózatokat építenek ki, amelyek révén a járművek „látják” a sarkon túli eseményeket, vagy például előre tudják, mikor vált pirosra a jelzőlámpa. Ez nemcsak kényelmesebbé, de jelentősen biztonságosabbá is teszi a közlekedést.

2.5 Technológiai és etikai kihívások

Az autonóm járművek fejlesztése során nemcsak technológiai, hanem társadalmi és etikai kérdések is felmerülnek. Ilyen például a felelősség kérdése baleset esetén: ki hibázott – a jármű szoftverét író fejlesztő, a gyártó vagy az utas? További kihívások:

- Az adatvédelem és a személyes információk kezelése
- A kiberbiztonság (hackertámadások elleni védelem)
- Az algoritmusok „etikája” – például hogyan dönt egy jármű vészhelyzetben?

Ezen kérdések megoldása nem csak műszaki, hanem jogi, szabályozási és társadalmi szinten is elengedhetetlen



.

3. ábra: Etikai dilemma az önvezető autók döntéseivel kapcsolatban az “Uncomfortable ethics for autonomous vehicles” cikkéből [Publikus forrás] (researchoutreach.org/articles/uncomfortable-ethics-autonomous-vehicles/)

3. Okos tömegközlekedés és városi mobilitási stratégiák

3.1 A városi közlekedés új kihívásai

A városok világszerte egyre komolyabb mobilitási kihívásokkal néznek szembe: növekvő népességkoncentráció, zsúfolt utak, légszennyezés, zajterhelés, valamint a közlekedéshez kapcsolódó szén-dioxid-kibocsátás. A hagyományos tömegközlekedési rendszerek – bár alapvető elemei a városi mobilitásnak – nem mindig képesek hatékonyan kezelni ezeket a problémákat. A jövő városi közlekedése ennek megfelelően egyre inkább az okos mobilitás irányába mozdul el, amely integrált, digitális alapokon működő, rugalmas és környezetbarát megoldásokat kínál.

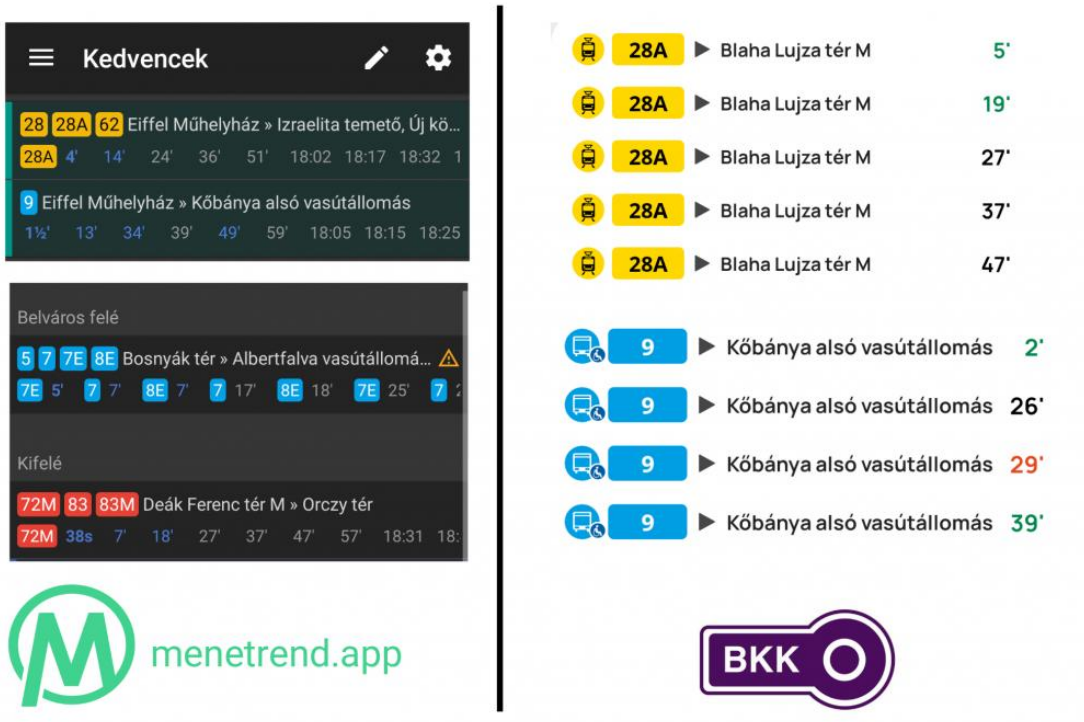
Az „okos tömegközlekedés” fogalma olyan intelligens technológiák, rendszerek és stratégiák együttesét jelenti, amelyek célja a közösségi közlekedés hatékonyságának, pontosságának, biztonságának és környezeti fenntarthatóságának növelése. Ezek közé tartoznak a valós idejű adatközvetítés, az elektromos járművek, az önvezető buszok, a dinamikus menetrendek és az utazói szokásokat elemző algoritmusok.

4. ábra: Ábra az intelligens rendőrlámpákról a “Civic Analytics 2018” cikkéből [Publikus forrás] (medium.com/civic-analytics/smart-traffic-lights-or-intelligent-traffic-lights-are-a-vehicle-traffic-control-system-that-ab5429ca0c40)

3.2 Intelligens tömegközlekedési technológiák

Az okos közlekedés gerincét a digitális infrastruktúra és az azt támogató technológiai megoldások képezik. Az alábbi eszközök és rendszerek képezik a modern tömegközlekedés technológiai alapját:

- GPS-alapú nyomkövetés és valós idejű információmegosztás: az utasok a mobiltelefonjukon valós időben láthatják, mikor érkezik a következő busz vagy villamos.
- Intelligens jegyrendszerek: lehetővé teszik a jegyvásárlást mobilalkalmazással vagy kontaktmentes bankkártyával.
- IoT-alapú járműmonitoring: az okoseszközökkel felszerelt járművek valós idejű adatokat küldenek a jármű állapotáról, terheltségéről, energiafogyasztásáról.
- AI-alapú forgalomoptimalizálás: algoritmusok elemzik a forgalmi adatokat, és dinamikusan módosítják a menetrendeket, útvonalakat.
- E technológiák célja a közlekedés hatékonyságának növelése, a késések csökkentése, a járműpark jobb kihasználása, valamint a környezeti terhelés minimalizálása.



5. ábra a valós idejű tömegközlekedési eszközöket követő telefonos alkalmazásokról a “Menetrend.app – miért használom?” cikkéből [Publikus forrás] (https://kozlekedes.org/menetrend-app-miert-hasznalom/)

3.3 Elektromos buszok és alacsony kibocsátású zónák

A városi levegőminőség javítása érdekében világszerte egyre több nagyváros vezeti be az elektromos autóbuszokat és az alacsony kibocsátású zónákat (LEZ – Low Emission Zones). Az elektromos buszok működésük során nem bocsátanak ki kipufogógázt, zajszintjük alacsonyabb, és üzemeltetésük hosszú távon gazdaságosabb lehet, különösen ha megújuló energiával töltik őket.

Az ilyen járművek töltése történhet hagyományos kábeles rendszerekkel, indukciós töltéssel vagy pantográfos megoldással, amely lehetővé teszi a jármű út közbeni töltését. Az elektromos buszok alkalmazása különösen hatékony lehet zárt, jól szabályozott útvonalakon, például belvárosi vagy repülőtéri transzferek esetén.

6. ábra az elektromos buszokról és azok töltőállomásáról Milánban. [Publikus forrás] (https://www.sustainable-bus.com/electric-bus/fast-charging-station-electric-buses-atm-milano/)

3.4 Mobilitási központok és multimodális integráció

Az okos városokban egyre gyakrabban jelennek meg úgynevezett mobilitási központok (mobility hubs), ahol a különböző közlekedési módok – például tömegközlekedés, közösségi kerékpármegosztás, elektromos

rollerbérlés, taxi, car-sharing – egyszerre, integrált módon érhetők el. A cél: egyetlen alkalmazáson belül, egy jeggyel lehetővé tenni a teljes út megtervezését, fizetését és lebonyolítását.

Ezt a koncepciót nevezzük MaaS-nak (Mobility-as-a-Service). A MaaS nem csupán technológiai fejlesztés, hanem közlekedésszervezési paradigma is, amely a személyes autóhasználat visszaszorításával egy fenntarthatóbb, kevésbé zsúfolt városi közlekedési struktúrát támogat.

3.5 Adatvezérelt várostervezés és adaptív forgalomirányítás

A városi mobilitás jövője az adatvezérelt városirányításban rejlik. Az intelligens városok szenzorai, forgalmi kamerái, tömegközlekedési rendszerei és mobilalkalmazásai folyamatosan hatalmas mennyiségű adatot gyűjtenek. Ezek elemzése lehetővé teszi:

- a torlódási pontok azonosítását,
- a közlekedési mintázatok felismerését,
- a forgalom dinamikus szabályozását.

Az adaptív forgalomirányítási rendszerek képesek azonnal reagálni a változó körülményekre: például zöldhullámot biztosítanak a tömegközlekedésnek csúcsidőben, vagy módosítják a lámpák ciklusát baleset vagy útlezárás esetén. Ezzel jelentősen csökken a felesleges várakozási idő, a szén-dioxid-kibocsátás, és nő az utazási élmény minősége.

3.6 Társadalmi és környezeti hatások

Az okos tömegközlekedési rendszerek hatása nemcsak műszaki, hanem társadalmi és környezeti szinten is jelentős. A megfelelően kialakított rendszerek csökkentik a közlekedési egyenlőtlenségeket, mivel elérhetőbbé teszik a közlekedést az alacsony jövedelmű lakosság számára is. Emellett mérséklik a városi hőszigethatást, csökkentik a légszennyezést, valamint növelik a város élhetőségét.

Az ENSZ fenntartható fejlődési céljaival (SDG) összhangban az okos tömegközlekedés hozzájárul a klímaváltozás elleni küzdelemhez, az energiatakarékossághoz, és a társadalmi egyenlőség előmozdításához is.

4. Önvezető járművek: technológia, működés és integráció

4.1 Az önvezető járművek fejlődése és jelentősége

Az önvezető járművek (Autonomous Vehicles – AV-k) nem csupán technológiai csodák, hanem a modern városi közlekedés alapvető átalakulásának kulcsszereplői. Az AV-k olyan járművek, amelyek emberi beavatkozás nélkül képesek közlekedni, a környezet érzékelése, a döntéshozatal és a manőverezés teljes egészében szoftveres és gépi intelligenciára van bízva. Az önvezetés jelentősége messze túlmutat a kényelemen: a cél a közlekedés biztonságosabbá, hatékonyabbá és környezetbaráttá tétele, miközben csökkenthető a balesetek, torlódások és a károsanyag-kibocsátás aránya.

Az önvezető technológia fejlődését a 2010-es évektől kezdve elsősorban olyan technológiai vállalatok vezették, mint a Google (Waymo), Tesla, Uber, illetve autóipari óriások, például a GM, a Ford és a Mercedes-

Benz. Az első generációs rendszerek még csak egyszerű vezetéstámogató funkciókat kínáltak, de ma már léteznek olyan önvezető rendszerek, amelyek Level 4 vagy Level 5 autonómiát kínálnak (a SAE-szabvány szerinti skálán), azaz emberi felügyelet nélkül is képesek közlekedni bizonyos környezetekben.

7. ábra: Tesla autópilóta önvezetési módban levő overlay-e az “All Tesla Visualizations and What They Mean” [Publikus forrás] (notateslaapp.com/tesla-reference/636/all-tesla-fsd-visualizations-and-what-they-mean)

4.2 Az autonóm járművek érzékelési rendszerei

Az önvezető járművek működésének alapja a környezet pontos és valós idejű érzékelése. Ehhez a következő szenzortípusokat alkalmazzák, gyakran kombinálva:

- LIDAR (Light Detection and Ranging): lézeres letapogatással térképezi fel a környezet háromdimenziós szerkezetét. Nagy pontosságú, de költséges technológia.
- RADAR: rádióhullámokat használ a járművek és tárgyak távolságának, sebességének meghatározásához. Rossz látási viszonyok között is jól működik.
- Kamerák: vizuális adatokat gyűjtenek, amelyek fontosak a közlekedési táblák, sávjelzések, gyalogosok azonosítására.
- Ultrahangos szenzorok: elsősorban rövidtávú, alacsony sebességű manőverezésnél, például parkoláskor használják.
- IMU (Inertial Measurement Unit) és GPS: a jármű saját mozgását és pozícióját követik nyomon nagy pontossággal.

Az érzékelőfúzió révén ezek a szenzorok együttesen adják az AV számára a valósághű, redundáns és robusztus környezetérzékelést, amely kulcsfontosságú a biztonságos működéshez.

4.3 Mesterséges intelligencia és döntéshozatal

Az érzékelt adatok értelmezését, valamint az ez alapján történő döntéshozatalt a mesterséges intelligencia (AI) végzi, amely több alrendszerre épül:

- Kép- és objektumfelismerés (Computer Vision): a kamera- és LIDAR-adatok alapján felismeri az autókat, gyalogosokat, kerékpárosokat, közlekedési táblákat stb.
- Prediktív modellek: megpróbálják előre jelezni a többi közlekedő viselkedését, például hogy egy gyalogos elindul-e átkelni.
- Pályatervezés és mozgásvezérlés: meghatározza a jármű optimális útvonalát és sebességét úgy, hogy elkerülje az akadályokat, betartsa a szabályokat és biztosítsa a kényelmet.
- Gépi tanulás és mélytanulás: folyamatosan javítja a jármű viselkedését a begyűjtött tapasztalatok alapján.

E rendszerek kulcsa a megbízhatóság és a valósidejűség: az AI-nak másodperc törtrésze alatt kell helyes döntést hoznia kritikus helyzetekben, például ha egy gyalogos lép ki az úttestre.

4.4 ADAS rendszerek: a részleges automatizálástól a teljes önvezetésig

A legtöbb ma elérhető autó még nem teljesen autonóm, de rendelkezik fejlett vezetéstámogató rendszerekkel (ADAS – Advanced Driver Assistance Systems), amelyek a teljes önvezetés felé tett lépéseknek tekinthetők. Ilyen rendszerek:

Adaptív tempomat: automatikusan szabályozza a sebességet és követési távolságot.

Sávelhagyásra figyelmeztető és sávtartó rendszer: korrigálja a jármű irányát.

Automatikus vészfékezés: balesetveszély esetén aktiválja a fékeket.

Holttérfigyelő rendszer: segíti a biztonságos sávváltást.

E rendszerek már most csökkentik a balesetek számát, és fokozatosan készítik elő a közvéleményt és a jogi környezetet a teljes autonómia befogadására.

4.5 V2V, V2I és V2X kommunikáció: hálózatra kapcsolt járművek

Az önvezető járművek önmagukban is intelligensek, de képességeik jelentősen kibővíthetők, ha kommunikálnak más járművekkel és a környezettel. Ezt hívjuk Vehicle-to-Everything (V2X) kommunikációnak, amely három fő komponensből áll:

- V2V (Vehicle-to-Vehicle): járművek közvetlenül kommunikálnak egymással például fékezésről, sávelhagyásról, sebességváltozásról.
- V2I (Vehicle-to-Infrastructure): kapcsolat a közlekedési lámpákkal, forgalomirányító rendszerekkel, úthibákat észlelő szenzorokkal.
- V2P (Vehicle-to-Pedestrian): járművek és gyalogosok vagy kerékpárosok között zajló kommunikáció, például okostelefonokon keresztül.

Ezek a rendszerek hozzájárulnak a kooperatív közlekedéshez, amely során a járművek előre tudnak tervezni, reagálni és segíteni egymást a balesetek, torlódások és félreértések elkerülése érdekében.

4.6 Etikai, jogi és társadalmi kérdések

Az önvezető járművek elterjedése számos etikai és szabályozási kihívást is felvet. Kiemelkedő kérdés például az úgynevezett morális döntéshozatal: hogyan döntsön egy AV egy elkerülhetetlen baleset esetén? Kit védjen jobban – az utast, a gyalogost, a másik jármű vezetőjét?

Emellett a felelősség kérdése is összetett: ha egy baleset önvezető jármű miatt következik be, ki a felelős – a gyártó, a szoftverfejlesztő, az utas? Az adatvédelem is komoly kihívás, hiszen az AV-k hatalmas mennyiségű adatot gyűjtenek a környezetükről és az utasokról.

A jogalkotás világszerte igyekszik lépést tartani a technológia fejlődésével, de jelenleg még sok országban hiányoznak az átfogó szabályozási keretek. A társadalom elfogadása is fokozatos: bizalom, transzparencia és oktatás szükséges ahhoz, hogy az AV-k valóban integrálódhassanak a városi közlekedésbe.

5. Drónok és autonóm légi közlekedés a városokban

5.1 Bevezetés az Urban Air Mobility (UAM) világába

Az Urban Air Mobility (UAM) olyan közlekedési forma, amely a városi légteret használja ki a gyors, hatékony és gyakran autonóm utas- vagy áruszállítás céljából. A városokban tapasztalható egyre nagyobb közúti forgalom, a légszennyezés, valamint az infrastruktúra túlterheltsége új megoldásokért kiáltanak – ezekre kínál választ a légiközlekedés vertikális dimenzióba történő kiterjesztése. A UAM célja, hogy kiegészítse a meglévő közlekedési módokat, enyhítse a felszíni torlódásokat, és gyorsabb, dinamikusabb mobilitást biztosítson a nagyvárosi térségekben.

Az elképzelés lényege, hogy kis méretű, többnyire elektromos hajtású, autonóm légi járművek (AAV – Autonomous Aerial Vehicles) végeznek majd utasszállítást (eVTOL – electric Vertical Take-Off and Landing) vagy áruszállítást (pl. drónos csomagkézbesítés), integrálódva a városi közlekedési hálózatokba.

8. ábra egy VTOL járműről a városi közlekedésben. [Publikus forrás] (https://newatlas.com/urban-aeronautics-cityhawk-flying-car-vtol/55589/)

5.2 Dróntechnológia a városi közlekedésben

A drónok, hivatalos nevükön pilóta nélküli légi járművek (UAV – Unmanned Aerial Vehicles) már most is számos alkalmazási területen jelen vannak: áruszállítás, forgalomfigyelés, térképezés, vészhelyzeti reagálás. Ezekben az esetekben a fő előnyük a gyorsaság, a rugalmasság és az, hogy nem terhelik a közúti infrastruktúrát.

Főbb városi alkalmazások:

- Csomagkézbesítés: cégek, mint az Amazon Prime Air, UPS Flight Forward vagy a DHL drónos rendszerei már pilot-projekteket működtetnek. A cél, hogy 10–15 perces időtávon belül történjen a kiszállítás.
- Orvosi szállítás: életmentő vér, gyógyszer vagy szerv szállítása forgalmi dugók kikerülésével, például a Zipline vagy a Matternet rendszerei révén.
- Közlekedési felügyelet: drónokkal valós időben lehet monitorozni a forgalmat, baleseteket vagy tömegrendezvényeket.
- Vészhelyzet-kezelés: tűz, földrengés vagy árvíz esetén drónok segíthetik a mentést, az áldozatok felkutatását vagy az információgyűjtést.

9. ábra: csomagszállító drónr a városban a “Cargo drones” cikkéből [Publikus forrás] (https://www.rolandberger.com/en/Insights/Publications/Cargo-drones-The-urban-parcel-delivery-network-of-tomorrow.html)

5.3 Autonóm légi járművek rendszerei és működése

Az AAV-k működésének alapját hasonlóan az önvezető járművekhez, a valós idejű szenzoros érzékelés, navigáció és döntéshozatal alkotja. A fő technológiai elemek:

- Inerciális navigáció + GNSS (Global Navigation Satellite Systems) kombinációja a pozíció pontos meghatározására.
- Obstacle Avoidance rendszerek: lidar és optikai szenzorok segítik az akadályok elkerülését.
- Automatikus pályatervezés és repülési szabályozás: mesterséges intelligencia és prediktív algoritmusok segítségével.
- Adatkapcsolat (C2 link): valós idejű kommunikációs csatornák a földi irányítás, más járművek és az infrastruktúra felé.

A rendszer kulcsa a redundancia és a biztonság. Mivel ezek a járművek lakott területek felett közlekednek, a rendszerhibák kizárására háromszoros hardveres és szoftveres védelem szükséges. A hajtásrendszerek jellemzően elektromosak, több rotorral, és képesek a függőleges felszállásra és landolásra (VTOL).

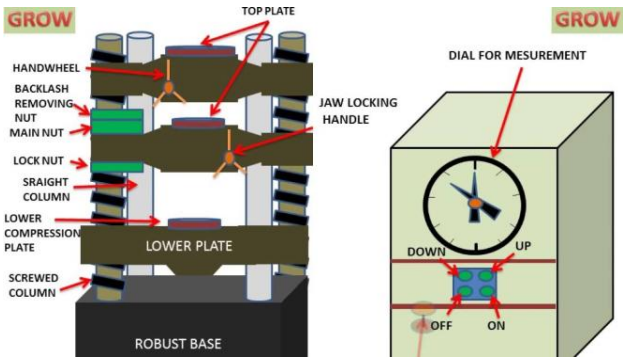
5.4 Légiforgalmi irányítás városi légtérben

A városi légiközlekedés egyik legnagyobb kihívása nem a technológia, hanem a légiforgalom irányításának megoldása. A jelenlegi repülési szabályozások nem teszik lehetővé a nagyszámú alacsonyan repülő drón egyidejű, biztonságos működését.

Erre a problémára az UTM (Unmanned Traffic Management) rendszert fejlesztik, amely egyfajta „digitális légiirányítás” a pilóta nélküli légi járművek számára. Az UTM funkciói:

- Légifolyosók kijelölése, automatikus konfliktuskezelés
- Dinamikus légtérmenedzsment (pl. vészhelyzet esetén)
- Repülési engedélyek automatizált kiadása
- Zónák kijelölése (pl. tiltott, előnyben részesített vagy szigorúan ellenőrzött területek)

A jövőben várhatóan a mesterséges intelligenciával támogatott UTM rendszerek valós időben fognak irányítani több ezer drónt egyidejűleg egy város légterében.



10. ábra: UTM működési elve. [Publikus forrás]
(https://www.youtube.com/watch?app=desktop&v=4z_UFvl8rjw)

5.5 Társadalmi elfogadás, zajszennyezés és adatbiztonság

A városi drónközlekedés elterjedéséhez nemcsak technológiai, hanem társadalmi elfogadás is szükséges. Számos lakos tart az állandó zajterheléstől, a magánszféra megsértésétől (kamerás megfigyelés), illetve a biztonsági kockázatoktól.

A legfőbb aggályok:

- Zajszennyezés: a rotoros járművek által keltett zaj zavaró lehet a sűrűn lakott területeken. Ennek csökkentésére elektromos hajtású, csendes működésű rotorokat fejlesztenek.
- Adatvédelem és megfigyelés: a drónok kamerái és szenzorai személyes adatokat is rögzíthetnek. Ez új szabályozási és etikai kérdéseket vet fel.
- Biztonság és hackelés: az autonóm drónrendszerek kibertámadásokkal szembeni sebezhetősége komoly kockázat, ezért szigorú kiberbiztonsági architektúrákra van szükség.

Szabályozás és lakossági konzultáció: az elfogadottság növelése érdekében a helyi közösségek bevonása, edukációs programok és tesztprojektek bevezetése elengedhetetlen.

5.6 A jövő városai és a vertikális mobilitás integrációja

A városi légi közlekedés nem önmagában, hanem a többi mobilitási forma részeként tud hatékonyan működni. A jövő városában multimodális közlekedési csomópontokat képzelhetünk el, ahol az utas néhány perces átszállással válthat elektromos buszról drón-taxiszolgáltatásra, vagy fordítva.

Ehhez szükséges:

- Skyportok (légiállomások) kiépítése a városi csomópontokban.
- Digitális infrastruktúra integrálása a földi közlekedés irányító rendszereivel.
- Egységes mobilitási platformok kialakítása, ahol egy applikáción keresztül tervezhető és foglalható minden utazás (pl. MaaS – Mobility as a Service modell).

11. ábra: Koncepciós terv egy Skyportról a városban. [Publikus forrás] (skyports.net/)

6. A közlekedés intelligens jövője

6.1 A közlekedési rendszerek átalakulása a digitális korban

Az elmúlt évtizedek közlekedési paradigmája drasztikus átalakuláson megy keresztül a digitális technológiák fejlődésének köszönhetően. A klasszikus, emberi vezérlésű járművektől indulva ma már a teljesen autonóm rendszerek felé tartunk. A dolgozat során részletesen áttekintettük az önvezető járművek működését, a fejlett vezetéstámogató rendszerek (ADAS) szerepét, a járművek közötti (V2V) és infrastruktúrához történő (V2I) kommunikáció fontosságát. Külön foglalkoztunk a városi tömegközlekedés digitalizációjával, az elektromos buszokkal, valós idejű utastájékoztató rendszerekkel, dinamikus útvonaltervezéssel és prediktív forgalomszabályozással.

Az autonóm légi közlekedés területén a drónok váltak a legfontosabb szereplőkké, amelyek ma már nemcsak logisztikai, hanem mentési és térinformatikai feladatokat is ellátnak a városi környezetben. A smart közlekedés fejlődése azonban nemcsak technológiai kérdés: kulcsfontosságú az adatbiztonság, a felhasználók személyes adatainak védelme, valamint a kiberbiztonsági fenyegetések elleni védekezés. A szabályozói környezetnek ehhez a változáshoz szinte minden szinten alkalmazkodnia kell: a felelősségi viszonyok újradefiniálása, az autonóm rendszerek etikai dilemmái és az infrastruktúra újratervezése egyaránt elengedhetetlen feltételei a sikeres átmenetnek.

6.2 Jövőkép: Merre tart a smart közlekedés?

A jövő intelligens közlekedése nem csupán járműtechnológiai kérdés, hanem egy komplex ökoszisztéma, amely integrálja az urbanisztikát, az energetikát, a környezetvédelmet, a mesterséges intelligenciát és a társadalomtudományokat. Néhány meghatározó trend már most kirajzolódik:

6.2.1 Integrált multimodális rendszerek

A jövő közlekedése nem önálló járművekről, hanem integrált mobilitási megoldásokról fog szólni. Az autó, a busz, a metró, a kerékpár, a gyalogos közlekedés, és akár a légi járművek is egy egységes digitális platformba fognak integrálódni, amely az egyéni igényekhez igazodva, valós időben tervez útvonalat. Az "MaaS" (Mobility as a Service) koncepció szerint a felhasználó már nem birtokol járművet, hanem szolgáltatásként veszi igénybe a mobilitást.

A városlakó egyetlen applikáció segítségével kiválaszthatja, hogy mikor melyik közlekedési módot szeretné használni, és a rendszer automatikusan megtervezi az útvonalat, lefoglalja az eszközöket, optimalizálja az utazást és akár a fizetést is elintézi. A szolgáltatások személyre szabottá válnak, és az algoritmusok figyelembe veszik a felhasználó szokásait, egészségi állapotát, ökológiai lábnyomát és időkereteit is.

6.2.2 Környezetbarát, fenntartható közlekedés

A közlekedés átalakulása nem választható el a klímavédelmi törekvésektől. A jövő városai számára prioritás lesz a szén-dioxid-kibocsátás csökkentése, az energiahatékonyság növelése és a zöld közlekedési alternatívák támogatása. Az elektromos járművek mellett egyre fontosabbá válik a hidrogénmeghajtás, a megújuló energiával működtetett tömegközlekedési eszközök és az energia-visszanyerés technológiája (rekuperáció, intelligens fékrendszerek stb.).

A városi tervezés középpontjába kerülnek az autómentes zónák, az intelligens parkolási rendszerek, valamint az olyan megoldások, amelyek csökkentik a járművek számát a közutakon. A digitális technológiák segítenek optimalizálni a közlekedést, csökkentik a torlódásokat, és lehetővé teszik az adaptív forgalomszabályozást, amely dinamikusan reagál a valós idejű adatokra.

6.2.3 Városi légiközlekedés és vertiportok

A városi légi közlekedés – különösen a VTOL (Vertical Take-Off and Landing) eszközök elterjedésével – egyre közelebb kerül a megvalósításhoz. Az autonóm személyszállító drónok (pl. Volocopter, Joby Aviation, Lilium Jet) tesztelése már több országban is zajlik. A jövő városaiban megjelenhetnek a vertiportok, azaz olyan kis méretű, városon belüli repülőterek, ahol drónok és VTOL járművek landolhatnak és felszállhatnak, integrálva az utasokat a hagyományos tömegközlekedési rendszerbe.

Ehhez természetesen szükség lesz új típusú várostervezésre is: a légiközlekedési útvonalakat, zajszinteket, biztonsági zónákat, energiaellátást és karbantartási infrastruktúrát mind figyelembe kell venni a jövő városainak kialakításakor.

6.2.4 Mesterséges intelligencia által vezérelt városi közlekedés

A jövő közlekedésének gerincét a mesterséges intelligencia (AI) adja majd. Az AI alapú rendszerek képesek lesznek milliónyi adatpontot feldolgozni valós időben, felismerni a mintázatokat, és előre jelezni a közlekedési viszonyokat, torlódásokat vagy balesetveszélyes helyzeteket. A prediktív modellezés alapján a rendszer javaslatokat tehet az útvonal optimalizálására, vagy akár önállóan átállítja a forgalomirányító lámpákat.

Az autonóm járművek irányításán túl az AI szerepet kap az erőforráselosztás optimalizálásában is: mikor hova küldjön elektromos buszt, hol helyezzen el megosztott járműveket, mikor kell bővíteni egy töltőállomás kapacitását. Az AI továbbá támogatja a várostervezési döntéshozatalt, az adatok alapján javaslatokat tesz a forgalomsűrűség csökkentésére, a levegőminőség javítására, vagy új közlekedési útvonalak kialakítására.

12. ábra: Jövőbeni Vertiport koncepciója, szemlélteti, hogy a földi, légi és vízi közlekedést egybekötik a nagyvárosokban. [Publikus forrás] (https://www.dezeen.com/2020/03/04/mvrdv-airbus-vertiports-flying-vehicle-city-report/)

7. Etikai, társadalmi és biztonsági kihívások az intelligens közlekedésben

A smart közlekedési rendszerek fejlődése nem csupán technológiai, hanem mélyen etikai, társadalmi és biztonsági kérdéseket is felvet. Az autonóm járművek, az intelligens infrastruktúra és a szenzorhálózatok olyan mértékben avatkoznak be a városi életbe, hogy az adatbiztonság, az egyéni felelősség és az etikus döntéshozatal kérdései megkerülhetetlenné válnak. Egy valóban okos közlekedési rendszer nemcsak műszakilag megbízható, hanem társadalmilag is igazságos és etikailag is elfogadható kell hogy legyen. Ez a fejezet ezen komplex kihívások részletes vizsgálatára vállalkozik.

7.1 Az autonóm döntéshozatal etikai dilemmái

Az önvezető járművek egyik legsúlyosabb etikai kérdése a "trolibusz-dilemma" modern verziója. Ha egy jármű elkerülhetetlen balesethelyzetbe kerül, vajon kit kell előnyben részesítenie a döntéshozatal során? A szoftvernek meg kell tudnia különböztetni gyalogost a járművezetőtől, vagy épp figyelembe kell vennie az életkort, a mozgáskorlátozottságot vagy más szempontokat? Bár ezek a kérdések filozófiai mélységűek, mégis gyakorlati jelentőségük van, hiszen a döntéshozatali algoritmusokat emberek írják – és ezek a programozási döntések élet-halál kérdéseket érintenek.

Továbbá kérdéses, hogy az etikai választások mennyire lehetnek standardizáltak különböző kultúrák és társadalmi normák szerint. Egy olyan világban, ahol eltérnek a jogi és erkölcsi elvárások, nehéz univerzális „helyes döntést” beprogramozni. A MIT által készített **Moral Machine** kísérlet is kimutatta, hogy a különböző országokban élő emberek jelentősen eltérően ítélik meg ugyanazokat a szituációkat.

7.2 Felelősség és jogi szabályozás

Egy másik fontos kérdés, hogy ki a felelős egy önvezető jármű által okozott balesetért. A hagyományos járművek esetében a sofőr viseli a felelősséget, ám autonóm rendszerek esetén ez elmosódik. A gyártó, a szoftverfejlesztő, a szenzorgyártó, vagy épp az utas lenne felelős? A jogrendszerek világszerte küzdenek ennek a kérdésnek a tisztázásával.

Az Európai Unió 2021-ben tett javaslatot az MI-alapú rendszerek szabályozására, az ún. **AI Act** keretében, amely kockázati alapon kategorizálná a rendszereket, és előírná a magas kockázatú alkalmazások (mint az önvezető járművek) szigorúbb vizsgálatát. Az USA-ban az NHTSA (National Highway Traffic Safety Administration) fokozatosan próbálja módosítani a járműbiztonsági szabályokat, hogy azok figyelembe vegyék a vezető nélküli rendszerek sajátosságait. Jelenleg azonban a legtöbb országban nincs egységes és átfogó törvényi keret ezekre az esetekre.

7.3 Társadalmi elfogadottság és hozzáférés

Bármennyire is fejlettek a technológiák, ha a társadalom nem fogadja el őket, a bevezetésük akadályokba ütközhet. A közvélemény kutatások szerint az emberek jelentős része még mindig nem bízik meg az önvezető járművekben, különösen a teljesen autonóm (Level 5) rendszerekben. A bizalomhiány különösen magas az idősebb korosztály és az alacsonyabb iskolai végzettségű csoportok körében.

Emellett fennáll a veszélye annak is, hogy a smart közlekedés „luxus technológiává” válik, amely csak a jómódú városrészek és társadalmi rétegek számára lesz elérhető. Ez digitális kirekesztéshez vezethet, ahol az alacsonyabb jövedelmű, vagy vidéki területeken élők nem részesülnek a fejlesztések előnyeiből. A

közlekedés azonban alapvető emberi szükséglet, ezért a tervezésnél és a szabályozásnál különös figyelmet kell fordítani az egyenlő hozzáférés biztosítására.

7.4 Kiberbiztonság és adatvédelem

Az intelligens közlekedési rendszerek szoftveralapú működése miatt fokozottan ki vannak téve a kibertámadások veszélyének. Egy feltört önvezető autó vagy egy manipulált városi forgalomirányító rendszer akár katasztrofális következményekkel járhat. A **V2X kommunikáció** lehetővé teszi, hogy a járművek valós időben kommunikáljanak egymással és az infrastruktúrával – de ha ez a kommunikáció nem megfelelően titkosított és hitelesített, akkor egy támadó könnyen bejuthat a rendszerbe.

A másik kulcskérdés az **adatvédelem**. Az autonóm rendszerek rengeteg érzékeny információt gyűjtenek a felhasználókról: tartózkodási hely, utazási szokások, biometrikus azonosítók, arcfelismerési adatok stb. Ezek az információk könnyen visszaélésre adhatnak lehetőséget. Az EU általános adatvédelmi rendelete, a **GDPR**, ugyan szigorú szabályokat ír elő az ilyen típusú adatkezelésre, de a gyorsan fejlődő technológia gyakran megelőzi a szabályozást.

8. Jogszabályi és szabályozási környezet

Az intelligens közlekedési technológiák, különösen az önvezető járművek, autonóm drónok és V2X rendszerek fejlődése szükségessé tette, hogy a jogi szabályozások is lépést tartsanak a technológiai változásokkal. Az új közlekedési megoldások nemcsak műszaki, hanem jogi kihívások elé is állítják a társadalmat. A szabályozási környezet egyrészt a közlekedés biztonságát és hatékonyságát kívánja biztosítani, másrészt felelősségi kérdéseket is kezelnie kell — például ki felel egy balesetért, ha az önvezető jármű hibázik?

A világ különböző régióiban eltérő megközelítések születtek. Az Európai Unió a szabályozási keretet a közlekedés átalakulásához igazítja a „Sustainable and Smart Mobility Strategy” és a „SUMP” (Sustainable Urban Mobility Plan) irányelvek révén. Ezek célja a digitális mobilitás fejlesztése, az alternatív üzemanyagok támogatása, valamint a közlekedés automatizálásának szabályozása. Emellett az EU létrehozta az UNECE WP.29 munkacsoportot, amely a járművek jóváhagyási követelményein dolgozik, külön figyelmet fordítva az ADAS és önvezető rendszerek engedélyeztetésére.

Az Amerikai Egyesült Államok inkább decentralizált szabályozási modellt alkalmaz. Az egyes államok saját hatáskörükben szabályozzák az autonóm járművek tesztelését és üzemeltetését. Kalifornia például úttörő szerepet tölt be ezen a területen: a Department of Motor Vehicles (DMV) külön engedélyezési rendszert vezetett be az autonóm járművek számára, melynek keretében cégek, mint a Waymo vagy a Cruise, közúti teszteket végezhetnek emberek szállításával is. Az USA Szövetségi Közlekedési Minisztériuma (USDOT) ugyanakkor országos irányelveket is megfogalmaz, mint például az AV 4.0 keretrendszer, amely iránymutatást ad az autonóm járművek fejlesztéséhez.

Kína rendkívül gyorsan reagált a technológiai újításokra, és célja világvezető szerep elérése az autonóm mobilitás terén. A kínai szabályozás erősen központosított: az autonóm járművekre és drónokra vonatkozó tesztelési engedélyeket a központi és tartományi szintű hatóságok együttesen bírálják el. A pekingi autonóm zóna például egyike azoknak a városrészeknek, ahol az önvezető járművek közúti forgalomban közlekedhetnek. A drónközlekedés területén Kína a CAAC (Civil Aviation Administration of China) révén komoly szabályozási és kutatási infrastruktúrát hozott létre.

A szabályozási kérdések egyik legösszetettebb része az etikai és felelősségi kérdések megoldása. Amikor egy önvezető jármű balesetet okoz, sok esetben a hiba nem a vezetőhöz, hanem a szoftverhez vagy a rendszertervezőhöz köthető. Ilyenkor felmerül a termékfelelősség, a gyártói kockázat, illetve az is, hogy hogyan lehet jogi úton „meghatározni" a gépi döntéshozatalt. A jövő jogalkotásának egyik fő kihívása tehát az lesz, hogyan lehet olyan keretrendszert létrehozni, amely a mesterséges intelligencia által vezérelt döntéseket is felelősséggel társítja.

Az intelligens közlekedés tehát nemcsak technológiai kérdés, hanem egyúttal jogi reformokat is igénylő társadalmi átalakulás. A nemzetközi és nemzeti szabályozások harmonizálása, valamint az etikai dilemmák kezelése kulcsfontosságú feltétel lesz a széles körű bevezetés sikeréhez.

9. Kiberbiztonság az intelligens közlekedésben

Az intelligens közlekedési rendszerek (ITS) és autonóm járművek elterjedése nemcsak technológiai, hanem kiberbiztonsági kihívásokat is magában hordoz. Az önvezető autók, okos tömegközlekedési eszközök, drónok és a városi infrastruktúrával való V2X-kommunikáció (vehicle-to-everything) hatalmas mennyiségű adatot generálnak és dolgoznak fel valós időben. Ezek az adatok alapvetően fontosak a közlekedés biztonságához, hatékonyságához és folyamatosságához. Ugyanakkor minden ilyen rendszer egyben támadási felület is: a járművek és infrastruktúra közötti kommunikáció manipulálása vagy feltörése súlyos következményekkel járhat, akár emberéletek veszélyeztetésével is.

9.1 Kritikus fenyegetések

A legnagyobb kockázatot a járművek feletti távoli kontroll lehetősége jelenti. Korábbi kutatások és éles helyzetek is bizonyították, hogy egy feltört önvezető jármű szoftvere révén a támadó átveheti az irányítást a fékrendszer, kormány, sebesség vagy navigáció felett. A 2015-ös Jeep Cherokee esete, amikor etikus hackerek távolról átvették a jármű vezérlését, ébresztőt fújt a teljes iparágnak.

Az önvezető járművek nem önmagukban állnak a fenyegetések kereszttüzében: a V2X kommunikációs csatornák is célpontok lehetnek. A támadók képesek lehetnek hamis adatok küldésére (spoofing), megszakíthatják a kommunikációt (jamming), vagy man-in-the-middle típusú támadásokat indíthatnak, amelyek során módosított adatokat továbbítanak a járműnek vagy az infrastruktúrának. Ezek hatására a járműek rossz döntéseket hozhatnak: például azt hihetik, hogy szabad az út, amikor valójában piros a lámpa, vagy elhiszik, hogy egy kereszteződés szabad, miközben egy másik jármű már behajtott oda.

Nemcsak a járművek, de az intelligens forgalomirányító rendszerek (pl. közlekedési lámpák, digitális táblák, központi irányító szerverek) is ki vannak téve támadásoknak. Egy koordinált támadással lehetséges lenne megbénítani egész városrészek forgalmát vagy káoszt okozni a tömegközlekedésben. Ugyanígy a drónok is célponttá válhatnak: GPS-jeleiket el lehet téríteni, vagy be lehet avatkozni repülési útvonalaikba.

9.2 Kiberbiztonsági stratégiák

A kockázatok miatt az intelligens közlekedési rendszerek megtervezésekor alapvető fontosságú a beépített kiberbiztonsági védelem. A védekezési stratégiák három fő szinten jelennek meg: az eszközök szintjén (jármű, drón), a hálózati szinten (kommunikáció, adatátvitel), valamint az alkalmazási szinten (adatfeldolgozás, döntéshozatal).

Az egyik alapvető módszer a kriptográfiai védelem, amely biztosítja, hogy a kommunikáció titkosított legyen, és ne legyen könnyen hozzáférhető harmadik fél számára. A digitális aláírások és tanúsítványok segítségével az eszközök hitelesíthetik egymást, így megelőzhető a hamis adatok befogadása. A járművek egyedi digitális identitása alapján eldönthető, hogy a bejövő adat valódi forrásból származik-e.

Ezen túlmenően többrétegű behatolás-észlelő rendszerek (IDS) is szükségesek. Ezek képesek azonosítani a szokatlan viselkedést vagy forgalmat, amely támadásra utalhat. Ha például egy jármű a megszokottól eltérően kezd kommunikálni másokkal, vagy adatcsomagok tömege érkezik szokatlan időpontokban, a rendszer riasztást adhat, és akár automatikusan karanténba helyezheti az érintett eszközt.

A rendszerredundancia egy másik fontos védelmi eszköz. Ez azt jelenti, hogy egy jármű nem csak egy szenzorra vagy kommunikációs csatornára támaszkodik, hanem több forrásból is be tudja szerezni ugyanazt az információt. Például ha a GPS meghibásodik, a jármű képes a LiDAR és a kamera adatai alapján tájékozódni. Ha a V2V adat nem érkezik meg, az érzékelők révén még mindig képes lehet felismerni a környező járműveket.

Végül megemlítendő a kiberbiztonsági szabványok és auditálási rendszerek szerepe. A nemzetközi szabványosítási szervezetek (például az ISO/SAE 21434 – „Road vehicles – Cybersecurity engineering”) részletes előírásokat dolgoztak ki az autóipari kiberbiztonság megvalósítására. Ezek nemcsak a fejlesztési szakaszra, hanem a teljes életciklusra – tervezés, gyártás, karbantartás, frissítés – is kiterjednek.

9.3 A jövő kihívásai

Ahogy a technológia fejlődik, úgy változnak a fenyegetések is. A mesterséges intelligencia által vezérelt támadások (például adaptív adathamisítás), vagy a kvantumkomputerek megjelenése újabb kihívásokat támasztanak. Elengedhetetlen lesz a frissíthető és adaptív védekezési mechanizmusok beépítése. A jövő intelligens járműveinek képesnek kell lenniük „tanulni” a támadásokból, valamint valós időben frissíteni saját védelmi rendszereiket.

A közlekedés kiberbiztonsága tehát nem csupán technikai, hanem stratégiai kérdés is. A jövő intelligens városainak stabilitása múlik azon, hogy ezeket a rendszereket mennyire sikerül biztonságossá és megbízhatóvá tenni.

10. Fenntarthatóság és környezetvédelem az intelligens közlekedésben

A 21. századi városi közlekedés egyik legégetőbb problémája a környezeti fenntarthatóság. A gyors urbanizáció, a növekvő gépjárműforgalom és a globális klímaváltozás súlyos következményekkel jár mind a városi életminőségre, mind a globális ökológiai egyensúlyra nézve. Az intelligens közlekedési rendszerek egyik legfontosabb célkitűzése tehát nem csupán a hatékonyság és a biztonság javítása, hanem a környezeti terhelés drasztikus csökkentése is.

10.1 Az emissziócsökkentés szerepe

A közlekedési szektor – különösen a közúti közlekedés – a világ üvegházhatásúgáz-kibocsátásának jelentős részéért felel. A belső égésű motorral működő járművek nemcsak szén-dioxidot, hanem nitrogén-oxidokat, szálló port és egyéb mérgező anyagokat is kibocsátanak, amelyek súlyos káros hatással vannak a levegő

minőségére, az emberi egészségre és a klímára. Az intelligens közlekedési rendszerek egyik fő előnye, hogy képesek optimalizálni a forgalmat, csökkentve ezzel a felesleges üzemanyag-felhasználást és a károsanyag-kibocsátást.

Például a forgalomirányító algoritmusok – különösen a mesterséges intelligenciával támogatott rendszerek – olyan mértékben tudják hangolni a jelzőlámpák működését, hogy minimalizálják az állásidőt és a torlódásokat. Mindez közvetlenül hozzájárul az üzemanyag-hatékonyság javulásához. A dinamikusan szabályozott közlekedési lámpák, a zöldhullám stratégiák és az intelligens navigációs rendszerek segítségével a járművek kevesebbet állnak, ritkábban gyorsítanak, így csökken az emisszió és a zajszennyezés is.

10.2 Elektromos és alternatív hajtású járművek integrációja

A fenntarthatóságot támogató egyik legfontosabb technológiai váltás az elektromos járművek (EV-k) és hidrogénüzemű járművek elterjedése. Az intelligens közlekedési rendszerek kiváló lehetőséget kínálnak arra, hogy ezen járműveket hatékonyan integrálják a városi közlekedési hálózatba. Az okos töltőállomásokkal összekapcsolt járművek például valós időben képesek jelezni töltöttségi állapotukat, és a rendszer képes irányítani őket a legoptimálisabb töltési pontra, elkerülve a torlódásokat.

További lehetőséget kínál az úgynevezett vehicle-to-grid (V2G) technológia, amely lehetővé teszi, hogy az elektromos járművek ne csak fogyasztói, hanem időszakosan energiaforrásai is legyenek az elektromos hálózatnak. Ez különösen fontos lehet a megújuló energiaforrások – például a nap- vagy szélerőművek – integrációja esetén, amelyek időszakosan ingadozó termelése mellett kiegyensúlyozó szerepet játszhatnak az EV-k akkumulátorai.

A közösségi közlekedésben is megjelennek a fenntartható megoldások: az elektromos és hidrogénüzemű buszok nemcsak csendesebbek és tisztábbak, de hosszú távon gazdaságosabbak is lehetnek, különösen ha az üzemeltetésüket támogató szoftverekkel és prediktív karbantartással kombinálják őket.

13. ábra: Villamos kinézetű elektromos buszok Londonban. [Publikus forrás] az Independent.uk cikkéből (https://www.independent.co.uk/travel/news-and-advice/london-bus-tram-crystal-palace-b2651107.html)

10.3 Zöld infrastruktúra és várostervezés

A környezetbarát közlekedés nem valósulhat meg hatékonyan megfelelő várostervezési stratégiák nélkül. Az intelligens közlekedés térnyerésével egyre fontosabb szerepet kap a zöld infrastruktúra – azaz olyan

közterületek, közlekedési hálózatok és zónák kialakítása, amelyek minimalizálják a környezeti hatásokat. Ennek része lehet a gyalogos- és kerékpáros közlekedés előnyben részesítése, az alacsony kibocsátású övezetek (LEZ) kijelölése, vagy az autómentes városrészek kialakítása.

A városi mobilitás újragondolásának részeként egyre több helyen alkalmaznak mikromobilitási megoldásokat – például e-rollerek, e-kerékpárok, mini elektromos járművek – amelyek ideálisak a rövid távú, „last mile" közlekedéshez. Ezen eszközök intelligens dokkolórendszerei, GPS-alapú követésük és digitális azonosításuk révén jól integrálhatók a nagyobb ITS rendszerekbe, miközben rendkívül alacsony környezeti lábnyommal működnek.

10.4 Környezeti adatok gyűjtése és feldolgozása

Az intelligens közlekedési rendszerek része az is, hogy folyamatosan monitorozzák a levegőminőséget, a zajszennyezést, valamint a forgalmi torlódásokból eredő káros hatásokat. Ezeket az adatokat szenzorok, kamerák, drónok és műholdas rendszerek segítségével gyűjtik be, majd központi rendszerekben elemzik. A begyűjtött adatok alapján valós idejű döntések születhetnek – például egy szennyezett övezetbe irányított forgalom automatikus átterelése más irányba.

Ezek az adatok hosszú távon is hasznosak: segítenek a várostervezőknek az új szabályozások és stratégiák kialakításában, illetve megalapozzák a közpolitikai döntéshozatalt is. Emellett fontos szerepük lehet a polgárok tájékoztatásában, hiszen az adatvizualizációval ellátott nyílt hozzáférésű környezeti térképek segíthetik a lakosokat a zöldebb életmód kialakításában.

10.5 A környezetvédelem és technológia egyensúlya

Az intelligens közlekedési technológiák önmagukban nem garanciái a fenntarthatóságnak. Kulcsfontosságú, hogy ezek a megoldások felelősségteljesen, a környezeti hatásokat szem előtt tartva kerüljenek bevezetésre. Egy olyan rendszer, amely ugyan technológiailag fejlett, de kizárólag az autós forgalmat támogatja a tömegközlekedés vagy a gyalogos mobilitás kárára, nem tekinthető fenntarthatónak.

Fontos az is, hogy a gyártás során felhasznált anyagok, a járművek akkumulátorainak újrahasznosítása, valamint az infrastruktúra karbantartása is megfeleljen a környezetvédelmi előírásoknak. Az EU és más nemzetközi szervezetek számos olyan szabályozást hoztak, amelyek a jövő közlekedési rendszereit nemcsak intelligenssé, hanem környezeti szempontból is felelőssé teszik.

11. Összegzés

Az intelligens közlekedési rendszerek és az autonóm technológiák forradalmasítják azt, ahogyan a modern városok működnek, fejlődnek és reagálnak a társadalmi, gazdasági és környezeti kihívásokra. A dolgozat átfogó módon vizsgálta az önvezető járművek, az okos tömegközlekedési rendszerek, a városi mobilitási stratégiák, valamint a drónok és autonóm légi közlekedés különböző aspektusait, mindezt technológiai, társadalmi és környezeti szempontok alapján. A cél nem csupán az volt, hogy bemutassa a jelenlegi fejlettségi szintet, hanem hogy értelmezze a mögöttes trendeket, lehetőségeket és kockázatokat is.

A kutatás rávilágított arra, hogy az önvezető járművek terjedése nem egyszerű technológiai újítás, hanem egy komplex társadalmi-gazdasági átalakulás része. Az automatizált vezetési rendszerek, mint az ADAS és

az autonóm navigációs algoritmusok, újfajta városi infrastruktúrát és szabályozási keretet igényelnek, miközben újraírják a közlekedési szokásokat is. A biztonság, az etikai kérdések és a jogi felelősségek központi szerepet kapnak ezen a területen, és az elfogadás mértéke jelentősen függ a társadalmi bizalomtól és a technológiák megbízhatóságától.

Az okos tömegközlekedési rendszerek esetében a hangsúly egyre inkább a hálózati integrációra, a valós idejű adatelemzésre és a felhasználói élmény optimalizálására helyeződik. A szenzorokkal és AI-megoldásokkal támogatott rendszerek nemcsak hatékonyabbá és kiszámíthatóbbá teszik az utazást, hanem hozzájárulnak a városi torlódások csökkentéséhez és a környezeti lábnyom mérsékléséhez is. A tömegközlekedés digitalizációja új szolgáltatási modellek – mint az on-demand buszok és a dinamikusan változó útvonalak – előtt nyitja meg az utat.

A városi mobilitási stratégiák sikeressége nagymértékben múlik a döntéshozók hosszú távú gondolkodásán és az érintettek közötti együttműködésen. A hagyományos közlekedési modellekkel szemben az intelligens rendszerek rugalmasságot, prediktív működést és adatvezérelt döntéshozatalt tesznek lehetővé. Az olyan fogalmak, mint az intermodális közlekedés, a "15 perces város" vagy az alacsony kibocsátású övezetek ma már nem elvont koncepciók, hanem konkrétan megvalósítható, sőt, sok esetben már működő stratégiák világszerte.

A dolgozat egy másik jelentős fejezete a drónok és autonóm légi közlekedés szerepét mutatta be, amelyek egyre fontosabbá válnak a csomagszállítás, a sürgősségi beavatkozások és a jövő városi mobilitása szempontjából. Bár a technológia fejlődése látványos, még számos akadály áll a tömeges elterjedés útjában, beleértve a szabályozás kérdéseit, az infrastruktúra hiányát és a társadalmi elfogadottságot. Ennek ellenére a légiközlekedés autonómiája kulcsfontosságú lehet a jövő városainak dekoncentrált és gyors logisztikai rendszereiben.

Nem lehet szó nélkül elmenni a jogszabályi és szabályozási környezet szerepe mellett sem. Az új technológiákhoz nemcsak technikai szabványokat kell kialakítani, hanem jogi kereteket is, amelyek képesek lefedni az etikai, adatvédelmi és felelősségi kérdéseket. A közlekedési eszközök és rendszerek digitalizációja új kihívásokat jelent a jogalkotók számára, amelyhez proaktív, adaptív és nemzetközi szintű együttműködés szükséges.

A fenntarthatósági szempontokat vizsgálva elmondható, hogy az intelligens közlekedési rendszerek az egyik legerősebb eszközt jelentik a környezeti terhelés csökkentésére. A károsanyag-kibocsátás minimalizálása, az elektromos járművek integrációja, a zöld infrastruktúra fejlesztése, valamint a környezeti adatok folyamatos monitorozása mind hozzájárulnak ahhoz, hogy a közlekedés ne akadálya, hanem eszköze legyen a környezetvédelmi célok megvalósításának.

Összefoglalva, az intelligens közlekedés nem csupán egy technológiai trend, hanem egy komplex társadalmi-gazdasági és környezeti átalakulás része, amely alapjaiban határozza meg a jövő városait. Az autonóm rendszerek, a hálózatba kapcsolt eszközök és az adatalapú döntéshozatal nemcsak kényelmet és hatékonyságot kínálnak, hanem lehetőséget is a fenntartható és élhető városi környezet megteremtésére. A kihívások, amelyek előttünk állnak – a szabályozás, a technológiai integráció, az elfogadás – komplexek, de a lehetőségek is hatalmasak. A legnagyobb kérdés az, hogy képesek leszünk-e ezeket a rendszereket úgy tervezni és működtetni, hogy ne csak a technológia, hanem az ember és a környezet érdekei is érvényesüljenek.

Irodalomjegyzék

1. SAE International. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. SAE J3016_202104, 2021.
2. Thrun, S., Montemerlo, M., Dahlkamp, H. et al. “Stanley: The Robot That Won the DARPA Grand Challenge.” *Journal of Field Robotics*, vol. 23, no. 9, 2006, pp. 661–692.
3. Litman, Todd. *Autonomous Vehicle Implementation Predictions: Implications for Transport Planning*. Victoria Transport Policy Institute, 2023.
4. Anderson, J. M., Kalra, N., Stanley, K. D. et al. *Autonomous Vehicle Technology: A Guide for Policymakers*. RAND Corporation, 2016.
5. Cugurullo, Federico. “Urban Artificial Intelligence: From Automation to Autonomy in the Smart City.” *Frontiers in Sustainable Cities*, vol. 2, 2020.
6. Gharibi, M., Boutaba, R., and Waslander, S. L. “Internet of Drones.” *IEEE Access*, vol. 4, 2016, pp. 1148–1162.
7. Goodchild, Anne, and Alvin Tse. “Urban Freight Deliveries and the Rise of On-Demand Logistics.” *Transportation Research Record: Journal of the Transportation Research Board*, 2018.
8. European Commission. *Sustainable and Smart Mobility Strategy – Putting European Transport on Track for the Future*. COM/2020/789 final.
9. Rodrigue, Jean-Paul. *The Geography of Transport Systems*. Routledge, 2020. ISBN: 9780367331786.
10. Bösch, Patrick M., Becker, Felix, Becker, H., Axhausen, K. W. “Cost-Based Analysis of Autonomous Mobility Services.” *Transport Policy*, vol. 64, 2018, pp. 76–91.
11. Zhang, W. and Guhathakurta, S. “Parking Spaces in the Age of Autonomous Vehicles.” *Journal of the American Planning Association*, vol. 84, no. 1, 2018, pp. 49–61.
12. Papadopoulos, T. et al. “The Use of Digital Technologies by Logistics Service Providers in Sustainable City Logistics.” *Sustainable Cities and Society*, vol. 76, 2022.
13. Alvarez, Luis and Viscaino, Juan. “LiDAR in Autonomous Vehicles.” *IEEE Instrumentation & Measurement Magazine*, vol. 24, no. 3, 2021.
14. Kröger, Lars. *Automated and Connected Driving – Challenges and Opportunities for Urban Transport Planning*. Springer Vieweg, 2020.
15. Banister, David. *Transport Planning*. Taylor & Francis, 2002.
16. United Nations Economic Commission for Europe (UNECE). *Regulations and Guidelines on Automated Driving*. Geneva, 2021.
17. International Transport Forum (OECD). *Urban Mobility System Upgrade: How Shared Self-Driving Cars Could Change City Traffic*. ITF Corporate Partnership Board Report, 2015.
18. World Economic Forum. *Shaping the Future of Mobility*. White Paper Series, 2018.
19. National Renewable Energy Laboratory (NREL). *Electrification Futures Study: Scenarios of Electric Technology Adoption and Power Consumption for the United States*. 2022.
20. Ferrell, C. et al. “The Role of Smart Transit and Mobility-as-a-Service.” *Transportation Research Board*, 2022 Annual Meeting.
21. GeSI. *Smarter 2030: ICT Solutions for 21st Century Challenges*. Global e-Sustainability Initiative Report, 2020.
22. NASA Aeronautics Research Institute. *Urban Air Mobility (UAM) Market Study*. NASA, 2021.
23. McKinsey & Company. *The Future of Mobility is at Our Doorstep*. Mobility Insights Report, 2020.
24. KPMG. *Autonomous Vehicles Readiness Index 2023*. KPMG Global.
25. European Union Agency for Cybersecurity (ENISA). *Cybersecurity Challenges in Autonomous Vehicles*. ENISA Report, 2022.

2.11. Az intelligens robotika fejlődése és a KUKA ipari robotok szerepe A KUKA robotok és a robotika Pálfalvi Áron

Az intelligens robotika fejlődése és a KUKA ipari robotok szerepe

A KUKA robotok és a robotika

Pálfalvi Áron

Mérnökinformatikus, aron.palfalva1@gmail.com

A dolgozat központi célja annak bemutatása, hogy az intelligens robotikai megoldások miként alakítják át az ipari gyártási folyamatokat, különös tekintettel a KUKA vállalat fejlesztéseire. A KUKA, mint ipari szereplő évtizedek óta vezető pozíciót tölt be a robotika területén, fejlesztései pedig jól illusztrálják azokat a technológiai és társadalmi trendeket, amelyek az automatizált és intelligens rendszerek térnyerését jellemzik a globális iparban.

A dolgozat elsődleges célkitűzése, hogy áttekintést adjon a KUKA ipari robotjainak technikai felépítéséről, működési logikájáról, valamint a bennük alkalmazott mesterséges intelligencia-komponensekről. Különös figyelmet fordítunk azokra a technológiákra, amelyek lehetővé teszik az autonóm működést, az ember-robot együttműködést (HRC), valamint az adaptív folyamatvezérlést.

A dolgozat második fókusza az ipari robotok alkalmazási területeinek elemzése. Ezen belül bemutatásra kerülnek a legfontosabb ágazatok – például az autóipar, logisztika, élelmiszer- és gyógyszeripar –, ahol a KUKA rendszerek sikeresen alkalmazhatók. Külön figyelmet szentelünk azoknak az ipari környezeteknek, ahol a higiéniás, pontossági vagy környezeti követelmények magas szintű technológiai megoldásokat igényelnek.

A dolgozat harmadik célja a technológiai fejlődési trendek vizsgálata. Ide tartoznak például a szenzorfúzió, az edge computing, a felhőalapú robotvezérlés, valamint a gépi tanulással támogatott optimalizálás lehetőségei. E fejlesztési irányok nemcsak a robotok autonómiáját növelik, hanem hozzájárulnak az ipari folyamatok rugalmasságához és fenntarthatóságához is.

Végül, a dolgozat negyedik célkitűzése a társadalmi és munkaerőpiaci hatások feltérképezése. A robotika térnyerése újfajta készségeket és munkaköröket igényel, miközben bizonyos manuális munkák fokozatosan háttérbe szorulnak. A dolgozat értékeli azokat a kihívásokat, amelyek az emberi munka átalakulásával, a munkavállalók képzésével, valamint az ipari etika és adatvédelem kérdéskörével kapcsolatosak.

Összességében a dolgozat célja, hogy komplex és többdimenziós képet nyújtson a KUKA robotikai rendszerek technológiai, ipari és társadalmi jelentőségéről az intelligens automatizáció korszakában.

Kulcsszavak: KUKA, Szenzortechnológia, HRC

1. BEVEZETÉS

Az ipari termelés automatizálása évtizedek óta központi célkitűzés a gyártóiparban. A modern technológiai innovációk – köztük a kiberfizikai rendszerek (CPS), a mesterséges intelligencia (AI), valamint az ipari IoT – új szintre emelték az automatizáció lehetőségeit. Az ipari robotika ezen keretek között folyamatos fejlődésen ment keresztül, és mára az intelligens robotok váltak a negyedik ipari forradalom (Ipar 4.0) egyik legfontosabb technológiai alappillérévé. E fejlődési irányt meghatározó szereplők közül kiemelkedik a német KUKA AG, amely nemcsak az ipari robotok egyik úttörő gyártója, hanem a gépi tanulás és mesterséges intelligencia alkalmazásának is vezető szereplője az ipari környezetben.

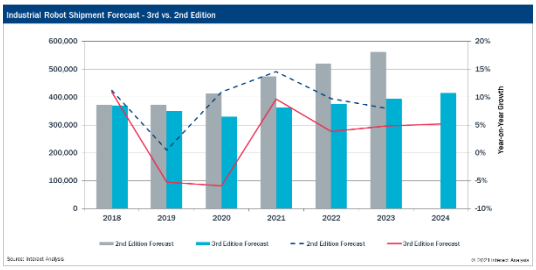
Az intelligens robotika nem csupán programozott mozgássorok végrehajtását jelenti, hanem olyan autonóm vagy félautonóm rendszereket, amelyek képesek érzékelni a környezetüket, alkalmazkodni a változó körülményekhez, valamint prediktív döntéseket hozni adatvezérelt elemzések alapján. A gépi látás, az adaptív vezérlés, valamint a mélytanulási modellek (pl. konvolúciós neurális hálók) lehetővé teszik, hogy a robotok ne csak végrehajtók, hanem aktív résztvevők legyenek a termelési folyamatban. Ezek a technológiák teszik lehetővé a rugalmas gyártási rendszerek kialakítását, ahol a robotok gyorsan reagálni tudnak a termelési igények változásaira, és csökkentik az emberi beavatkozás szükségességét.

A KUKA robotikai portfóliója – az autonóm gyártósoroktól a precíziós hegesztőrobotokon át az orvosi steril robotikáig – jól mutatja, hogy az intelligens robotok már nemcsak a nehéziparban, hanem a logisztikában, az élelmiszeriparban és a gyógyszergyártásban is kulcsszerepet játszanak. A robotok képesek szenzoros információk alapján dönteni, optimalizálni a munkafolyamatokat, és olyan minőségellenőrzési funkciókat ellátni, amelyeket korábban csak emberi szakértelemmel lehetett biztosítani.

A dolgozat célja, hogy átfogó képet nyújtson az intelligens robotika fejlődéséről, különös tekintettel a KUKA ipari robotok szerepére. A tanulmány ismerteti a technológiai háttér fejlődési irányait, bemutatja a legfontosabb alkalmazási területeket, elemzi a robotok által támasztott műszaki és társadalmi kihívásokat, valamint kitér a munkaerőpiaci és etikai vonatkozásokra is. A fókuszban az a kérdés áll, hogy miként tudják a KUKA által fejlesztett robotikai rendszerek támogatni a hatékony, fenntartható és rugalmas ipari termelést a jövőben.

1.1 Az intelligens robotika szerepe az ipari szektor átalakulásában

Az ipari szektor az elmúlt évtizedek során jelentős strukturális és technológiai változásokon ment keresztül, amelyek középpontjában a digitalizáció, az automatizáció és az adatvezérelt működés áll. Az intelligens robotika megjelenése ebben a folyamatban kulcsszerepet játszik, hiszen olyan rendszereket kínál, amelyek nemcsak végrehajtják az előre meghatározott műveleteket, hanem képesek önálló döntésekre, alkalmazkodásra és tanulásra is. Ezzel új működési modellek és termelési paradigmák váltak lehetővé, amelyek alapjaiban formálják át az ipari termelés szerkezetét és logikáját.

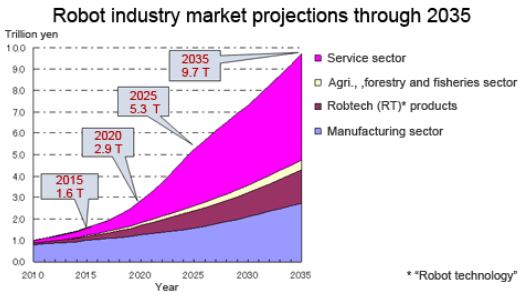


{1} Várható növekedés az ipari robotok szektorában [121]

Az intelligens robotok – szemben a hagyományos automatizált gépekkel – képesek érzékelni a környezetüket, feldolgozni a szenzor adatokat, és prediktív módon optimalizálni működésüket. Ez különösen fontos az Ipar 4.0 környezetben, ahol a gyártási rendszerek dinamikusak, modulárisak és folyamatosan alkalmazkodni kénytelenek a piaci vagy műszaki változásokhoz. Az ilyen robotikai rendszerek lehetővé teszik a „batch size one” – azaz egyedi, testreszabott termékek költséghatékony gyártását is, miközben fenntartják a tömeggyártás előnyeit.

A gyártási láncok átalakulása több szinten is érzékelhető. A robotok egyre gyakrabban lépnek interakcióba emberekkel (human-robot collaboration – HRC), például összeszerelés vagy minőségellenőrzés során. Emellett képesek kommunikálni más gépekkel (machine-to-machine – M2M), és valós időben kapcsolódni a vállalati információs rendszerekhez (pl. ERP, MES). Ez a fajta integráció olyan átláthatóságot és reakcióképességet eredményez, amely jelentősen csökkenti a selejtarányt, növeli a gyártási hatékonyságot, és lehetővé teszi az energia- és erőforrás-felhasználás optimalizálását.

Az intelligens robotika hatására átalakul a munkaerő szerepe is: a repetitív, alacsony hozzáadott értékű feladatokat fokozatosan automatizálják, míg az emberi munka a felügyeletre, irányításra és magasabb szintű döntéshozatalra helyeződik át. Ennek köszönhetően új készségek és kompetenciák válnak szükségessé, amely ösztönzi az oktatási rendszerek és képzések korszerűsítését is.



{2} Robot ipari piac előrejelzése [122]

Összességében az intelligens robotika nem csupán technológiai újítás, hanem egy átfogó ipari átalakulás motorja, amely új lehetőségeket kínál a versenyképesség, a termelékenység és a fenntarthatóság terén. A KUKA által fejlesztett rendszerek jól szemléltetik ezeket a tendenciákat, hiszen nemcsak technológiai szempontból kifinomultak, hanem tökéletesen illeszkednek a digitális ipari környezet elvárásaihoz is.

1.2 Automatizáció és mesterséges intelligencia hatása

Az automatizáció a modern ipari rendszerek alapvető működési elvévé vált. Az egyszerű, mechanikus automatizálástól kezdve a teljesen autonóm rendszerekig terjedő fejlődési pálya az elmúlt évtizedek során fokozatosan haladt a gépi intelligencia irányába. A klasszikus automatizálási rendszerek fix programozásra, zárt logikára épültek, és kizárólag előre definiált környezetben tudtak hatékonyan működni. Ezzel szemben a mesterséges intelligencia (AI) integrációja lehetővé teszi, hogy a rendszerek adaptívvá, kontextusérzékennyé és tanulóképesé váljanak.

A mesterséges intelligencia ipari alkalmazása elsősorban a gépi tanulás (machine learning, ML) és a mélytanulás (deep learning) révén valósul meg. Ezek az algoritmusok lehetővé teszik, hogy a robotikai rendszerek szenzoros adatokat dolgozzanak fel, és azokra reagálva optimalizálják működésüket. Például egy hegesztőrobot képes megtanulni az ideális hegesztési paramétereket különféle anyagokra és körülményekre, vagy egy vizuális ellenőrzőrendszer automatikusan észleli a hibás alkatrészeket a gyártósoron. A mesterséges intelligencia alkalmazása így nemcsak a termelés sebességét, hanem annak pontosságát és megbízhatóságát is növeli.

Az automatizált és intelligens rendszerek előnyei között szerepel a működési hatékonyság növekedése, a selejtarány csökkentése, valamint a prediktív karbantartás megvalósítása. Utóbbi lehetővé teszi a berendezések állapotának folyamatos monitorozását, amely alapján előre jelezhetőek a meghibásodások, csökkentve ezzel a váratlan leállások kockázatát és a karbantartási költségeket.

Az AI-alapú automatizáció hatása túlmutat a fizikai gyártáson. A rendszerek képesek valós idejű adatcserére más vállalati rendszerekkel (pl. ERP, MES), ezáltal támogatva a digitális ikrek (digital twins) koncepcióját is. Ezzel nem csupán a gépek, hanem a teljes gyártási folyamat szimulálható, optimalizálható és menedzselhető digitális környezetben. Ez a fajta integráció a rendszerhatékonyság új szintjét nyitja meg, amely elengedhetetlen a rugalmas és személyre szabott gyártási modellekhez.

Fontos azonban kiemelni, hogy az automatizáció és az MI nem önálló technológiai elemek, hanem komplex ökoszisztémák részei. A robotikai hardver, a szoftveres algoritmusok, a szenzoros infrastruktúra és az adatelemző platformok együttes működése hozza létre azt a rendszerszintű intelligenciát, amely képes önálló, emberi beavatkozás nélküli működésre. A KUKA robotikai rendszerei élen járnak ezen integrált megközelítés alkalmazásában, lehetővé téve a fejlett autonóm ipari folyamatok megvalósítását.

2. AZ INTELLIGENS ROBOTIKA FEJLŐDÉSE

Az intelligens robotika nem egyetlen technológiai ugrás eredménye, hanem egy évtizedeken átívelő, fokozatos fejlődési folyamat, amely a mechanikus automaták korától vezetett el a mesterséges intelligenciával támogatott, autonóm rendszerekig. Míg az 1950-es és 60-as évek első ipari robotjai még statikus, ismétlődő feladatokra lettek tervezve, a mai intelligens rendszerek már képesek alkalmazkodni a környezetükhöz, értelmezni az adatokat, és döntéseket hozni valós időben [1].

A robotika fejlődésének fontos mérföldkövei közé tartozik az első programozható ipari robot (Unimate) megjelenése, a PLC-alapú vezérlőrendszerek integrálása, majd a 2000-es évektől kezdődően a mesterséges intelligencia, a gépi tanulás és a szenzorfúzió robbanásszerű fejlődése. Ezek a technológiák tették lehetővé az úgynevezett intelligens robotok megjelenését, amelyek nemcsak végrehajtók, hanem kognitív képességekkel bíró rendszerek, képesek tanulni, alkalmazkodni és előre jelezni a folyamatokat [2][3].

A Deloitte szerint az intelligens robotok nem csupán a termelékenység növelését szolgálják, hanem stratégiai szerepet töltenek be a munkaerőpiac átalakításában is: „velünk, helyettünk és értünk” dolgoznak, azaz képesek támogatni az emberi munkaerőt, kiegészíteni vagy akár részben kiváltani azt [3]. Ez a fejlemény új kérdéseket vet fel az oktatás, az etika, valamint a vállalati felelősségvállalás terén is.

A technológiai fejlődés következtében ma már nemcsak a nehéziparban alkalmaznak robotokat, hanem a logisztikától kezdve az egészségügyön át a szolgáltatói szektorig mindenhol megjelennek. A Techmonitor és más ipari elemzések szerint az intelligens robotok kulcsszereplői az Ipar 4.0 korszakának, ahol az adatalapú működés, a valós idejű visszacsatolás és a hálózati integráció egyaránt elvárás [4].

Ezzel párhuzamosan a munkaerőpiac is átalakul: a HRPWR szaklap szerint a robotizáció hatására számos korábbi munkakör automatizálódik, miközben új típusú kompetenciák – például digitális rendszerismeret, adatértelmezés, gépi interakciók kezelése – válnak alapvetővé [5]. Az intelligens robotika tehát nemcsak technológiai újítás, hanem társadalmi és gazdasági szempontból is strukturális változásokat hoz.

2.1 A robotika történeti áttekintése

A robotika története szorosan összefügg az ember azon törekvésével, hogy automatizálja a fizikai munkavégzést, különösen az ipari termelésben. A robotika technológiai fejlődése több szakaszban zajlott, amelyek során a kezdeti mechanikus automatákból fokozatosan alakultak ki az intelligens, érzékelőkkel és szoftverrel ellátott robotrendszerek. Az első mérföldkőnek a George Devol által 1954-ben szabadalmaztatott Unimate ipari robot tekinthető, amelyet később az autóiparban alkalmaztak, különösen hegesztési és anyagmozgatási feladatokra [6].

A 20. század második felében a robotika rohamos fejlődésnek indult, főként a mikroelektronika és az informatikai rendszerek előretörésének köszönhetően. Az 1970-es években megjelentek a programozható logikai vezérlők (PLC-k), amelyek lehetővé tették a robotok rugalmasabb vezérlését és integrációját az ipari környezetekbe. A következő évtizedekben egyre összetettebb szenzorok, gyorsabb processzorok és fejlettebb vezérlőalgoritmusok kerültek beépítésre a robotikai rendszerekbe, amelyek képessé váltak a környezet érzékelésére és a visszacsatolt adatok feldolgozására is [7].

Az ezredfordulót követően a robotika fejlődése új szakaszba lépett az Ipar 4.0 koncepció megjelenésével. A szenzorhálózatok, az internetalapú kommunikáció, valamint a felhőszolgáltatások együttesen lehetővé tették a valós idejű, hálózatba kapcsolt robotrendszerek létrejöttét. A Deloitte és más iparági elemzések szerint ekkor kezdtek el terjedni az úgynevezett intelligens robotok, amelyek már képesek tanulásra, prediktív karbantartásra, valamint autonóm döntéshozatalra [8].

Az elmúlt néhány évben a gépi tanulás, különösen a mélytanulás (deep learning) technológiái még tovább bővítették a robotika lehetőségeit. Az olyan algoritmusok, mint a konvolúciós neurális hálók (CNN), már lehetővé teszik a képi adatok automatikus értelmezését, amely például minőségellenőrzési feladatokban vagy együttműködő robotikában (cobots) is alkalmazható [9]. Ezáltal a robotok már nemcsak végrehajtják a parancsokat, hanem aktív résztvevőivé válnak az ipari folyamatoknak, együttműködve az emberi munkaerővel.

A robotika története tehát nem lineáris fejlődési görbe, hanem egy összetett technológiai evolúció, amely során a gépek mechanikus eszközökből önállóan gondolkodó rendszerekké váltak. Ez a fejlődés mára elvezetett az intelligens robotok korához, amelyek nemcsak a gyártás hatékonyságát növelik, hanem új szerepet is betöltenek a vállalati működés és a társadalmi struktúrák átalakításában [10].

2.1.1 Mechanikus robotok kezdetei

A robotika történetének első szakasza a mechanikus automaták korszakával vette kezdetét, amikor a gépek még kizárólag mechanikai elveken alapultak, és emberi beavatkozás nélkül csak előre beállított mozgássorokat tudtak végrehajtani. A legkorábbi példák közé tartoznak a középkorban tervezett óraművek és önműködő szerkezetek, amelyek főként szórakoztatási vagy reprezentációs célt szolgáltak, de már akkor is az automatizálás gondolatát testesítették meg [11].

Az ipari forradalom idején jelentős technológiai előrelépések történtek: a gőzgépek, majd később az elektromos motorok alkalmazása lehetővé tette a gyártási folyamatok részleges gépesítését. Ugyanakkor a 20. század közepéig nem beszélhetünk modern értelemben vett ipari robotokról. A robotika ipari alkalmazásának első komoly mérföldköve az 1954-ben George Devol által szabadalmaztatott Unimate robotkar volt, amelyet később az amerikai General Motors gyárában állítottak üzembe [12].

Az Unimate volt az első programozható ipari robot, amelyet anyagmozgatásra és hegesztésre használtak az autógyártásban. A robot mozgását mágnesszalagról vezérelt programok szabályozták, amelyek statikus, nem adaptív műveletsort tettek lehetővé. Ennek ellenére jelentős áttörést jelentett, mivel az emberi munkavégzés helyettesítésére, veszélyes munkakörülmények kiváltására és a termelési hatékonyság növelésére irányult [13].

A 60-as és 70-es években megjelentek az első kereskedelmi forgalomban is elérhető ipari robotok, amelyeket főként az autóiparban kezdtek alkalmazni. E robotok feladatai jellemzően egyszerűek voltak, például ponthegesztés, festés, vagy tárgyak szortírozása. A vezérlésük fix programozás alapján történt, vagyis nem reagáltak a környezeti változásokra, és nem rendelkeztek érzékelőkkel.

A mechanikus robotok korszaka megalapozta az ipari robotika további fejlődését, és bebizonyította, hogy a gépek képesek hatékonyan végrehajtani az ismétlődő és monoton feladatokat. Bár ezek a robotok még nem tekinthetők intelligens

rendszereknek, alkalmazásuk jelentősen hozzájárult az automatizáció és az ipari hatékonyság növekedéséhez, valamint előkészítették a terepet az adaptív, érzékelőkkel és mesterséges intelligenciával felszerelt rendszerek elterjedéséhez [14].

2.1.2 Automatikus rendszerek fejlődése

A robotika következő fejlődési szakaszát az automatizált rendszerek megjelenése és elterjedése jelentette. A 20. század második felében a robotikai rendszerek egyre összetettebbé váltak, köszönhetően a számítástechnika, az elektronika és az irányítástechnika fejlődésének. Az automatizált rendszerek célja az volt, hogy a korábban statikus, manuálisan újraprogramozott robotokat dinamikusabb, rugalmasabb és pontosabb működésre képessé tegyék.

A legfontosabb mérföldkő a programozható logikai vezérlők (PLC-k) megjelenése volt az 1960-as évek végén. Ezek a vezérlőegységek lehetővé tették, hogy a robotok viselkedése egyszerűen módosítható legyen új szoftver betöltésével, így csökkentve a gépek átállási idejét és növelve az üzem rugalmasságát. A PLC-k emellett képesek voltak különféle szenzorokból és bemeneti eszközökből származó jelek feldolgozására is, ezzel megnyitva az utat a valós idejű irányítás felé [15].

Az automatizált rendszerek fejlődésének fontos eleme volt az érzékelők integrációja, amely lehetővé tette a robotok számára a környezeti változások detektálását. Például optikai szenzorok, nyomásérzékelők vagy hőmérséklet-mérők segítségével a gépek képesek lettek valós időben korrigálni mozgásukat, vagy folyamatparamétereiket. A szenzoradatok alapján történő vezérlés (closed-loop control) jelentősen növelte a pontosságot, valamint a hibák automatikus felismerésének és kezelésének képességét [16].

Az 1980-as és 1990-es évek során az ipari robotok egyre komplexebb feladatok ellátására lettek képesek. Az automatizált gyártósorokban a robotok már nemcsak izolált munkafolyamatokat végeztek el, hanem együttműködtek más gépekkel és vezérlőegységekkel is. Ezzel párhuzamosan megjelent az ipari kommunikációs hálózatok (pl. Profibus, Modbus, Ethernet/IP) használata, amely lehetővé tette a rendszerek közötti adatcserét és koordinációt [17].

A modern automatizált rendszerek tehát már nemcsak előre programozott utasításokat hajtanak végre, hanem képesek az adatok feldolgozására, optimalizálásra és döntéshozatalra is. Ez a képesség szolgált alapul az intelligens robotika megjelenéséhez, amely az automatizált rendszerekre épülve, de annál jóval fejlettebb logikával működik. A különbség abban rejlik, hogy míg az automatizált rendszerek az ismert szabályokra építenek, az intelligens rendszerek képesek új szabályokat felismerni és adaptálni a működésük során [18].

A KUKA vállalat már a 90-es évektől kezdve integrálta robotjaiba az ilyen fejlett automatizálási technológiákat, beleértve a többtengelyes mozgásvezérlést, az érintésérzékeny ütközésfigyelést, valamint a valós idejű hálózati adatfeldolgozást. Ezek a képességek tették lehetővé az ipari robotika átalakulását egy statikus eszközrendszerből egy dinamikus, rugalmas gyártási megoldássá [19].

2.1.3 AI-alapú rendszerek megjelenése

A mesterséges intelligencián (AI) alapuló robotikai rendszerek megjelenése az ipari robotika fejlődésének következő forradalmi szakaszát jelentette. Míg a korábbi automatizált robotok előre programozott szabályok és érzékelőalapú vezérlés alapján működtek, az AI-alapú rendszerek képesek tanulni, alkalmazkodni, és komplex környezeti ingerekre reagálva önálló döntéseket hozni. Ezzel új minőségi szintre emelték a robotika lehetőségeit, különösen az Ipar 4.0 keretrendszerein belül.

Az AI-alapú rendszerek központi eleme a gépi tanulás (machine learning, ML), különösen a mélytanulás (deep learning), amely lehetővé teszi, hogy a robotok szenzoros adatok alapján felismerjenek mintázatokat, és ezek alapján módosítsák működésüket. A konvolúciós neurális hálók (CNN-ek) például képesek vizuális inputokat – például hibás alkatrészek vagy helytelen pozíciók – automatikusan felismerni, így alkalmazhatók minőségellenőrzési vagy útvonaltervezési feladatokra is [20].

A Deloitte szerint az intelligens robotok képesek „helyettünk, velünk és értünk” dolgozni, ami arra utal, hogy már nemcsak a fizikai munkát végzik el, hanem adatokat is gyűjtenek, feldolgoznak, és elemzéseket készítenek – akár autonóm módon is [21]. Az ilyen rendszerek képesek az előre nem definiált környezetekhez alkalmazkodni, és optimalizálni a működésüket valós idejű visszacsatolás alapján. Ez különösen fontos az olyan gyártási környezetekben, ahol kis szériás, változó termékek előállítására van szükség.

Az AI alkalmazása a robotikában lehetővé teszi a prediktív karbantartást, amely során a robotok előre jelzik saját alkatrészeik elhasználódását, így csökkentve a leállások számát és a karbantartási költségeket. Emellett fejlődik a személyre szabott gyártás, ahol a robotok képesek egyedi igények alapján módosítani működésüket, akár termékenként eltérő konfigurációban.

A KUKA már az elmúlt években beépítette robotikai rendszereibe az intelligens vezérléseket, különösen a kollaboratív robotok (pl. KUKA LBR iiwa) esetében. Ezek a rendszerek nemcsak érzékelik az emberi jelenlétet, hanem képesek

alkalmazkodni a munkatársak mozgásához és beavatkozásaihoz is. Ezzel a robotika túllépett az izolált, zárt működési környezeteken, és aktív szereplővé vált az emberekkel közösen végzett munkafolyamatokban [22].

Fontos megjegyezni, hogy az AI-alapú rendszerek nem csupán technológiai újítások, hanem kultúraváltást is eredményeznek az iparban: az adatvezérelt döntéshozatal, a digitális visszacsatolás és a mesterséges intelligencia által támogatott folyamatirányítás újfajta szervezeti gondolkodást és kompetenciákat követel meg. Ez különösen igaz a gyártásirányításra, a karbantartásra, valamint a minőségbiztosításra is [23].

2.2 Mesterséges intelligencia és gépi tanulás szerepe

A mesterséges intelligencia (AI) és a gépi tanulás (machine learning, ML) az intelligens robotika legmeghatározóbb technológiai összetevőivé váltak az elmúlt évtizedben. Az ipari környezetben alkalmazott robotok már nemcsak ismétlődő feladatok végrehajtására képesek, hanem adatvezérelt döntéshozatalra, tanulásra és adaptív viselkedésre is. Ezek a képességek jelentős hatással vannak a gyártás rugalmasságára, minőségére és hatékonyságára.

A gépi tanulás egyik leggyakoribb alkalmazása az anomaliedetekció, amely során a robot képes felismerni a normálistól eltérő működést vagy gyártási hibát – például egy rosszul illesztett alkatrészt vagy szokatlan rezgésmintát. Ez lehetővé teszi a prediktív karbantartás megvalósítását, ami csökkenti az állásidőt és növeli az eszközök élettartamát [24].

A mélytanulási (deep learning) technológiák, különösen a konvolúciós neurális hálók (CNN-ek), különösen hasznosak a gépi látás (machine vision) rendszerekben. Ezek képesek a kameraképek automatikus feldolgozására, például termékek osztályozására, hibák észlelésére, vagy akár objektumok lokalizálására egy háromdimenziós térben. Az ilyen rendszerek már képesek „látni és értelmezni” a környezetüket, ami korábban kizárólag emberi operátorokra volt bízva [25].

Az AI-alapú megközelítések jelentős előnye, hogy nemcsak előre programozott utasításokat hajtanak végre, hanem képesek az új helyzetek felismerésére és tanulásra is. A felügyelt (supervised), felügyelet nélküli (unsupervised) és megerősítéses (reinforcement learning) tanulási módok különböző ipari szcenáriókban alkalmazhatók: például mozgásoptimalizálás, gyártási ciklusok gyorsítása, vagy éppen veszélyes helyzetek automatikus elkerülése esetén [26].

A Deloitte szerint a mesterséges intelligenciával rendelkező robotok már nem csupán végrehajtók, hanem a döntéshozatali lánc aktív elemei, amelyek képesek akár emberi beavatkozás nélkül is újratervezni saját feladatvégzésüket [27]. Ezzel a szerepükkel hozzájárulnak az ipari rendszerek decentralizálásához, és új típusú ember-robot együttműködési modelleket tesznek lehetővé (HRC – Human-Robot Collaboration).

A KUKA vállalat számos fejlesztése integrálja az MI-t és ML-t a gyártási rendszereibe. Az LBR iiwa kollaboratív robot például képes a felhasználó mozgását követni, az érintésekből és rezgésekből tanulni, valamint automatikusan módosítani saját viselkedését az együttműködés során. Ezek a funkciók különösen fontosak a dinamikus környezetekben – például autóipari szerelősorokon vagy orvosi laboratóriumokban –, ahol a gép és ember közötti interakció biztonságos és hatékony működése kulcsfontosságú [28].

2.2.1 Önálló döntéshozatal

Az önálló döntéshozatal képessége jelenti az egyik legfontosabb vízválasztót a klasszikus automatizált robotok és az intelligens, mesterséges intelligenciával támogatott robotikai rendszerek között. Míg a hagyományos ipari robotok kizárólag előre programozott utasításokat hajtottak végre, a modern rendszerek képesek értelmezni a környezeti adatokat, felismerni mintázatokat, és ezek alapján saját működésüket dinamikusan módosítani. Ez a képesség alapvetően változtatja meg az ipari automatizálás szerepét és lehetőségeit.

Az önálló döntéshozatal gyakorlati megvalósítását elsősorban a gépi tanulási algoritmusok, különösen a megerősítéses tanulás (reinforcement learning) és az adaptív szabályalapú rendszerek teszik lehetővé. A robot a szenzorai által begyűjtött adatok alapján elemzi a működési környezetét, értékeli a lehetséges válaszreakciókat, majd az adott helyzethez legjobban illeszkedő műveletet választja ki. Mindezt gyakran valós időben, emberi beavatkozás nélkül végzi el [29].

A döntéshozatali képesség különösen fontos az olyan változó ipari környezetekben, ahol a robotnak nem áll minden lehetséges forgatókönyv rendelkezésére előre programozva. Ilyen helyzet lehet például, ha a robot egy nem szabványos elhelyezkedésű alkatrészt kell, hogy megfogjon, vagy ha egy hibás működést észlel a termelési soron. Az intelligens robot képes az ilyen szituációk felismerésére és a legcélszerűbb megoldás végrehajtására, akár korábbi tapasztalatai alapján is [30].

A KUKA által fejlesztett robotok közül több is rendelkezik ilyen képességekkel. A vállalat LBR iiwa modellje például képes érzékelni az érintést és nyomatékot, majd ezek alapján biztonsági vagy együttműködési döntéseket hozni. Emellett a KUKA.AI nevű platform integrálja a mesterséges intelligencia-komponenseket a vezérlési logikába, lehetővé téve a gyártási paraméterek adaptív optimalizálását, vagy például a gyártási hibák automatikus korrekcióját [31].

Az önálló döntéshozatal lehetősége nemcsak a hatékonyságot növeli, hanem jelentősen csökkenti a humán beavatkozás szükségességét is. Ezáltal a szakemberek felszabadulhatnak az ismétlődő, alacsony hozzáadott értékű tevékenységek alól, és magasabb szintű feladatokra koncentrálhatnak, mint például felügyelet, rendszeroptimalizálás vagy stratégiai döntéshozatal [32].

Fontos megjegyezni, hogy az ilyen autonóm működés új kihívásokat is felvet, különösen az etikai, biztonsági és jogi szempontok tekintetében. Ki a felelős, ha egy robot rossz döntést hoz? Milyen keretek között engedhetők el a döntéshozatali jogosítványok? Ezek a kérdések az ipari robotika jövőjének fontos kutatási területei [33].

2.2.2 Adaptív vezérlés

Az adaptív vezérlés az intelligens robotrendszerek egyik kulcstulajdonsága, amely lehetővé teszi a környezet változásaira való folyamatos és automatikus reagálást. Szemben a hagyományos, merev vezérlési algoritmusokkal, az adaptív rendszerek képesek a működési feltételek dinamikus újrakalibrálására, ezzel biztosítva a folyamatos, hatékony és biztonságos működést. A modern ipari robotikában ez a képesség elengedhetetlen az egyre komplexebb és rugalmasabb gyártási folyamatok megvalósításához.

Az adaptív vezérlés alapja az, hogy a robot szenzoros visszacsatolás alapján módosítja saját viselkedését. Például, ha egy robot karja egy szokatlan ellenállást érzékel – például egy nem megfelelően pozícionált tárgy miatt –, akkor képes azonnal módosítani a mozgási útvonalát, vagy lelassítani a sebességét, anélkül, hogy erre külső parancs érkezne. Ehhez szükség van fejlett szenzortechnológiára, gyors adatfeldolgozásra, valamint intelligens vezérlési algoritmusokra [34].

A gépi tanulás – különösen a neurális hálókon alapuló modellek – jelentősen hozzájárulnak az adaptív viselkedés kialakításához. A robot nemcsak előre megírt szabályok szerint reagál, hanem képes saját tapasztalatai alapján javítani működését, például egy adott anyagmegmunkálás során optimalizálni az erőkifejtést, sebességet vagy eszközhasználatot. Ezzel a képességgel a robotrendszer fokozatosan „alkalmazkodik” a feladathoz, így nemcsak hibátlanul, hanem hatékonyabban is dolgozik [35].

A KUKA robotjai – különösen az LBR iiwa kollaboratív robot – kiváló példát nyújtanak az adaptív vezérlésre. Ez a robot érzékeny nyomatékszenzorokkal van ellátva minden tengely mentén, és ezek segítségével képes valós időben reagálni az emberi beavatkozásokra vagy a munkadarab változásaira. Így egy emberrel közösen végzett szerelési folyamat során a robot képes csökkenteni az erejét, ha ellenállást érzékel, vagy újraigazítani a mozgását az emberrel való ütközés elkerülése érdekében [36].

Az adaptív vezérlés nemcsak a fizikai működésre vonatkozik, hanem a digitális gyártási rendszerekhez való illeszkedésre is. Az intelligens robotok képesek a vállalati információs rendszerektől (pl. ERP vagy MES) érkező adatok alapján automatikusan módosítani működésüket: például egy új gyártási rendelés vagy termékváltoztatás esetén nem szükséges manuális újraprogramozás. Ez lehetővé teszi a tömeges testreszabást („mass customization”) és a gyártási folyamatok jelentős gyorsítását [37].

Az adaptív vezérlés tehát nemcsak technológiai előnyt jelent, hanem alapvető feltétele a jövő ipari rendszereiben elvárt rugalmas, skálázható és intelligens működésnek. A Deloitte elemzései szerint a vállalatok egyre inkább olyan robotikai megoldásokat keresnek, amelyek képesek valós időben reagálni a gyártási és környezeti változásokra – ennek pedig a kulcsa az adaptív vezérlési technológiák integrálása [38].

2.3 Ember–robot együttműködés (HRC – Human-Robot Collaboration)

A hagyományos ipari robotok hosszú ideig elzárt térben, biztonsági kerítések mögött működtek, kizárva a közvetlen emberi interakció lehetőségét. Az intelligens robotika fejlődésével azonban megjelent egy új paradigma: az ember–robot együttműködés, azaz Human-Robot Collaboration (HRC). Az ilyen típusú rendszerek lényege, hogy az emberi dolgozók és a robotok közös munkaterületen, egymást kiegészítve dolgoznak, biztonságosan és hatékonyan.

Az együttműködő robotokat (collaborative robots – cobots) úgy tervezték, hogy érzékeljék az ember jelenlétét és mozgását, valamint képesek legyenek valós időben reagálni rá. Az ilyen rendszerekbe beépített nyomatékszenzorok, kamerák és ütközésérzékelők lehetővé teszik, hogy a robot azonnal leállítson egy műveletet, ha akadályt – például egy emberi kezet – észlel a mozgási pályáján [39].

A KUKA egyik kiemelkedő fejlesztése ezen a területen az LBR iiwa (intelligent industrial work assistant) robot, amelyet kifejezetten együttműködő munkavégzésre fejlesztettek ki. A robot minden tengelyén integrált nyomatékszenzorokkal rendelkezik, így érzékeli a legkisebb fizikai ellenállást is, és azonnal képes reagálni. Ez a képesség lehetővé teszi, hogy a robot biztonságosan működjön egy térben az emberrel, például precíziós összeszerelés vagy laboratóriumi mintaátadás során [40].

A HRC előnyei közé tartozik, hogy a robot és az ember a saját erősségeikre koncentrálhatnak: a robot végzi a monoton, ismétlődő vagy nehéz fizikai feladatokat, míg az ember a kreatív, problémamegoldást igénylő munkafolyamatokra koncentrálhat. Ez nemcsak hatékonyságot eredményez, hanem javítja a dolgozói elégedettséget és munkabiztonságot is [41].

A mesterséges intelligencia jelentős szerepet játszik abban, hogy a robot képes legyen értelmezni az emberi mozgást, hangparancsokat vagy vizuális jeleket, és ezek alapján megfelelően reagáljon. A gépi látás, a természetes nyelvfeldolgozás (NLP), valamint a gesztusfelismerés olyan technológiák, amelyek egyre gyakrabban integrálódnak az együttműködő robotikai rendszerekbe [42].

A Deloitte elemzése szerint az együttműködésen alapuló munkamodellek nem csupán technikai, hanem szervezeti és stratégiai változásokat is igényelnek. Az ipari környezetnek úgy kell átalakulnia, hogy támogatni tudja az ember és robot közötti biztonságos és hatékony kapcsolatot. Ide tartozik a megfelelő munkaterület kialakítása, a dolgozók képzése és az emberközpontú gyártás elvének érvényesítése [43].

Összefoglalva, az ember–robot együttműködés új távlatokat nyit az ipari robotika alkalmazásában. A jövő intelligens gyártási környezeteiben a robotok nem leváltják, hanem kiegészítik az emberi munkaerőt, támogatva a komplex, rugalmas és fenntartható termelést.

3. FŐBB ALKALMAZÁSI TERÜLETEK

Az intelligens ipari robotika, különösen a mesterséges intelligenciával és szenzortechnológiával támogatott rendszerek, egyre szélesebb körben jelennek meg a termelési, logisztikai és szolgáltatási ágazatokban. A robotok már nemcsak a nagy volumenű, automatizálható folyamatok végrehajtására alkalmasak, hanem komplex, gyorsan változó környezetben is képesek hatékonyan működni. Ezt a képességet jelentősen megerősíti az adattudomány, a gépi tanulás, a felhőalapú integráció, valamint az ember–robot együttműködés elterjedése.

A KUKA robotikai rendszerei kiváló példái az intelligens alkalmazásoknak. A vállalat különböző iparágakban nyújt rugalmas és testreszabható megoldásokat, többek között az autóiparban, a logisztikában, a gyógyszeriparban, valamint a precíziós fémmegmunkálásban. A KUKA robotok az egyszerű anyagmozgatási feladatoktól kezdve a steril környezetben történő mintakezelésig széles spektrumon alkalmazhatók, köszönhetően moduláris felépítésüknek, nyitott programozási felületüknek és intelligens vezérlési képességeiknek [44].

Az ipari robotok alkalmazásának egyik fő mozgatórugója a termelékenység növelése mellett a minőség javítása és a munkaerőhiány kezelése. Különösen a kollaboratív robotok (cobotok) terjedése tette lehetővé, hogy a robotika már nem kizárólag a nagyteljesítményű gyártósorokra korlátozódjon, hanem a kis- és középvállalkozások számára is elérhető megoldássá váljon. A robotok képesek precízen, ismétlődően és biztonságosan végrehajtani feladatokat – akár emberi munkatárs mellett is –, ezzel csökkentve a hibaarányt és növelve a gyártás megbízhatóságát [45].

Az alkalmazási területek egyre bővülnek az olyan jövőorientált szegmensek felé is, mint a mezőgazdasági automatizálás, élelmiszeripari kezelési rendszerek vagy az orvosi robotika. Ezekben az ágazatokban különösen fontos a higiéniai szabványok betartása, a kis méretű és érzékeny komponensekkel való munkavégzés, valamint az alkalmazkodóképesség a gyors termékváltásokhoz. A KUKA robotrendszerei többek között ezen feltételekhez is igazodnak – köszönhetően a kompakt kialakításnak, a gyors újraprogramozhatóságnak és az egyszerűen integrálható kezelőfelületeknek [46].

A fejezet további részeiben részletesen bemutatásra kerülnek a KUKA robotok konkrét alkalmazásai az ipari gyártósorok, logisztika, minőségellenőrzés, autóipar, gyógyszeripar és élelmiszeripar területén. Az egyes szakaszok technikai példákkal, felhasználási modellekkel és jellemző kihívásokkal illusztrálják, hogy az intelligens robotika miként formálja át az ipari folyamatokat a gyakorlatban.

3.1 Autonóm gyártósorok

Az autonóm gyártósorok az Ipar 4.0 egyik legmeghatározóbb újítását jelentik, melyek középpontjában az intelligens, hálózatba kapcsolt robotikai rendszerek állnak. Ezek a rendszerek képesek valós idejű adatfeldolgozásra, döntéshozatalra, valamint önálló működésre emberi beavatkozás nélkül. Az autonóm gyártás alapelve, hogy a gyártósor minden eleme – a robotkaroktól az anyagmozgató rendszerekig – képes érzékelni, elemezni és alkalmazkodni a gyártási környezethez.

A KUKA vállalat autonóm gyártási megoldásai élen járnak ezen a területen. A KUKA Ready2_use rendszer például előre konfigurált, azonnal bevethető megoldásokat kínál különböző iparágak számára – hegesztéshez, raklapozáshoz, adagoláshoz vagy akár csavarozáshoz. Ezek a rendszerek integráltan tartalmazzák a robotkart, a vezérlőegységet és a szoftvert, így minimális beállítást igényelnek a telepítés után [47].

A KUKA robotok autonóm működését a KUKA.Sim és a KUKA.PLC mxAutomation szoftverek támogatják. A KUKA.Sim lehetővé teszi a teljes gyártási folyamat digitális iker (digital twin) modelljének létrehozását és optimalizálását, még a fizikai beüzemelés előtt. Ez csökkenti a tervezési hibák számát és a rendszer bevezetési idejét. A KUKA.PLC mxAutomation interfész révén pedig a robot közvetlenül vezérelhető a PLC-rendszerekből, így szorosan illeszkedik a gyártósor többi automatizált eleméhez [48].

Az autonóm rendszerek jellemzője a valós idejű szenzoralapú működés. A KUKA robotok képesek érzékelni az alkatrészek pozícióját, azok minőségi jellemzőit, és képesek reagálni az eltérésekre. Például egy szerelőrobot képes módosítani a mozgását, ha az alkatrész nem pontosan a várt helyen található, vagy ha a rögzítéshez más erőhatás szükséges. Ezzel elkerülhetők a hibás összeszerelések, és csökken a selejtarány.

A gyártási adatok feldolgozását a KUKA iiQoT platform végzi, amely valós idejű állapotfigyelést, karbantartási előrejelzést és teljesítményelemzést biztosít. A gépi tanulással támogatott előrejelző rendszerek lehetővé teszik az autonóm gyártósorok számára, hogy a működésüket folyamatosan finomhangolják és optimalizálják a gyártási környezethez [49].

Az autonóm gyártás különösen előnyös az alábbi területeken:

- Tömegszemélyre szabott gyártás (mass customization), ahol gyakori a termékváltás
- Nagy precizitást igénylő feladatok, mint a precíziós hegesztés vagy szerelés
- Munkaerőhiányos területek, ahol a robotok képesek önállóan fenntartani a termelési folyamatokat

A KUKA Robotics Hungária Kft. – a győri központtal működő leányvállalat – fontos szerepet játszik az ilyen rendszerek regionális fejlesztésében és integrációjában, különösen a közép-európai piacon. A cég szoros kapcsolatban áll a hazai egyetemekkel és ipari szereplőkkel is, elősegítve az autonóm robotika gyakorlati elterjedését Magyarországon [50].

3.1.1 KUKA gyártórobotok

A KUKA gyártórobotjai az ipari automatizálás élvonalát képviselik. A vállalat portfóliója számos különböző teherbírású, méretű és alkalmazási célú robottípust kínál, amelyek az autonóm gyártósorok szerves részeként működnek. A robotkarok kiváló példái a modern intelligens gyártási technológiáknak, mivel képesek gyors, precíz, ismétlődő feladatok elvégzésére, valamint adaptívan reagálnak a gyártási környezet változásaira.

A KUKA robotok alapját a KR QUANTEC sorozat jelenti, amely a legszélesebb körben alkalmazott ipari robotcsalád a vállalat kínálatában. Ezek a robotok 90–300 kg teherbírás-tartományban érhetők el, kifejezetten nehézipari és autóipari feladatokra optimalizált konfigurációkkal. A KR QUANTEC robotokat nagy sebesség, robusztus felépítés és hosszú karbantartási ciklus jellemzi, ami ideálissá teszi őket például hegesztésre, anyagmozgatásra és gépkiszolgálásra [51].

A KR CYBERTECH sorozat ezzel szemben a kisebb teherbírású (4–22 kg) alkalmazásokra lett tervezve, például összeszerelési, csomagolási vagy elektronikai gyártási feladatokra. Ezek a robotok kiemelkednek a pontosságukról és dinamikus mozgásképességükről, ami lehetővé teszi komplex és érzékeny műveletek elvégzését, akár szűk munkaterekben is [52].

A KUKA robotkarok minden esetben integrálhatók az Ipar 4.0 követelményeinek megfelelő vezérlőrendszerekbe. A KUKA KR C5 vezérlőegység, amely a legújabb generációs robotkontroller, biztosítja az alacsony energiafogyasztást, valós idejű adatfeldolgozást és könnyű hálózati integrációt. A KUKA robotok nyitott interfészei – például OPC UA, Profinet – lehetővé teszik a robotok egyszerű kapcsolódását más gyártósori elemekhez és gyártásirányítási rendszerekhez [53].

A gyártórobotok programozása és szimulációja a KUKA.WorkVisual és a KUKA.Sim szoftverkörnyezeteken keresztül történik. Ezek a fejlesztői eszközök támogatják a gyártási ciklus előzetes modellezését, optimalizálását és a hibák kiküszöbölését még a fizikai rendszer beüzemelése előtt. A szimulációs környezet a digitális iker (digital twin) koncepcióját is támogatja, amely kulcsfontosságú az autonóm működés megbízhatóságának biztosításához [54].

A KUKA gyártórobotok alkalmazása nemcsak a gyártási folyamat sebességét növeli, hanem hozzájárul a minőség javításához, a selejt arányának csökkentéséhez és a költséghatékony működéshez. Ezen előnyök miatt a robotkarok nemcsak nagyvállalati környezetben, hanem egyre gyakrabban KKV-szinten is megjelennek – különösen ott, ahol a humán erőforrás elérhetősége korlátozott, vagy a gyártási környezet különleges precizitást igényel.

3.1.2 Okosgyártás (Smart Factory) megoldások

Az okosgyártás – más néven Smart Factory – a digitálisan integrált, automatizált és adatvezérelt ipari gyártási rendszerek megvalósítását jelenti. Az ilyen rendszerekben a gépek, robotok, szenzorok, informatikai rendszerek és humán operátorok folyamatos adatcserében állnak egymással, így a gyártási folyamat valós időben optimalizálható. A Smart Factory megközelítés az Ipar 4.0 alapelveire épül, és célja a rugalmas, fenntartható és személyre szabott tömegtermelés biztosítása.

A KUKA vállalat élen jár az okosgyártás megoldásainak fejlesztésében. Rendszerei nem csupán automatizált gépegységekből állnak, hanem integrálják a felhőalapú szolgáltatásokat, gépi tanuláson alapuló prediktív rendszereket, valamint digitális ikermodelleket (digital twins) is. Ezek együttesen lehetővé teszik, hogy a gyártási folyamat önoptimalizáló módon működjön [55].

A KUKA által fejlesztett iiQoT (industrial intelligent Internet of Things) platform kulcsszerepet játszik az okosgyártási rendszerekben. Az iiQoT egy központi adatplatform, amely összegyűjti a robotokból, vezérlőegységekből és gyártási komponensekből származó adatokat, és valós idejű állapotmonitorozást, hibadiagnosztikát, valamint előrejelző karbantartást biztosít. A rendszer felhasználói grafikus felületen keresztül elemezhetik az eszközök teljesítményét, beállíthatják a riasztásokat, és proaktív módon beavatkozhatnak a termelésbe [56].

A KUKA Smart Factory megközelítésének része a digitális szimuláció és gyártástervezés is. A KUKA.Sim szimulációs környezetben még a fizikai rendszer telepítése előtt lehetőség van a teljes gyártósor digitális modellezésére, mozgáselemzésére és optimalizálására. Ez jelentősen csökkenti a bevezetési időt, a tervezési hibák számát, valamint támogatja a folyamatos fejlesztést is [57].

A Smart Factory rendszerek alapja a modularitás és skálázhatóság. A KUKA megoldásai különféle iparági követelményekhez igazíthatók: az autóipari tömeggyártástól a kis szériás gyógyszeripari vagy élelmiszeripari gyártásig. A gyártócellák tetszőlegesen konfigurálhatók, a robotok és gépek újraprogramozhatók, az adatelemzés pedig valós időben támogatja a döntéshozatalt.

A KUKA magyarországi leányvállalata, a KUKA Robotics Hungária Kft., szintén aktívan részt vesz Smart Factory rendszerek fejlesztésében, különösen a hazai ipari digitalizáció előmozdítása érdekében. A vállalat a hazai Ipar 4.0 Platform tagjaként közreműködik abban, hogy a magyarországi gyártóvállalatok is elérjék az automatizáció és intelligens működés magasabb szintjét [58].

3.2 Logisztika és raktározás

Az ipari termelés hatékonyságának egyik kulcstényezője a belső logisztikai folyamatok optimalizálása. Az anyagok, félkész- és késztermékek gyors, pontos és automatizált mozgatása jelentős időmegtakarítást, költségcsökkentést és biztonságot eredményez. Az intelligens robotikai rendszerek – különösen az autonóm mobil robotok (AMR) és az automatikus irányítású járművek (AGV) – az elmúlt években kulcsszereplőivé váltak a logisztika és raktározás területén.

A KUKA fejlett logisztikai megoldásokat kínál az ipari belső szállítás és raktárkezelés automatizálására. A KUKA KMP (KUKA Mobile Platform) mobil robotcsalád tagjai autonóm navigációra képes, intelligens szállítójárművek, amelyek képesek dinamikusan reagálni a gyártó- és raktárterek változásaira, valamint biztonságosan együttműködni az emberi dolgozókkal [59].

A KMP platform különböző méretben és teherbírásban érhető el (például KMP 1500, KMP 600-S diffDrive), és képes szabadon mozogni a térben – köszönhetően a beépített lézeres letapogatóknak, kameráknak és biztonsági szenzoroknak. Az autonóm navigáció lehetővé teszi a statikus útvonalak elhagyását, így a járművek automatikusan új útvonalat választanak akadály esetén vagy a forgalom alapján [60].

A mobil logisztikai rendszerek integrálhatók a KUKA robotkarokkal és gyártócellákkal, így komplex, end-to-end automatizált anyagáramlás valósítható meg. Például egy mobil platform önállóan szállít nyersanyagot a gyártósorra, ahol azt egy fix telepítésű robot beemeli a gyártási folyamatba, majd a kész termék ismételten autonóm úton jut a raktárba vagy minőségellenőrzésre [61].

A KUKA logisztikai megoldásainak szerves részét képezik a digitális vezérlő- és felügyeleti rendszerek is, amelyek lehetővé teszik a robotok valós idejű követését, beavatkozását és optimalizálását. A KUKA iiQoT platform a logisztikai eszközök működési paramétereit is monitorozza, például töltöttségi szint, karbantartási ciklusok, útvonalterhelés és működési hatékonyság alapján [62].

Az intelligens logisztikai rendszerek alkalmazása számos előnnyel jár:

- Csökkenti az anyagmozgatási időt és az ebből eredő állásidőt
- Minimalizálja a hibákat és sérüléseket a belső szállítás során
- Rugalmasan skálázható a gyártási volumen változásaihoz
- Biztonságos emberi környezetben történő működést biztosít

A KUKA Robotics Hungária Kft. aktívan fejleszt és telepít ilyen logisztikai rendszereket a magyarországi ipari partnerek számára, különös tekintettel a járműiparra, az elektronikai összeszerelésre és a raktárlogisztikai szektorokra [63].

3.2.1 KUKA AGV rendszerek (Automated Guided Vehicles)

Az Automated Guided Vehicles (AGV), vagyis automatikusan irányított járművek olyan mobil robotok, amelyek előre meghatározott útvonalak mentén mozognak az ipari és logisztikai környezetekben. Az AGV-k célja a gyártási és raktározási folyamatok közötti anyagmozgatás automatizálása, miközben minimális emberi beavatkozásra van szükség. A KUKA AGV megoldásai ezen a területen megbízható, intelligens és skálázható rendszert kínálnak a korszerű ipari működéshez.

A KUKA portfóliójában a legismertebb AGV típusok közé tartozik a KMP 1500 és a KMP 600-S diffDrive, amelyek autonóm navigációval, fejlett érzékelőkkel és magasfokú integrációs képességekkel rendelkeznek. Ezek az eszközök kifejezetten arra lettek tervezve, hogy szűk, dinamikus ipari terekben is hatékonyan mozogjanak, akár 1,5 tonnás terhek mozgatása mellett is [64].

A KUKA AGV-k működésének kulcsa a szenzoralapú navigáció. A járművek lézerszkennerekkel, kamerarendszerekkel és ütközésmegelőző szenzorokkal vannak felszerelve, amelyek segítségével képesek önállóan és biztonságosan közlekedni emberekkel megosztott munkatérben is. A navigáció történhet mágnesszalagos, vonalkódos vagy SLAM-alapú (Simultaneous Localization and Mapping) módszerrel, amely lehetővé teszi a környezet valós idejű feltérképezését és dinamikus útvonaltervezést [65].

A KUKA AGV rendszerei modulárisan integrálhatók más gyártócellákba, ERP/MES rendszerekbe, valamint ipari vezérlőhálózatokba (pl. OPC UA, MQTT). Ennek köszönhetően az AGV-k nemcsak szállítanak, hanem valós idejű adatot is közölnek a központi rendszerekkel: például aktuális pozícióról, töltöttségi szintről vagy karbantartási igényekről. Az iiQoT platform támogatja ezen adatok összegyűjtését, elemzését és vizuális megjelenítését [66].

Az AGV-k alkalmazási előnyei közé tartozik:

- Az anyagmozgatási hibák minimalizálása
- Az emberi munkaerő tehermentesítése
- A folyamatos, 24/7 működés lehetősége
- A gyártási folyamatok automatizált szinkronizálása

A KUKA AGV rendszerek különösen jól alkalmazhatók az autóiparban, ahol komplex, szinkronizált gyártósorokat kell kiszolgálni, valamint a logisztikai központokban, ahol a hatékony anyagáramlás kritikus. A rendszer előnye, hogy a járművek önállóan térnek ki az akadályok elől, optimalizálják az útvonalakat, és forgalomirányító algoritmusokkal is működtethetők több jármű összehangolt vezérléséhez [67].

A KUKA Robotics Hungária Kft. már számos hazai üzembe telepített AGV rendszert, különösen az autóipari és feldolgozóipari szereplők körében. Ezek a megoldások jelentős mértékben csökkentették a kézi logisztikai tevékenységek szükségességét, és hozzájárultak az automatizálás mélyebb szintű bevezetéséhez [68].

3.2.2 Anyagmozgatás és autonóm szállítórendszerek

Az ipari termelés egyik legkritikusabb területe az anyagmozgatás és a gyártási folyamatokon belüli alkatrészek, félkész termékek, valamint készáru mozgatása. A hagyományos, manuális vagy gépi eszközökkel történő anyagmozgatás sok esetben rugalmatlan, hibalehetőségekkel terhelt és humán erőforrás-igényes. Az autonóm szállítórendszerek és intelligens anyagmozgató megoldások éppen ezen kihívásokra válaszolnak – a folyamatos, rugalmas, automatizált működés révén.

A KUKA autonóm szállítórendszerei központi szerepet játszanak az intelligens belső logisztikai rendszerekben, ahol a termelés során az anyagok mozgatása dinamikus, gyakran változó környezetben zajlik. A vállalat által fejlesztett mobil platformok, például a KMP 1500 vagy KMP 600-S, képesek a gyártócsarnok bármely pontjára eljuttatni az alkatrészeket – mindezt emberi beavatkozás nélkül, valós idejű útvonaltervezéssel és akadályelkerüléssel [69].

A rendszer működése a következő fő komponenseken alapszik:

- Fejlett érzékelőtechnológia (lézerszkenner, kamera, ultrahangos érzékelők)
- SLAM-alapú lokalizáció (Simultaneous Localization and Mapping)
- Adatvezérelt útvonaloptimalizálás
- Valós idejű flottakezelés több AGV párhuzamos vezérléséhez

A KUKA megoldásai nemcsak egyedi járműveket kínálnak, hanem teljes szállítórendszert képesek kiépíteni, amely szoftveresen integrálható ERP- vagy MES-rendszerekbe. Ennek köszönhetően a gyártási és logisztikai műveletek szinkronizáltan működhetnek: például egy beérkező megrendelés automatikusan elindíthat egy belső szállítási folyamatot, amely során az AGV a megfelelő alkatrészt a megadott gyártócellához szállítja [70].

A KUKA.NavigationSolution szoftver biztosítja az autonóm szállítórendszerek központi vezérlését. A platform képes valós időben követni az egyes járművek pozícióját, optimalizálni a forgalmat, valamint kezelni az új útvonalakat és prioritásokat. Emellett képes együttműködni más automatizált rendszerekkel, például raktárliftekkel, automata ajtókkal vagy konvejorpályákkal [71].

Az ilyen rendszerek bevezetése számos előnnyel jár:

- Rugalmas anyagmozgatás, még komplex, nem-lineáris termelési elrendezések esetén is
- Valós idejű szállítás, minimális várakozási idővel és optimalizált útvonalakkal
- Kisebb balesetveszély és kevesebb munkahelyi sérülés
- Integrálhatóság bármilyen gyártási környezetbe, utólagosan is

A KUKA autonóm szállítórendszerei nemcsak az iparban, hanem logisztikai központokban, kórházi rendszerekben, valamint elektronikai gyártásban is alkalmazhatók, ahol a gyors, pontos és hibamentes anyagmozgatás kulcsfontosságú tényező [72].

A magyarországi piacon a KUKA Robotics Hungária Kft. aktívan támogatja ezen rendszerek testreszabott bevezetését, különösen az autóipari és logisztikai vállalatoknál, ahol a belső anyagáramlás sebessége és megbízhatósága közvetlen hatással van a versenyképességre [73].

3.3 Minőségellenőrzés

A gyártási folyamatok során az egyik legfontosabb követelmény a termékek következetes minőségének biztosítása. A manuális minőségellenőrzés azonban időigényes, szubjektív és gyakran hibalehetőségekkel terhelt. Az ipari robotika fejlődésével párhuzamosan megjelentek azok az intelligens, automatizált minőségellenőrző rendszerek, amelyek nemcsak gyorsabb és pontosabb mérést tesznek lehetővé, hanem képesek az adatok valós idejű feldolgozására és elemzésére is. A KUKA robotikai megoldásai ezen a területen is meghatározó szereplők.

A KUKA robotkarok – például a KR AGILUS vagy KR CYBERTECH szériák – nagy pontosságukkal és ismétlőképességükkel ideálisak vizuális, vagy tapintásos minőségellenőrzési feladatokra. Ezek a robotok alkalmasak például furatellenőrzésre, méretellenőrzésre, pozíciómérésre, vagy akár optikai jelfeldolgozásra (OCR) is. A vizsgálatokat gyakran kamerarendszerrel, lézerszkennerrel vagy tapintófejjel kiegészítve végzik [74].

A KUKA megoldásai szorosan együttműködnek olyan mesterséges intelligenciával támogatott gépi látás (machine vision) rendszerekkel, amelyek képesek a gyártott alkatrészek vizuális jegyeit automatikusan felismerni és kiértékelni. A rendszer képes azonosítani az apró felületi hibákat, repedéseket, elszíneződéseket vagy nem megfelelő illesztéseket is. Az AI-modellek folyamatosan tanulnak az új mintákból, így az idő előrehaladtával egyre pontosabbá válik a hibafelismerés [75].

A robotizált minőségellenőrzés előnyei:

- Gyors és következetes vizsgálat minden egyes munkadarabnál
- Objektív értékelés, emberi hibák kiküszöbölésével
- Valós idejű hibajelzés, amely lehetővé teszi a gyártási folyamat azonnali korrekcióját
- Teljes nyomon követhetőség, köszönhetően a digitálisan rögzített vizsgálati eredményeknek

A minőségellenőrzés során keletkező adatokat a KUKA iiQoT és más adatgyűjtő platformok gyűjtik, tárolják és elemzik. Ezek a rendszerek képesek trendeket felismerni, statisztikai folyamatkontrollt (SPC) alkalmazni, valamint összekapcsolódni a vállalatirányítási rendszerekkel (ERP, MES), hogy a teljes értékláncban biztosítsák a minőség fenntartását [76].

A KUKA magyarországi leányvállalata egyre több hazai projektben alkalmaz robotizált minőségellenőrző rendszereket, különösen az autóiparban és az elektronikai összeszerelés területén, ahol a hibamentes termelés üzletkritikus tényező [77].

3.4 Autóipar és fémmegmunkálás

A robotika egyik legkorábbi és legjelentősebb alkalmazási területe az autóipar, ahol az automatizálás, precizitás és ciklusidő-optimalizálás kritikus tényezők. A KUKA – történelmi gyökerei révén is – az autógyártás egyik legmeghatározóbb robotikai beszállítója. A vállalat robotrendszerei a járműipari gyártási lánc szinte minden szakaszában megtalálhatók: karosszériahegesztéstől a festésen át a végszerelésig.

Az autóipari felhasználás egyik legfontosabb területe a ponthegesztés, ahol a KUKA KR QUANTEC sorozat nagy teherbírású robotjai biztosítják a gyors, precíz és ismétlődő ponthegesztési műveleteket. A robotkarok képesek szinkronizált mozgásra, így több robot egyidejűleg tudja elvégezni az autókarosszéria hegesztési pontjait, miközben a KUKA saját fejlesztésű hegesztéstechnológiai szoftverei valós időben figyelik és szabályozzák a folyamatot [78].

A lézerhegesztés és -vágás, illetve az alumínium illesztéstechnika szintén kulcsszerepet játszik a modern járműgyártásban, különösen az elektromos járművek (EV-k) struktúráinak kialakításánál. A KUKA robotok milliméter alatti pontossággal képesek elvégezni ezeket a műveleteket, miközben gépi látással és szenzoros visszacsatolással ellenőrzik a kötés minőségét [79].

A fémmegmunkálás másik kiemelt területe a plazmavágás, csiszolás, polírozás és fúrás, ahol a KUKA robotok robusztus mechanikai kialakításuk és integrált vezérlőrendszereik révén képesek bármilyen orientációban stabilan dolgozni. A KUKA KR FORTEC robotcsalád például kifejezetten nehézipari környezetre készült, és különösen alkalmas acél vagy öntöttvas alkatrészek nagy pontosságú megmunkálására [80].

Az autóipari gyártósorok gyakran moduláris robotcellákból állnak, amelyek könnyen átkonfigurálhatók új járműmodellek esetén. A KUKA ezen igényt a KUKA cell4_production koncepcióval támogatja, amely rugalmasan skálázható, újrahasználható komponensekből épül fel, és gyorsan testreszabható a változó gyártási igényekhez [81].

Magyarországon is jelentős a KUKA jelenléte az autóipari gyártósorok automatizálásában. A KUKA Robotics Hungária Kft. részt vesz többek között az Audi Hungaria, a Mercedes-Benz kecskeméti üzeme, valamint számos beszállító robotizálási projektjeiben. Ezek a rendszerek hozzájárulnak a termelési minőség, sebesség és hatékonyság globális szinten is versenyképes fenntartásához [82].

3.4.1 Precíziós hegesztés, karosszériaépítés

A karosszériaépítés az autógyártás egyik legkomplexebb és legprecízebb szakasza, amely során a különálló fémalkatrészek szilárd, strukturális egységgé állnak össze. A folyamat alapját a precíziós hegesztés különböző formái – például a ponthegesztés, ívhegesztés vagy lézerhegesztés – képezik. A KUKA robotikai megoldásai kulcsszerepet töltenek be ezek automatizálásában, köszönhetően nagy teherbírású robotkarjaiknak, fejlett mozgásvezérlésüknek és a hozzájuk kapcsolódó intelligens szoftveres rendszereknek.

A KUKA KR QUANTEC sorozat a vállalat egyik leggyakrabban alkalmazott robotcsaládja a karosszériahegesztés területén. Ezek a robotok akár 300 kg teherbírásra is képesek, miközben mozgáspontosságuk eléri az ±0,06 mm értéket – ami kritikus fontosságú a szűk tűréshatárral rendelkező illesztések során. A robotok mozgásának koordinálása valós időben történik, lehetővé téve az egymással szinkronban dolgozó több robotkar pontos összehangolását [83].

A KUKA integrált hegesztéstechnológiai megoldásokat kínál, mint például a KUKA.ArcTech vagy KUKA.RoboSpin, amelyek biztosítják a varrat minőségének állandóságát, valamint lehetővé teszik az ív stabilitásának automatikus szabályozását. A rendszer képes felismerni a hegesztés során fellépő eltéréseket (pl. nem megfelelő varrat, túlmelegedés, anyaghibák), és automatikusan beállítani a paramétereket ezek korrigálására [84].

A modern járművek – különösen az elektromos modellek – karosszériaszerkezete egyre nagyobb arányban tartalmaz alumínium és könnyűfém komponenseket, amelyek speciális hegesztési technológiát igényelnek. A KUKA lézeres és súrlódásos illesztési megoldásai lehetővé teszik ezen anyagok biztonságos és precíz összeépítését, amely hozzájárul a jármű súlycsökkentéséhez és energiahatékonyságához [85].

A robotizált karosszériaépítés előnyei:

- Kiváló ismétlőképesség, ami a gyártási minőség állandóságának záloga
- Gyors ciklusidők, amelyek hozzájárulnak a nagy volumenű sorozatgyártáshoz
- Integrált minőségellenőrzés, például szenzoros visszacsatolás hegesztési hibák észlelésére
- Rugalmas cellaarchitektúra, amely lehetővé teszi a gyártósor gyors újrakonfigurálását

A KUKA magyarországi leányvállalata, a KUKA Robotics Hungária Kft., aktívan vesz részt hazai karosszériaépítő sorok tervezésében, telepítésében és karbantartásában, különösen az Audi Hungaria és más járműipari szereplők győri, kecskeméti és szentgotthárdi gyártóegységeiben [86].

3.4.2 Robotcellák ipari integrációja

A robotcellák olyan önálló, zárt vagy félig zárt gyártóegységek, amelyek egy vagy több ipari robotot, érzékelőket, kezelőmodulokat és perifériás berendezéseket tartalmaznak. Ezek a rendszerek lehetővé teszik az automatizált műveletek – például hegesztés, szerelés, csiszolás vagy ellenőrzés – teljesen önálló végrehajtását, miközben biztosítják az emberi operátoroktól való védelmet és az ismétlődő feladatok hatékony kiszervezését.

A KUKA cell4_production koncepciója egy moduláris robotcella-rendszer, amelyet az ipari gyártási igényekhez igazítva alakítottak ki. A cellák különböző komponensekből – robotkar, biztonsági burkolat, kezelőpanel, szoftvervezérlés – épülnek

fel, így könnyen testreszabhatók és gyorsan telepíthetők. A rendszer lehetőséget ad a standardizált, mégis rugalmas robotikai alkalmazások integrálására a gyártósorokba [87].

A robotcellák ipari integrációjának főbb előnyei:

- Gyors telepíthetőség, akár néhány napon belül
- Skálázhatóság, új robotcellák egyszerű hozzáadásával
- Integrálhatóság ERP, MES és IoT platformokkal
- Karbantarthatóság és modularitás, a komponensek gyors cseréjével

A KUKA robotcellák jellemzően egyedi gyártási feladatokra vannak konfigurálva, de gyakran találkozni velük az autóipari karosszériahegesztésben, akkumulátorcellák összeszerelésében, vagy nehézipari fémmegmunkálási folyamatokban is. Az olyan robotok, mint a KR FORTEC vagy a KR CYBERTECH nano, a nagy pontosságú, erőigényes műveletek elvégzésére is alkalmasak a robotcellákon belül [88].

A szoftveres irányítást a KUKA.WorkVisual és a KUKA.SafeOperation környezetek biztosítják, amelyek lehetővé teszik a mozgáspályák tervezését, a biztonsági zónák meghatározását és a működési paraméterek valós idejű figyelését. Az integrált biztonsági rendszerek (pl. vészleállító gomb, fényfüggöny, nyomatékérzékelők) garantálják a megfelelést az ISO 10218 és ISO/TS 15066 ipari szabványoknak [89].

A KUKA robotcellák nem csupán gyártásra alkalmasak, hanem tanulási és kutatás-fejlesztési célokra is alkalmazzák őket, például duális robotrendszerek szinkronizált vezérlésének tesztelésére, vagy ember–robot együttműködés modellezésére. Magyarországon több egyetem és kutatóintézet is használ KUKA robotcellákat kísérleti környezetben [90].

A KUKA Robotics Hungária Kft. ipari partnerekkel együttműködve segíti a robotcellák gyártósorba való beillesztését – akár új rendszerek tervezésénél, akár meglévő gyártási folyamatok modernizálásakor. A testreszabott szolgáltatáscsomagok – tervezéstől az oktatáson át a karbantartásig – lehetővé teszik a hosszú távú, fenntartható integrációt [91].

3.5 Gyógyszer- és élelmiszeripar

A gyógyszer- és élelmiszeripar olyan iparágak, amelyek különösen szigorú követelményeket támasztanak a gyártási környezet higiéniájával, a termékbiztonsággal és az ismétlődő folyamatok pontosságával szemben. A robotizáció ezekben a szektorokban elsősorban a steril munkakörnyezet biztosítása, a humán hibák minimalizálása és a gyártási kapacitás növelése érdekében kap egyre fontosabb szerepet. A KUKA speciálisan kialakított robotikai megoldásai kiválóan alkalmazhatók mindkét területen, mivel megfelelnek a tisztatéri és élelmiszeripari szabványoknak is.

A gyógyszeriparban a robotizáció különösen jelentős szerepet játszik a laboratóriumi automatizálásban, mintakezelésben, adagolásban és csomagolásban. A KUKA kis méretű, nagy precizitású robotkarjai – például a KR AGILUS hygienic machine változatai – rozsdamentes acél házzal, zárt rendszerű kábelezéssel és fertőtlenítőszer-álló kialakítással készülnek. Ezek a robotok GMP- és FDA-kompatibilis környezetben is működtethetők, így alkalmasak gyógyszerészeti tisztaterekben való alkalmazásra [92].

Az élelmiszeriparban a KUKA robotjai a szeletelés, adagolás, csomagolás és palettázás feladatainak automatizálására használhatók. Az olyan modellek, mint a KR DELTA vagy a KR SCARA, gyors, precíz és nagy ciklusidejű mozgásra képesek, és megfelelnek az élelmiszeripari gépek higiéniai előírásainak (pl. EHEDG és 3-A Sanitary Standards). Ezeket gyakran alkalmazzák például pékáru, tejtermék vagy húsipari termékek automatizált kezelésére [93].

Mindkét iparágban fontos szempont a keresztfertőzések elkerülése, amelyhez a KUKA speciális robotkialakítása, az antibakteriális felületkezelés, valamint a mosható és zárt karburkolatok is hozzájárulnak. A robotok képesek együttműködni szenzoros rendszerekkel, például hőmérséklet- és páratartalom-figyelő szenzorokkal, amelyek biztosítják a folyamatos kontrollt a kritikus környezetekben [94].

A KUKA megoldásai lehetővé teszik a rugalmas termelést, ami különösen fontos a személyre szabott gyógyszerkészítmények vagy kis tételben gyártott élelmiszerek esetén. Az egyszerű programozás, a gyors újrakonfigurálhatóság és a rendszerintegrációs lehetőségek (pl. ERP, MES, LIMS) lehetővé teszik a gyors termékváltást vagy gyártási paraméterek finomhangolását [95].

Magyarországon a KUKA Robotics Hungária Kft. egyre több együttműködést folytat gyógyszeripari és élelmiszeripari vállalatokkal, különösen olyan területeken, ahol a precizitás, higiénia és az automatizálási szint meghatározó tényező a termelési hatékonyság szempontjából [96].

4. FEJLESZTÉSI MÓDSZEREK ÉS TECHNOLÓGIAI KIHÍVÁSOK

Az intelligens ipari robotika fejlődése az elmúlt években nemcsak a gyártási hatékonyság növelését tette lehetővé, hanem új szintre emelte a gépek autonómiáját, adaptivitását és együttműködési képességét is. A KUKA az élvonalban jár ezen technológiák fejlesztésében, amelyeket a robotikai rendszerek megbízhatóságának, rugalmasságának és intelligenciájának fokozására irányuló kutatások és innovációk támasztanak alá. A következő szakaszokban a fejlesztés legfontosabb technológiai pillérei és az ipari bevezetés során felmerülő kihívások kerülnek bemutatásra.

4.1 Big Data és gépi tanulás

Az ipari robotika fejlődése szorosan összefonódik a digitális technológiák térnyerésével, különösen a Big Data és a gépi tanulás (machine learning) alkalmazásával. Az ipari környezetben keletkező adatok – mint például szenzorértékek, mozgáspályák, környezeti paraméterek vagy gyártási hibák – hatalmas mennyiségben és sebességgel keletkeznek, ami új lehetőségeket és kihívásokat teremt a robotikai rendszerek fejlesztésében.

A KUKA rendszerei élvonalbeli megoldásokat kínálnak a nagy mennyiségű adatok strukturált gyűjtésére, tárolására és elemzésére. A vállalat iiQoT (Industrial Internet of Things) platformja lehetővé teszi a robotok által generált adatok valós idejű gyűjtését és vizualizációját. A rendszer több ezer paramétert képes nyomon követni – például hőmérséklet, nyomaték, rezgés, energiafelhasználás –, amelyeket később gépi tanuló algoritmusok felhasználhatnak mintázatfelismerésre és prediktív modellek készítésére [97].

A gépi tanulás integrációja lehetővé teszi a robotok számára, hogy a múltbeli adatok alapján előre jelezzék a várható hibákat (pl. szerszámkopás, karbantartási igény), felismerjék a gyártási folyamat anomáliáit, vagy adaptívan módosítsák a működési paramétereket. Az ilyen algoritmusok alkalmazása csökkenti az állásidőt, növeli a termelési stabilitást, és lehetővé teszi a valós idejű döntéshozatalt automatizált módon [98].

Tipikus gépi tanulási felhasználások KUKA rendszerekben:

- Előrejelző karbantartás: Az AI elemzi a rezgésmintákat, hőmérséklet-ingadozásokat és más jeleket a meghibásodások előrejelzésére.
- Hibafelismerés: Képfeldolgozási algoritmusok azonosítják a nem megfelelő illesztéseket, repedéseket vagy anyaghibákat.
- Folyamatoptimalizálás: A rendszer folyamatosan tanul a gyártási ciklusokból és a minőségi visszajelzésekből.

A gépi tanulás ipari alkalmazása során különösen fontos a megbízható adatminőség, a szenzorok megfelelő kalibrálása, valamint az algoritmusok validálása. A KUKA ehhez nyílt API-kat és integrációs lehetőségeket kínál, amelyek lehetővé teszik harmadik féltől származó analitikai megoldások, például Python vagy MATLAB alapú modellek integrálását az ipari vezérlőrendszerbe [99].

A gépi tanulás és Big Data alkalmazása nemcsak a gyártási hatékonyságot növeli, hanem stratégiai előnyt is biztosít a gyártóvállalatok számára: lehetővé teszi az intelligens, önoptimalizáló gyártási folyamatok kialakítását, amelyek emberi beavatkozás nélkül képesek alkalmazkodni a külső és belső változásokhoz.

4.1.1 Adatok feldolgozása a gyártási optimalizációhoz

Az ipari gyártás során keletkező hatalmas mennyiségű adat – beleértve a szenzorjelek, vezérlőutasítások, energiafogyasztási értékek, hibajelzések és környezeti paraméterek – strukturált feldolgozása és elemzése kulcsfontosságú a termelési folyamatok optimalizálása szempontjából. A KUKA robotikai rendszerei kiemelten támaszkodnak az adatalapú működésre, amelynek célja a minőség, a megbízhatóság és a költséghatékonyság növelése.

A KUKA iiQoT platform az adatok központi aggregálásáért és elemzéséért felel. A rendszer nemcsak rögzíti a gépállapotokat és eseményeket, hanem képes:

- Valós idejű adatvizualizációra (pl. működési idő, ciklusidő, hőmérséklet, terhelés),
- Anomáliaészlelésre (pl. szokatlan rezgésminták, nyomatékingadozás),
- Gyártási trendek azonosítására, például fokozatos teljesítményromlás felismerésére.

Az így előállított adathalmazokat gépi tanulási modellek dolgozzák fel, amelyek képesek azonosítani azokat az optimalizálási pontokat, ahol a folyamat finomhangolásával növelhető a gyártási kapacitás, csökkenthető a selejtarány, vagy minimalizálható az energiafelhasználás [100].

Például egy KUKA robotkar esetében a mozgáspályák adatainak elemzésével a rendszer képes javaslatot tenni alternatív útvonalra, amely rövidebb vagy kevesebb mozgáskomponenst igényel. Ugyanígy az érzékelők által rögzített anyagmozgatási

ciklusadatokból következtethető, mely paraméterek befolyásolják leginkább a ciklusidő eltéréseit, így azok módosításával optimalizálható a teljes munkafolyamat [101].

Az adatok feldolgozását támogató rendszerek jellemző funkciói:

- Statisztikai folyamatkontroll (SPC) a hibaarányok csökkentésére,
- Előrejelző algoritmusok gyártási zavarok vagy túlmelegedés megelőzésére,
- Automatikus visszacsatolás a vezérlőrendszer felé (pl. paraméterek módosítása hibás trend észlelésekor),
- Energiafogyasztás-mérési modellek, amelyek segítenek az ökológiai lábnyom csökkentésében.

Egy további gyakorlati példa: ha egy robot által végzett hegesztési művelet során az adatelemzés ismétlődő minőségromlást jelez, a rendszer képes felismerni, hogy az adott művelethez kapcsolódó karbantartási ciklust érdemes rövidíteni, vagy az energiaintenzitást újrakalibrálni. Ezzel megelőzhető a selejtképződés, és javul a folyamat stabilitása.

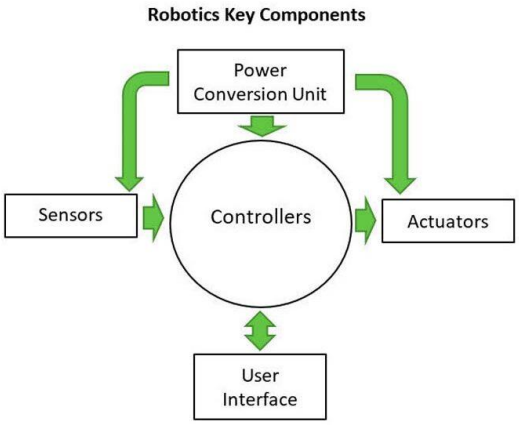
Az ilyen típusú adatelemzés és feldolgozás nemcsak az automatizálás hatékonyságát növeli, hanem lehetővé teszi a tudásalapú döntéshozatalt, amely elengedhetetlen a dinamikusan változó piaci igényekhez történő alkalmazkodásban – különösen olyan ágazatokban, mint az autóipar, az elektronikai összeszerelés vagy a gyógyszergyártás [102].

4.2 Szenzortechnológia

A modern ipari robotok működésének egyik alapfeltétele a fejlett szenzortechnológia, amely lehetővé teszi a környezeti tényezők érzékelését, a pontos helymeghatározást, valamint a valós idejű reagálást. A KUKA ipari robotjai számos különböző típusú szenzort alkalmaznak a robotkarok mozgásának szabályozására, az ember–robot együttműködés biztosítására, illetve a gyártási folyamatok minőségének fenntartására.

A szenzorok három fő funkciókörben játszanak kiemelkedő szerepet:

- Pozíció- és mozgásérzékelés: A robotkar pontos térbeli pozícióját enkóderek, inerciális mérőegységek (IMU) és lézeres távolságmérők határozzák meg.
- Erő- és nyomatékérzékelés: Ezek az érzékelők lehetővé teszik a finom mozdulatokat és a dinamikus illesztési műveletek végrehajtását, például préselés vagy alkatrész-illesztés során.
- Biztonsági szenzorok: Ultrahangos, lézeres vagy optikai szenzorok érzékelik az ember jelenlétét, akadályokat vagy szokatlan eseményeket a munkatérben, lehetővé téve a robot automatikus leállását vagy lassítását [103].



{3} Egy tipikus robot diagram [123]

A KUKA robotjai jellemzően integrált érzékelőkkel rendelkeznek, ugyanakkor a vállalat nyitott architektúrájú szenzorinterfészeket is biztosít (pl. EtherCAT, OPC UA), így külső szenzorok, gépi látásrendszerek és környezeti monitorozó eszközök is könnyedén integrálhatók a robotrendszerbe.

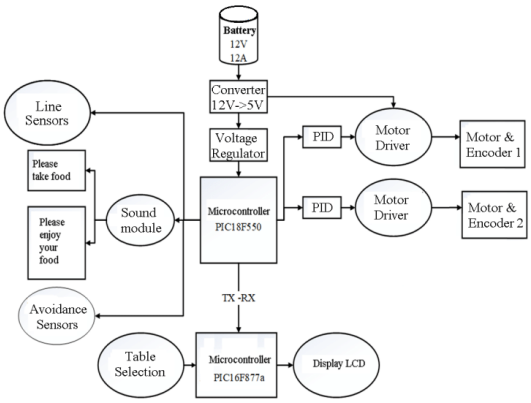
Kiemelkedő szenzoralapú alkalmazás a KUKA.ForceTorqueSensor, amely lehetővé teszi az erő-visszacsatolásos vezérlést, például finom polírozás vagy bonyolult szerelési műveletek során. Emellett a KUKA.SafeOperation szoftvermodul különféle biztonsági szenzoradatokat használ a munkatér dinamikus felügyeletére, és képes például sebességhatárokat beállítani attól függően, hogy a közelben van-e emberi operátor [104].

A szenzortechnológia egyre fontosabb szerepet tölt be az autonóm robotrendszerek működésében is, különösen a mobil platformok esetében (pl. KMP 1500), ahol az akadályfelismerés, a navigáció és az útvonaltervezés kizárólag szenzoradatokra

támaszkodik. Az ilyen rendszerek gyakran SLAM (Simultaneous Localization and Mapping) algoritmusokkal dolgoznak, amelyek valós idejű térképet alkotnak a munkatérről [105].

A KUKA szenzortechnológiai fejlesztései hozzájárulnak a:

- Gyártási pontosság növeléséhez,
- Robotok adaptív viselkedéséhez dinamikusan változó környezetben,
- Munkahelyi biztonság fokozásához ember–robot együttműködés során,
- Folyamatok minőségbiztosításához, például hibaészlelés vagy beállításkorrekció révén.



{4} Egy robot áramköri rendszere [124]

A magyar iparban különösen az autóipari és elektronikai gyártásban alkalmaznak szenzoralapú KUKA rendszereket, ahol elengedhetetlen a mikronpontosság, valamint a gyártás folyamatos monitorozása.

4.2.1 Valós idejű adatgyűjtés, szenzor-fúzió

Az ipari robotok autonóm és megbízható működésének egyik alapköve a valós idejű adatgyűjtés és szenzor-fúzió, azaz különböző típusú érzékelők összehangolt használata. A cél, hogy a robot a lehető legteljesebb képet kapja a környezetéről, saját mozgásáról és a munkadarab állapotáról, így képes legyen gyorsan és pontosan reagálni a változásokra.

A valós idejű adatgyűjtés során a robotrendszer másodpercenként több száz vagy akár több ezer mérési adatot rögzít a beépített és külső érzékelőkből, többek között:

- Pozíció- és mozgásérzékelő szenzorokból (pl. enkóderek, giroszkópok),
- Erő- és nyomatékérzékelőkből,
- Lézeres távolságmérőkből (LiDAR),
- Gépi látórendszerekből (kamera, 3D szkenner),
- Környezeti érzékelőkből (hőmérséklet, páratartalom, rezgés).

A szenzor-fúzió célja ezen különböző típusú érzékelőadatok szinkronizált kombinálása, hogy azokból megbízható, redundáns és pontos információ keletkezzen. A KUKA robotok például egyidejűleg használhatják a kameraképet, a lézertávolságot és a robotkar nyomatékát egy összetett művelet – például szerelés, illesztés vagy hibafelismerés – végrehajtásához [106].

A szenzor-fúzió alkalmazási területei:

- Navigáció és ütközéselkerülés mobil platformoknál (pl. KMP 600-S),
- Precíz pozicionálás alkatrészfelismeréssel kombinálva,
- Adaptív robotmozgás, például rugalmas alkatrészek illesztésénél,
- Valós idejű hibafelismerés, ahol a látás- és nyomatékadatok együttes elemzése alapján dönt a rendszer.

A KUKA rendszerei képesek a valós idejű adatfolyamokat nagy sebességű vezérlőegységek segítségével feldolgozni (pl. KUKA Sunrise.OS), valamint a mért adatokat azonnal visszacsatolni a mozgásvezérlésbe. Ezzel lehetővé válik az ultragyors beavatkozás, például amikor a robot hirtelen külső akadályt észlel, vagy az anyag pozíciója eltér az elvárttól [107].

Ezen technológia egyik legfontosabb fejlesztési iránya a szenzoradatok intelligens szűrése és súlyozása, amely során a rendszer képes automatikusan azonosítani, melyik adatforrás relevánsabb egy adott helyzetben. Például egy zajos gyártási környezetben a kamera képe torzított lehet, míg a lézeres érzékelő pontosabb információt ad – ezt a robot képes felismerni és az alapján dönteni [108].

A valós idejű szenzor-fúzió eredményeként a robotok:

- Gyorsabban és biztonságosabban működnek emberekkel közös térben,
- Alkalmazkodnak a gyártási toleranciákhoz és anyagváltozásokhoz,
- Csökkentik a hibás műveletek és beavatkozások számát,
- Hatékonyabbak komplex, nem determinisztikus feladatok végrehajtásában.

A szenzor-fúzió kiemelten fontos szerepet játszik a KUKA intelligens robotikai stratégiájában, különösen az ember–robot együttműködés (HRC) és a mobil robotrendszerek fejlesztésében.

4.3 Energiahatékonyság és fenntarthatóság

A modern ipari automatizálás egyik kiemelkedő kihívása az energiafelhasználás optimalizálása és a környezeti terhelés minimalizálása. A robotikai rendszerek nagy mennyiségű villamos energiát igényelnek működésük során, ezért egyre fontosabbá válik, hogy a gyártók – mint például a KUKA – olyan technológiákat fejlesszenek, amelyek csökkentik az energiafogyasztást, növelik az eszközök élettartamát, és támogatják a fenntartható ipari működést.

A KUKA több szinten kötelezte el magát a fenntarthatóság iránt, amely az alábbi területeken nyilvánul meg:

4.3.1 Energiatakarékos robotarchitektúra

A KUKA új generációs robotkarjai – például a KR QUANTEC és KR IONTEC szériák – kifejezetten energiatakarékos kinematikai és hajtásrendszerekkel lettek kialakítva. A robotkarok kisebb önsúlya és optimalizált mozgáspályái kevesebb energiát igényelnek, miközben a teljesítményük változatlan marad. A gyártó adatai szerint a modern robotok akár 30–40%-kal kevesebb energiát használnak, mint a korábbi generációk [109].

Emellett a robotok működését intelligens készenléti (standby) módok is támogatják, amelyek automatikusan csökkentik a fogyasztást inaktív állapotban, anélkül, hogy ez hátráltatná az újraindítást vagy a reakcióidőt.

4.3.2 Intelligens energiafelügyelet

A KUKA által fejlesztett iiQoT platform és a KUKA.EnergyMonitoring szoftvermodul lehetővé teszi az egyes robotok, gyártócellák vagy teljes rendszerek energiafogyasztásának valós idejű nyomon követését és elemzését. Az adatok elemzése alapján a felhasználók optimalizálhatják a gyártási folyamatokat, azonosíthatják a pazarlási pontokat, és beavatkozásokat tervezhetnek a hatékonyság növelésére [110].

Ezen rendszerek támogatják a célzott energiaelosztást (demand-based consumption), így például egy csúcsidőn kívüli gyártási ciklus során alacsonyabb teljesítményszintre állíthatók a robotkarok.

4.3.3 Környezeti fenntarthatóság

A KUKA robotikai rendszerei a hosszú élettartam, az alacsony karbantartási igény, valamint a moduláris, újrahasznosítható komponensek révén is elősegítik a fenntarthatósági célok elérését. A gyártó környezetkímélő eljárásokat alkalmaz az alkatrészek gyártása és az élettartam végén történő újrahasznosítás során is.

A vállalat emellett elkötelezett a CO_2-kibocsátás csökkentése mellett, amelyet az üzemeiben alkalmazott zöld energiahasználat és szállításoptimalizálás is támogat. A robotikai rendszerek alkalmazásával elérhető gyártási pontosság és selejtcsökkentés pedig közvetlenül hozzájárul az erőforrás-hatékonyság növeléséhez [111].

5. TÁRSADALMI ÉS MUNKAERŐPIACI HATÁSOK

Az intelligens ipari robotok térnyerése nemcsak technológiai és gazdasági változásokat hoz magával, hanem mélyreható társadalmi és munkaerőpiaci átalakulásokkal is jár. A robotika – különösen a mesterséges intelligenciával támogatott rendszerek – újraértelmezik az ember szerepét a termelési láncban, miközben új foglalkozások születnek és régiek szorulnak vissza. A KUKA, mint globális robotgyártó és rendszerintegrátor, aktívan részt vesz e folyamat formálásában.

5.1 Munkahelyek átalakulása

Az intelligens ipari robotok elterjedése gyökeresen átalakítja a munkahelyek szerkezetét, tartalmát és a munkavégzés körülményeit. Az ipari automatizálás – amelynek egyik meghatározó szereplője a KUKA – elsősorban a rutinszerű, ismétlődő és fizikailag megterhelő feladatok kiváltását célozza, miközben új, magasabb hozzáadott értékű munkakörök jönnek létre.

Hagyományos munkakörök visszaszorulása

Az automatizált rendszerek, mint például a KUKA robotkarok és autonóm anyagmozgató eszközök (AGV-k), képesek kiváltani olyan munkaköröket, mint:

- Fizikai szerelő és összeszerelő munkák,
- Anyagmozgatás (pl. targoncakezelő),
- Csomagolás, válogatás, raklapozás,
- Kézi minőségellenőrzés.

A gyártósorokon a manuális munka szerepe csökken, különösen a nagy volumenű, sorozatgyártásban működő iparágakban, mint az autóipar, a fémmegmunkálás vagy az elektronikai gyártás [112].

Új munkakörök megjelenése

A megszűnő vagy átalakuló munkakörök helyett új, technológiaorientált foglalkozások jelennek meg, amelyekhez magasabb szintű szaktudás, digitális kompetencia és rendszerismeret szükséges. Ilyen munkakörök például:

- Robotkezelő és -programozó,
- Ipari informatikus (pl. MES-, SCADA-rendszerek üzemeltetése),
- Karbantartó automatizálási technikus,
- Adatmérnök, aki a robotikai rendszerek által generált adatokkal dolgozik,
- Szoftvermérnök a robotvezérlés és HMI fejlesztés területén [113].

Ezekhez a munkakörökhöz sok esetben nem elegendő a hagyományos szakképzés, hanem speciális, gyakorlatorientált képzési formák szükségesek – például duális képzés, ipari tanfolyamok vagy egyetemi partnerségek keretében.

Képzettségi elvárások és kompetenciaváltás

A robotika térnyerése nemcsak a munkakörök fizikai tartalmát változtatja meg, hanem a munkavállalókkal szembeni elvárásokat is. Egyre inkább előtérbe kerülnek a következő készségek:

- Digitális jártasság (pl. érintőképernyős vezérlők, szoftveres interfészek használata),
- Rendszerszintű gondolkodás (pl. teljes gyártási folyamatok átlátása),
- Problémamegoldó és döntéshozatali képességek,
- Élethosszig tartó tanulásra való nyitottság.

A KUKA vállalati szinten is támogatja a kompetenciaváltást: nemcsak oktatási intézményekkel működik együtt, hanem saját KUKA College képzési programjaiban is kínál tanfolyamokat mérnököknek, technikusoknak és gyártósori dolgozóknak egyaránt [114].

Munkahelyi környezet változása

A robotizálással párhuzamosan a munkakörnyezet is átalakul. A robotok fizikai jelenléte miatt fontosabbá válik a:

- Munkatér ergonómiája (különösen HRC környezetekben),
- Biztonságtechnikai megfelelés (szenzoros biztonsági zónák, sebességkorlátozások),
- Ember–gép interfészek (HMI) egyszerű kezelhetősége és áttekinthetősége.

A jövő gyáraiban a dolgozók feladata egyre inkább felügyeleti, koordináló és optimalizáló jellegű lesz, amely magasabb fokú bevonódást és döntési felelősséget is jelent.

5.2 Ember–robot együttműködés kihívásai

Az ipari robotika fejlődése egyre inkább az ember és gép közötti együttműködésre, nem pedig a teljes kiváltásra fókuszál. A kollaboratív robotok (cobotok), mint például a KUKA LBR iiwa, olyan fejlett szenzoros és vezérlőrendszerekkel működnek, amelyek lehetővé teszik az emberekkel közös térben való biztonságos munkavégzést. Ez a modell – HRC, azaz Human–Robot Collaboration – számos előnyt hordoz, ugyanakkor komoly kihívásokat is támaszt a technológia, a biztonság, a munkahelyi kultúra és a szabályozás terén.

5.2.1 Technikai kihívások

A biztonságos ember–robot együttműködéshez a rendszereknek valós időben kell reagálniuk az emberi jelenlétre és mozgásra. Ez olyan fejlett technológiák alkalmazását igényli, mint:

- Erő-nyomaték érzékelők a túlzott nyomás elkerülésére,
- Kameraalapú térérzékelés a mozgáspályák folyamatos újratervezésére,
- Sebesség- és távolságfüggő mozgásvezérlés (pl. KUKA.SafeOperation).

A robotprogramozásnak és konfigurációnak olyan paraméterekkel kell dolgoznia, amelyek figyelembe veszik a munkatér dinamikáját, a váratlan emberi mozdulatokat és a működési ciklusokat is. Ez fokozott követelményeket támaszt a robotikai mérnökökkel és integrátorokkal szemben is [115].

5.2.2 Munkahelyi biztonság

A kollaboratív környezetekben alapvető fontosságú a munkavédelmi megfelelés, amelyet nemzetközi szabványok – pl. ISO 10218, ISO/TS 15066 – írnak elő. Ezek meghatározzák:

- A robotkar maximális sebességét és erejét,
- A munkatér fizikai kialakítását (pl. lekerekített élek, szenzoros védőzónák),
- A szükséges vészleállító mechanizmusokat és optikai érzékelőket.

A KUKA HRC-rendszerei ezen szabványok szerint készülnek, azonban a tényleges integráció során minden egyes alkalmazást egyedileg kell elemezni és validálni – ami idő- és költségigényes folyamat lehet [116].

5.2.3 Pszichológiai és szervezeti kihívások

A robotokkal való közös munkavégzés pszichológiai elfogadottsága is jelentős kihívást jelenthet. A dolgozók kezdetben bizonytalanságot, ellenállást vagy félelmet érezhetnek a robot jelenlétében, különösen, ha nem teljesen értik annak működését. Ennek kezelése érdekében szükség van:

- Tréningekre és oktatásra,
- Transzparens működésre (pl. vizuális kijelzők, visszajelző rendszerek),
- Kommunikációs protokollokra, amelyek biztosítják a kétirányú együttműködést.

Szervezeti szinten is alkalmazkodni kell: a HRC-környezetek bevezetése új munkakultúrát, folyamatátszervezést és felelősségi körök újragondolását teszi szükségessé. A siker kulcsa a technológiai és humán tényezők összehangolása [117].

5.2.4 Jogszabályi és etikai kihívások

Az ember–robot együttműködéshez kapcsolódó jogi kérdések is egyre hangsúlyosabbá válnak, többek között:

- Ki viseli a felelősséget baleset esetén?
- Milyen adatokat gyűjthet a robot a dolgozóról?
- Hogyan garantálható a munkavállaló jogainak védelme?

A jogi keretek nemzetközi szinten folyamatosan fejlődnek, de jelenleg is számos szürke zónát tartalmaznak. Az etikai kérdések – például a felügyelet, a döntéshozatal vagy az adatvédelem – szintén reflektálásra szorulnak a HRC-rendszerek tervezésekor és üzemeltetésekor.

5.3 Etikai és jogi kérdések

Az ipari robotika, különösen a mesterséges intelligenciával támogatott rendszerek elterjedése új kihívások elé állítja a szabályozási környezetet, valamint etikai szempontból is komoly kérdéseket vet fel. A KUKA fejlett robotikai megoldásai – amelyek képesek önálló döntéshozatalra, emberrel való közös munkavégzésre és adatok gyűjtésére – egyre inkább reflektorfénybe helyezik az ipari alkalmazások jogi megfelelőségét és társadalmi elfogadottságát.

Felelősségi kérdések és döntéshozatal

Az autonóm működésű robotok használata során az egyik legfontosabb kérdés: ki a felelős, ha a rendszer hibázik? Egy nem megfelelően végrehajtott hegesztés, egy hibás alkatrész beillesztése vagy egy ember–robot együttműködés során bekövetkező baleset esetén a felelősség elhatárolása nem egyértelmű.

Az ilyen esetekben vizsgálni kell:

- A gyártó (pl. KUKA) által biztosított technikai megfelelőséget,
- A rendszerintegrátor beállításait és validációját,
- Az üzemeltető karbantartási és biztonsági protokolljait.

Jelenleg a legtöbb országban ezek a kérdések az általános termékfelelősség és munkavédelmi jogszabályok körébe tartoznak, azonban a mesterséges intelligencia által vezérelt rendszerek esetén új, külön szabályozások bevezetése is várható [118].

Adatvédelem és munkavállalói jogok

A KUKA rendszerei – különösen az iiQoT platform – képesek nagy mennyiségű adat gyűjtésére, amelyek nemcsak a gépek működését, hanem közvetetten a dolgozók teljesítményét, jelenlétét és viselkedését is rögzíthetik. Ez felveti a következő kérdéseket:

- Milyen típusú adatot rögzít a rendszer?
- Ki férhet hozzá ezekhez az adatokhoz?
- Mennyi ideig és milyen célból tárolhatók?

Az adatvédelmi szabályozás, különösen az EU GDPR rendelete, előírja, hogy a dolgozókat tájékoztatni kell az adatgyűjtésről, és hozzájárulásuk nélkül nem alkalmazhatók olyan megfigyelési módszerek, amelyek közvetetten az ő viselkedésüket elemzik [119].

Etikai kérdések és társadalmi felelősség

A robotizáció etikai szempontból is érzékeny terület. A leggyakoribb etikai kérdések:

- **Méltóság kérdése**: Vajon a robotizált munkahelyeken az ember nem válik-e „ellenőrzött végrehajtóvá”?
- **Gazdasági kizárás**: Az automatizáció nem növeli-e a társadalmi egyenlőtlenségeket, például alacsonyabb képzettségű dolgozók kiszorításával?
- **Technológiai transzparencia**: A dolgozók tudják-e, milyen döntéseket hoz a rendszer, és milyen logika alapján?

A KUKA – és a hasonló ipari technológiaszállítók – fontos szerepet játszanak abban, hogy az új rendszerek átlátható módon működjenek, és ne sértsék az emberi jogokat és méltóságot. A technológiai fejlődés nemcsak gazdasági, hanem társadalmi felelősséggel is jár, amelyet a szabályozó szervek, a vállalatok és a munkavállalók közösen alakítanak [120].

Szabályozási jövőkép

Az EU-ban és más fejlett gazdaságokban már napirenden van a mesterséges intelligencia és autonóm rendszerek szabályozási keretrendszerének kialakítása. Ennek célja, hogy:

- Biztosítsa a biztonságos és átlátható működést,
- Meghatározza a felelősségi láncolatot baleset esetén,
- Védje az egyéni és kollektív munkavállalói jogokat.

Magyarországon is szükség van e kérdések további jogi és társadalmi reflexiójára, különösen ahogy a KUKA és más robotikai megoldások egyre szélesebb körben jelennek meg a hazai iparban.

6. ÖSSZEGZÉS

Az intelligens robotika napjaink ipari forradalmának egyik központi eleme, amely alapjaiban formálja át a gyártási folyamatokat, a munkahelyi struktúrákat és a technológiai innováció irányát. A dolgozat célja az volt, hogy bemutassa a KUKA ipari robotikai megoldásain keresztül, miként valósul meg az ipari automatizálás, és hogyan járul hozzá a hatékonyabb, rugalmasabb és fenntarthatóbb termeléshez.

A dolgozat első részében áttekintettük a robotika történeti fejlődését a mechanikus szerkezetektől a mesterséges intelligenciával támogatott autonóm rendszerekig. Részletesen bemutattuk a mesterséges intelligencia és gépi tanulás szerepét a modern ipari robotok működésében, valamint az ember és gép együttműködésének lehetőségeit, különös tekintettel a KUKA kollaboratív megoldásaira.

Az alkalmazási területek elemzése során láthatóvá vált, hogy a KUKA robotok nemcsak az autonóm gyártósorok működésében, hanem a logisztikában, a minőségellenőrzésben, az autóiparban és a steril iparágakban is kiemelkedő szerepet játszanak. A szenzortechnológia, a valós idejű adatfeldolgozás és a digitális integráció révén ezek a rendszerek képesek intelligensen reagálni a környezeti és gyártási változásokra.

A fejlesztési irányok között kiemelt figyelmet fordítottunk a Big Data alapú optimalizálásra, a fenntartható energiafelhasználásra és a környezetbarát gyártástechnológiákra. Ezek a szempontok nemcsak gazdasági, hanem társadalmi és környezeti szinten is jelentős hatást gyakorolnak.

A társadalmi és munkaerőpiaci hatások elemzése során megállapítható, hogy a robotika fejlődése kettős jelenség: miközben egyes hagyományos munkakörök megszűnnek, új, magasabb képzettséget igénylő szakmák jönnek létre. Az ember–robot együttműködés újfajta biztonságtechnikai, pszichológiai és szervezeti megközelítést igényel, amelyhez elengedhetetlen a folyamatos oktatás és készségfejlesztés.

Végezetül a dolgozat kitért az etikai és jogi kérdésekre, amelyek az autonóm döntéshozatal, az adatkezelés és a munkavállalói jogvédelem területén jelennek meg. A szabályozási környezet fejlődése, az átlátható felelősségi láncok kialakítása és a technológia etikus alkalmazása elengedhetetlen feltétele a robotika társadalmi beágyazódásának.

Összességében elmondható, hogy a KUKA által képviselt intelligens robotikai megoldások nemcsak az ipar 4.0 megvalósulásának kulcsfontosságú elemei, hanem a jövő ipari termelésének alapkövei is. A technológiai, gazdasági és társadalmi szempontokat egyaránt figyelembe véve ezek a rendszerek fenntartható és emberközpontú ipari működés felé terelhetik a globális termelést.

Irodalomjegyzék

[1], [6], [12], [16], [21], [26], [30], [35], [40], [44]

Érettségik.hu, „A robotika fejlődése – a mechanikus robotoktól az intelligens rendszerekig,” 2025. [Online]. Elérhető: https://erettsegik.hu/2025/02/16/a-robotika-fejlodese/

[2], [9], [13], [17], [20], [24], [29], [34], [38], [43], [71]

Műszaki Magazin, „Intelligens robot stratégia: A mesterséges intelligencia szerepe a munka világában,” 2024. [Online]. Elérhető: https://www.muszaki-magazin.hu/2024/12/12/intelligens-robot-strategia-deloitte-munka/

[3], [8], [22], [25], [31], [33], [39], [47], [49]

Deloitte Hungary, „Intelligens robotok – nekünk, velünk, helyettünk dolgoznak,” Deloitte Kockázatkezelési üzletág, [Online]. Elérhető: https://www.deloitte.com/hu/hu/services/risk-advisory/perspectives/intelligens-robotok-nekunk-velunk-helyettunk-dolgoznak.html

[4], [7], [11], [15], [19], [28], [37], [42], [46]

Techmonitor, „A robotika rövid története,” 2022. [Online]. Elérhető: https://www.techmonitor.hu/tudastar/a-robotika-rovid-tortenete-20220613

[5], [10], [14], [18], [23], [27], [32], [36], [41], [45], [50] HRPWR.hu, „Hogyan írja át a munkaerőpiacot a robotika fejlődése?” [Online]. Elérhető: https://hrpwr.hu/cikk/hogyan-irja-at-a-munkaeropiacot-a-robotika-fejlodese

[48] KUKA AG, „Ipari robotok alkalmazási területei,” 2024. [Online]. Elérhető: https://www.kuka.com

[51] KUKA AG, „Ready2_use robotmegoldások,” 2024. [Online]. Elérhető: https://www.kuka.com/hu-hu

[52] KUKA AG, „KUKA.Sim és mxAutomation rendszerek,” 2024. [Online]. Elérhető: https://www.kuka.com/

[53] KUKA AG, „iiQoT – Industrial IoT platform,” 2024. [Online]. Elérhető: https://www.kuka.com

[54] KUKA Robotics Hungária Kft., Cégtár: Céginformáció.hu. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[55] KUKA AG, „KR QUANTEC – nagy teherbírású robotok,” 2024. [Online]. Elérhető: https://www.kuka.com

[56] KUKA AG, „KR CYBERTECH – kis és közepes teherbírású robotok,” 2024. [Online].

[57] KUKA AG, „KR C5 vezérlőegység,” 2024. [Online].

[58] KUKA AG, „KUKA.WorkVisual és KUKA.Sim szimulációs eszközök,” 2024. [Online].

[59] KUKA AG, „Smart Factory – intelligens gyártási rendszerek,” 2024. [Online]. Elérhető: https://www.kuka.com

[60] KUKA AG, „iiQoT – Industrial IoT megoldások,” 2024. [Online].

[61] KUKA AG, „KUKA.Sim – digitális szimulációs szoftver,” 2024. [Online].

[62] Ipar 4.0 Platform, „KUKA Robotics Hungária Kft. – tagvállalat,” 2024. [Online]. Elérhető: https://i40platform.hu/hu/szervezet/tagok/kuka-robotics-hungaria-kft

[63] KUKA AG, „KMP – KUKA Mobile Platform,” 2024. [Online]. Elérhető: https://www.kuka.com

[64] KUKA AG, „Autonóm navigáció mobil robotokkal,” 2024.

[65] KUKA AG, „Mobil logisztikai megoldások integrálása ipari robotikába,” 2024.

[66] KUKA AG, „iiQoT platform – logisztikai modulok,” 2024.

[67] KUKA Robotics Hungária Kft., „Hazai mobil robotikai alkalmazások,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[68] KUKA AG, „KMP 1500 és KMP 600-S mobil robotok,” 2024. [Online]. Elérhető: https://www.kuka.com

[69] KUKA AG, „Autonóm navigáció és SLAM megoldások AGV rendszerekhez,” 2024.

[70] KUKA AG, „iiQoT platform – adatvezérelt AGV felügyelet,” 2024.

[72] KUKA Robotics Hungária Kft., „AGV rendszerek magyarországi alkalmazása,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[73] KUKA AG, „KMP mobil platformok – autonóm szállítórendszerek,” 2024. [Online]. Elérhető: https://www.kuka.com

[74] KUKA AG, „Smart logistics: anyagmozgatás automatizálása,” 2024.

[75] KUKA AG, „KUKA.NavigationSolution – flottairányítás és útvonaloptimalizálás,” 2024.

[76] Műszaki Magazin, „Önvezető logisztikai robotok a jövő iparában,” 2024.

[77] KUKA Robotics Hungária Kft., „Ipari belső logisztikai rendszerek magyarországi alkalmazása,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[78] KUKA AG, „KR AGILUS és KR CYBERTECH – precíziós robotkarok,” 2024. [Online]. Elérhető: https://www.kuka.com

[79] Műszaki Magazin, „AI-alapú minőségellenőrzés robotokkal,” 2024.

[80] KUKA AG, „iiQoT platform – adatvezérelt minőségbiztosítás,” 2024.

[81] KUKA Robotics Hungária Kft., „Minőségellenőrző rendszerek magyarországi alkalmazása,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[82] KUKA AG, „KR QUANTEC sorozat – ponthegesztés autóipari gyártásban,” 2024. [Online]. Elérhető: https://www.kuka.com

[83] Műszaki Magazin, „Lézerhegesztés KUKA robotokkal,” 2024.

[84] KUKA AG, „KR FORTEC – nagy igénybevételű fémmegmunkálás,” 2024.

[85] KUKA AG, „cell4_production – rugalmas robotcella koncepciók,” 2024.

[86] KUKA Robotics Hungária Kft., „Autóipari automatizálási projektek Magyarországon,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[87] KUKA AG, „KR QUANTEC – ipari robot ponthegesztéshez,” 2024. [Online]. Elérhető: https://www.kuka.com

[88] KUKA AG, „KUKA.ArcTech és RoboSpin – intelligens hegesztésvezérlés,” 2024.

[89] Műszaki Magazin, „Alumínium hegesztés az autógyártásban – KUKA megoldások,” 2024.

[90] KUKA Robotics Hungária Kft., „Karosszériahegesztés robotizálása a magyar autóiparban,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[91] KUKA AG, „cell4_production – moduláris robotcellák,” 2024. [Online]. Elérhető: https://www.kuka.com

[92] KUKA AG, „KR FORTEC és KR CYBERTECH – ipari robotok cellás integrációhoz,” 2024.

[93] KUKA AG, „KUKA.SafeOperation és biztonságtechnika,” 2024.

[94] Techmonitor, „Kutatási célú robotcellák a magyar felsőoktatásban,” 2024.

[95] KUKA Robotics Hungária Kft., „Robotcellák telepítése hazai gyártóüzemekben,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[96] KUKA AG, „KR AGILUS hygienic machine – gyógyszeripari robotika,” 2024. [Online]. Elérhető: https://www.kuka.com

[97] KUKA AG, „KR DELTA és SCARA – élelmiszeripari alkalmazások,” 2024.

[98] Techmonitor, „Robotok steril környezetekben – higiéniai tervezés,” 2024.

[99] Deloitte, „Rugalmasság és automatizáció az élelmiszeriparban,” 2023.

[100] KUKA Robotics Hungária Kft., „Robotikai rendszerek a hazai gyógyszeriparban,” 2024. [Online]. Elérhető: https://www.ceginformacio.hu/cr9310048733

[101] KUKA AG, „iiQoT – adatvezérelt ipari rendszerfelügyelet,” 2024. [Online]. Elérhető: https://www.kuka.com

[102] Műszaki Magazin, „Gépi tanulás a prediktív karbantartás szolgálatában,” 2024.

[103] Deloitte, „Big Data és mesterséges intelligencia az ipari digitalizációban,” 2023.

[104] KUKA AG, „iiQoT – valós idejű adatgyűjtés és analitika,” 2024. [Online]. Elérhető: https://www.kuka.com

[105] Deloitte, „Adatalapú gyártás és robotikai optimalizáció,” 2023.

[106] Techmonitor, „Big Data feldolgozás és gépi tanulás a gyártásban,” 2024.

[107] KUKA AG, „Ipari robotok érzékelőintegrációja és mozgásvezérlése,” 2024. [Online]. Elérhető: https://www.kuka.com

[108] KUKA AG, „KUKA.ForceTorqueSensor és SafeOperation – szenzoros vezérlés és biztonság,” 2024.

[109] Techmonitor, „SLAM és autonóm navigáció ipari mobil robotokban,” 2024.

[110] KUKA AG, „Multiszenzoros vezérlés és robotadaptivitás,” 2024. [Online]. Elérhető: https://www.kuka.com

[111] KUKA AG, „Sunrise.OS – nagysebességű adatfeldolgozás és szabályozás,” 2024.

[112] Műszaki Magazin, „Szenzor-fúzió és mesterséges intelligencia a robotikában,” 2024.

[113] KUKA AG, „KR QUANTEC és KR IONTEC – energiatakarékos ipari robotok,” 2024. [Online]. Elérhető: https://www.kuka.com

[114] KUKA AG, „iiQoT és KUKA.EnergyMonitoring – valós idejű energiafelügyelet,” 2024.

[115] Deloitte, „Fenntarthatóság az ipari automatizálásban,” 2023.

[116] Deloitte, „Robotizáció és foglalkoztatási szerkezetváltás az iparban,” 2023.

[117] KUKA AG, „Új szerepkörök a robotikai rendszerek körül,” 2024. [Online]. Elérhető: https://www.kuka.com

[118] Techmonitor, „Digitális kompetenciák és ipari képzés a jövő munkahelyeihez,” 2024.

[119] KUKA AG, „LBR iiwa – kollaboratív robot fejlett érzékeléssel,” 2024. [Online]. Elérhető: https://www.kuka.com

[120] ISO, „ISO 10218 és ISO/TS 15066 – biztonsági szabványok ember–robot együttműködésre,” 2023.

[121] https://www.researchgate.net/figure/Diagram-of-robots-circuit-system_fig2_335499691

[122] https://mogi.bme.hu/TAMOP/robotalkalmazasok/ch01.html

[123] https://bsybeedesign.com/business/robot-diagram-a-visual-guide-to-robotics/

[124] https://www.researchgate.net/figure/Diagram-of-robots-circuit-system_fig2_335499691

2.12. Okosotthonok energiahatékonysági megoldásai: Fenntarthatóság és költségcsökkentés a modern technológiák segítségével

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF COMPUTER SCIENCE

Ipar 4.0 technológiák

GKNB_INTM087

Okosotthonok energiahatékonysági megoldásai: Fenntarthatóság és költségcsökkentés a modern technológiák segítségével

Klement Viktor [redacted]

Mérnökinformatikus, BSc, nappali

Készült: 2025. április-május

Tartalomjegyzék

Bevezetés 3
Mi az okosotthon? 3
Okosotthonok fejlődése 4
Célkitűzés 4
1. Okosotthon rendszerek és eszközök [1] 5
1.1 Okos világítás 5
1.2 Okos fűtés és hűtés [3] 6
1.2 Okos biztonsági rendszerek 6
1.3 Hangvezérelt asszisztensek 7
1.4 Energiahatékonysági megoldások [4] 7
2. Az okosotthonok technológiai alapjai 7
2.1 IoT és beágyazott rendszerek [6] 8
2.2 Szenzorok, automatizáció és vezérlés [6] 8
2.3 Mesterséges intelligencia és gépi tanulás [5] 9
3. Az okosotthonok előnyei és kihívásai [4] 10
3.1 Előnyök és hátrányok [11] 10
3.2 Költségek és rendszer komplexitás [8] 10
3.3 Adatvédelmi aggályok 11
3.4 Energiafelhasználás csökkentése [7][5] 11
4. Felhasználói élmény és alkalmazások [2] 12
4.1 Mobilalkalmazások és vezérlőfelületek 13
4.2 Platformok közötti kompatibilitás 14
4.3 Automatikus élethelyzetek kezelése [2] 14
5. Jövőbeli trendek és fejlesztések [9] 15
5.1 5G és gyorsabb kommunikáció 15

5.2 AI továbbfejlesztése [5] 16
5.3 Fenntarthatóság [1] 17
6. Okosotthonok társadalmi és gazdasági hatásai 18
6.1 Lakóépületek értékének növekedése 18
6.2 Szerep a városi energiafogyasztás csökkentésében [6] 19
6.3 Társadalmi rétegek közötti hozzáférési különbségek 20
6.4 Munkahelyteremtés és új iparágak kialakulása 20
Összegzés 21
Hozzájárulás az energiahatékonysághoz és fenntarthatósághoz 21
Jövőbeli kilátások 22
Összegzés és javaslatok 22
Irodalomjegyzék 23

Bevezetés

Mi az okosotthon?

Az okosotthon egy olyan lakókörnyezet, ahol a különféle háztartási eszközök, rendszerek és szolgáltatások digitálisan összekapcsolva működnek. *(1. ábra)* Ezeket gyakran egy központi rendszer vagy applikáció irányítja, de sokszor maguktól, automatikusan reagálnak a környezet változásaira vagy a felhasználó szokásaira. Ide tartozhat például az automatikus világítás, az időjáráshoz igazodó fűtés, a hangvezérelt zenelejátszás, vagy a távolról vezérelhető biztonsági rendszer. Azért nevezzük ezeket „okosnak”, mert képesek adatokat gyűjteni, tanulni a felhasználó viselkedéséből, és ezek alapján önálló döntéseket hozni – például lekapcsolni a villanyt, ha nem érzékelnek mozgást egy helyiségben.

A rendszer alapja az úgynevezett IoT (Internet of Things). Ez teszi lehetővé, hogy az egyes berendezések (pl. termosztát, redőny, lámpa) kommunikálni tudjanak egymással és egy központi egységgel – legyen az egy mobilalkalmazás, okoshangszóró vagy vezérlőpanel. Az egész célja, hogy az otthon kényelmesebb, energiatakarékosabb és biztonságosabb legyen.

1. ábra: Okosotthon szemléltetése (forrás: commons.wikimedia.org)

Okosotthonok fejlődése

Az okosotthon koncepciója nem teljesen új, de a mai értelemben vett megoldások csak az utóbbi évtizedben kezdtek elterjedni. Kezdetben a „programozható” eszközök jelentették az első lépést: ilyen volt például az időzítős termosztát vagy a mozgásérzékelős világítás.

A nagy fordulatot az internetelérés általánossá válása, a vezeték nélküli technológiák fejlődése (pl. Wi-Fi, Bluetooth, Zigbee) és a felhőalapú rendszerek hozták el. Ma már elérhetők olyan központi alkalmazások, amelyek egyidejűleg több különböző eszközt képesek vezérelni. Ezen kívül megjelentek a hangvezérelt asszisztensek (mint az Alexa vagy a Google Assistant), amelyekkel szóbeli utasításokat is adhatunk. A fejlettebb rendszerek már mesterséges intelligenciát is használnak, például figyelik, hogy a felhasználó mikor szokott hazaérni, és előre beállítják a hőmérsékletet, világítást vagy akár a kávéfőzőt is.

Ma már nemcsak a drága luxusotthonok kiváltsága az okosmegoldások alkalmazása – sok eszköz viszonylag megfizethető, és akár utólag is beépíthető a meglévő lakásokba. Ez a hozzáférhetőség nagyban hozzájárul ahhoz, hogy az okosotthonok egyre inkább terjednek, és a jövő lakótereinek szerves részévé válnak.

Célkitűzés

A beadandóm célja, hogy bemutassam, hogyan járulnak hozzá az okosotthon rendszerek az energiahatékonysághoz és a fenntarthatósághoz. *(2. ábra)* Megvizsgáljam az elérhető eszközöket és technológiákat, elemezzem azok működését és gyakorlati hasznát, illetve szó lesz az esetleges hátrányokról és kihívásokról is. Fontos kérdés például az adatvédelem, a technikai megbízhatóság vagy az, hogy mennyire könnyen kezelhetőek ezek a rendszerek egy átlagfelhasználó számára.

2. ábra: Energiahatékonyság (forrás: unsplash.com)

Kitérek a jövőbeli fejlesztési irányokra is – ilyen például az 5G hálózatok hatása az eszközök közötti kommunikációra, a mesterséges intelligencia további térnyerése, vagy a még fenntarthatóbb, környezettudatosabb megoldások. A cél nemcsak az, hogy bemutassam az aktuális állapotot, hanem hogy képet kapjunk arról, merre tart ez a technológia, és milyen szerepet játszhat a jövő otthonaiban.

1. Okosotthon rendszerek és eszközök [1]

Az okosotthonok működésének alapját azok az eszközök és rendszerek adják, amelyek képesek együttműködni, kommunikálni, és önállóan vagy programozott módon reagálni különféle helyzetekre. Ezek az eszközök nem csupán kényelmesebbé teszik az otthoni környezetet, hanem segítenek az energiahatékony működésben is.

1.1 Okos világítás

Az intelligens világítási rendszerek legnagyobb előnye, hogy rugalmasan és személyre szabottan működnek. A hagyományos villanykapcsolók helyett alkalmazhatóak mozgásérzékelők, időzítők vagy éppen mobiltelefonos vezérlés. *(3. ábra)* Egyes rendszerek képesek alkalmazkodni a napszakhoz, az időjáráshoz vagy akár a felhasználói szokásokhoz is. A fényerő és színhőmérséklet szabályozása nemcsak hangulatteremtésre alkalmas, hanem az energiafogyasztás optimalizálásában is szerepet játszik. Mindez különösen hatékonnyá válik, ha LED-es világítótestekkel kombinálva használják a rendszert.

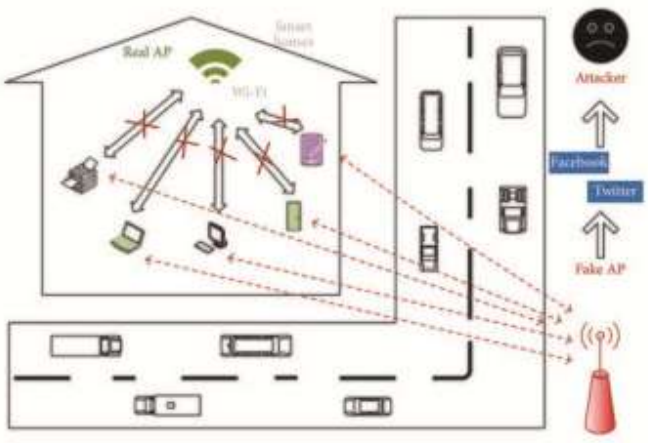
3. ábra: Okos világítás app (forrás: unsplash.com)

1.2 Okos fűtés és hűtés [3]

Az energiafelhasználás szempontjából a fűtés és hűtés vezérlése kiemelt terület. Az okos termosztátok és klímaberendezések lehetővé teszik a hőmérséklet finomhangolását, akár automatikusan is, az előző napok szokásai vagy az aktuális időjárás alapján. A rendszer képes felismerni, mikor tartózkodik valaki otthon, és ennek megfelelően szabályozza a működést, elkerülve a felesleges energiahasználatot. Egy jól beállított rendszerrel nemcsak komfortosabb lesz a hőérzet, hanem jelentős energiamegtakarítás is elérhető.

1.2 Okos biztonsági rendszerek

A biztonságtechnika területén az okosotthonok szintén komoly előrelépést jelentenek. A kamerák, szenzorok, nyitásérzékelők és mozgásdetektorok hálózatba kapcsolva képesek komplex rendszert alkotni. Ezek az eszközök nemcsak riasztanak, hanem információt is továbbítanak – akár egy mobiltelefonra –, így bármilyen esemény azonnal észlelhető. Egyes rendszerek képesek szimulálni a jelenlétet is, például esti fények bekapcsolásával, ami távol tartja a hívatlan látogatókat. A rendszerek távolról is vezérelhetők, ami további kényelmet és biztonságot nyújt.



4. ábra: Támadás egy okosotthon Wi-Fi hálózatában (forrás: commons.wikimedia.org)

1.3 Hangvezérelt asszisztensek

Az intelligens hangasszisztensek egyre több háztartásban jelennek meg. Ezek az eszközök (Google Assistant, Amazon Alexa *(5. ábra),* Apple Siri) lehetővé teszik, hogy a lakás különböző rendszereit szóban kiadott utasításokkal lehessen vezérelni. A világítás, a fűtés, a zenelejátszás vagy akár az internetes keresések is elérhetők pusztán hangutasításokkal. Bár ezek önmagukban nem feltétlenül energiahatékonysági eszközök, a rendszerbe illesztve jelentősen javítják az okosotthon funkcionalitását.

5. ábra: Alexa (forrás: pexels.com)

1.4 Energiahatékonysági megoldások [4]

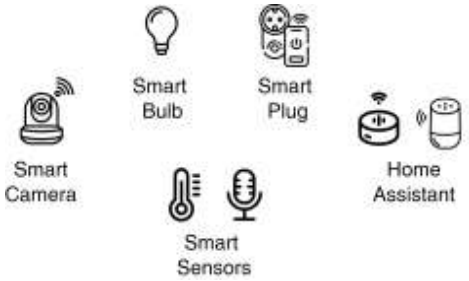
Az okosotthonok egyik legfontosabb előnye a tudatos és hatékony energiahasználat. Ehhez különféle eszközök állnak rendelkezésre, például okos konnektorok, fogyasztásmérők vagy akár napelemes rendszerekhez kapcsolódó vezérlők. Ezek képesek részletes információt nyújtani az energiafelhasználásról, és segítenek abban, hogy a háztartás az igényekhez igazodva működjön. Egyes rendszerek automatikusan lekapcsolják a nem használt eszközöket, vagy optimalizálják az energiaelosztást például időzített működéssel. A hosszú távú cél nemcsak a költségcsökkentés, hanem a fenntarthatóbb működés biztosítása is.

2. Az okosotthonok technológiai alapjai

Egy okosotthon működésének alapját olyan technológiák adják, amelyek lehetővé teszik az eszközök közötti folyamatos kommunikációt, az automatikus működést, és a valós idejű reagálást a környezeti változásokra. Az ilyen rendszerek lényege, hogy láthatatlanul, de hatékonyan működnek a háttérben, miközben a felhasználó kényelmesen és egyszerűen tudja őket kezelni.

2.1 IoT és beágyazott rendszerek [6]

Az IoT, vagyis a „dolgok internete” azt jelenti, hogy különböző fizikai eszközök *(6. ábra),* például termosztátok, izzók, szenzorok vagy zárak, képesek az interneten keresztül adatokat küldeni és fogadni. Ezek az eszközök beépített számítási egységekkel és kommunikációs modulokkal rendelkeznek, amelyek lehetővé teszik, hogy ne csak egyszerű végrehajtók legyenek, hanem aktív résztvevői egy hálózatnak. A beágyazott rendszerek kis méretű, célzott feladatokra optimalizált vezérlőegységek, amelyek például egy fűtésvezérlőben vagy mozgásérzékelőben találhatók. Ezek az eszközök önálló működésre képesek, és az IoT-hálózat részeként folyamatosan adatokat dolgoznak fel, illetve kommunikálnak más eszközökkel.



6. ábra: IoT eszközök (forrás: commons.wikimedia.org)

2.2 Szenzorok, automatizáció és vezérlés [6]

Az okosotthonok egyik kulcseleme a különféle szenzorok használata. Ezek az érzékelők információt gyűjtenek a környezetről *(7.,8. ábra)* (hőmérsékletről, fényviszonyokról, páratartalomról, mozgásról vagy akár levegőminőségről). Ezeket az adatokat a rendszer kiértékeli, majd a meghatározott szabályok vagy algoritmusok alapján döntéseket hoz. Például ha a fényerő lecsökken egy helyiségben, a világítás automatikusan bekapcsolhat, vagy ha egy ablak nyitva van, a fűtés visszaveszi a teljesítményét.

7. ábra: Smart Mold Sensor (forrás: commons.wikimedia.org)

8. ábra: Heart Rate Sensor (forrás: commons.wikimedia.org)

Az automatizáció azt jelenti, hogy ezek a műveletek nem manuális beavatkozással történnek, hanem előre meghatározott logika alapján, automatikusan. A vezérlés történhet központi irányítópulton, mobilalkalmazáson keresztül vagy akár teljesen önállóan is. Az egyszerűbb automatizálások mellett lehetőség van komplexebb működések beállítására is – például napi rutinok vagy több szenzor adatainak kombinált értelmezése alapján. Ez a technológiai alap biztosítja, hogy az okosotthon ne csak „kapcsolható” legyen, hanem valóban intelligensen alkalmazkodjon a környezethez.

2.3 Mesterséges intelligencia és gépi tanulás [5]

Az okosotthonok működésében egyre nagyobb szerepet kap a mesterséges intelligencia, különösen a gépi tanulás. Ezek a rendszerek képesek idővel felismerni mintákat a felhasználói szokásokban, és ez alapján optimalizálni a működésüket. Például ha egy lakó rendszeresen este 7-kor hazaér, a világítás, fűtés vagy akár a zenelejátszás is ehhez alkalmazkodhat. A gépi tanulás segítségével a rendszer megtanulja, mikor van szükség energiára és mikor nincs, így folyamatosan finomítja az energiafelhasználást.

Az AI képes olyan helyzetek felismerésére is, amelyeket egy egyszerű szabályrendszer nem tudna kezelni. Ha például egy adott napon eltérő viselkedés tapasztalható, a rendszer rugalmasan tud ehhez igazodni, anélkül, hogy kézi beavatkozásra lenne szükség. Emellett az AI alapú rendszerek képesek idővel javaslatokat is tenni a hatékonyabb működésre, például fogyasztási szokások alapján.

3. Az okosotthonok előnyei és kihívásai [4]

Egy okosotthon rendszer bevezetése több szempontból is jelentős hatással van a mindennapokra, legyen szó kényelemről, energiahatékonyságról vagy biztonságról. Ugyanakkor fontos átlátni azokat a kihívásokat is, amelyekkel a használók szembesülhetnek. Például a technikai összetettséget, az adatvédelemmel kapcsolatos kérdéseket vagy a kezdeti beruházási költségeket.

3.1 Előnyök és hátrányok [11]

Az egyik legnagyobb előny az automatizációban és a rendszer rugalmasságában rejlik. Egy jól megtervezett okosotthon képes a felhasználó napi rutinjához igazodni, optimalizálni az energiafogyasztást, és automatikusan reagálni különféle eseményekre. Ezen kívül javítja a biztonságot is: a távolról vezérelhető riasztók, kamerák, mozgásérzékelők és okos zárak növelik az otthon védelmét, akár akkor is, ha senki nincs otthon.

Ezzel szemben a rendszerek összetettsége hátrányt is jelenthet. A különféle gyártók termékei nem mindig kompatibilisek egymással, így az integráció problémás lehet. Emellett a rendszer kiépítése és karbantartása technikai ismereteket igényelhet, vagy külső szakember bevonását teszi szükségessé. A szoftverfrissítések, hálózati problémák vagy egyes eszközök meghibásodása pedig működési zavarokat is okozhat.

3.2 Költségek és rendszer komplexitás [8]

Az okosotthon kialakításának költségei széles skálán mozognak. Egy alap szintű már viszonylag elérhető áron kiépíthető. Azonban ha a teljes otthon vezérlésére kiterjedő, integrált rendszerről van szó, a költségek jelentősen megnőhetnek. Ide tartoznak az eszközök ára mellett a telepítési, karbantartási és rendszerintegrációs díjak is.

A komplexitás sokszor azzal jár, hogy a felhasználónak meg kell tanulnia a rendszer működését, alkalmazásait, és azt is, hogyan reagáljon hibákra vagy hálózati problémákra. Egyesek számára ez visszatartó erő lehet, különösen akkor, ha a technológia nem intuitív vagy túlságosan bonyolult.

3.3 Adatvédelmi aggályok

Az okosotthonok működésének egyik alapja az adatok gyűjtése és feldolgozása. Az eszközök érzékeny információkat is rögzíthetnek, például arról, mikor van otthon valaki, milyen szokásai vannak, vagy milyen eszközöket használ rendszeresen. Ezeket az adatokat sokszor felhőalapú szolgáltatásokon keresztül tárolják és elemzik, ami adatvédelmi kockázatokat vethet fel.

9. ábra: Adatvédelem Illusztráció (forrás: commons.wikimedia.org)

A felhasználóknak tisztában kell lenniük azzal, hogy az adatok milyen formában kerülnek továbbításra, hol tárolódnak, és ki férhet hozzájuk. A nem megfelelően beállított jogosultságok, a gyenge jelszavak vagy a nem frissített szoftverek sebezhetővé tehetik a rendszert. *(9. ábra)* Az adatbiztonság tehát nemcsak jogi vagy technikai kérdés, hanem a rendszer megbízhatóságának egyik alapvető tényezője is.

3.4 Energiafelhasználás csökkentése [7][5]

Az okosotthonok egyik leggyakoribb célja az energiahatékonyság javítása. A világítás, fűtés, hűtés és más háztartási eszközök működésének optimalizálása csökkentheti a fölösleges energiahasználatot. Például egy okos termosztát csak akkor fűt, ha valóban szükséges, vagy előre beállított időpontokban működik, alkalmazkodva a felhasználó napi szokásaihoz.

Ugyanígy, a mozgásérzékelőkkel működő világítás kikapcsol, ha nincs mozgás a helyiségben, és az okos redőnyök napfény alapján szabályozzák a hőmérsékletet, így csökkentve a légkondicionálás igényét. Ezek az apró optimalizálások hosszabb távon jelentős megtakarítást eredményezhetnek, és csökkentik a háztartás ökológiai lábnyomát is.

4. Felhasználói élmény és alkalmazások [2]

Az okosotthon-rendszerek működése szorosan összefügg azzal, hogy a felhasználók mennyire tudják azokat egyszerűen, kényelmesen és hatékonyan használni. A technológiai háttér önmagában nem elegendő, ha az irányítás túl bonyolult vagy nem intuitív. A fejlesztések egyik központi célja éppen az, hogy az eszközöket könnyen hozzáférhető és jól kezelhető felületeken keresztül *(10. ábra)* lehessen irányítani, akár távolról is. Az automatizálásnak úgy kell jelen lennie a háttérben, hogy ne igényeljen folyamatos felhasználói beavatkozást.

10. ábra: Smart Home Mobile Control (forrás: unsplash.com)

A felhasználói élmény javítását az is segíti, ha a rendszer különböző platformokon keresztül elérhető (okostelefonon, tableten vagy hangvezérléssel). Az egyszerű és gyors visszajelzések, mint például az értesítések a fogyasztási szokásokról vagy az azonnali hibajelzések, támogatják a tudatosabb energiahasználatot. Fontos, hogy az okosotthon ne terhelje a felhasználót felesleges technikai részletekkel, hanem átlátható és kezelhető módon segítse a döntéshozatalt.

4.1 Mobilalkalmazások és vezérlőfelületek

A legtöbb gyártó saját mobilalkalmazást *(11. ábra)* kínál, amelyen keresztül az eszközök vezérelhetők. Ezeken belül lehetőség van arra, hogy a világítást, a hőmérsékletet, a biztonsági rendszert vagy akár a redőnyöket is egyetlen felületről lehessen szabályozni. Egy jól megtervezett applikáció átlátható, logikus menürendszerrel rendelkezik, és nem igényel különösebb technikai előképzettséget.

Sok esetben ezeket a rendszereket már nemcsak okostelefonról, hanem tabletről, okosóráról vagy akár számítógépről is lehet vezérelni. A központi vezérlőfelületek (például egy fali érintőképernyő) lehetővé teszik, hogy egy helyről minden eszköz áttekinthető és szabályozható legyen.

11.ábra: Okos zár működése mobilalkalmazással (Forrás: www.pexels.com)

4.2 Platformok közötti kompatibilitás

Mivel különböző gyártók különféle megoldásokat kínálnak, egyre fontosabbá válik, hogy ezek a rendszerek képesek legyenek egymással együttműködni. Az egységes szabványok, például a Matter vagy a Zigbee segítenek abban, hogy eltérő márkák eszközei is közösen működjenek. Ez a kompatibilitás azért is lényeges, mert a felhasználók gyakran fokozatosan építik ki az okosotthon-rendszerüket, és nem minden alkotóelem származik ugyanattól a gyártótól.

A nyílt platformok lehetővé teszik, hogy a rendszert az igényekhez igazítva alakítsák ki, miközben elkerülhető az, hogy valaki egyetlen gyártó ökoszisztémájához legyen kötve. Ez hosszú távon rugalmasabb fejlesztést tesz lehetővé, valamint javítja a felhasználói élményt is.

4.3 Automatikus élethelyzetek kezelése [2]

Az okosotthonok egyik legnagyobb előnye az, hogy képesek az ismétlődő vagy előre tervezett élethelyzetek automatizálására. Ilyen lehet például egy reggeli rutin, ahol a rendszer magától felkapcsolja a világítást, felfűti a helyiségeket, és bekapcsolja a kávéfőzőt. Ugyanez igaz a távozásra is, amikor a rendszer lekapcsolja a lámpákat, bezárja az ajtókat, és lejjebb veszi a fűtést.

Ezek az automatizált jelenetek nemcsak kényelmet biztosítanak, hanem segítenek a felesleges energiahasználat csökkentésében is. A szenzorok, időzítők és helymeghatározási funkciók mind azt szolgálják, hogy a rendszer alkalmazkodjon a lakók szokásaihoz. A jelenlét-szimulációs funkciók például biztonsági célt is szolgálnak: távol lét esetén is azt az érzetet keltik, mintha valaki otthon tartózkodna.

5. Jövőbeli trendek és fejlesztések [9]

Az okosotthon-technológia folyamatosan fejlődik, és a következő években számos újítás várható, amelyek nemcsak a kényelmet, hanem a fenntarthatóságot és az energiahatékonyságot is tovább javíthatják. A technológiai környezet, amiben ezek az eszközök működnek, egyre gyorsabb és összetettebb, ezért fontos figyelemmel követni a legújabb trendeket.

5.1 5G és gyorsabb kommunikáció

Az 5G technológia *(12. ábra)* bevezetése alapjaiban változtatja meg az IoT (Internet of Things) eszközök közötti kommunikációt. A gyorsabb adatátvitel, alacsonyabb válaszidő és nagyobb hálózati kapacitás lehetővé teszi, hogy még több eszköz működjön párhuzamosan, akadozás nélkül. Ez különösen fontos lehet olyan otthonokban, ahol több tucat okoseszköz van használatban egyszerre – például világítás, fűtés, biztonsági rendszerek és háztartási gépek.

12. ábra: 5G illusztráció (forrás: unsplash.com)

A gyorsabb adatforgalom azt is lehetővé teszi, hogy az eszközök szinte valós időben reagáljanak a környezet változásaira. Egy intelligens rendszer például azonnal képes alkalmazkodni a felhasználó szokásaihoz, mozgásához vagy akár az időjárási viszonyokhoz. A fejlettebb hálózati kommunikáció révén a rendszer stabilabbá válik, csökken a hibalehetőség, és nő a felhasználói élmény.

5.2 AI továbbfejlesztése [5]

A mesterséges intelligencia az okosotthonok működésében már most is kulcsszerepet játszik, de a fejlődése még korántsem ért véget. A jövőben az AI-alapú rendszerek *(13. ábra)* nemcsak tanulni fognak a felhasználók szokásaiból, hanem képesek lesznek komplexebb döntések meghozatalára is. Az algoritmusok egyre pontosabban ismerik fel a mintázatokat, előrejelzik az igényeket, és önállóan optimalizálják az energiahasználatot.

A jövőben várható, hogy az okosotthonok rendszerei nem csak reagálnak, hanem megelőznek bizonyos eseményeket. Például, ha a rendszer azt érzékeli, hogy az áramfogyasztás szokatlanul magas, automatikusan javaslatot tehet bizonyos eszközök kikapcsolására. Hosszabb távon az AI akár karbantartási problémákra is figyelmeztethet, mielőtt azok valódi hibát okoznának.

Ezek a fejlesztések az otthonok „proaktívvá” válását segítik elő, vagyis az otthoni rendszerek egyre inkább saját maguk kezelik a környezeti és technikai változásokat, minimális emberi beavatkozással.

13. ábra: AI Smart Home (forrás: intuz.com)

5.3 Fenntarthatóság [1]

A fenntarthatóság az egyik legfontosabb cél, ami az okosotthon-fejlesztéseket motiválja. Az energiahatékony működés *(14. ábra)* már jelenleg is fontos szempont, de a jövőben várható, hogy a rendszerek még inkább integrálódnak a megújuló energiaforrásokkal. Például az okosotthon rendszerek képesek lehetnek arra, hogy összehangolják a háztartás energiafelhasználását a napelemek termelésével, vagy az energiatárolással.

Az intelligens rendszerek elősegíthetik az energiafogyasztás tudatosabb kezelését. Egyre elterjedtebb lehet az olyan megoldás, amely például a legolcsóbb vagy legkevésbé szennyező időszakokban indítja el a háztartási gépeket. Emellett a környezeti adatokra támaszkodva az okosrendszerek képesek lesznek úgy szabályozni a fűtést, hűtést vagy árnyékolást, hogy az a lehető legkisebb ökológiai lábnyommal járjon.

A fejlesztések célja, hogy az otthonok ne csak energiahatékonyak legyenek, hanem aktívan hozzájáruljanak a környezeti terhelés csökkentéséhez. A jövő okosotthona tehát nemcsak kényelmes és automatizált, hanem környezetbarát is lesz.

14. ábra: Fenntartható technológiák integrációja egy okosotthonban (forrás: jabil.com)

6. Okosotthonok társadalmi és gazdasági hatásai

Az okosotthon-technológiák elterjedése nemcsak az egyéni háztartások működését változtatja meg, hanem tágabb társadalmi és gazdasági hatásokkal is jár. Az ilyen rendszerek beépítése számos szempontból formálja az ingatlanpiacot, az energiafogyasztási mintákat, valamint a technológiai hozzáférés kérdését is.

15.ábra: Energiahatékonyság mint gazdasági tényező (forrás: unsplash.com)

6.1 Lakóépületek értékének növekedése

Az ingatlanok értékét több tényező befolyásolja, és az okosotthon-rendszerek egyre inkább ezek közé tartoznak. Egy modern, digitalizált otthon képes növelni az ingatlan piaci vonzerejét, különösen a fiatalabb korosztály és a technológia iránt nyitottabb vásárlók körében. Egy jól kiépített okosfűtés-rendszer, intelligens világítás, vagy akár egy központi automatizált vezérlő nagyobb kényelmet és energiahatékonyságot biztosít, ami az értékesítés vagy bérbeadás során előnyt jelenthet.

Emellett az energiahatékonyság közvetlen hatással van az ingatlan fenntartási költségeire. Ha egy épület kevesebb energiát használ, az alacsonyabb rezsiköltségeket jelenthet, amit a vevők hosszú távú megtakarításként értékelhetnek. A korszerű technológia tehát már nemcsak extraként jelenik meg, hanem egyre inkább alapelvárásként.

6.2 Szerep a városi energiafogyasztás csökkentésében [6]

A városi környezetben különösen nagy kihívást jelent a magas energiafogyasztás kezelése. Egyre több ország és város *(16. ábra)* fordul az okosmegoldások felé, hogy a fenntarthatóság irányába mozduljon el. Ha egyre több háztartás alkalmaz energiatakarékos, automatizált rendszereket, az hosszabb távon hozzájárulhat az általános fogyasztás mérsékléséhez.

Az olyan funkciók, mint az időjárás-érzékeny fűtésszabályozás vagy a mozgásérzékelő alapú világítás, jelentős energiamegtakarítást eredményezhetnek. Egy nagyváros esetén, ahol több ezer vagy százezer ilyen rendszer működik, a hatás már városi szinten is érzékelhető lehet. Ráadásul ezek az adatok visszacsatolhatók a városi energiahálózatokhoz, ami új lehetőségeket nyit az elosztás optimalizálására is.

16. ábra: Okos város (forrás: techaku.com)

6.3 Társadalmi rétegek közötti hozzáférési különbségek

Bár az okosotthonok fejlődése számos előnyt kínál, nem minden társadalmi réteg fér hozzá egyformán ezekhez a megoldásokhoz. A rendszerek kiépítése és fenntartása költségekkel jár, ami akadályt jelenthet az alacsonyabb jövedelmű háztartások számára. Egyes fejlettebb országokban már léteznek támogatási programok, amelyek célja, hogy a technológia ne csak a tehetősebbek számára legyen elérhető, de ezek nem mindenhol elérhetők.

Ezen kívül a digitális készségek szintje is fontos szempont. Az idősebb generációk vagy a kevésbé technológiai beállítottságú emberek számára a bonyolult rendszerek kezelése kihívást jelenthet, még akkor is, ha a hozzáférés anyagilag nem akadály. A fejlesztések során tehát figyelembe kell venni a használhatóságot is, nemcsak a funkcionalitást.

6.4 Munkahelyteremtés és új iparágak kialakulása

Az okosotthon-technológiák térnyerése nemcsak az egyéni háztartások energiahatékonyságát növeli, hanem új gazdasági lehetőségeket is teremt. A folyamatos fejlesztések és a technológiai igények bővülése hozzájárul új szakmák és iparágak megjelenéséhez. Ezek az új munkahelyek nemcsak a technológiai szektorban jelentenek bővülést, hanem közvetve az oktatásban, a szolgáltatóiparban és az építőiparban is.

Ezen felül az okosotthon-megoldások integrálásához szükséges képzések és tanúsítványok új oktatási formákat is életre hívnak, elősegítve a munkaerőpiac alkalmazkodóképességét és a digitális átállás gyorsítását.

Összegzés

Az okosotthonok fejlődése az utóbbi években jól mutatja, hogy a technológiai újítások hogyan illeszthetők be a mindennapi életbe úgy, hogy azok nemcsak kényelmet, hanem valós előnyöket is biztosítsanak. Az energiahatékonyságra és fenntarthatóságra való törekvés meghatározó szerepet kapott a fejlesztések irányában, és ez a tendencia várhatóan a jövőben is folytatódni fog.

Hozzájárulás az energiahatékonysághoz és fenntarthatósághoz

Az okos világítás, fűtés, hűtés, valamint az automatizált vezérlés lehetővé teszi az energiafelhasználás jelentős csökkentését anélkül, hogy a lakók kényelme csorbulna. A szenzorokkal és algoritmusokkal támogatott rendszerek képesek észlelni a felesleges fogyasztást, és automatikusan optimalizálni a működést. Emellett a megújuló energiaforrásokkal való integráció is egyre elérhetőbb, amivel tovább csökkenthető a környezetre gyakorolt hatás.

Az ilyen rendszerek elősegítik, hogy a háztartások ne csak fogyasztói, hanem részben termelői is legyenek az energiának. Ez különösen fontos abban a globális kontextusban, ahol az energiatudatosság, a fenntartható fejlődés és a környezet védelme kiemelt célként jelenik meg.

Jövőbeli kilátások

A technológiai fejlődés gyors üteme alapján várható, hogy az okosotthonok egyre elterjedtebbé válnak. Az eszközök ára fokozatosan csökken, a rendszerek egyre felhasználóbarátabbá válnak, és az új hálózati technológiák (például az 5G) további lehetőségeket teremtenek. Emellett az adatbiztonsági szabályozások fejlődése is hozzájárulhat ahhoz, hogy a felhasználók nagyobb bizalommal forduljanak az ilyen rendszerek felé.

Hosszú távon nemcsak az egyéni háztartásokban, hanem a társasházakban, közintézményekben és okosvárosok részeként is egyre több automatizált, energiatakarékos megoldás jelenhet meg. Az intelligens rendszerek összekapcsolása közművekkel, közlekedéssel és közösségi szolgáltatásokkal új dimenziókat nyithat meg a fenntartható urbanizáció területén is.

Összegzés és javaslatok

Az okosotthonok témája jól mutatja, hogyan lehet a technológiai fejlődést a környezeti és gazdasági szempontokkal összehangolni. A rendszerek fejlesztésének egyik legfontosabb iránya a még hatékonyabb energiahasználat, az egyszerűbb kezelhetőség és a fokozott adatbiztonság biztosítása. Ahhoz, hogy ezek a megoldások széles körben elterjedhessenek, továbbra is fontos marad a szabványosítás, a felhasználói oktatás és a megfizethetőség biztosítása.

A fenntarthatóbb jövő felé vezető úton az okosotthonok nem csupán technológiai újításként jelennek meg, hanem olyan eszközként is, amelyek hozzájárulnak egy energiahatékonyabb, környezetbarátabb életmód kialakításához.

Irodalomjegyzék

[1] Az okosotthonok szerepe a fenntarthatóságban "Okosotthon: megoldás az energiatakarékosság és a kényelem szolgálatában," *Prim Online*, https://hirek.prim.hu/cikk-proxy/152417/?noredir=1Prim Online+3Prim Online+3Prim Online+3

[2] 1.2 Energiahatékonysági kihívások a háztartásokban "Okosotthon trendek, amikre érdemes figyelni!," *Wavin Blog* https://blog.wavin.com/hu-hu/okosotthon-trendekblog.wavin.com+1Raketa+1

[3] 2.1 Okos világítás és termosztátok "Apple Homekit okos otthon bemutató," *Chameleon Smart Home* https://chameleon-smarthome.com/blog/cikk/az-apple-homekit-okosotthonos-rendszereChameleon Okosotthon+1Chameleon Okosotthon+1

[4] 2.2 Intelligens energiamenedzsment rendszerek "ABB okosotthon vezérlés a Jungfernsee tó partján emelt különleges passzívházban," *Magyar Nemzeti Napelem Szövetség* https://www.mnnsz.hu/abb-okosotthon-vezerles-a-jungfernsee-to-partjan-emelt-kulonleges-passzivhazban/Magyar Napelem Napkollektor Szövetség

[5] 3.1 Mesterséges intelligencia az okosotthonokban "S.A.R.A.H. – Mesterséges intelligencia az okosotthonokban," *Okosotthon Blog* https://okosotthonblog.hu/hirek/s-a-r-a-h-mesterseges-intelligencia-az-okosotthonokban/Okosotthon Blog

[6] 3.2 IoT eszközök és szenzorok "A Siemens az okos épületek vezető IoT platform szolgáltatója," *Prim Online*, https://hirek.prim.hu/cikk/2020/01/19/a_siemens_az_okos_epuletek_vezeto_iot_platform_szolgaltatojaPrim Online+2Prim Online+2Prim Online+2

[7] 4.1 Költségcsökkentés okosotthon technológiákkal "Költségcsökkentés épületautomatikával," *Elektro-Kamleithner Kft.*, https://www.elektro-kamleithner.hu/category/blog/page/2/elektro-kamleithner.hu+1E-Villamos+1

[8] 4.2 Energiamegtakarítási tippek és trükkök "Okosotthon, okos döntés?," *Prim Online* https://hirek.prim.hu/cikk-proxy/160507/?noredir=1Prim Online+3Prim Online+3Prim Online+3

[9] 5.1 Jövőbeli trendek és technológiák "8 okosotthon trend, amikre érdemes jövőre figyelni," *Raketa.hu* https://raketa.hu/8-okosotthon-trend-amikre-erdemes-jovore-figyelniRaketa+1blog.wavin.com+1

[10] 5.2 Környezeti hatások és fenntarthatóság "Az LG fenntartható jövője: környezetbarát okosotthon-eszközök," *LG Magyarország* https://www.lg.com/hu/lg-experience/inspiracio/kornyezetbarat-okosotthon-eszkozok/LG IT

[11] "Mi az okosotthon és mi nem az? (Okosotthon rendszerek fajtái, előnyei és egyéb tudnivalók)," *Smart Clinic*, https://smartclinic.hu/hu/blog/mi-okosotthon-es-mi-nem-az/

[12] ChatGPT ChatGPT

2.13. A digitális ikrek és a mesterséges intelligencia kapcsolata az iparban Kovács Ábel

IPAR 4.0 TECHNOLÓGIÁK

A digitális ikrek és a mesterséges intelligencia kapcsolata az iparban

Kovács Ábel

[redacted]

(GKNB_INTM087)

2024/2025/2

Abstract:

The advent of the fourth industrial revolution, commonly referred to as Industry 4.0, has brought about transformative changes in manufacturing and industrial processes worldwide. Central to this revolution is the integration of advanced digital technologies that enable smart, connected, and highly automated production systems. Among these technologies, digital twins have gained significant attention due to their ability to create precise virtual representations of physical assets, processes, or systems. These digital replicas allow for real-time monitoring, simulation, and optimization, providing manufacturers with unprecedented insight into the behavior and performance of their operations.

This thesis examines the fundamental principles of digital twin technology and its convergence with artificial intelligence (AI). By leveraging AI algorithms, digital twins can analyze vast volumes of sensor data to predict failures, optimize maintenance schedules, and improve operational efficiency. The research explores various architectures and implementation strategies for digital twins, highlighting their applications across different industrial domains such as automotive manufacturing and logistics. Case studies demonstrate how the use of digital twins combined with AI enhances production flexibility and supports sustainable manufacturing practices by minimizing waste and energy consumption.

Furthermore, the study addresses the challenges associated with adopting these technologies, including data security concerns, integration complexities, and the need for standardized frameworks. Despite these hurdles, the potential benefits of digital twins powered by AI are immense, promising to revolutionize the way industries manage and optimize their assets.

In conclusion, the integration of digital twins and artificial intelligence represents a critical step toward realizing the vision of fully connected, intelligent factories. This synergy not only drives increased productivity and cost savings but also fosters innovation and sustainability within industrial ecosystems. As industries continue to evolve, embracing these technologies will be essential for maintaining competitiveness and achieving long-term growth in the era of Industry 4.0.

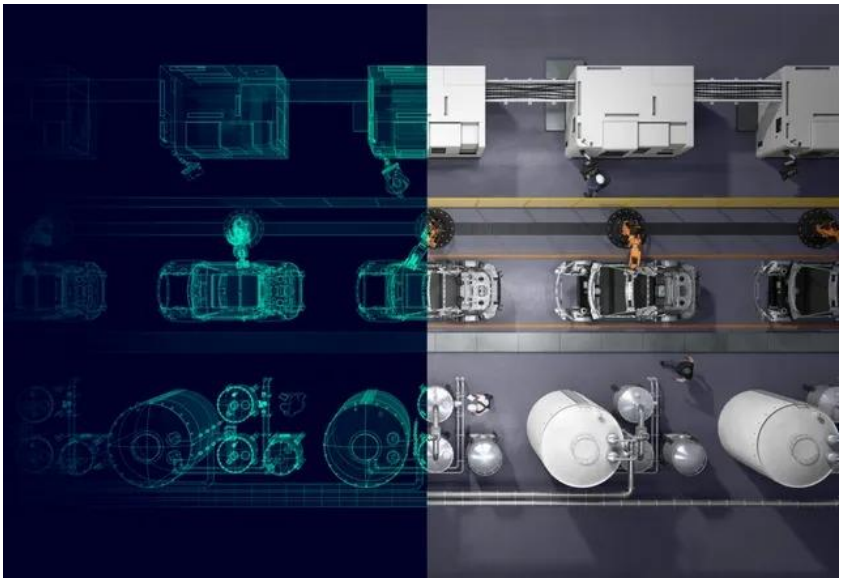
Tartalom

Abstract:.....2
Bevezetés:.....4
A digitális ikrek technológiájának alapjai:.....6
A mesterséges intelligencia ipari alkalmazása:.....9
A digitális ikrek és a mesterséges intelligencia integrációja:.....11
Előnyök és kihívások:.....14
Jövőbeli kilátások és összegzés:.....16
Irodalomjegyzék:.....19

Bevezetés:

Az ipari digitalizáció napjaink egyik legdinamikusabban fejlődő területe, mely alapjaiban formálja át a gyártási folyamatokat és a termelési rendszereket. A digitális ikrek és a mesterséges intelligencia (MI) kombinációja lehetővé teszi, hogy a fizikai rendszerek digitális másolatai valós időben leképezzék és előre jelezzék a működést, ezzel új lehetőségeket nyitva meg a hatékonyság, rugalmasság és fenntarthatóság terén. Ez az írás ennek az összetett technológiai világnak a megértésére vállalkozik, részletezve a digitális ikrek és az MI ipari alkalmazásainak előnyeit, valamint a bevezetésükhöz kötődő kihívásokat.

A digitális ikrek olyan virtuális modellek, amelyek nem csupán leképezik a fizikai rendszerek aktuális állapotát, hanem képesek azok jövőbeni viselkedésének előrejelzésére is. Ez a képesség alapvető szerepet játszik a prediktív karbantartásban és a gyártási folyamatok optimalizálásában, hozzájárulva ahhoz, hogy a vállalatok hatékonyabban használják ki erőforrásaikat és csökkentsék a költségeket [1], [2]. Az MI további értéket teremt azzal, hogy nagy adathalmazokból képes mintázatokat felismerni, összetett folyamatokat modellezni, és intelligens döntéstámogatást nyújtani, ami elengedhetetlen a modern okos gyárak működéséhez [3].



1. ábra: (Kép) A digitális iker koncepcionális modellje

Az ipari szereplők körében a digitális ikrek és MI együttes alkalmazása egyre inkább megszokottá válik, ami az autóipar, az elektronikai gyártás és az energetikai szektor számára

egyaránt lehetőségeket kínál a termelékenység növelésére, a minőség javítására és a termékfejlesztési ciklusok lerövidítésére [4], [5]. Ugyanakkor a technológia terjedése során számos kérdés és probléma is felmerül, mint például az adatvédelem és -biztonság, a rendszerek összehangolásának bonyolultsága, valamint a magas beruházási költségek [6].

Ebben az írásban az olvasó részletes képet kap arról, hogy a digitális ikrek és az MI miként járulnak hozzá az ipari termelés megújításához, milyen előnyöket hoznak, és milyen akadályokkal kell megküzdeniük azoknak, akik e technológiák bevezetése mellett döntenek. Külön figyelmet kap az is, hogy a változó piaci és technológiai környezetben ezek az innovációk hogyan alakítják át az üzleti folyamatokat, és miként támogatják a fenntartható fejlődést.

A digitális ikrek jelentősége abban rejlik, hogy nem csupán leképezik a jelen állapotot, hanem aktív szereplőként elősegítik a rendszer jövőbeli működésének megértését és fejlesztését. Ez a képesség az MI által válik igazán hatékonnyá, amely intelligens elemzésekkel és előrejelzésekkel segíti a gyártási folyamatokat abban, hogy még pontosabban és gyorsabban reagáljanak a változásokra [1], [3]. Így a vállalatok nem csupán versenyképesebbé, hanem fenntarthatóbbá is válhatnak.

A következő fejezetek részletesen bemutatják a digitális ikrek és mesterséges intelligencia fogalmát, fejlődésének mérföldköveit, majd áttekintik az ipari alkalmazások aktuális helyzetét, különös tekintettel az előnyökre és a gyakorlati kihívásokra. A munka végén összegzésként fogalmazódnak meg a legfontosabb tanulságok és javaslatok a további fejlesztések és az ipari alkalmazások sikeres bevezetése érdekében.

Összességében ez az elemzés arra törekszik, hogy hozzájáruljon a digitális ikrek és az MI ipari szerepének mélyebb megértéséhez, valamint iránymutatást nyújtson azok számára, akik az ipar jövőjét formáló technológiák alkalmazását tervezik.

A digitális iker technológia alapjai:

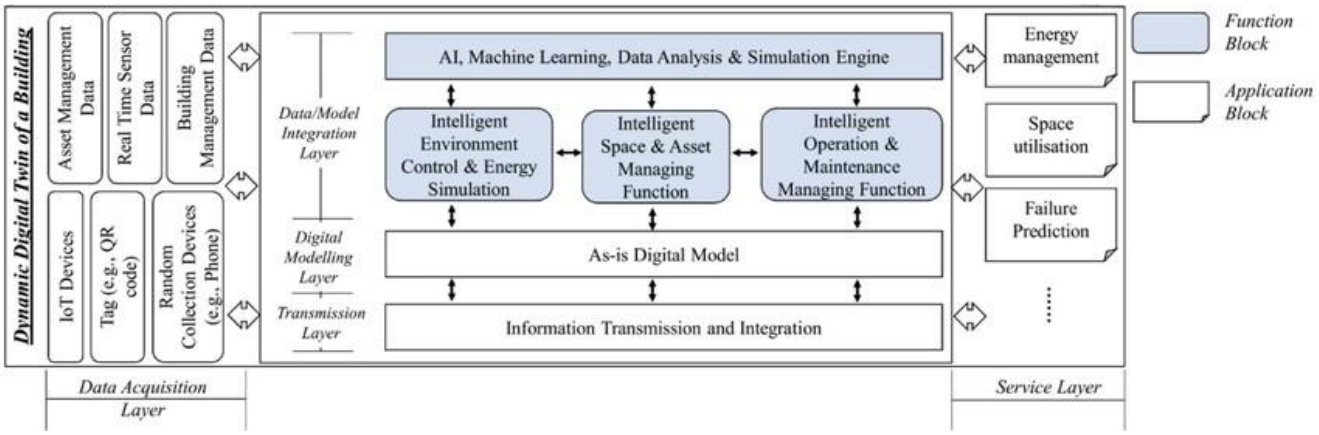
Az ipar digitális átalakulásának központi elemeivé váltak a digitális ikrek, melyek napjaink egyik leginnovatívabb technológiai megoldását képviselik. A digitális iker (digital twin) fogalma a fizikai rendszerek és azok virtuális megfelelőinek valós idejű, folyamatos szinkronizálásán alapul, lehetővé téve az ipari folyamatok pontosabb megértését, elemzését és optimalizálását. A

digitális iker technológia fejlődése szoros kapcsolatban áll az ipar 4.0 koncepciójával, amely az intelligens gyártási rendszerek megvalósítását célozza az információs és kommunikációs technológiák segítségével. [1]

A digitális iker lényegi eleme, hogy egy fizikai eszköz, gép vagy akár egész gyártósor digitális másolata jön létre, amely valós idejű adatokat kap a fizikai rendszer működéséről, állapotáról és környezetéről. Ezek az adatok leggyakrabban különféle szenzorokon keresztül érkeznek, melyek folyamatosan mérik a fizikai eszköz paramétereit, mint például hőmérséklet, rezgés, nyomás vagy energiafogyasztás. A digitális iker ezeket az adatokat feldolgozza, szimulációs és elemzési eszközökkel kombinálva, lehetővé téve a rendszer viselkedésének megértését és előrejelzését.

A digitális iker technológia három alapvető komponensből áll:

- A fizikai rendszer: Ez a valós eszköz vagy folyamat, amelyet digitálisan leképezünk. Lehet egy gép, berendezés, gyártósor vagy akár egy egész üzem.
- A digitális modell: A fizikai rendszer virtuális másolata, amely reprezentálja annak szerkezetét, viselkedését és dinamikáját. Ez a modell tartalmazza a rendszer matematikai és fizikai jellemzőit, továbbá a digitális környezetben szimulációk futtatására is alkalmas.
- Az adatgyűjtési és kommunikációs infrastruktúra: Ez biztosítja az adatfolyam folyamatos áramlását a fizikai rendszertől a digitális iker felé. Ide tartoznak a szenzorok, hálózati eszközök és adatfeldolgozó rendszerek, amelyek valós időben továbbítják az információkat.



2. ábra: (Kép) Gyári digitális iker referenciaarchitektúra

A digitális ikrek működésének egyik alapvető eleme a valós idejű adatfeldolgozás, amely lehetővé teszi az ipari folyamatok monitorozását és elemzését. Az adatokat nem csupán gyűjtik, hanem előfeldolgozzák, tisztítják és integrálják a digitális modellbe, amely ennek alapján folyamatosan frissül és finomhangolódik. Ez az állandó visszacsatolási kör rendkívül értékes információkat biztosít a termelésről, lehetővé téve például a prediktív karbantartást, a termelékenység növelését, vagy akár a termékfejlesztés támogatását.

Az ipari alkalmazások széles skáláján használják a digitális ikreket. Az autóiparban például a járművek különböző alkatrészeinek digitális másolatai segítségével követik nyomon az alkatrészek állapotát, optimalizálják a gyártási folyamatokat, és előre jelzik a meghibásodásokat. A logisztikában a raktárak és szállítási rendszerek digitális ikrei hozzájárulnak az áruk mozgásának és tárolásának hatékonyabb menedzsmentjéhez.

A digitális iker megközelítés előnye, hogy csökkenti a fejlesztési és üzemeltetési költségeket, növeli a folyamatok rugalmasságát és megbízhatóságát, valamint javítja a termékek és szolgáltatások minőségét. Az ipari környezetben való alkalmazásának azonban vannak technikai és szervezeti kihívásai is. Az egyik legjelentősebb kihívás az adatok megfelelő kezelése, tárolása és elemzése, mivel a digitális ikrek hatékonysága nagyban függ a minőségi és mennyiségi adatbevitel biztosításától. Ezen túlmenően a digitális modellek fejlesztése és karbantartása összetett feladat, amely komoly szakértelmet igényel.

A digitális iker modellezés során gyakran alkalmaznak különböző szimulációs technikákat, mint például fizikai alapú modellezést, adatvezérelt modelleket vagy ezek kombinációját. A fizikai alapú modellezés a rendszer ismert fizikai törvényein alapul, míg az adatvezérelt megközelítés statisztikai vagy gépi tanulási algoritmusokat használ az adatokból történő mintázatok felismerésére. Az ipari gyakorlatban a két megközelítés kombinációja egyre elterjedtebb, mivel így egyaránt kihasználható a fizikai ismeretek és az adatalapú predikciók előnye.

Az adatgyűjtés szempontjából fontos a szenzorok megbízhatósága, pontossága és a hálózati infrastruktúra stabilitása. A digitális ikrek számára kritikus, hogy a valós idejű adatáramlás zavartalan legyen, különösen olyan alkalmazásoknál, ahol azonnali beavatkozásra van szükség, például gyártósorok hibáinak felismerésekor vagy vészhelyzetek kezelésénél.

A digitális ikrek további előnye, hogy támogatják az iteratív fejlesztést és a termék-életciklus menedzsmentet (PLM). A digitális modell segítségével tesztelhetőek új megoldások, optimalizálható a termelés, és könnyebben integrálhatók az innovációk. Ezáltal a gyártók gyorsabban reagálhatnak a piaci változásokra és vevői igényekre.

Az ipari digitalizáció előrehaladtával a digitális ikrek egyre komplexebb rendszerek leképezésére is képesek, ideértve az ember-gép interakciókat, a gyártási folyamatok környezeti hatásait vagy az ellátási láncok dinamikáját. Ezek az integrált modellek hozzájárulnak a fenntartható és környezettudatos ipari működés megvalósításához, ami a globális klímaváltozás elleni küzdelemben is jelentős szerepet játszik.

Összefoglalva, a digitális iker technológia az ipar digitális átalakulásának egyik kulcseleme, amely lehetővé teszi a fizikai rendszerek valós idejű, pontos és komplex digitális leképezését. Ezáltal támogatja a döntéshozatalt, a folyamatok optimalizálását és az innovációt. Az előrelépés azonban nem mentes a kihívásoktól, amelyek között az adatkezelés, a modellfejlesztés és a megbízható infrastruktúra kiépítése a legfontosabbak. A digitális ikrek alkalmazása így az ipar jövőjének alapját képezi, különösen a mesterséges intelligenciával való integráció által, amely további lehetőségeket nyit meg az intelligens és önállóan működő rendszerek kialakításában. [2]

Mesterséges intelligencia az iparban:

A mesterséges intelligencia (MI) napjaink egyik legjelentősebb technológiai újítása, amely alapvetően átalakítja az ipari folyamatokat. Az MI lehetővé teszi az adatok gyors és hatékony feldolgozását, támogatja a döntéshozatalt, valamint segíti a termelési rendszerek optimalizálását. Az ipari alkalmazások széles skáláján jelen van, beleértve a gépi tanulást, a mélytanulást és a prediktív elemzést, amelyek együttesen hozzájárulnak a gyártási folyamatok automatizálásához és fejlődéséhez. [1]

A gépi tanulás az MI egyik kulcsterülete, amely algoritmusok segítségével tanítja meg a számítógépeket adatokból minták felismerésére és következtetések levonására anélkül, hogy explicit programozásra lenne szükség. A mélytanulás, amely a gépi tanulás speciális ága, mély neurális hálózatokat alkalmaz komplex problémák megoldására, például kép- vagy hangfelismerésben, illetve prediktív karbantartásban.

Az ipari környezetben az MI számos előnnyel jár. Elősegíti a prediktív karbantartást, amely lehetővé teszi a berendezések meghibásodásának előrejelzését és így a termelés zavartalanságának fenntartását. Az ellátási lánc menedzsmentjében a mesterséges intelligencia képes optimalizálni a készletezést, előrejelezni a keresletet, valamint javítani a logisztikai folyamatokat, ezáltal csökkentve a költségeket és növelve a hatékonyságot. Ezen felül az MI alkalmazható robotikában, ahol az intelligens gépek képesek önállóan alkalmazkodni a változó környezethez, így javítva a termelékenységet és a munkabiztonságot.

3. ábra: (Kép) A mesterséges intelligencia alkalmazásának áttekintése a gyártásban

Az adatok minősége és rendelkezésre állása kritikus tényező az MI sikeres alkalmazásához. Az ipari környezetben gyakran előfordul, hogy a szenzoradatok zajosak, hiányosak vagy inkonzisztensek, ami megnehezíti az algoritmusok pontos működését. Ezen túlmenően az adatok biztonsága kiemelten fontos, mivel az ipari rendszerek egyre inkább kiberfenyegetéseknek vannak kitéve. Az MI modellek fejlesztése során az is kihívást jelent, hogy az algoritmusok működésének átláthatósága és magyarázhatósága javuljon, különösen a kritikus ipari alkalmazások esetében. [2]

A mesterséges intelligencia jelentős mértékben hozzájárul az ipar digitalizációjához és automatizálásához. Az ipari környezetekben alkalmazott MI rendszerek fejlődése tovább erősíti

a termelékenységet, csökkenti a költségeket, és elősegíti a fenntarthatóbb gyártási megoldások kialakítását.

Digitális ikrek és mesterséges intelligencia együttműködése:

Az ipar 4.0 korszakában a digitális ikrek és a mesterséges intelligencia (AI) integrációja egyre inkább meghatározó szerepet tölt be az ipari folyamatok optimalizálásában. A digitális ikrek egy valós idejű digitális másolatot jelentenek egy fizikai rendszer vagy eszköz állapotáról, amely folyamatos adatgyűjtés és -feldolgozás segítségével pontosan leképezi a valóságot. Az AI ezen adatok elemzésével, modellezésével és előrejelzéseivel teszi lehetővé a folyamatok intelligens irányítását és optimalizálását. Ez a fejezet részletesen bemutatja, miként kapcsolódik össze a digitális iker technológia az AI-val, hogyan egészítik ki egymást, valamint milyen ipari alkalmazásokban és milyen előnyökkel használják a kettő kombinációját.

A digitális ikrek és az AI közötti együttműködés elsődleges alapja az adat. A digitális iker a fizikai rendszerből valós időben gyűjti az adatokat, melyek lehetnek szenzorok által mért paraméterek (például hőmérséklet, rezgés, nyomás), működési állapotok, vagy akár környezeti tényezők. Ezek az adatok egy központi adatfeldolgozó rendszerbe kerülnek, ahol az AI különféle algoritmusok segítségével elemzi és értékeli az információkat. A mesterséges intelligencia feladata nem csupán az adatok feldolgozása, hanem a tanulás is, amelynek során az AI folyamatosan finomítja modelljeit, előrejelzéseit, és képes alkalmazkodni a változó körülményekhez.

Az AI által nyújtott elemzések és predikciók alapján a digitális iker nem csak passzív tükörképe a valós rendszernek, hanem aktív résztvevője lehet a folyamatok irányításának. Például prediktív karbantartási algoritmusok képesek előre jelezni a berendezések meghibásodását, így a karbantartást még a hiba bekövetkezése előtt el lehet végezni, ami jelentős költségmegtakarítást és termelékenységnövekedést eredményez. Ugyanígy az AI optimalizálhatja a gyártási folyamatokat, csökkentheti az energiafogyasztást, vagy javíthatja a termék minőségét azáltal, hogy valós idejű visszacsatolással támogatja a döntéshozatalt. [1]

Az integráció kulcsa a rendszer architektúrájában rejlik, ahol a digitális iker platformjai és az AI komponensei egymásra épülnek. A digitális iker egy több rétegű architektúrán alapul, amely magában foglalja a fizikai réteget (a valós eszközök és szenzorok), a digitális modellt, az adatfeldolgozási réteget és az alkalmazási réteget, ahol az AI algoritmusok működnek. Az AI ezen architektúra tetején helyezkedik el, és közvetlenül kapcsolódik a digitális ikerhez, hogy az adatokat valós időben elemezze, és intelligens döntéseket generáljon.

4. ábra: (Kép) A digitális iker és a mesterséges intelligencia integrációjának keretrendszere

Az ipari alkalmazások között kiemelt helyen szerepel az autóipar, ahol a digitális ikrek az autók fizikai komponenseinek, például a motor vagy a fékrendszer valós idejű digitális másolataként szolgálnak. Az AI ezeken az adatokon alapulva képes előre jelezni a komponensek állapotát, optimalizálni a jármű teljesítményét és biztonságát. A logisztikában a digitális ikrek segítenek a raktárkészletek, szállítási útvonalak és gépjárművek állapotának valós idejű monitorozásában, míg az AI elemzései javítják az ellátási lánc hatékonyságát és rugalmasságát. [2]

Egy másik fontos iparág az energiaipar, ahol a digitális ikrek és az AI együttműködése lehetővé teszi a hálózati rendszerek optimalizálását, a megújuló energiaforrások integrálását és a fogyasztás előrejelzését. Itt különösen fontos az AI képessége, hogy kezelje az adatforgalom nagy volumenét és a rendszerek komplexitását, biztosítva a megbízható és hatékony működést.

Az együttműködés során számos technológiai és szervezeti kihívással kell szembenézni. Az egyik legnagyobb probléma az adatbiztonság és az adatvédelem kérdése, hiszen a digitális ikrek hatalmas mennyiségű érzékeny adatot kezelnek, amelyeket meg kell védeni a jogosulatlan hozzáféréstől. Emellett a megfelelő adatinfrastruktúra kialakítása – beleértve a nagysebességű adatátviteli hálózatokat, adatfeldolgozó központokat és megbízható szenzorokat – alapvető követelmény a rendszerek működéséhez.

Az AI modellek tanítása és validálása is jelentős kihívást jelent. A modellek hatékonysága nagyban függ a bemeneti adatok minőségétől és mennyiségétől, valamint az alkalmazott algoritmusok típusától. Az ipari környezetben gyakran előfordulhatnak zajos, hiányos vagy torzított adatok, amelyek megnehezítik a pontos előrejelzéseket. Ezért elengedhetetlen a megfelelő adat-előkészítés, a hibakezelés és a folyamatos modellfrissítés.

Az integrált digitális iker és AI rendszerek hatékony működésének előfeltétele a szabványosítás és az interoperabilitás. Mivel az ipari környezetben számos különböző gyártó és technológia működik, a rendszereknek képesnek kell lenniük együttműködni egymással. Ez lehetővé teszi, hogy a digitális ikrek különböző eszközökre és folyamatokra kiterjedjenek, az AI pedig globális szinten optimalizálja a teljes ipari láncot. [3]

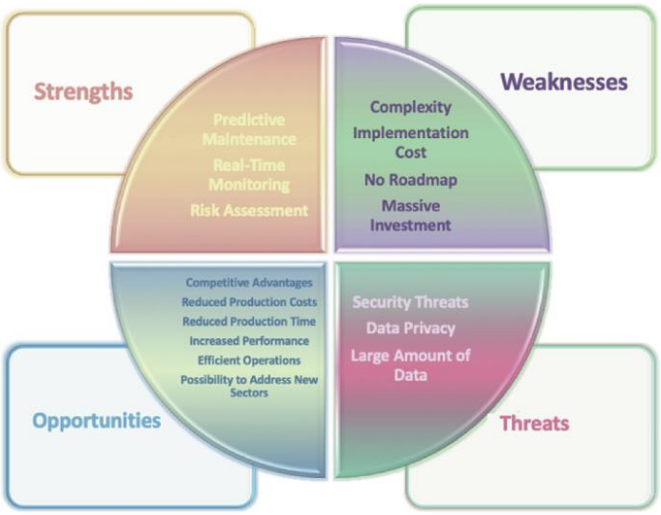
Az együttműködés hatására az iparban megvalósul a prediktív karbantartás, a valós idejű folyamatoptimalizálás és a termékfejlesztés gyorsítása, amelyek mind hozzájárulnak a versenyképesség növeléséhez. A digitális ikrek által biztosított valós idejű adatok és az AI elemzései révén a gyártók képesek proaktívan reagálni a piaci változásokra, csökkenteni a selejtet, és rugalmasabb termelési rendszereket kialakítani.

A digitális ikrek és a mesterséges intelligencia együttműködése az iparban forradalmi változásokat hoz, lehetővé téve a valós idejű adatfeldolgozást, az intelligens döntéshozatalt és a folyamatok optimalizálását. Az integráció azonban nem mentes a kihívásoktól, amelyek megoldása nélkülözhetetlen a technológia teljes potenciáljának kiaknázásához. A jövőbeni

fejlesztések ezen a területen várhatóan tovább erősítik majd az együttműködést, új lehetőségeket nyitva az ipari digitalizációban.

Előnyök és kihívások:

A digitális ikrek és a mesterséges intelligencia (MI) együttes alkalmazása az iparban jelentős előnyöket kínál, ugyanakkor számos kihívással is szembesülnek a vállalatok a technológiák bevezetése és működtetése során. A legfontosabb előny a termelési folyamatok hatékonyságának növelése, amelynek alapja a valós idejű adatokon alapuló szimuláció és optimalizáció. A digitális ikrek lehetővé teszik a gyártási folyamatok pontos leképezését, ezáltal minimalizálható a selejt, csökkenthetőek a leállások, és javítható az erőforrások kihasználtsága. Az MI alkalmazásával előre jelezhetővé válik a gépek meghibásodása, így a prediktív karbantartás révén csökkennek a váratlan leállások és a karbantartási költségek. Ezzel a kombinációval a termelékenység jelentősen növelhető, miközben a működési költségek mérsékelhetők [1].



5. ábra: (Kép) A digitális ikrek és a mesterséges intelligencia SWOT

A termékfejlesztés és -tesztelés területén is egyre fontosabb szerep jut a digitális ikreknek, mivel lehetővé teszik a prototípusok virtuális tesztelését és finomhangolását, így gyorsabbá téve a piacra jutást. Ez a rugalmasság versenyelőnyt jelent az ipari szereplők számára, hiszen lehetőség nyílik a piac igényeinek gyorsabb és pontosabb kielégítésére, valamint a termékek minőségének folyamatos javítására.

A fenntarthatósági szempontok is jelentős hangsúlyt kapnak a digitális ikrek és MI alkalmazása kapcsán. Az energiafelhasználás és az anyagveszteség csökkentése, valamint a hulladék minimalizálása révén hozzájárulnak a környezetkímélő gyártáshoz [2]. A valós idejű adatelemzések segítségével pontosabban megérthetők a rendszerek működési folyamatai, ami támogatja a fenntarthatóbb és hosszabb távon is működőképes gyártási megoldások kialakítását. Ezen túlmenően az ellátási láncok átláthatósága és rugalmassága javul a digitális ikrek és MI integrált alkalmazásával, így a vállalatok gyorsabban és hatékonyabban tudnak reagálni a kereslet és kínálat változásaira, valamint a logisztikai kihívásokra.

Ugyanakkor a technológiák alkalmazása számos nehézséget is magában rejt. Az egyik legnagyobb kihívás a megfelelő mennyiségű és minőségű adat beszerzése és kezelése. Az ipari környezetből származó szenzoradatok gyakran zajosak, hiányosak vagy rendszertelenek, ami megnehezíti a pontos digitális iker modellek felépítését és az MI algoritmusok megbízható működését [3]. Az adatok előfeldolgozása, tisztítása és validálása nélkülözhetetlen, de idő- és erőforrásigényes feladat.

Az adatinfrastruktúra fejlesztése szintén komoly kihívást jelent. A folyamatos adatgyűjtés és -feldolgozás miatt szükség van megbízható hálózatokra, skálázható adattárolási megoldásokra és megfelelő adatbiztonsági intézkedésekre, amelyek biztosítják a rendszerek zavartalan működését és az érzékeny információk védelmét. Az adatvédelmi és iparbiztonsági követelmények szigorú betartása elengedhetetlen a technológiák elfogadásához és elterjedéséhez [4].

A mesterséges intelligencia alkalmazásakor gyakran problémát jelent az algoritmusok átláthatósága és magyarázhatósága, különösen olyan kritikus ipari folyamatokban, ahol a döntések következményei jelentősek lehetnek. A „fekete doboz” jelenség, amely az MI működésének belső mechanizmusainak nehéz megértését jelenti, korlátozhatja a technológia széleskörű alkalmazását, mivel a szakértők és döntéshozók számára fontos az eredmények megbízhatósága és értelmezhetősége [5].

Az emberi tényező sem elhanyagolható szempont. A digitális ikrek és MI bevezetése átalakítja a munkafolyamatokat, ami a dolgozók részéről alkalmazkodóképességet és folyamatos képzést igényel. A munkaerő motiválása és bevonása kulcsfontosságú a sikeres integráció érdekében, különösen azért, mert a technológiák sokszor új szakértelmet és szemléletmódot követelnek meg.

Végezetül, a technológiák bevezetése jelentős anyagi befektetést igényel, amely magában foglalja a hardverbeszerzést, szoftverfejlesztést, rendszerintegrációt és az alkalmazottak képzését. A beruházások megtérülése hosszú távon várható, ezért a gazdasági és műszaki kockázatok alapos elemzése, valamint a projektek gondos tervezése és menedzselése elengedhetetlen.

A digitális ikrek és mesterséges intelligencia együttes alkalmazása jelentős versenyelőnyt biztosít az ipari vállalatok számára, miközben hozzájárul a fenntarthatóbb, rugalmasabb és hatékonyabb gyártási folyamatok kialakításához. A siker kulcsa azonban a technológiai, adatkezelési és emberi kihívások együttes kezelése, amelyek nélkülözhetetlenek a hosszú távú fejlődés és innováció megvalósításához.

Jövőbeli kilátások:

Az ipari digitalizáció és a mesterséges intelligencia folyamatos fejlődése egyre nagyobb hatással van a gyártási folyamatok és rendszerek működésére. A digitális ikrek és az AI kombinációja új lehetőségeket teremt a hatékonyság, rugalmasság és fenntarthatóság javítására. A jövőbeni kilátások e technológiák továbbfejlesztésében és integrációjában rejlenek, amelyek révén az ipar egyre inkább önállóan működő, adaptív rendszerekké válhat [1].

6. ábra: (Kép) A digitális ikrek jövője

A digitális ikrek fejlődése várhatóan szorosabb kapcsolatba kerül a mesterséges intelligencia különböző ágaival, különösen a gépi tanulással és a prediktív analitikával. Ez lehetővé teszi, hogy a digitális másolatok ne csak passzív adatgyűjtők legyenek, hanem aktív szereplőkké váljanak a döntéshozatalban és a folyamatok optimalizálásában. Például a gépi tanuló algoritmusok képesek lesznek az eszközök állapotának folyamatos elemzésére, az anomáliák azonnali felismerésére és az önjavító mechanizmusok beindítására [2].

Az ipar 4.0 trendjeinek folytatásaként a digitális ikrek és az AI integrációja elősegítheti a gyártás teljes körű automatizálását, amelyben a gépek önállóan alkalmazkodnak a változó környezethez, minimalizálják a hibákat, és optimalizálják az energiafelhasználást [3]. Ezzel párhuzamosan nő az igény a fenntartható és környezetbarát technológiák iránt, melyekben a digitális ikrek segíthetnek az erőforrások hatékonyabb kihasználásában és a hulladék csökkentésében [4].

Azonban a jövőbeni fejlesztések nem csupán technológiai kihívásokat jelentenek, hanem etikai és jogi kérdéseket is felvetnek. Az adatbiztonság és az adatvédelem kiemelten fontos, különösen a nagy mennyiségű, valós idejű adat kezelésénél. A mesterséges intelligencia döntéseinek átláthatósága és magyarázhatósága szintén alapvető fontosságú a megbízhatóság és a felhasználói bizalom szempontjából [5].

Összegzésképpen, a digitális ikrek és az AI együttműködése az iparban nem csupán a jelenlegi folyamatok hatékonyságát növeli, hanem alapvetően átalakítja a gyártás és karbantartás módszereit. A fejlődés iránya a még inkább automatizált, adaptív és fenntartható ipari rendszerek felé mutat, amelyek hosszú távon jelentős gazdasági és környezeti előnyöket kínálnak. A jövőben a technológiák fejlesztése és alkalmazása során a multidiszciplináris megközelítés és a megfelelő szabályozási keretek kialakítása lesz kulcsfontosságú a sikeres integrációhoz és a társadalmi elfogadáshoz.

Források:

[1] ScienceDirect – Digital Twins in Industry 4.0 – Opportunities and Challenges
(https://www.sciencedirect.com)

[2] AI-Driven Predictive Maintenance for Smart Manufacturing Systems Using Digital Twin Technology
(https://www.ijcesen.com)

[3] ScienceDirect – Digital Twin: Benefits, Use Cases, Challenges, and Opportunities
(https://www.sciencedirect.com)

[4] How AI and robotics can help prevent breakdowns in factories - and save manufacturers big bucks
(https://www.businessinsider.com)

[5] Simulating with AI and digital twins for a secure and resilient future
(https://www.theaustralian.com.au)

[6] 9 advantages and disadvantages of digital twin technology*
(https://www.techtarget.com)

[7] Revolutionizing Predictive Maintenance with Digital Twins and AI
(https://smartshape.com)

[8] A Comprehensive Review of AI-Based Digital Twin Applications in Manufacturing
(https://www.mdpi.com)

[9] Digital Twins and the Power of Predictive Maintenance
(https://www.zuken.com)

[10] 6 Ways of Boosting ROI Using Digital Twin Technology
(https://twinsights.co)

[11] Digital Twins' Could Revolutionize Planes, Cars and Hearts The Wall Street Journal
(https://www.wsj.com)

[12] How Digital Twins Are Transforming Manufacturing, Medicine and More
(https://time.com)

[13] Will a Treatment Work? Try the 'Digital Twin' First.The Wall Street Journal Podcast, 2024
https://www.wsj.com)

[14] AI and the R&D revolution
(https://www.ft.com)

[15] How to address the challenges of AI-driven digital twins
(https://www.techtarget.com)

2.14. Szövegszerkesztési Sablon az Ipar 4.0 Technológiák című Tárgyhoz Okosvárosok energiafelhasználása, a sablon az ACM megfelelő sablonján alapul

Szövegszerkesztési Sablon az Ipar 4.0 Technológiák című Tárgyhoz

Okosvárosok energiafelhasználása, a sablon az ACM megfelelő sablonján alapul

Gosztola Gábor Donát

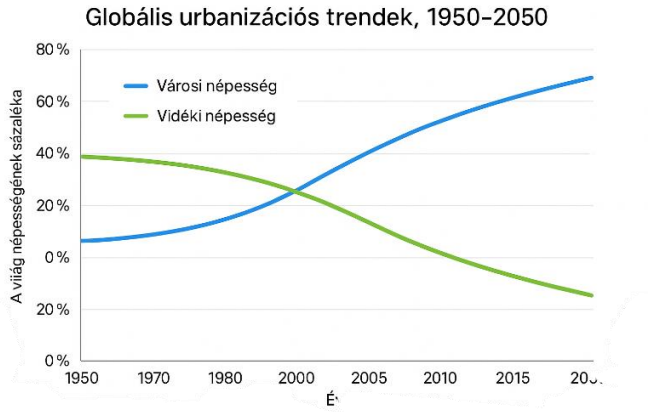
mechatronikai mérnök, gosztola9@gmail.com

A városiasodás globális tendenciája az utóbbi évtizedekben példátlan mértéket öltött, amely jelentős kihívások elé állítja az energiaellátást, a környezeti fenntarthatóságot és a városi életminőséget. A smart city koncepció egy integrált megközelítést kínál ezen problémák kezelésére, ötvözve a digitális technológiákat, a társadalmi részvételt és az okos energiamenedzsmentet. A házi feladat célja a smart cityk elméleti hátterének, dimenzióinak és technológiai pilléreinek bemutatása, különös tekintettel az energiahatékonyságot és megújuló energiaforrásokat támogató megoldásokra.Kiemelt figyelmet kapnak az IoT-alapú rendszerek, az okosmérők, valamint a felhasználói oldalra helyezett energiairányítási stratégiák. Az elemzés alapját esettanulmányok, szakirodalmi áttekintés és nemzetközi jó gyakorlatok képezik. A városi fenntarthatóság kulcsa nem csupán a technológiai innováció, hanem a rendszerszintű szemléletmód és az intézményi együttműködés erősítése.

Kulcsszavak: okosváros, energia, energiafelhasználás

1 BEVEZETÉS

A 21. század gyors urbanizációs folyamatai új kihívások elé állítják a világ városait, amelyeknek egyre nagyobb népességet kell fenntartható módon ellátniuk energiaforrásokkal, közlekedéssel, vízzel, hulladékkezeléssel és más alapvető szolgáltatásokkal. Az ENSZ előrejelzése szerint 2050-re a világ népességének több mint 68%-a városi környezetben fog élni [1]. Ez a tendencia szükségessé teszi a városi rendszerek hatékonyabbá, fenntarthatóbbá és intelligensebbé tételét.



1. ábra: Urbanizációs trendek, 1950-2050 között (saját szerkesztás, forrás: United Nations (2018))

E problémák kezelésére jött létre az okosváros koncepciója, amely az infokommunikációs technológiák (ICT – Information and Communication Technologies), a közlekedési infrastruktúra, az energiaellátás, a hulladékgazdálkodás és az épített környezet szoros integrációján alapul. Az okosváros célja, hogy technológiai megoldásokkal javítsa a városi életminőséget, növelje a szolgáltatások hatékonyságát, és csökkentse a környezeti terhelést [2].

Az egyik legfontosabb terület az okosvárosok fejlesztésében az intelligens energiagazdálkodás, amely kulcsszerepet játszik abban, hogy a városok energiafogyasztása optimalizálhatóvá váljon, miközben a környezeti terhelés és az üvegházhatású gázok kibocsátása csökken. Mindez különösen fontossá válik a globális klímaváltozás és az energiaforrások szűkössége miatt, amelyek egyre nagyobb nyomást gyakorolnak a jelenlegi városi rendszerekre.

Az okos energiagazdálkodás átfogó fogalom, amely magában foglalja a modern technológiák – mint például az okos hálózatok az Internet of Things (IoT), a big data elemzés, valamint a mesterséges intelligencia alkalmazását annak érdekében, hogy az energiatermelés, -elosztás és -felhasználás hatékonyabbá és fenntarthatóbbá váljon [3].

A megújuló energiaforrások (pl. napenergia, szélenergia, geotermikus energia) integrálása az energiarendszerekbe szintén az intelligens megközelítés részét képezi. Mivel ezek az energiaforrások időjárásfüggők és kiszámíthatatlanabbak, új megoldásokra van szükség az energiatárolás, elosztás és felhasználás koordinálására. Az energiahatékonyság növelése nem csupán környezetvédelmi szempontból indokolt, hanem gazdaságilag is megtérülő befektetés, különösen hosszú távon.

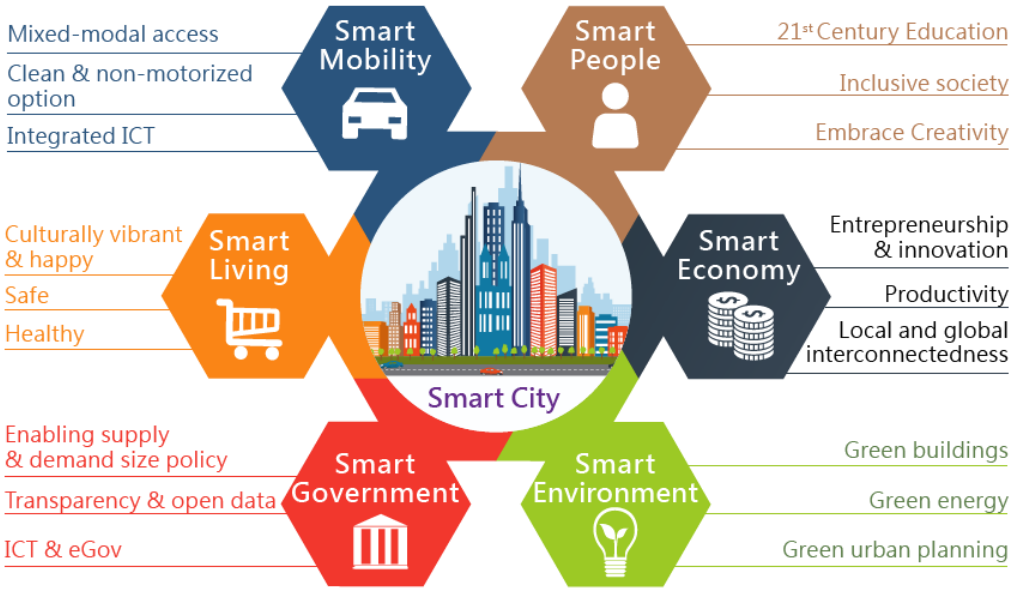
A házi feladat célja, hogy átfogó képet nyújtson az okos energiagazdálkodás helyéről és szerepéről az okosvárosok fejlődésében. A házi feladat három fő célkitűzése a következő:

- Bemutatni a jelenlegi energiatermelési és -felhasználási gyakorlatokat az okosvárosok kontextusában, különös tekintettel a kihívásokra.
- Részletesen elemezni azokat az okos technológiákat, amelyek elősegítik a fenntartható energiagazdálkodást
- Valós példák és statisztikai adatok segítségével bemutatni olyan városokat, amelyek már sikeresen alkalmazzák ezeket a megoldásokat.

Az okos energiagazdálkodás nemcsak környezeti és gazdasági szempontból jelentős, hanem stratégiai fontosságú is: városaink jövőjének egyik kulcsa, hogy képesek vagyunk-e olyan rendszereket kialakítani, amelyek képesek alkalmazkodni a gyorsan változó környezeti és technológiai feltételekhez. A digitalizáció, a decentralizált energiatermelés, valamint az adatvezérelt döntéshozatal nem lehetőség, hanem elkerülhetetlen lépés egy fenntarthatóbb és élhetőbb jövő felé.

2 AZ OKOSVÁROS KONCEPCIÓJA

Az „okosváros” (smart city) fogalma nem csupán technológiai újításokat jelent, hanem egy komplex, multidiszciplináris megközelítést is, amely az urbanisztika, a környezetvédelem, az információs technológia és a társadalomtudományok határterületén helyezkedik el. Lényege, hogy a város működésének minden aspektusát – legyen szó közlekedésről, közművekről, egészségügyről, biztonságról vagy energiagazdálkodásról – a legmodernebb digitális technológiákkal támogassák és optimalizálják.



2. ábra: Okosváros felépítése, egységei
(https://smartcity.org.hk/images/aboutus/about_us_6pillars.png)

2.1 Fogalmi meghatározás

A szakirodalomban az okosváros definíciója eltérő lehet attól függően, hogy milyen szemszögből közelítjük meg a kérdést. A legtöbb meghatározásban közös, hogy az okosváros nemcsak technológiai, hanem társadalmi és környezeti célokat is szolgál. Egy átfogó definíció szerint:

„Az okosváros egy olyan városi térség, amely infokommunikációs technológiákat és adatvezérelt rendszereket alkalmaz az erőforrások hatékony kezelésére, az életminőség javítására és a fenntarthatóság előmozdítására.” [2]

Nam és Pardo [2] három fő dimenziót azonosítottak az okosváros fogalmában:

- Technológia: IKT-rendszerek, szenzorhálózatok, hálózati infrastruktúrák és mesterséges intelligencia.
- Emberi tényező: lakossági részvétel, digitális írástudás, oktatás, kreativitás.
- Intézményi háttér: kormányzati nyitottság, jogi szabályozás, szervezeti rugalmasság.
- Az okosvárosok tehát nem kizárólag technológiai fejlesztések összességeként értelmezhetők, hanem olyan integrált rendszerek hálózataként, ahol az ember, a technológia és az intézményi struktúrák egymással szoros kölcsönhatásban működnek.

Az okosvárosok tehát nem kizárólag technológiai fejlesztések összességeként értelmezhetők, hanem olyan integrált rendszerek hálózataként, ahol az ember, a technológia és az intézményi struktúrák egymással szoros kölcsönhatásban működnek.

2.2 Az okosváros kulcselemei

A smart city koncepció számos alrendszert foglal magában, amelyek együttműködésén múlik a városi környezet hatékonysága és élhetősége. A legfontosabb komponensek közé az alábbiak tartoznak:

- **Okos közlekedés:** integrált tömegközlekedés, közlekedési adatgyűjtés, forgalomoptimalizálás, elektromos járműtöltés.
- **Okos energia:** megújuló energiaforrások integrációja, okos hálózatok (smart grids), energiahatékonyság.
- **Okos környezet:**környezetfigyelő szenzorok, levegőminőség-mérés, zajszennyezés-monitoring.
- **Okos gazdaság:** digitális vállalkozásfejlesztés, e-kereskedelem, innováció ösztönzése.
- **Okos életminőség:** egészségügyi távfelügyelet, digitális oktatás, okos otthonok.
- **Okos kormányzás:** részvételi demokrácia, e-közigazgatás, átláthatóság.

Az Európai Unió Smart Cities Marketplace kezdeményezése szerint egy város akkor tekinthető okosnak, ha képes a technológiai innovációkat a polgárai javára fordítani, miközben gazdaságilag is fenntartható marad [4].

2.3 Technológiai alapok

Az okosvárosokat lehetővé tevő technológiák közé tartoznak:

IoT (Internet of Things): fizikai eszközök hálózatba kapcsolása és adatcseréje (pl. szenzorok, mérők).
Big Data és analitika: a nagy mennyiségű városi adat feldolgozása és értelmezése döntéstámogatás céljából.
Felhőalapú számítástechnika: skálázható háttérrendszerek az adattároláshoz és -feldolgozáshoz.
Mesterséges intelligencia: gépi tanulás, prediktív elemzés, adaptív rendszerek alkalmazása.
5G és kommunikációs protokollok: gyors, megbízható adatátvitel a városi rendszerek között.

Ezek az infrastruktúrák lehetővé teszik, hogy a város valós időben reagáljon a változó igényekre, előrejelezzék a problémákat, és automatizáltan optimalizálják az erőforrás-elosztást. Például egy AI-alapú közlekedésirányítási rendszer csökkentheti a dugókat, vagy egy IoT-szenzorokkal ellátott energiahálózat automatikusan szabályozhatja az energiaáramlást a fogyasztási szokások alapján.

3 ENERGIATERMELÉS ÉS -FELHASZNÁLÁS AZ OKOSVÁROSOKBAN

Az energiarendszerek kiemelt szerepet töltenek be az okosvárosok kialakításában, mivel közvetlen hatást gyakorolnak a környezetterhelésre, a gazdasági fenntarthatóságra és a város élhetőségi mutatóira. Az energiatermelés és -felhasználás optimalizálása lehetővé teszi az erőforrások hatékonyabb elosztását, csökkenti a károsanyag-kibocsátást, valamint támogatja a klímavédelmi célok elérését.

3.1 Energiahordozók típusai és jellemzőik

Az okosvárosi energiarendszerekben alkalmazott energiaforrásokat két fő csoportba sorolhatjuk: fosszilis és megújuló energiaforrások.

1. **Fosszilis energiaforrások**: A kőolaj, földgáz és szén alapú rendszerek ma is a világ energiaellátásának nagy részét képezik. Ezek az energiaforrások azonban nem megújulók, korlátozott mennyiségben állnak rendelkezésre, valamint jelentős szén-dioxid-kibocsátással jár a felhasználásuk [6].
2. **Megújuló energiaforrások**:

- **Napenergia**: Fotovoltaikus panelek révén történő villamosenergia-termelés.
- **Szélenergia**: Szélturbinák mechanikus energiája elektromos energiává alakítható.
- **Geotermikus energia**: A Föld belső hőenergiájának hasznosítása fűtésre vagy áramtermelésre.
- **Biomassza**: Szerves anyagból történő energianyerés.
- **Vízenergia**: A víz mozgási energiájának átalakítása elektromos energiává.

Ezen források előnye, hogy fenntarthatók és jellemzően alacsony üvegházhatásúgáz-kibocsátással járnak. Hátrányuk az időjárásfüggőség és a decentralizált termelésből adódó rendszerszintű kihívások [7].

3.2 A jelenlegi energiarendszerek kihívásai

A hagyományos, központosított energiarendszerek korlátozottan alkalmasak a modern okosvárosi működés igényeinek kielégítésére. Az alábbi problémák jellemzőek:

- **Erőforráshiány**: A fosszilis energiahordozók készletei kimerülőben vannak.
- **Elosztási veszteségek**: A központi termelésből eredő hosszú távvezetékek magas energiaátviteli veszteségeket okoznak.
- **Rugalmasság hiánya**: A hagyományos rendszerek nem képesek gyorsan reagálni a terhelésváltozásokra vagy a decentralizált megújuló források termelésingadozására.

3.3 Decentralizált energiatermelés szerepe

Az okosvárosi környezetben a decentralizált energiatermelés egyre nagyobb hangsúlyt kap. Ilyen például a háztartási méretű napelemes rendszerek, mikroszélgenerátorok, illetve közösségi energiaszövetkezetek alkalmazása. Ezek a rendszerek csökkentik a hálózati függőséget, valamint lehetővé teszik a fogyasztók számára, hogy „prosumer”-ként (termelő-fogyasztóként) részt vegyenek az energiarendszer működésében [9].

A decentralizált energiatermelés ugyanakkor olyan kihívásokkal jár, mint:

- Termelési ingadozások időjárásfüggés miatt
- Hálózati szinkronizálási problémák

- Energiatárolás szükségessége a csúcstermelés és -fogyasztás időeltolódása miatt

3.4 Jövőorientált energiagazdálkodás

A városok energiaigénye a jövőben tovább fog növekedni az urbanizációs trendek és az elektromobilitás elterjedése miatt. Az okosvárosok energiastratégiája ennek megfelelően olyan rendszereket igényel, amelyek képesek:

1. Valós idejű energiafelhasználási adatokat gyűjteni (pl. okosmérők alkalmazásával),
2. A keresletet és kínálatot dinamikusan összehangolni (pl. mesterséges intelligenciával támogatott predikció segítségével),
3. A megújuló energiaforrások változó teljesítményéhez rugalmasan alkalmazkodni (pl. energiatároló rendszerek révén).

Az alábbi táblázat az energiarendszerekkel szemben támasztott főbb elvárásokat és a rájuk adható technológiai válaszokat foglalja össze.

1. táblázat: Az energiarendszerek kihívásai és megoldásai az okosvárosokban.
Forrás: saját készítés [6], [8], [10] alapján

Kihívás	Technológiai válasz
Ingerlékeny kereslet	Demand Response rendszerek
Időjárásfüggő termelés	Akkumulátoros energiatárolás, Power-to-X
Elosztási veszteségek	Lokális termelés, mikrohálózatok
Terheléscsúcsok	Prediktív tervezés mesterséges intelligenciával
Átláthatóság hiánya	Smart Metering, valós idejű adatmonitoring

4 OKOS HÁLÓZATOK

Az okos hálózatok (smart grids) az energiaelosztás és -felhasználás új generációját képviselik, amelyek célja a hagyományos villamosenergia-hálózatok hatékonyságának, megbízhatóságának és rugalmasságának növelése. Az okos hálózat alapvető jellemzője az információtechnológiai rendszerek és az energiarendszerek szoros integrációja, amely lehetővé teszi a valós idejű adatgyűjtést, az automatikus irányítást és a dinamikus rendszeroptimalizálást.

4.1 A smart grid főbb jellemzői és komponensei

A smart grid architektúrája több rétegből áll, amelyek egymással szoros kapcsolatban működnek:

1. **Érzékelő- és mérőrendszerek** – pl. szenzorhálózatok, okosmérők (smart meters), amelyek folyamatosan monitorozzák a fogyasztást, feszültséget, frekvenciát és egyéb hálózati paramétereket.
2. **Kommunikációs infrastruktúra** – valós idejű adatátvitel biztosítása vezetékes vagy vezeték nélküli hálózatokon keresztül.
3. **Vezérlési és irányítási rendszerek** – prediktív algoritmusok, döntéstámogató rendszerek, amelyek optimalizálják a hálózati működést.
4. **Energiatárolási egységek és decentralizált energiaforrások** – képesek alkalmazkodni a keresleti és kínálati viszonyokhoz.

Ezek az elemek összehangoltan működnek, lehetővé téve a kétirányú energia- és információáramlást, ami a hagyományos rendszerekkel szemben jelentős előrelépést jelent [10].

4.2 Advanced Metering Infrastructure (AMI)

Az Advanced Metering Infrastructure (AMI) az egyik alapvető technológia a smart grid rendszerekben. Az AMI olyan rendszer, amely:

- **valós idejű adatgyűjtést végez** az energiafogyasztásról,
- lehetővé teszi a **távleolvasást** és a **távoli ki-/bekapcsolást**,
- alapot biztosít a **dinamikus árazáshoz** (pl. time-of-use tarifák),
- segíti a hálózati hibák gyors felismerését.

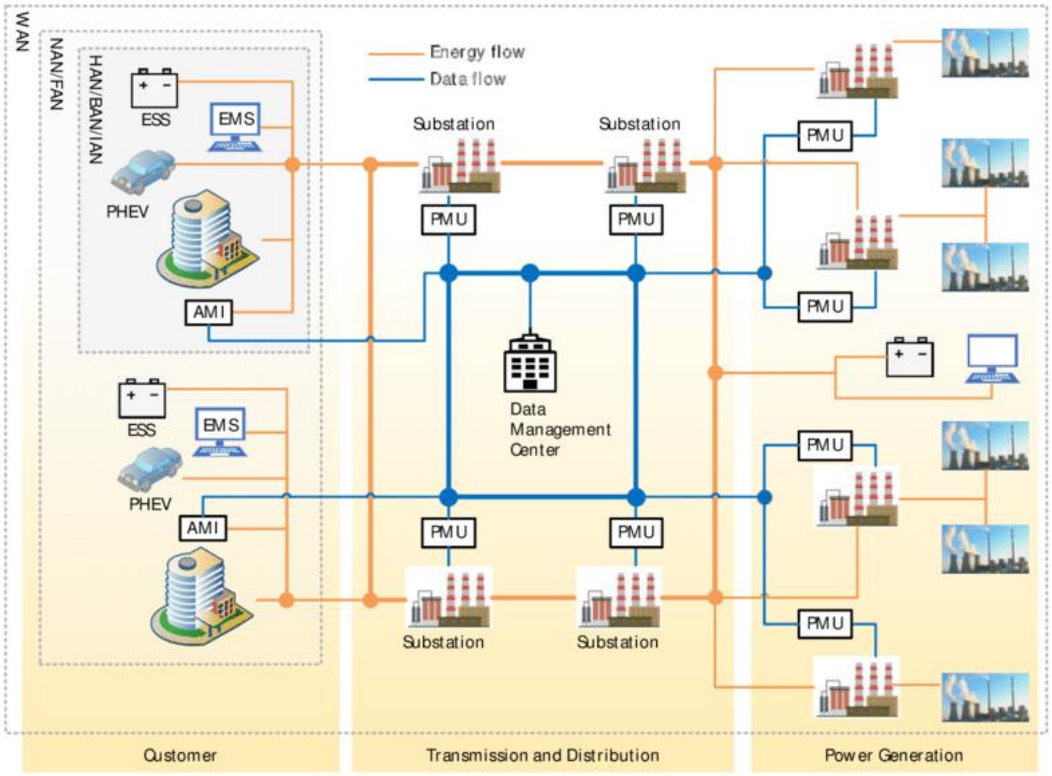
Az AMI integrálható más technológiákkal, például **Demand Response** (DR) rendszerekkel, amelyek a kereslet oldalán befolyásolják a fogyasztást.

4.3 Demand Response rendszerek

A Demand Response rendszerek célja a villamosenergia-fogyasztás dinamikus szabályozása, a hálózat aktuális állapotának figyelembevételével. E rendszerek működése a következő lépésekben írható le:

1. A rendszer folyamatosan monitorozza a hálózati terhelést.
2. A csúcsidőszakokban jelet küld az előfizetők okoseszközeinek.
3. Az eszközök (pl. hőszivattyúk, klímaberendezések) automatikusan lekapcsolnak vagy csökkentett üzemmódra váltanak.
4. A fogyasztók értesítést kapnak, és választhatnak az automatikus vagy manuális mód között.

A DR rendszerek csökkentik a hálózati csúcsterhelést, elősegítik a költségek optimalizálását, és növelik az ellátás biztonságát [11].



3. ábra: Okoshálózatok komponensei és információ, valamint adatáramlása (https://www.researchgate.net/publication/342005158/figure/fig4/AS:900132035887104@1591619609014/Data-and-energy-flow-architecture-in-Smart-Grid.png)

4.4 Előnyök és kihívások

Előnyök:

- Megbízhatóbb energiaellátás
- Csökkenő üzemeltetési költségek
- Alacsonyabb veszteségek a hálózatban
- Hatékony integráció a megújuló energiaforrásokkal

Kihívások:

- Nagy mennyiségű adat feldolgozása és biztonsága
- Technológiai kompatibilitás a régi rendszerekkel
- Kiberbiztonság és adatvédelem kérdései
- Magas beruházási költségek

A smart grid rendszerek sikeres megvalósítása a műszaki és informatikai fejlesztések mellett jogi, gazdasági és társadalmi szempontokat is figyelembe vesz [12].

4.5 Példák megvalósított rendszerekre

- **Észak-Amerika:** Kaliforniában működik a Pacific Gas and Electric (PG&E) vállalat smart grid rendszere, amely több millió AMI eszközt alkalmaz [13].
- **Európa:** Olaszországban az Enel cég már 2001 óta működtet távoli leolvasásra képes okosmérő hálózatot, több mint 30 millió egységgel.
- **Ázsia:** Japánban és Dél-Koreában fejlett DR rendszerek működnek, különösen a hőmérsékletfüggő terhelés kiegyensúlyozására [14].

5 INTERNET OF THINGS (IOT) ESZKÖZÖK SZEREPE AZ OKOSVÁROSOK ENERGIAGAZDÁLKODÁSÁBAN

Az Internet of Things (IoT) technológia kulcsszerepet játszik az okosvárosok energiahatékonyságának növelésében. Az IoT eszközök – például szenzorok, okosmérők és hálózatra kapcsolt vezérlők – lehetővé teszik az energiafogyasztás valós idejű monitorozását és optimalizálását.

5.1 IoT eszközök típusai és funkciói

Az okosvárosokban alkalmazott IoT eszközök főbb típusai:

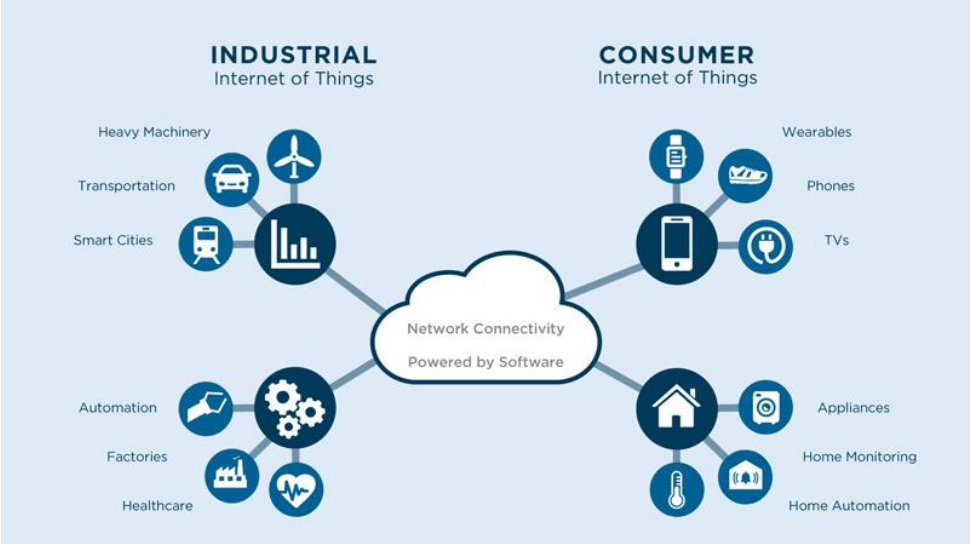
- **Szenzorok**: Mérik a hőmérsékletet, páratartalmat, fényerősséget és egyéb környezeti paramétereket.
- **Okosmérők**: Rögzítik az energiafogyasztást, és valós idejű adatokat szolgáltatnak a szolgáltatóknak és a fogyasztóknak.
- **Hálózatra kapcsolt vezérlők**: Automatikusan szabályozzák az épületek fűtését, világítását vagy az elektromos járművek töltését.

Ezek az eszközök együttműködve hozzájárulnak az energiafelhasználás optimalizálásához és a költségek csökkentéséhez.

5.2 IoT alkalmazások az energiagazdálkodásban

Az IoT technológia számos területen alkalmazható az energiagazdálkodásban:

1. **Épületautomatizálás**: Az IoT eszközök lehetővé teszik az épületek energiafelhasználásának optimalizálását, például a fűtés és világítás automatikus szabályozásával.
2. **Okos közvilágítás**: A mozgásérzékelőkkel és fényerőszabályozókkal ellátott LED-es közvilágítási rendszerek csökkentik az energiafogyasztást.
3. **Elektromos járművek töltése**: Az IoT eszközök segítségével optimalizálható az elektromos járművek töltése, figyelembe véve a hálózat terhelését és az energiaárakat.



4. ábra: IoT eszközök
(https://sealog.hu/images/IIoT-vs.-IoT.png)

5.3 Kihívások és megoldások

Az IoT technológia bevezetése számos kihívással jár, például:

- **Adatbiztonság**: Az IoT eszközök által gyűjtött adatok védelme kiemelten fontos.
- **Interoperabilitás**: Különböző gyártók eszközeinek együttműködése technikai kihívásokat jelenthet.
- **Skálázhatóság**: Az IoT rendszereknek képesnek kell lenniük a növekvő eszközszám kezelésére.

E kihívások kezelése érdekében szabványosításra és fejlett adatvédelmi megoldásokra van szükség.

6 FENNTARTHATÓSÁG ÉS GAZDASÁGI ELŐNYÖK AZ OKOS ENERGIAMEGOLDÁSOK RÉVÉN

Az okos városi energiagazdálkodási rendszerek bevezetése nemcsak környezeti, hanem jelentős gazdasági előnyökkel is jár. A fenntarthatósági szempontból ezek a rendszerek csökkentik a szén-dioxid-kibocsátást, optimalizálják az energiafelhasználást, miközben a hosszú távú költséghatékonyságot is elősegítik. A digitális technológiák alkalmazása – mint például az automatizált vezérlőrendszerek, a prediktív karbantartás vagy az adaptív világítás – mind hozzájárulnak a városok energiafelhasználásának racionalizálásához.

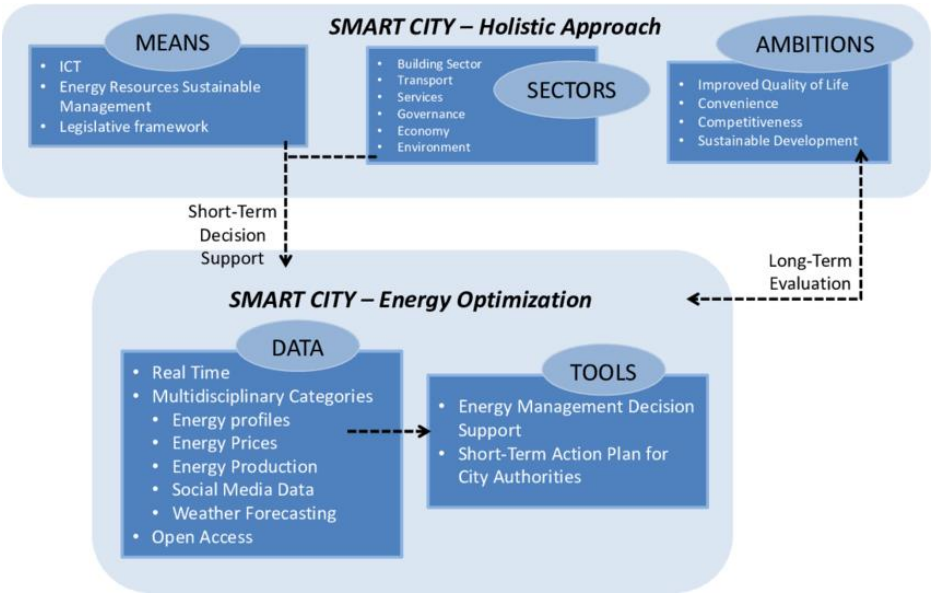
6.1 Energiamegtakarítás okos rendszerek segítségével

Az egyik legelterjedtebb alkalmazás az okos közvilágítás, amely jellemzően LED-es lámpatesteket alkalmaz, mozgásérzékelőkkel és fényerőszabályozással kombinálva. E rendszerek akár 40–70%-os energiafogyasztás-csökkenést is eredményezhetnek a hagyományos közvilágításhoz képest [18].

Példa: Koppenhága "Smart Street Lighting" projektje során 45%-kal csökkentették a közvilágítás energiafelhasználását [19].

További példák:

- Épületmenedzsment-rendszerek (BEMS), amelyek hőmérséklet-, fény- és jelenlétérzékelők alapján automatizálják az energiafelhasználást.
- Prediktív karbantartási algoritmusok, amelyekkel elkerülhetők a meghibásodások, így csökkenthetők az üzemeltetési költségek.



5. ábra: Okosváros energiaoptimalizálása (https://www.researchgate.net/profile/Evangelos-Spiliotis/publication/303011705/figure/fig1/AS:652773574066177@1532644756702/Smart-City-holistic-and-energy-optimization-approach.png)

6.2 Gazdasági megtérülés és költségcsökkentés

A beruházások gazdasági megtérülése különböző időtávon realizálódik. Az intelligens világítás vagy épületautomatizálás beruházási költsége jellemzően 3–7 éven belül térül meg [20]. Emellett a rendszerek üzemeltetési költsége alacsonyabb, mint a hagyományos megoldásoké.

2. táblázat: Okos energiamegoldások gazdasági előnyei

Megoldás	Átlagos energiamegtakarítás	Megtérülési idő	Egyéb előny
Intelligens közvilágítás	40–70%	3–5 év	Kevesebb karbantartás
Épületautomatizálás (BEMS)	20–30%	4–6 év	Komfortnövekedés
Okos hálózati vezérlés	10–20%	5–7 év	Stabilabb rendszer
Prediktív karbantartás	—	2–4 év	Kevesebb kieső idő

6.3 Környezeti hatások csökkentése

Az okos energiamegoldások alkalmazása hozzájárul az üvegházhatású gázok kibocsátásának csökkentéséhez is. A Nemzetközi Energiaügynökség (IEA) szerint az okos hálózatok és energiahatékony technológiák elterjedése 2040-re 1,5 gigatonna CO_2-kibocsátás elkerülését eredményezheti [21].

7 MEGÚJULÓ ENERGIAFORRÁSOK INTEGRÁCIÓJA AZ OKOSVÁROSI ENERGIARENDSZEREKBE

A megújuló energiaforrások – mint a nap-, szél- és geotermikus energia – beépítése az energiarendszerekbe kulcsfontosságú az éghajlatváltozás mérséklése és az energiafüggetlenség elérése szempontjából. Az okosvárosok esetében külön kihívást jelent ezek decentralizált, időjárásfüggő természete, ami megbízhatósági és szabályozási kérdéseket vet fel. Az okos technológiák és energiairányítási rendszerek lehetővé teszik a megújuló források hálózatba integrálását, valamint a termelés és fogyasztás közötti dinamikus egyensúly megteremtését.

7.1 Technikai kihívások a megújulók integrálásában

A hagyományos, központosított energiarendszerek nem alkalmasak a decentralizált energiatermelési formák (pl. háztartási napelemek, mikroszélturbinák) dinamikus kezelésére.

A főbb problémák:

1. **Termelés kiszámíthatatlansága**: A nap- és szélerőművek kimenete időjárásfüggő, ezért nehezen tervezhető.
2. **Energiatárolás szükségessége**: A termelés és a fogyasztás időbeli eltérése miatt tárolási megoldásokra van szükség.
3. **Hálózati stabilitás**: A nagyszámú kistermelő (proszumerek) integrálása megnehezíti a hálózati frekvencia és feszültség stabilitásának fenntartását.

7.2 Megoldási lehetőségek

Az alábbi technológiák és koncepciók segítik a megújuló energiaforrások hatékony integrációját:

- **Energiatárolási rendszerek**:
    - Lítium-ion akkumulátorok (pl. Tesla Powerwall)
    - Redox flow akkumulátorok
    - Hőenergia-tárolók
    - Szivattyús energiatározók (Pumped Hydro Storage)
        - **Power-to-X technológiák**: Az elektromos energiát más energiahordozóvá alakítják, pl. hidrogénné (Power-to-Gas), szintetikus metánná vagy metanollá.
        - **Virtuális erőművek (Virtual Power Plants, VPP)**: Olyan rendszerek, amelyek különböző kisebb termelő egységeket (napelemek, akkumulátorok, szélgenerátorok) együttesen vezérelnek, mintha egyetlen nagy erőmű lennének.
        - **Prediktív elemzés és időjárásmodellek**: A megújulók várható termelésének előrejelzésére szolgáló algoritmusok jelentősen növelhetik az integráció hatékonyságát [22].

7.3 Jó gyakorlatok és működő példák

- **Németország (Energiewende program)**: A decentralizált energiatermelés és az okos hálózatok integrációjának úttörője. 2022-ben a villamosenergia-termelés 46%-a megújuló forrásból származott [24].
- **Hollandia – "PowerMatching City" projekt**: Egy kísérleti városrész, ahol a háztartások napenergia-termelése, akkumulátorai és fogyasztása egy központi mesterséges intelligencián alapuló rendszer által szabályozott [25].

8 8. ADATFELDOLGOZÁS ÉS TÁROLÁS AZ INTELLIGENS VÁROSI ENERGIARENDSZEREKBEN

Az okosvárosok energiamenedzsment rendszerei hatalmas mennyiségű adatot generálnak és igényelnek. Ezek az adatok különböző forrásokból származnak: okos mérőórákból, szenzorokból, forgalmi rendszerekből, időjárási előrejelzésekből és felhasználói szokásokból. Az adatok hatékony feldolgozása és értelmezése elengedhetetlen a megbízható, fenntartható és optimalizált energiaellátás biztosításához. Ebben a környezetben kiemelt szerepet kap a Big Data analitika, a gépi tanulás (Machine Learning – ML), valamint a felhőalapú számítástechnika (Cloud Computing).

8.1 Adatok jellemzői és forrásai

Az okosenergia-rendszerekre jellemző adatok:

- **Nagy mennyiségű és gyorsan keletkező (Big Data)**
- **Sokféleség**: strukturált (pl. fogyasztási adatok) és strukturálatlan (pl. időjárási képadatok)
- **Valós idejűség**: másodpercenkénti frissítések, események és döntések
- **Elosztottság**: földrajzilag és hálózatilag szétszórt adatforrások

Főbb adatforrások:

1. **Advanced Metering Infrastructure (AMI)** – okosmérők és aggregált energiafogyasztás.
2. **IoT szenzorhálózatok** – hőmérséklet, páratartalom, fényintenzitás, jelenlétérzékelés stb.
3. **Energiatermelési adatok** – napelemek, szélturbinák aktuális kimenete.
4. **Időjárás és predikciós adatok** – meteo API-k, lokális szenzorok alapján.

8.2 Big Data és analitika szerepe

A Big Data technológiák lehetővé teszik az óriási adatmennyiségek párhuzamos feldolgozását, elemzését és a rendszeroptimalizálás támogatását. A feldolgozás során alkalmazott eszközök és platformok:

- **Apache Hadoop** – elosztott adattárolás és feldolgozás
- **Apache Spark** – memóriában történő gyors adatelemzés
- **NoSQL adatbázisok** – időalapú szenzoradatok kezelésére (pl. MongoDB, InfluxDB)

Ezek segítségével lehetséges:

- Fogyasztási trendek előrejelzése
- Terhelési csúcsok dinamikus kezelése
- Hálózati hibák és anomáliák gyors azonosítása
- Prediktív karbantartás és eszközállapot-monitoring

8.3 Cloud Computing alkalmazása

A felhőalapú platformok kulcsfontosságú szerepet játszanak az adattárolás és számítási kapacitások biztosításában. A leggyakrabban használt rendszerek:

- **Amazon Web Services (AWS)** – pl. AWS IoT Core, S3, Lambda
- **Microsoft Azure** – pl. Azure Machine Learning, Azure IoT Hub
- **Google Cloud Platform (GCP)** – pl. BigQuery, Cloud AI

A felhőszolgáltatások előnyei:

- Rugalmas skálázhatóság
- Magas rendelkezésre állás (availability)
- Alacsonyabb kezdeti infrastrukturális költség
- Beépített biztonsági protokollok és hozzáférés-kezelés

8.4 Gépi tanulási modellek szerepe

A gépi tanulás lehetőséget kínál az adatok automatikus értelmezésére, predikciókra és adaptív működésre. A fő alkalmazási területek:

- **Idősor-elemzés (Time Series Forecasting)**: fogyasztási előrejelzések, pl. LSTM-hálózatok alkalmazása
- **Klaszterezés (Clustering)**: hasonló fogyasztási mintázatok azonosítása (pl. k-means)
- **Anomáliadetektálás**: hibás szenzoradatok, hálózati meghibásodások kiszűrése
- **Reinforcement Learning**: dinamikus töltésvezérlés elektromos járműveknél, intelligens világítási rendszerek önhangolása

9 MESTERSÉGES INTELLIGENCIA (AI) SZEREPE AZ ENERGIAOPTIMALIZÁLÁSBAN

A mesterséges intelligencia alkalmazása az energiarendszerekben lehetővé teszi a valós idejű, automatizált és önfejlesztő irányítást, amely nemcsak a fogyasztás hatékonyságát növeli, hanem a rendszer egészének stabilitását és fenntarthatóságát is elősegíti. Az AI különösen hasznos az okosvárosi energiamenedzsmentben, ahol a decentralizált források, dinamikus fogyasztási minták és környezeti hatások összetett kölcsönhatásokat eredményeznek.

9.1 AI alkalmazási területei az energiarendszerekben

Az AI különböző módszertanai több szinten is alkalmazhatók:

1. **Fogyasztási előrejelzés** – idősor-analízis, amely előrevetíti az energiaigényt órás, napi vagy heti szinten.
2. **Termelés-fogyasztás szinkronizálás** – különösen időjárásfüggő megújulók esetében (pl. napelemek, szélenergia).
3. **Rendszeroptimalizálás** – dinamikus vezérlés, például fűtési rendszerek vagy elektromos járműtöltők terheléselosztása.
4. **Anomáliadetektálás** – hibás mérési értékek vagy rendellenes hálózati viselkedés kiszűrése.
5. **Prediktív karbantartás** – a meghibásodás előtt észlelt viselkedési minták alapján időzített beavatkozás.
6. **Demand Side Management (DSM)** – kereslet oldali menedzsment, melyben AI vezérelt döntéshozatal történik.

9.2 Alkalmazott AI technikák

Neurális hálózatok

- **LSTM (Long Short-Term Memory)** hálók az időfüggő adatok, például a napi fogyasztási csúcsok modellezésére szolgálnak.
- **Convolutional Neural Networks (CNN)** időjárási képek vagy szenzortérképek alapján végzett predikciókhoz alkalmazhatók.

Döntési fák és ensemble módszerek

- Random Forest és Gradient Boosting Machines segítenek nagy mennyiségű heterogén adat gyors feldolgozásában.
- Robusztusak a hiányos adatokkal szemben, jól skálázhatók.

Reinforcement Learning (RL)

- Ideális dinamikusan változó környezetekhez, például elektromos járműflották intelligens töltésmenedzsmentjéhez vagy az intelligens világítás adaptív szabályozásához.

9.3 Példák gyakorlati alkalmazásra

Intelligens fűtésvezérlés

Egyes európai városokban AI-alapú algoritmusok szabályozzák az épületek fűtését az időjárás-előrejelzések, belső szenzoradatok és energiaárak figyelembevételével. Ennek eredményeképpen akár 20–30% energiamegtakarítás is elérhető [28].

Elektromos járművek töltési ciklusainak menedzselése

AI-rendszerek képesek optimalizálni a töltési ciklusokat úgy, hogy figyelembe veszik:

- Hálózati terheltséget
- Időjárást (napenergia termelés várható alakulása)

- Felhasználói szokásokat (pl. reggeli indulás ideje)

Villamosenergia-kereskedelem

A mesterséges intelligencia részt vesz a valós idejű árampiaci döntésekben, például mikor célszerű eladni vagy tárolni a felesleges megújuló energiát, melyekhez prediktív és optimalizációs modelleket használ.

10 ESETTANULMÁNYOK ÉS STATISZTIKAI ELEMZÉSEK – MŰKÖDŐ OKOSVÁROSOK PÉLDÁI

10.1 Koppenhága

Koppenhága célkitűzése, hogy 2025-re a világ első karbonsemleges fővárosává váljon. Ennek érdekében az önkormányzat átfogó stratégiát vezetett be, amelyben kiemelt szerepet kapnak az intelligens energiahálózatok és az adatvezérelt várostervezés.

Az energiagazdálkodási rendszer kulcsfontosságú eleme a **távfűtési és távhűtési hálózat**, amely összeköti a lakossági és ipari létesítményeket. A rendszer működését IoT-eszközök és szenzorhálózatok támogatják, amelyek valós időben figyelik a hőigény változásait, lehetővé téve a fogyasztási mintázatokra reagáló hőtermelést [19].

A város emellett jelentős beruházásokat hajtott végre megújuló energiaforrásokba, különösen a **szélenergia** területén. 2020-ra a város energiaellátásának több mint 40%-a származott szélből, részben a város közvetlen környezetében telepített turbináknak köszönhetően.

10.2 Szingapúr

Szingapúr az egyik legfejlettebb intelligens városként ismert, ahol az energiaoptimalizálásra és a környezeti hatások csökkentésére külön hangsúlyt fektetnek. A város „Smart Nation” kezdeményezése keretében komplex adatgyűjtő és elemző rendszereket alkalmaz az energia- és közlekedésirányítás, valamint a környezeti monitorozás területén.

A **Building and Construction Authority (BCA)** által vezetett „Green Mark” program ösztönzi az intelligens épületmenedzsment-rendszerek bevezetését. Ezek magukban foglalják az automatikus világítás- és klímaszabályozást, prediktív karbantartási algoritmusokat, valamint valós idejű energiafogyasztás-figyelést [20].

Szingapúr emellett vezető szerepet tölt be az **elektromos járművek integrációjában**, valamint a **vehicle-to-grid (V2G)** rendszerek tesztelésében, amelyek képesek az autók akkumulátorait energiatárolóként bevonni az elosztóhálózatba.

10.3 Amszterdam

Amszterdam szintén élen jár az intelligens városmegoldások bevezetésében. A **"Amsterdam Smart City"** program keretében több mint 80 projekt fut, amelyek célja a közlekedés, energia és városi infrastruktúra hatékonyságának javítása.

Az egyik kulcsprojekt a **City-Zen**, amelyben az alábbi technológiákat alkalmazzák:

1. **Intelligens energiamérők** – lehetővé teszik a valós idejű fogyasztáskövetést és energiatudatos viselkedés kialakítását a lakosság körében.
2. **Energiatároló rendszerek** – lítium-ion akkumulátorok alkalmazása a hálózati csúcsterhelések csökkentésére.
3. **Hálózati szimulációk és Digital Twin** – a teljes városi energiahálózat szimulációja, amely lehetővé teszi a prediktív karbantartást és a működés optimalizálását.

Amszterdam emellett jelentős **közösségi energia** kezdeményezéseket is támogat, amelyekben a lakók együttműködve telepítenek napelemes rendszereket vagy mikrogrid hálózatokat.

10.4 Összehasonlító statisztika

Az alábbi táblázat az egyes városok főbb jellemzőit foglalja össze az okos energiamegoldások szempontjából:

Város	Intelligens hálózat	Megújulók aránya	IoT alkalmazás	Elektromos járművek	AI/Big Data integráció
Koppenhága	Igen	>40% (szél)	Magas	Közepes	Közepes
Szingapúr	Igen	Közepes	Nagyon magas	Magas	Magas
Amszterdam	Igen	Közepes	Magas	Közepes	Magas

10.5 Következtetések

Az elemzett városok példája jól mutatja, hogy az okos technológiák alkalmazása jelentős környezeti és gazdasági előnyökkel jár. A hatékony energiaelosztás, a megújulók integrációja, a prediktív rendszerek használata, valamint a fogyasztói szokások elemzésén alapuló irányítási modellek alkalmazása egyre inkább alapfeltétellé válik a fenntartható városfejlesztés szempontjából.

11 KONKLÚZIÓ ÉS JÖVŐBELI KILÁTÁSOK

A dolgozat során bemutatott technológiák, irányítási modellek és esettanulmányok alapján megállapítható, hogy az **okos városok** és az azokhoz kapcsolódó **okos energiarendszerek** fejlesztése egyre inkább komplex, multidiszciplináris megközelítést igényel. A decentralizált energiatermelés, a valós idejű adatgyűjtés, a prediktív elemzések és a fogyasztói szokások figyelembevétele nem csupán technológiai, hanem társadalmi és gazdasági dimenziókban is jelentős változásokat hoz.

11.1 Összegzés

Az okos energiarendszerek főbb jellemzői az alábbiak szerint foglalhatók össze:

1. **Decentralizáltság és rugalmasság**: A klasszikus, egyirányú energiaelosztási modell helyét fokozatosan átveszik a decentralizált hálózatok, amelyek képesek reagálni a lokális igényekre és termelésre.
2. **Adatvezérelt döntéshozatal**: A szenzorhálózatok és IoT-eszközök révén gyűjtött adatokat gépi tanulási modellek és prediktív algoritmusok elemzik, támogatva az energiaelosztás és -felhasználás optimalizálását.
3. **Fogyasztói integráció**: Az energiapiacon a felhasználók egyre inkább aktív résztvevőként jelennek meg (pl. prosumerek), így az energiarendszereknek figyelembe kell venniük a felhasználói viselkedést is.
4. **Megújuló energiaforrások integrációja**: A nap- és szélenergia változékonysága új kihívásokat és lehetőségeket jelent, különösen az energiatárolás és a hálózati stabilitás biztosítása terén.

11.2 Jövőbeli kihívások és lehetőségek

A jövőben az alábbi területek kulcsszerepet játszanak majd az okosvárosi energiarendszerek fejlődésében:

- **Energiatárolási megoldások**: A lítium-ion akkumulátorok mellett alternatív technológiák, mint a hidrogén vagy szuperkondenzátorok is egyre nagyobb figyelmet kapnak.
- **Hálózati szintű mesterséges intelligencia**: A városi energiarendszerek működtetéséhez elengedhetetlen lesz a prediktív és autonóm döntéshozatali rendszerek fejlesztése.
- **Kiberbiztonság**: Az energia-infrastruktúrák digitalizációja új támadási felületeket teremt. A jövő rendszereinek ellenállónak kell lenniük nemcsak technikai hibákkal, hanem szándékos kibertámadásokkal szemben is.
- **Politikai és szabályozási keretek fejlődése**: Az okosváros-projektek gyakran ütköznek jogi és adatvédelmi akadályokba. A harmonizált szabályozás kulcsfontosságú lesz a technológiai fejlődés támogatásához.

11.3 Záró gondolat

Az okos energiarendszerek és városok fejlesztése nem csupán technikai kérdés. A valódi áttöréshez interdiszciplináris együttműködésre, felhasználói edukációra, transzparens szabályozási környezetre és hosszú távú stratégiai gondolkodásra van szükség. A jelenlegi példák – mint Koppenhága, Szingapúr vagy Amszterdam – jól mutatják, hogy a siker nem kizárólag a technológián, hanem az integrált várospolitikán és a közösségi részvételen is múlik.

IRODALOMJEGYZÉK

[1] United Nations Department of Economic and Social Affairs, “World Urbanization Prospects: The 2018 Revision,” United Nations, 2019. [Online]. Available: https://population.un.org/wup

[2] T. Nam and T. A. Pardo, “Conceptualizing smart city with dimensions of technology, people, and institutions,” in *Proc. 12th Annu. Int. Conf. Digital Government Res.*, New York, NY, USA: ACM, 2011, pp. 282–291.

[3] M. Batty, K. W. Axhausen, F. Giannotti et al., “Smart cities of the future,” *Eur. Phys. J. Special Topics*, vol. 214, no. 1, pp. 481–518, 2012.

[4] European Commission, “Smart Cities Marketplace,” 2020. [Online]. Available: https://smart-cities-marketplace.ec.europa.eu

[5] R. Giffinger et al., “Smart Cities: Ranking of European Medium-Sized Cities,” Vienna University of Technology, 2007.

[6] International Energy Agency, “World Energy Outlook 2021,” IEA, 2021. [Online]. Available: https://www.iea.org/reports/world-energy-outlook-2021
[7] REN21, “Renewables 2022 Global Status Report,” REN21 Secretariat, 2022.
[8] M. F. Shaikh and S. B. Zeadally, “Energy Management in Smart Cities: A Survey,” *Sustainable Cities and Society*, vol. 45, pp. 695–713, 2019.
[9] J. Parag and B. K. Sovacool, “Electricity market design for the prosumer era,” *Nature Energy*, vol. 1, 2016, Art. no. 16032.
[10] A. A. Khan et al., “Energy management in smart cities: State of the art and future challenges,” *Sustainable Energy Technologies and Assessments*, vol. 43, 2021, Art. no. 100951.

[10] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4), 529-539.

[11] Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Transactions on Industrial Informatics*, 7(3), 381-388.

[12] Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, 14(4), 944-980.

[13] PG&E SmartMeter™ Program Overview. https://www.pge.com/en_US/about/smart-grid/smart-meter/smart-meter.page (Elérve: 2025. május)

[14] IEA – International Energy Agency. "Smart Grids and Demand Side Integration." https://www.iea.org/reports/smart-grids (Elérve: 2025. május)

[15] A. Zanella, N. Bui, A. Castellani, L. Vangelista, és M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, 2014.

[16] M. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510-527, 2016.

[17] L. Atzori, A. Iera, és G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[18] J. Suárez, J. Martínez, és R. Hornero, "Energy-efficient public lighting system based on wireless sensor networks," *Sensors*, vol. 15, no. 7, pp. 16712–16736, 2015.

[19] Copenhagen Solutions Lab, “Smart City Copenhagen - Solutions for Sustainable Cities,” [Online]. Available: https://cphsolutionslab.dk/

[20] R. Baer, "The Economics of Smart Building Retrofits," *Smart Energy Decisions*, 2021. [Online]. Available: https://www.smartenergydecisions.com

[21] International Energy Agency, “Digitalisation and Energy,” 2022. [Online]. Available: https://www.iea.org/reports/digitalisation-and-energy

[22] F. Luo, J. Zhao, J. Wang, és M. Shahidehpour, "Distributed Energy and Smart Grid Integration: A Review," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3590–3603, 2019.

[23] International Renewable Energy Agency (IRENA), “Smart Electrification with Renewables,” 2022.

[24] Bundesministerium für Wirtschaft und Klimaschutz, “Energiedaten: Gesamtausgabe,” 2023. [Online]. Available: https://www.bmwi.de/

[25] PowerMatching City, ECN Netherlands, [Online]. Available: https://www.ecn.nl/projects/PowerMatching-City

[26] IBM, "The Smarter Planet Initiative," IBM White Paper, 2021. [Online]. Available: https://www.ibm.com/smarterplanet

[27] U.S. Department of Energy, "Grid Modernization Laboratory Consortium," 2022. [Online]. Available: https://www.energy.gov/gmlc
[28] A. Shrestha et al., “AI-Driven Smart Heating Systems for Residential Buildings,” *Energy and Buildings*, vol. 268, 2023.

2.15. A mobilkommunikáció fejlődése: Az 1G-től a 6G-ig, technológiai architektúrák, eszközök és ipari hatások

Tartalom

Bevezetés ... 3
Mobilhálózat generációi ... 3
- Első generációs mobilhálózatok ... 4
- Második generációs hálózatok ... 5
- Harmadik generációs mobilhálózatok ... 8
- Negyedik generációs hálózatok ... 10
- Ötödik generációs mobilhálózat ... 12

5G Architektúrája ... 16
Mobilgyártók szerepe a mobilhálózatok fejlesztésében ... 18
- Nokia ... 18
- Ericsson ... 19
- Motorola ... 20

6G Hálózat ... 22
- 6G jelentősége ... 22
- 6G jellemzői ... 22
- A 6G lehetséges alkalmazásai ... 23
- A 6G fejlesztésének kihívásai ... 24
- 6G és az 5G közötti különbség ... 25
- Fenntarthatóság és 6G ... 25
- Etikai és társadalmi következmények ... 25

Záró gondolatok ... 25
Források ... 26

Bevezetés

A mai digitális kommunikációs környezetben a mobilitás kulcsfontosságú szerepet játszik, melynek egyik fő mozgatórugója az 5G technológia. Az 5G – a modern telekommunikáció egyik legkiemelkedőbb innovációja – nem csupán a hálózati kapacitások drámai bővítését teszi lehetővé, hanem új, forradalmi szolgáltatások megjelenését is elősegíti. Hatása egyértelműen érzékelhető a közlekedéstől kezdve az iparon, a mezőgazdaságon át az egészségügyön, energiagazdálkodáson és a szórakoztatóiparon belül is.

A Covid-19 világjárvány idején a digitális kapcsolódás fontossága még nyilvánvalóbbá vált, rávilágítva arra, mennyire alapvető szerepet töltenek be a telekommunikációs hálózatok és a digitális infrastruktúra a társadalom működésében. Ennek fényében az 5G hálózatok gyors és biztonságos kiépítése kulcsfontosságúvá vált. A mobiltechnológia e fordulópontján a változás mértéke várhatóan hasonló jelentőséggel bír, mint a 3G-ről 4G-re történő átállás [1] , amely a technológiai fejlődés egy új korszakát nyitotta meg. Az átállás jelenleg is zajlik, ami további lehetőségeket és kihívásokat hordoz a gazdaságinformatikai megközelítésben.

Ezt a témát azért választottam, mert a digitális kapcsolódás és az innováció egyre nagyobb szerepet játszik a mindennapokban, és az 5G fejlődése meghatározó lesz a jövő technológiai irányvonalai szempontjából.

Mobilhálózat generációi

Az emberi fejlődés ugyanúgy kapcsolódik az ember által alkotott dolgokhoz, mint a természet által létrehozottakhoz. A különbség abban rejlik, hogy míg az ember technológiát fejleszt, addig a természet az evolúció révén fejlődik. A mobilhálózatokban is nyomon követhető a technológiai fejlődés, amelynek állomásait generációknak nevezzük. A generáció szó megjelenik az elnevezésükben is („G”), ami a mobiltelefon-technológia időbeli fejlődésére utal. Mielőtt rátérnék az 5. generációs mobilhálózatok biztonsági kérdéseire és sajátosságaira, fontosnak tartom bemutatni a korábbi generációk történetét és működését. Az elemzéshez mindenképpen ajánlott megismerni a mobiltelefonos kommunikáció működését és a generációk biztonsági kérdéseit, mivel ezek elengedhetetlenek a levont következtetésekhez.

1. ábra Egyes mobilgenerációk megjelenései

- Első generációs mobilhálózatok

Az 1. generációs mobilhálózat (1G) a vezeték nélküli cellás hálózatok első változata volt, amely az 1970-es évek végén és az 1980-as évek elején jelent meg. Bár a rendszer a rádiótornyok összekapcsolásához már digitális jeleket is használt, a hangátvitel továbbra is analóg (FM) alapú maradt.

A világ különböző országaiban eltérő 1G szabványokat alkalmaztak. A skandináv országokban, Kelet-Európában és Oroszországban az NMT (Nordic Mobile Telephone) rendszert használták, míg az Egyesült Államokban az AMPS (Advanced Mobile Phone System) volt elterjedt. Az Egyesült Királyságban a TACS (Total Access Communications System), Japánban a JTACS (Japan Total Access Communications System) és az NTT (Nippon Telegraph and Telephone Corporation) szabványai működtek. Nyugat-Németországban a C-Netz, Franciaországban a Radiocom 2000, míg Olaszországban az RTMI (Radio Telefono Mobile Integrato) rendszert alkalmazták. Ezek a hálózatok a 450 MHz-es és 900 MHz-es frekvenciatartományban működtek.

Az analóg mobilhálózatok legnagyobb hátránya az volt, hogy az eltérő rendszerek nem voltak kompatibilisek egymással, így a készülékek kizárólag a saját hálózatukon működtek, és jellemzően csak egy adott ország területét fedték le. A szolgáltatás kizárólag hangalapú kommunikációra korlátozódott, amelyet valós időben lehetett továbbítani és fogadni.

Az NMT szabványokat nyíltan és ingyenesen lehetett használni, ami segítette a nagy mobilgyártók, például a Nokia, az Ericsson és a Motorola fejlődését. Magyarországon az első mobilhálózat 1990-ben indult Budapesten, három bázisállomással, az NMT technológiára építve. A szolgáltatást a Westel Rádiótelefon Kft. nyújtotta, amelynek kínálata gyorsan népszerűvé vált a hazai felhasználók körében.

Az 1G technológia azonban több problémával is küzdött. A hangminőség gyenge volt, a lefedettség korlátozott, és nem létezett roaming, vagyis nem lehetett más szolgáltatók hálózatán használni a telefonokat. Komoly biztonsági kockázatot jelentett, hogy a hívások nem voltak titkosítva, így bárki, aki rendelkezett megfelelő rádiós szkennerrel, lehallgathatta a beszélgetéseket.

A lehallgatás megnehezítése érdekében az NMT frekvenciákat eltávolították a szkennerekből, de ezeket könnyen újraprogramozhatták, így a lehallgatás továbbra is problémát jelentett. Későbbi verziók már lehetőséget biztosítottak opcionális analóg kódolásra, amelyet a mobil és a bázisállomás közötti megegyezés alapján lehetett aktiválni. Az AMPS rendszer esetében a lehallgatók egy speciális eszközzel elfoghatták a telefon sorozatszámát és telefonszámát, majd egy másik eszközre másolva klónozhatták a telefont, így ingyen használhatták a szolgáltatást. Az érintett előfizető ezt csak a következő számláján észlelhette, amikor váratlanul magasabb díjat kellett fizetnie. [2]

- Második generációs hálózatok

A mobilhálózatok második generációja (2G) az 1990-es évek elején került kereskedelmi forgalomba. Míg az első generációs (1G) hálózatok analóg rádiójeleket használtak, addig a 2G már digitális technológiát alkalmazott a hangátvitelre és a rendszer elemeinek egymás közötti kommunikációjára. A 2G a következő újításokat hozta a korábbi generációkhoz képest:

- A digitális átvitellel lehetőség nyílt titkosított kommunikációra.
- A rádióspektrum jobb kihasználásával több felhasználó tudott egyszerre beszélni.
- Lehetőség nyílt szöveges üzenetek (SMS) küldésére.
- Megjelent az adatátvitel, kezdetben 9,6 kb/s sebességgel.

A szabványok viszonylagos egységességének köszönhetően verseny alakult ki a gyártók között, ami az árak és a telefonok méretének csökkenéséhez vezetett.

A 2G szabványok megszüntették a korábbi szabványok és rendszerek közötti inkompatibilitást. A világon a legelterjedtebb 2G technológia az ETSI (European Telecommunications Standards Institute) által 1991-ben kifejlesztett GSM (Global System for Mobile Communication) volt. További technológiák közé tartozik az Észak-Amerikában használt IS-95 (Interim Standard 95) vagy cdmaOne és a Digital-AMPS, valamint a Japánban alkalmazott PDC (Personal Digital Cellular). Magyarországon a 2G szolgáltatás 1994-ben indult el a Pannon GSM (későbbi Telenor) révén.

A GSM a legelterjedtebb 2G szabvány a világon, amely a 900 MHz-es és az 1800 MHz-es sávokban működik. A 900 MHz körüli hullámok követik a földfelszínt, így ez a sáv nagyobb területek lefedésére alkalmas, és az átvitt jel kisebb csillapítást szenved el, ami kisebb teljesítményigényt eredményez. Az 1800 MHz-es sáv nagyobb sávszélességgel rendelkezik, de a hullámok rosszabb terjedési tulajdonságokkal bírnak. A GSM egyik legfontosabb újítása az előfizetői azonosító modul, azaz a SIM-kártya megjelenése volt, amely az előfizető személyes adatait és telefonkönyvét tartalmazza, így készülékcsere esetén a SIM-kártya áthelyezésével az előfizető megtarthatja adatait és átvihesse azokat egy másik készülékbe. Bár a GSM hálózatot biztonságosnak tervezték, a rendszer sebezhető különböző típusú támadásokkal szemben, amelyek a GSM-hálózat különböző részeit érhetik. A GSM rendelkezik felhasználói azonosítással és éteren keresztüli titkosítással. Számos éteren keresztüli titkosítást használ, de az egyik legnagyobb hiba a tervezés során az volt, hogy a titkosítási algoritmusokat igyekeztek titokban tartani és nem nyújtották be őket felülvizsgálatra, így az algoritmusok kiszivárgása után a sebezhetőségek könnyen azonosíthatók voltak.

A 2G kapcsán megemlítendő a 2.5G szabvány, a GPRS (General Packet Radio Service) és a 2.75G szabvány, az EDGE (Enhanced Data Rates for GSM Evolution). A GSM-et folyamatosan fejlesztették az évek során, ennek eredményeképpen jöttek létre ezek a generációk. A GPRS a

GSM kiegészítése csomagkapcsolt átvitellel, mely 60-80 kb/s sebességet ért el. A klasszikus telefonhálózatok áramkörkapcsolással működtek, amely minőséget garantált a hívás felépítése és lebontása között. A csatorna csak a hívás közben volt használva. A csomagkapcsolás a számítógépes hálózatok újdonsága, mellyel az átvinni kívánt információt kisebb csomagokra, kisebb részekre bontjuk. Ennek eredménye a jobb kihasználtság és nagyobb forgalom, de egyes csomagok elveszhetnek az átvitel során, így a minőség nem garantált. Az EDGE javított adatátviteli sebességet tett lehetővé (150-180 kb/s).

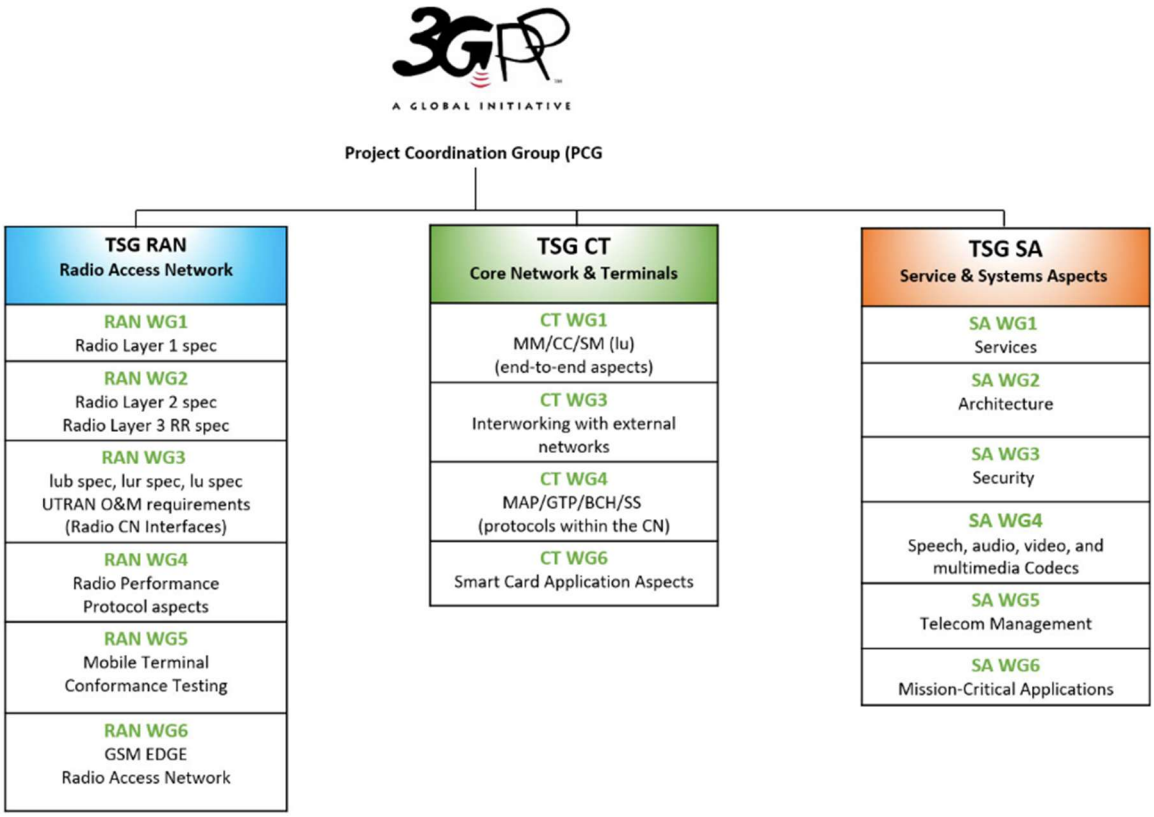
Mindkét fejlesztés a 3GPP-hez (3rd Generation Partnership Project) kötődik, amely innentől kezdve fontos szerepet töltött be a mobilhálózat generációkhoz kapcsolódó szabványok létrehozásában és fejlesztésében. A 3GPP a világ különböző pontjain lévő távközlési szabványfejlesztő szervezeteket egyesíti, biztosítva a szervezetek közötti együttműködést és elősegítve a szabványok létrehozását. A 3GPP-hez az alábbi szervezetek tartoznak:

- Association of Radio Industries and Businesses (ARIB, Japán)
- Alliance for Telecommunications Industry Solutions (ATIS, USA)
- China Communications Standards Association (CCSA, Kína)
- European Telecommunications Standards Institute (ETSI, Európa)
- Telecommunications Standards Development Society (TSDSI, India)
- Telecommunications Technology Association (TTA, Dél-Korea)
- Telecommunication Technology Committee (TTC, Japán)

A projekt három specifikációs csoporttal (Technical Specification Group, TSG) rendelkezik, melyek a következők:

- **Radio Access Networks (RAN):** felelős a hálózat és az eszközök, valamint az air-interfész specifikációiért.
- **Services & System Aspects (SA):** felelős a 3GPP-specifikációkon alapuló rendszerek általános architektúrájáért és szolgáltatási képességeiért, valamint a TSG-k közötti koordinációért.
- **Core Network & Terminal (CT):** felelős a terminál interfészek, a terminálképességek és a Core hálózat meghatározásáért.

A TSG-k további munkacsoportokból épülnek fel, amelyeknek köszönhetően fejlődtek a mobilhálózati technológiák. Amikor egy fejlesztési pontot elérnek, azt a generációban "Release"-nek nevezik, ami már megvalósítható állapotot jelent. A 3GPP kiadásoknál a fő hangsúly a rendszer visszafelé és előre kompatibilitásán van, hogy biztosítsák a felhasználói berendezések zavartalan működését. A 3GPP egyszerre több kiadáson dolgozik, így az aktuális munka befejezése előtt már megkezdik a jövőbeli munkát is.

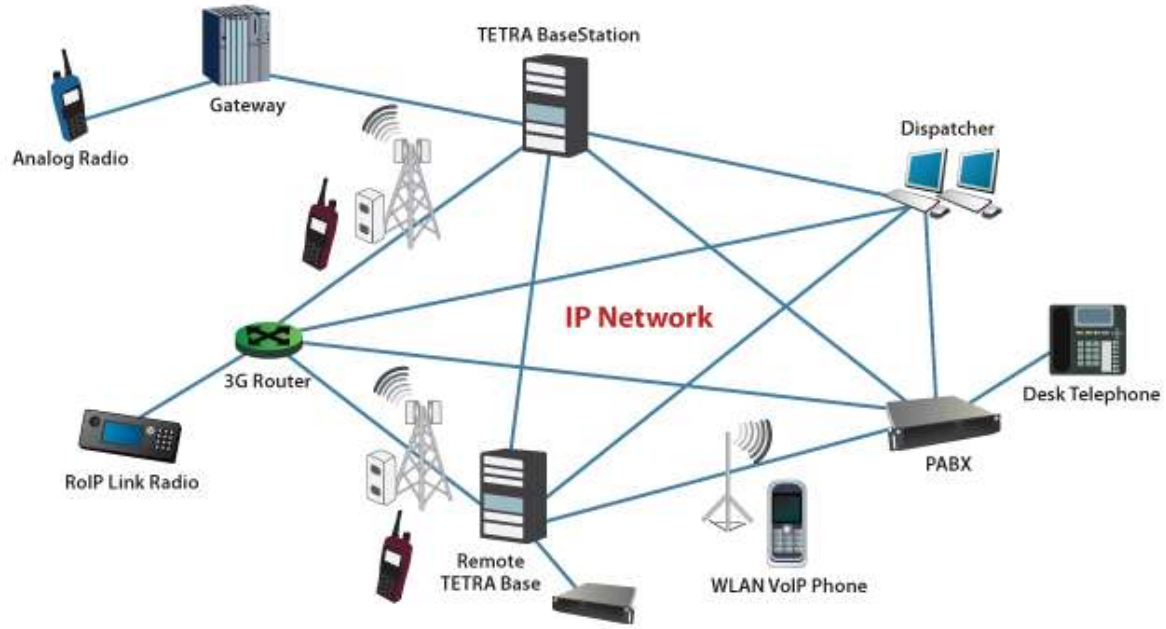


2. ábra A 3GPP modell

A 2G szabványokkal párhuzamosan jelent meg a TETRA (Terrestrial Trunked Radio) rendszer. A TETRA egy digitális, trönkölt, zártcélú hálózat, amelynek szabványa 1995-ben jelent meg az ETSI által, kifejezetten kormányzati szervek és segélyszolgálatok részére. Magyarországon az Egységes Digitális Rádiótávközlő Rendszer (EDR) 2007-ben indult el a TETRA technológiára épülve és azt továbbfejlesztve. A TETRA összehasonlítható a GSM rendszerrel. A technológia előnyei a következők:

- Megbízható, magas rendelkezésre állású rendszer.
- Alacsonyabb frekvencián működik (380-395 MHz), ennek köszönhetően nagyobb hatótávolsággal és nagyobb földrajzi lefedettséggel rendelkezik.
- Létrehozható egy az egyhez, egy a többhöz, több a többhöz üzemmódok.
- Támogatja a hitelesítést, az eszközök regisztrációját, az air-interfész titkosítást és végpontok közötti titkosítást.
- Hálózat hiányában a mobiltelefonok közvetlen hívást használhatnak, vagy hálózati közvetítőként is üzemelhetnek.
- Gyorsan telepíthető infrastruktúra.

A TETRA egy jobban megtervezett és hatékonyabb rendszer, mint a GSM. Ez a rendszer a megfelelő technikai megoldásokkal, kibővült szolgáltatásokkal és magas szintű rendelkezésre állásával segíti a rendvédelmi szervek működését. Ugyanakkor a szükséges biztonsági követelményeket jóval magasabb szinten és széles körben kell alkalmazni, hiszen egy hagyományos rendszerhez képest sokkal nagyobb biztonsági kockázatot jelenthetnek, például a Magyar Honvédség esetében, ha nem titkosított az átvitel.



3. ábra Tetra hálózat topográfia

- Harmadik generációs mobilhálózatok

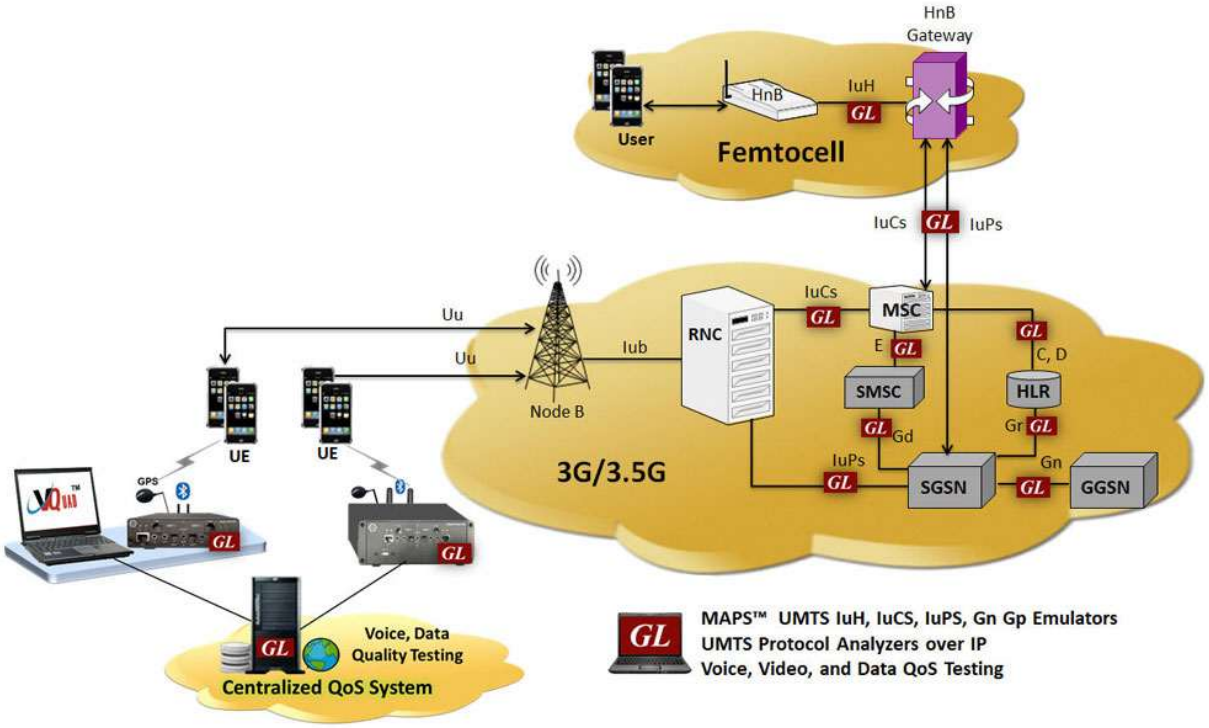
A mobilhálózatok harmadik generációja (3G) a 2000-es évek elején vált elérhetővé a nagyközönség számára. Ennek kialakulása az International Telecommunication Union (ITU) munkájának köszönhető, amely globális frekvenciasávot kívánt kijelölni a 2000 MHz-es tartományban, támogatva ezzel egyetlen vezeték nélküli kommunikációs szabványt. Ezt a kezdeményezést IMT-2000 (International Mobile Telephone 2000) ajánlásnak nevezik. Az ITU ajánlásokat fogad el a jövőbeli globális kommunikációs technológiákra vonatkozóan, de a konkrét szabványosítási és fejlesztési munkát más szervezetek, mint például az IEEE (Institute of Electrical and Electronics Engineers), a WiMAX Forum és a 3GPP végzik.

Az IMT-2000 specifikáció számos követelményt határoz meg, amelyeket a technológiáknak teljesíteniük kell. A főbb követelmények a következők:

- Világszerte használható legyen, integrálva a műholdas és a földi rendszereket a globális lefedettség biztosítása érdekében.
- Minden rádiós környezetben használható legyen (pl. LAN, vezeték nélküli, cellás, műholdas).
- Széles körű távközlési szolgáltatásokat nyújtson (pl. hang, adat, multimédia, internet).
- Támogassa mind a csomagkapcsolt, mind az áramkörkapcsolt adatátvitelt.
- Biztosítson magas adatátviteli sebességet, akár 2 Mbit/s-t beltéri környezetben, 144 kbit/s-t nagy mobilitás esetén, és 384 kbit/s-t mozgáskorlátozott környezetben.
- Hatékonyan használja a spektrumot.
- A 3G technológia a korábbi generációkhoz képest a következő fejlesztéseket kínálja:

- Jobb spektrális kihasználtság révén nagyobb hálózati kapacitás.
- Nagyobb adatátviteli sebesség.
- Fejlettebb és újabb szolgáltatások, mint a videohívás, internetelérés, IPTV, GPS és videokonferencia.

A GSM számára a 3G evolúció az UMTS-t (Universal Mobile Telecommunications System) eredményezte. A cdmaOne rendszerek fejlődése pedig a CDMA2000-hez vezetett. Az UMTS a GSM hálózatokra építve egy komplex hálózati rendszert határoz meg. A Release 99 384 kbit/s-os sebességet ír le az első UMTS-alapú rendszerekhez. Az UMTS rendszereket a roaming támogatásához is tervezték, és ha a telefon UMTS lefedettségen kívül esik, a hívás átadható a GSM hálózatnak, mivel a telefonok mindkettőt támogatják. Az interoperabilitást szem előtt tartva az UMTS telefonok több frekvenciát is támogatnak, mivel különböző országok különböző frekvenciatartományokat használnak. Európában a 2100 MHz-es sávot használják, míg az USA-ban a 850 MHz-es és 1900 MHz-es sávokat. Ennek eredményeként a gyártóknak többsávos GSM és UMTS módú telefonokat kellett készíteniük, ami alacsony üzemidejű készülékeket eredményezett.



4. ábra 3G Hálózat topográfia

Az UMTS fő konkurenciája a CDMA2000 és az EDGE. A CDMA2000 kisebb sávszélesség igényű az UMTS-nél, így a spektrumban könnyebb elhelyezni a szolgáltatóknak. Az EDGE a meglévő GSM spektrumokat használja, és telepítése sokkal könnyebb a meglévő GSM hálózatba, mint az UMTS esetén új berendezéseket telepíteni.

A 3G szabványokat a 3GPP továbbfejlesztette. A HSPA (High Speed Packet Access) két protokoll ötvözete, mely javítja és kiterjeszti a 3G hálózatok teljesítményét az UMTS

protokollokból kiindulva. A két protokoll a le- (High-Speed Downlink Packet Access, HSDPA) és a felfelé irányuló (High-Speed Uplink Packet Access, HSUPA) csomagkapcsolt hozzáférést különbözteti meg. Mindkét protokoll az adatátviteli sebességet javítja, növelve a kapacitást és csökkentve a késleltetést. A HSDPA 3.5G néven is ismert, amit a 3GPP a Release 5-ben vezetett be, és 14 Mbit/s adatátviteli sebességet kívánt elérni. A HSUPA a 3.75G, melyet a 3GPP a Release 6-ban specifikált 5,76 Mbit/s adatátviteli sebességgel. További jelentős adatátviteli sebesség növekedés érhető el a HSPA+ (Evolved High Speed Packet Access) által a Release 7, 8, 9, 11-ben leírtak alapján.

A 3G hálózatok nagyobb biztonságot nyújtanak, mint a 2G elődjeik. Az UMTS hozzáférési biztonsági szabványok új hitelesítési mechanizmuson alapulnak, amelyek kiterjednek az adatintegritásra, a kölcsönös hitelesítésre, a hálózati biztonságra, a rugalmasságra és a hosszabb kulcsok alkalmazására. Ezek együttes használata fokozott védelmet nyújt a hamis bázisállomás támadások ellen, mivel a mobileszköz képes a hálózat azonosítására bizonyos jelzőüzenetek segítségével. A hamis bázisállomás támadás során a támadó egy bázisállomásnak álcázza magát, és képes lehet a titkosítási algoritmusok elnyomására vagy megváltoztatására. Amennyiben új fenyegetettségek jelennek meg, a biztonsági funkciók igény szerint bővíthetők és javíthatók.

- Negyedik generációs hálózatok

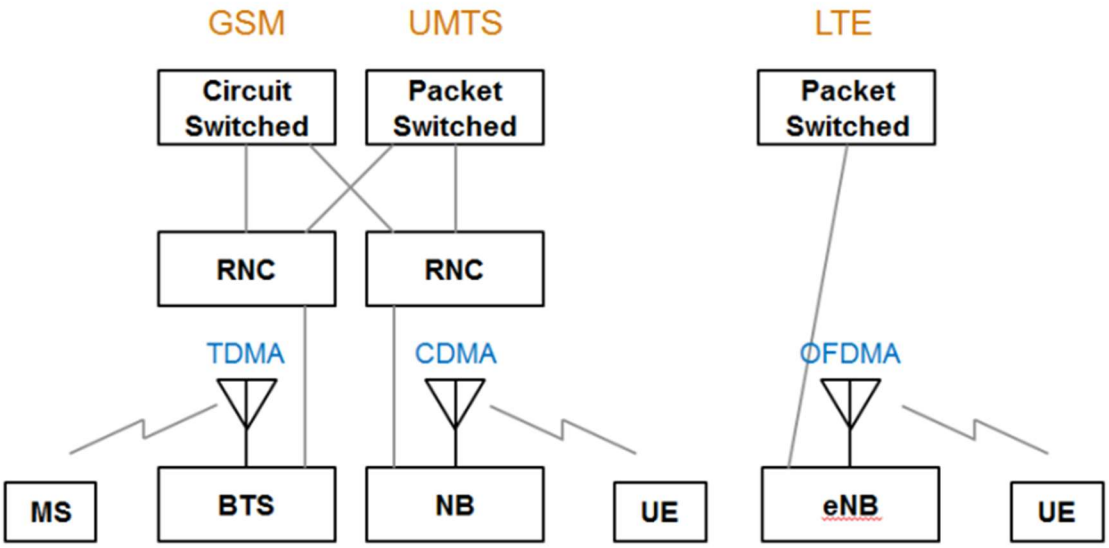
A mobilhálózatok negyedik generációja, azaz a 4G, a mobil technológia következő szintjét képviseli. Az ITU 2008-ban elkészítette az IMT-Advanced ajánlást, amely a 4G rendszerekre vonatkozik. Ez alapján a következő követelményeknek kell megfelelnie a 4G mobilrendszereknek:

- Teljesen IP-alapú csomagkapcsolt hálózatra kell épülnie.
- Képesnek kell lennie a hálózati erőforrások dinamikus megosztására és használatára, cellánként több felhasználó egyidejű támogatására.
- Skálázható csatornaszélességet kell használnia 5-20 MHz-ig, opcionálisan akár 40 MHz-ig.
- Magas mobilitás esetén kb. 100 Mbit/s, alacsony mobilitás esetén pedig 1 Gbit/s adatátviteli sebességet kell biztosítania.
- A kapcsolat spektrális hatékonyságának 15 bit/s Hz-nek kell lennie lefelé irányuló kapcsolaton, és 6,75 bit/s Hz-nek felfelé irányuló kapcsolaton.
- A rendszer spektrális hatékonyságának beltéri helyeken 3 bit/s Hz-nek kell lennie lefelé irányuló kapcsolaton, és 2,25 bit/s Hz-nek felfelé irányuló kapcsolaton.

Ezeknek a követelményeknek a megfelelését a 3GPP által szabványosított LTE (Long Term Evolution), a későbbi LTE Advanced, és az IEEE által létrehozott 802.16m vagy WiMAX szabványok biztosítják. Azonban kezdetben ezek a rendszerek sem garantálták az 1 Gbit/s adatátviteli sebességet.

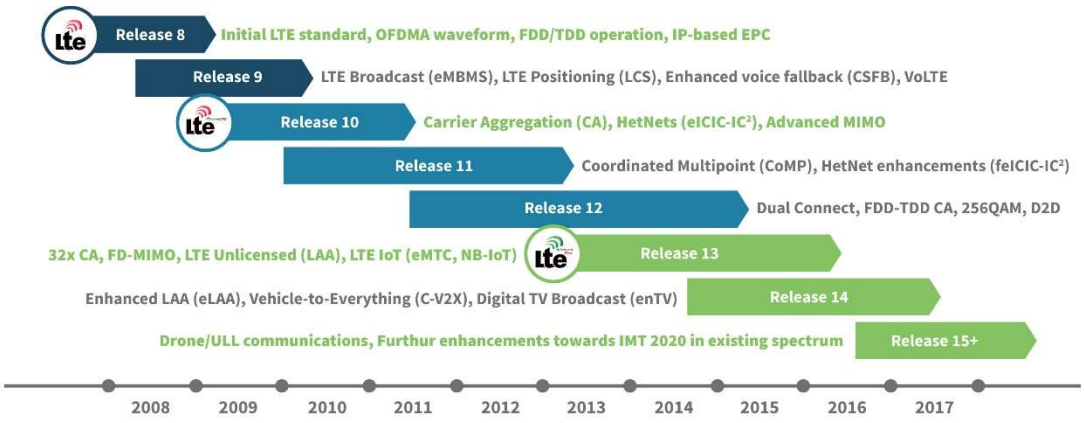
Az LTE egy nagy sebességű technológia mobil eszközök számára, amelyet a 3GPP a GSM/EDGE és az UMTS/HSPA technológiákra alapozva fejlesztett ki. Az LTE gyorsabb letöltési és feltöltési sebességet, alacsonyabb késleltetési időt és jobb lefedettséget kínál a régebbi hálózatokhoz képest. Az LTE képes kihasználni a meglévő 2G és 3G, valamint az új spektrumokat.

Magyarországon leginkább a 800, 1800 és 2600 MHz-es tartományokban működik, a népsűrűségtől függően. Gyakran 4G hálózatokkal együtt említik, de csak 100 Mbit/s letöltési és 50 Mbit/s feltöltési sebességet képes elérni. Magyarországon az első 4G szolgáltatást a Magyar Telekom indította el 2012-ben.



5. ábra Mobilhálózat architektúrájának fejlődése

Az LTE Advanced az LTE jelentős továbbfejlesztése, amelyet a 3GPP a Release 10-ben szabványosított. Az első LTE Advanced hálózat 2009-ben kezdte meg működését Svédországban és Norvégiában, majd a következő évben az USA-ban és Japánban is kiépült. Az LTE és az LTE Advanced közötti legnagyobb különbség az adatátviteli sebességben van, valamint az adótornyok és a készülékek közötti átvitel is jobban működik. Az LTE Advanced technológia egyik újdonsága a vivőaggregáció, amely lehetővé teszi, hogy több frekvenciablokkot egyesítsenek egy felhasználó számára, így növelve az átviteli sebességet és a rendszer erőforrás-kihasználtságát. Továbbá, a MIMO (Multiple Input and Multiple Output) technológia is jelentős előrelépés, mivel kétszer annyi antennát használva növeli a kapacitást az energiafogyasztás növelése nélkül.



6. ábra LTE egyes fejlesztési állomásai

Az LTE biztonsági architektúráját a 3GPP határozta meg. Biztonsági rések lehetnek a SIM kártyák, az UICC (Universal Integrated Circuit Card) tokenek, az eszköz és hálózat azonosítása, valamint az éteren keresztüli védelem és hálózatvédelem esetében. Ezeket a biztonsági réseket különböző titkosítási algoritmusokkal vagy a fizikai biztonság megfelelő kialakításával lehet védeni. Az LTE-től elvárják, hogy garantálja a bizalmas működést és az erős hitelesítést. Az LTE hálózatok azonban sebezhetők olyan biztonsági fenyegetésekkel szemben, amelyek megzavarják a rendelkezésre állást és a hitelesítést. Egyetemi kutatók egy alacsony költségvetésű, nyílt forráskódú szoftverrel további biztonsági réseket tártak fel a 4G hálózatokban. Eredményeik közül kiemelendő a hitelesítési támadás, amely lehetővé teszi a támadó számára, hogy csatlakozzon a maghálózathoz, miközben az áldozat mobileszközének adja ki magát. Ennek során a támadó meghatározhatja az áldozat helyét a hálózatban, és nemcsak a helyinformációkat használhatja saját céljaira, hanem szolgáltatásmegtagadási támadásokat is indíthat. Ezzel a szolgáltatásmegtagadási támadással elérheti, hogy az áldozat készüléke ne kapjon értesítéseket (*pl. hívás, SMS*), de akár kitalált üzeneteket is küldhet, ami energia kimerülést okozhat a készüléknél.

- Ötödik generációs mobilhálózat

Az 5G, azaz az ötödik generációs mobilhálózati technológia, jelentős előrelépést jelent a korábbi generációkhoz képest. Az 5G célja, hogy magasabb adatátviteli sebességet, alacsonyabb késleltetést és nagyobb hálózati kapacitást biztosítson, valamint támogassa az új és innovatív alkalmazásokat, mint például az IoT (Internet of Things), az önvezető autók, és a virtuális valóság (VR). [3]

Az ITU az 5G esetében is kidolgozta a követelményrendszert, amelyre a szabványosító szervezetek támaszkodhatnak. Az ITU IMT-2020 ajánlásában az alábbi követelményeket határozta meg az 5G rendszerek számára:

- Magas adatátviteli sebesség: Akár 20 Gbit/s csúcssebesség letöltés esetén.
- Alacsony késleltetés: A késleltetés csökkentése akár 1 ms alá.
- Nagy hálózati kapacitás: Sokkal több eszköz egyidejű csatlakoztatása, akár millió eszköz négyzetkilométerenként.
- Energiahatékonyság: Jobb energiahatékonyság a hosszabb akkumulátor-élettartam érdekében.
- Széleskörű lefedettség: Támogatás városi, vidéki és távoli területeken egyaránt.
- Nagyobb spektrális hatékonyság: Hatékonyabb spektrumkihasználás az adatátviteli kapacitás növelése érdekében.

Technológiai eltérések

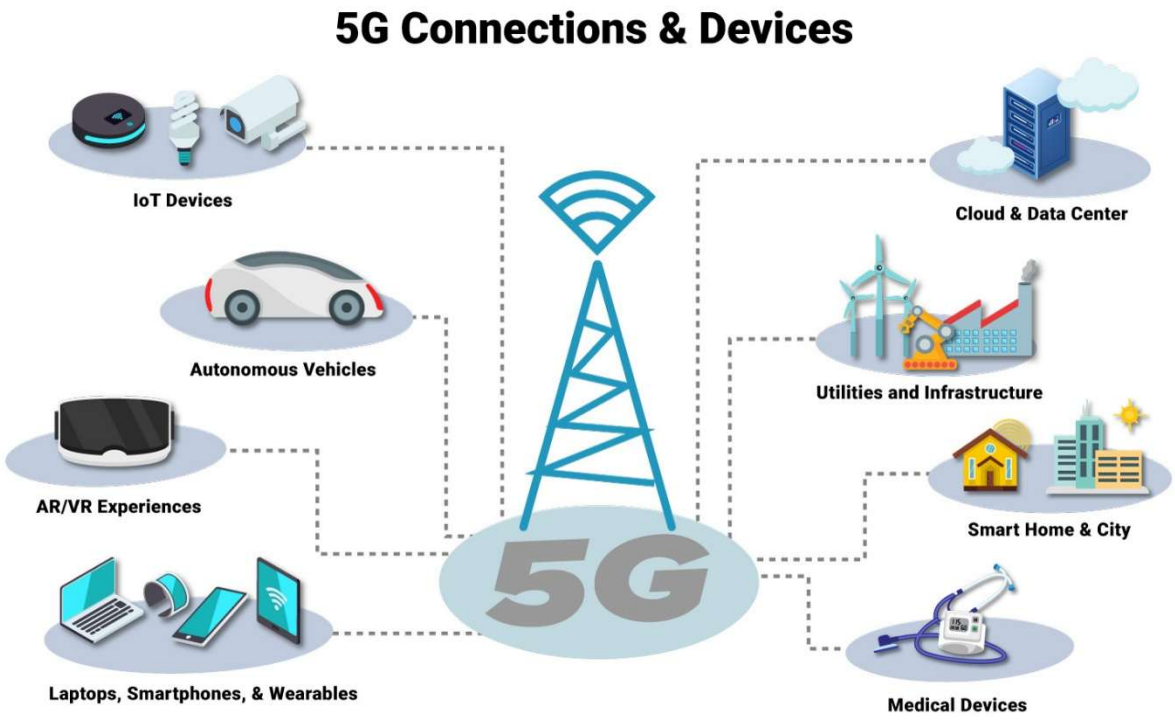
Az 5G technológia több újítást hoz a korábbi generációkhoz képest:

- **Milliméteres hullámok:** Az 5G a milliméteres hullámokat (24 GHz - 100 GHz) használja, amelyek nagyobb sávszélességet és gyorsabb adatátviteli sebességet biztosítanak.
- **Massive MIMO:** A Massive Multiple Input Multiple Output (MIMO) technológia sokkal több antennát használ az adatátvitelhez, növelve ezzel a hálózat kapacitását és megbízhatóságát.

- **Beamforming:** Az 5G hálózatok irányított jeleket használnak a pontosabb és hatékonyabb adatátvitel érdekében.
- **Network Slicing**: Az 5G hálózatok lehetővé teszik a hálózati erőforrások dinamikus és rugalmas elosztását a különböző alkalmazások és szolgáltatások számára.
- **Edge Computing:** Az 5G támogatja az edge computing technológiát, amely az adatfeldolgozást közelebb hozza a felhasználókhoz, csökkentve ezzel a késleltetést és növelve a válaszidőt.
- **Fejlett titkosítás:** Az 5G hálózatok erősebb titkosítási algoritmusokat használnak az adatvédelem érdekében.
- **Hitelesítés:** Az 5G rendszerek fejlettebb hitelesítési mechanizmusokat alkalmaznak az eszközök és a hálózat közötti biztonságos kommunikáció biztosítása érdekében.
- **Biztonsági monitoring:** Az 5G hálózatok folyamatos biztonsági monitoringot végeznek a fenyegetések észlelésére és elhárítására.

Alkalmazási területek

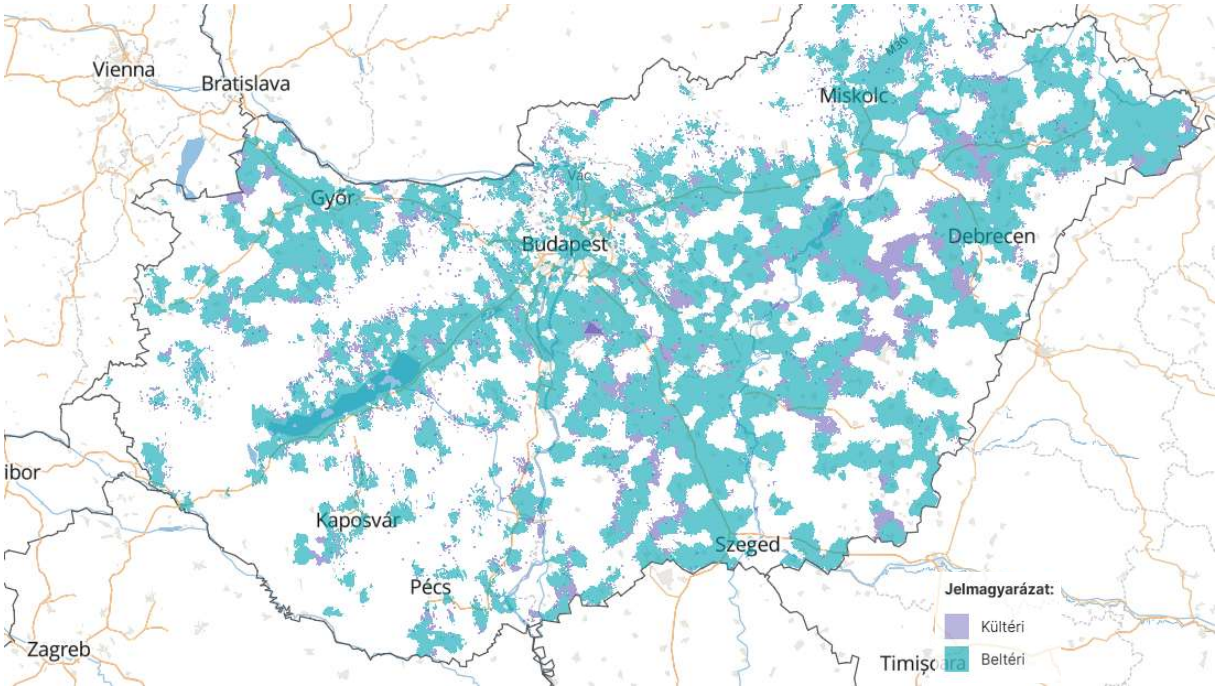
- **Okos városok:** Az IoT eszközök széleskörű elterjedése lehetővé teszi az okos városok kialakítását, ahol az infrastruktúra és a szolgáltatások hatékonyabban működnek.
- **Önvezető autók:** Az 5G hálózatok alacsony késleltetése és nagy megbízhatósága támogatja az önvezető autók biztonságos működését.
- **Virtuális és kiterjesztett valóság:** Az 5G lehetővé teszi a VR és AR alkalmazások valós idejű és magas minőségű működését.
- **Egészségügy:** Az 5G technológia támogatja a távorvoslást, a valós idejű betegmonitorozást és a gyors adatátvitelt az egészségügyi rendszerek között.



7. ábra 5G hálózathoz kapcsolódó eszközök

Magyarországi Helyzet

Magyarországon az 5G hálózatok kiépítése az utóbbi években kezdődött meg, és az ország több szolgáltatója is elindította az 5G szolgáltatásait. Az 5G hálózatok elsősorban nagyvárosokban és ipari területeken érhetők el, de folyamatosan bővítik a lefedettséget.



8. ábra One Magyarország 5G lefedettségi térképe (2025 március)

Az 5G társadalmi hatásai

Az 5G technológia bevezetése jelentős társadalmi ellenállásba ütközött, amilyen mértékben korábban egyetlen új mobilhálózati generáció sem. Az álhírek le ginkább az 5G egészségügyi hatásaira fókuszáltak, és egyes szélsőséges esetekben az emberek még az 5G tornyok megrongálásáig is elmentek. Korábban a mobilhálózatok más generációit is összefüggésbe hozták daganatos megbetegedésekkel, és hasonló vádak érték az 5G-t is. Az egészségügyi szervezetek folyamatosan vizsgálják az 5G lehetséges káros hatásait, de tudományos bizonyítékot erre eddig nem találtak. Egyes események, például Hollandiában egy 5G torony tesztelésekor bekövetkezett madárpusztulás, tovább erősítették az aggodalmakat, noha a pontos okokat nem sikerült megállapítani. Az 5G-t a COVID-19 járvánnyal is kapcsolatba hozták, egyes álhírek szerint a vírus az 5G sugárzás révén terjedt, amely teljesen alaptalan állítás volt, de mégis széles körben elterjedt. [4]

9. ábra Tájékozató szöveg, amely arra hívja fel a figyelmet, hogy az 5G technológia nem terjeszti a COVID-19 járványt.

Az 5G képes kiváltani a hagyományos vezetékes internet- és tévészolgáltatásokat, biztosítva ugyanazt a minőséget, sőt esetenként még jobbat is. A vezeték nélküli hálózat előnye, hogy olyan területeken is elérhetővé válik a megbízható internetkapcsolat, ahol eddig a vezetékes infrastruktúra kiépítése nehézségekbe ütközött.

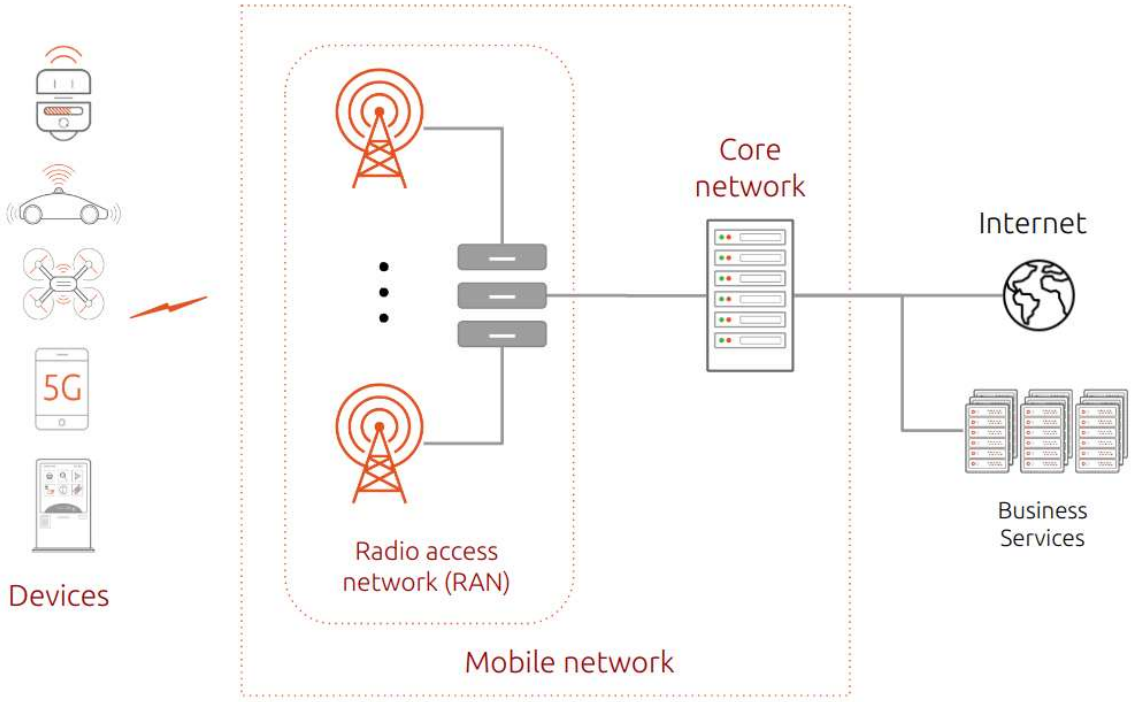
A biztonság és kiberbiztonság terén az 5G új kihívásokat is jelent. Míg a korábbi hálózatok (3G, 4G) elsősorban adatátviteli szerepet töltöttek be, az 5G sokkal szélesebb körű alkalmazási lehetőségei miatt a sebezhetőség is nő. A kiberbűnözők számára a távközlési infrastruktúra vonzó célponttá válhat, hiszen nemzetbiztonsági és üzleti adatokhoz férhetnek hozzá. A mobilhálózatok rádióhullámok segítségével kommunikálnak, ami miatt könnyebben bemérhetők, lehallgathatók és akár megsemmisíthetők is.

A biztonsági szabványok és előírások kidolgozása során kulcsfontosságú a megfelelő célok meghatározása és a pontos végrehajtási folyamatok kidolgozása. A hibák elkerülése érdekében a szakértők már megfogalmazták azokat az alapelveket, amelyek bármely vezeték nélküli hálózat, így az 5G esetében is alkalmazhatók. Az ezekhez való következetes igazodás biztosíthatja a biztonsági célok hatékony elérését, hozzájárulva a technológia sikeres és biztonságos elterjedéséhez.

5G Architektúrája

Az 5G technológia hálózati architektúrája több fontos komponensből épül fel, amelyek kulcsszerepet játszanak a modern kommunikációban.

RAN (Rádiós hozzáférési hálózat): A RAN az a hálózati rész, amely a felhasználói eszközöket (pl. okostelefonokat, IoT eszközöket) összekapcsolja a bázisállomásokkal. Az 5G-ben az új rádiótechnológia (NR - New Radio) alkalmazása révén jelentősen javult a spektrumhatékonyság és az adatátviteli sebesség. [5]

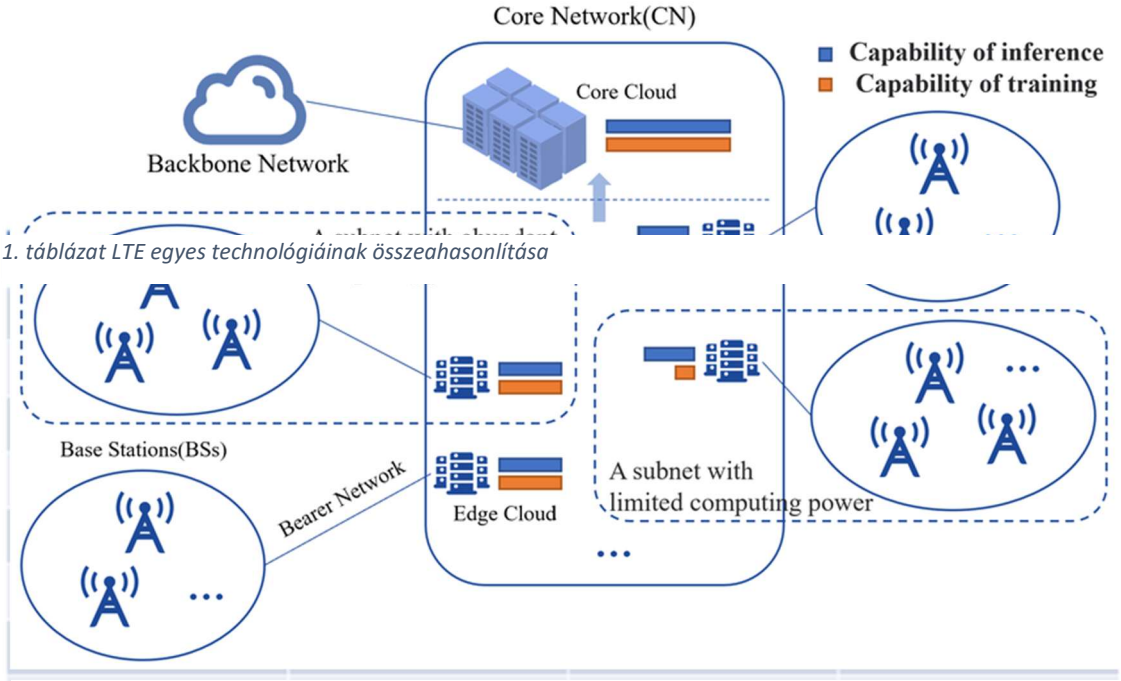


10. ábra 5G Hálózat architektúrája, adatáramlása

OFDM (Ortogonal Frequency Division Multiplexing): Az OFDM egy hatékony modulációs technika, melyet az 5G hálózatok széles körben alkalmaznak. Az OFDM lehetővé teszi a nagy adatsebességű átvitel fenntartását még interferenciás környezetben is, ami kritikus fontosságú a modern vezeték nélküli kommunikációban. [6]

QAM (Quadrature Amplitude Modulation): A QAM egy fejlett modulációs eljárás, amely az amplitúdó és a fázismoduláció kombinációját alkalmazza. Az 5G hálózatokban a magasabb szintű QAM (pl. 256-QAM) lehetővé teszi a nagyobb adatátviteli sebességet az adott sávszélességen belül. [7]

Core Network (Maghálózat): Ez a hálózat felelős az adatok irányításáért, kezeléséért és továbbításáért. Az 5G maghálózat felépítése modulárisabb és virtualizáltabb, lehetővé téve az alacsony késleltetést és a megbízható kapcsolatokat, amelyeket például önvezető járművek vagy ipari automatizálási rendszerek igényelnek. [8]

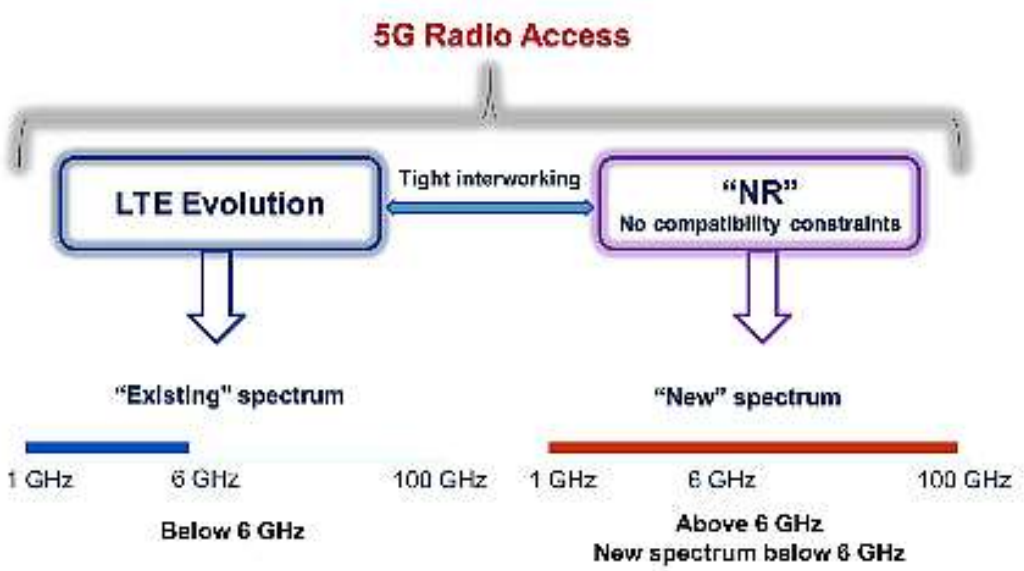


1. táblázat LTE egyes technológiáinak összeahasonlítása

11. ábra Számítási kapacitások eloszlása az 5G hálózatban

LTE-A (Long Term Evolution-Advanced): Az LTE-A az LTE továbbfejlesztett változata, amely nagyobb adatátviteli sebességet és jobb spektrumhatékonyságot biztosít. Az 5G rendszerekben az LTE-A technológia továbbra is fontos szerepet játszik a hibrid hálózati megoldásokban.

NR (New Radio): Az 5G NR az új generációs rádiótechnológia, amely az előző generációs megoldásokhoz képest szélesebb spektrumot és fejlettebb multiplexálási technikákat alkalmaz. Ez biztosítja a nagyobb adatátviteli sebességet és az alacsonyabb késleltetést.



12. ábra 5G Hozzáférés: Az LTE evolúciója és az új rádió (NR)

Mobilgyártók szerepe a mobilhálózatok fejlesztésében

- Nokia

  A Nokia az 1980-as évek elején kezdte meg mobilkommunikációs fejlesztéseit, és azóta kulcsszereplővé vált a mobilhálózatok evolúciójában. A cég úttörő szerepet játszott a GSM (Global System for Mobile Communications) szabvány kidolgozásában és elterjesztésében, amely az első digitális mobilhálózati szabványként forradalmasította a mobilkommunikációt.

  A Nokia egyik legnagyobb hozzájárulása a GSM technológia fejlesztése volt. A GSM egy nyílt, digitális mobilkommunikációs szabvány, amely lehetővé tette a globális roamingot és a széleskörű kompatibilitást a különböző gyártók eszközei között. A Nokia 1011, amely 1992-ben jelent meg, az egyik első kereskedelmi forgalomban kapható GSM telefon volt. A cég aktívan részt vett a GSM szabvány kidolgozásában, és számos innovációval járult hozzá annak sikeréhez.

  A 3G (UMTS) és a 4G (LTE) technológiák fejlesztésében a Nokia szintén vezető szerepet játszott. A 3G technológia lehetővé tette a gyorsabb adatátvitelt és új szolgáltatásokat, mint például a videohívás és a mobil internet. A 4G LTE technológia további előrelépést jelentett, még magasabb adatátviteli sebességet és alacsonyabb késleltetést biztosítva, ami új alkalmazások és szolgáltatások széles körét tette lehetővé.

A Nokia nem csak mobiltelefonok gyártásában jeleskedett, hanem jelentős szereplő volt a mobilhálózati infrastruktúra fejlesztésében is. A cég bázisállomásokat, hálózati berendezéseket és szoftvereket fejlesztett, amelyek a világ számos mobilhálózatának alapját képezték. A Nokia megoldásai hozzájárultak a hálózatok megbízhatóságának, kapacitásának és hatékonyságának növeléséhez.

A Nokia jelenleg is aktívan részt vesz az 5G technológia fejlesztésében, amely a következő generációs mobilhálózatok alapját képezi. Az 5G technológia célja, hogy még magasabb adatátviteli sebességeket, alacsonyabb késleltetést és nagyobb hálózati kapacitást biztosítson, támogatva az új és innovatív alkalmazásokat, mint például az IoT (Internet of Things), az önvezető autók és a virtuális valóság (VR). [9]

- Ericsson

Az Ericsson az 1876-ban alapított svéd telekommunikációs vállalat, amely azóta is vezető szerepet tölt be a mobilhálózatok fejlődésében. Az Ericsson úttörő szerepet játszott a különböző mobilhálózati generációk fejlesztésében és elterjesztésében, különösen a GSM, a 3G és a 4G technológiák terén.

Az Ericsson az egyik fő támogatója és fejlesztője volt a GSM technológiának. A cég aktívan részt vett a GSM szabvány kidolgozásában, amely az első digitális mobilhálózati szabványként forradalmasította a mobilkommunikációt. Az Ericsson bázisállomásai és hálózati berendezései világszerte elterjedtek, és jelentős mértékben hozzájárultak a GSM hálózatok kiépítéséhez és működtetéséhez.

Az Ericsson a 3G (UMTS) és a 4G (LTE) technológiák fejlesztésében is vezető szerepet játszott. A 3G technológia lehetővé tette a gyorsabb adatátvitelt és új szolgáltatásokat, mint például a videohívás és a mobil internet. Az Ericsson bázisállomásai és hálózati megoldásai hozzájárultak a 3G hálózatok globális elterjedéséhez. A 4G LTE technológia további előrelépést jelentett, még magasabb adatátviteli sebességet és alacsonyabb késleltetést biztosítva.

Az Ericsson a mobilhálózati infrastruktúra terén is vezető szereplő, számos innovációval járult hozzá a hálózatok hatékonyságának és megbízhatóságának növeléséhez. Az Ericsson által fejlesztett bázisállomások, hálózati berendezések és szoftverek világszerte elterjedtek, és a cég jelentős piaci részesedéssel rendelkezik a mobilhálózati berendezések piacán.

Az Ericsson jelenleg is aktívan részt vesz az 5G technológia fejlesztésében és elterjesztésében. Az 5G célja, hogy még magasabb adatátviteli sebességeket, alacsonyabb késleltetést és nagyobb hálózati kapacitást biztosítson, támogatva az új és innovatív alkalmazásokat, mint például az IoT, az önvezető autók és a virtuális valóság. Az Ericsson 5G megoldásai már számos országban elérhetők, és a cég aktívan részt vesz az 5G hálózatok kiépítésében. [10]

- Motorola

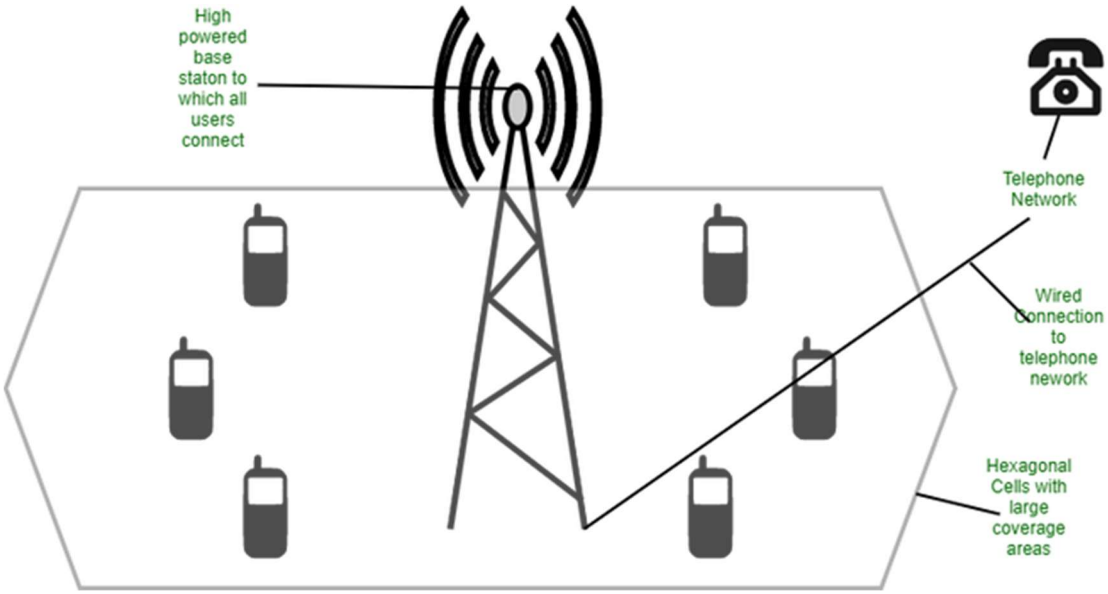
A Motorola az 1928-ban alapított amerikai telekommunikációs vállalat, amely az első kereskedelmi forgalomban elérhető mobiltelefont dobta piacra. A cég jelentős szerepet játszott az első generációs (1G) analóg mobilhálózatok fejlesztésében és a mobilkommunikáció forradalmasításában.

Első Mobiltelefon

A Motorola DynaTAC 8000X, amely 1983-ban jelent meg, az első kereskedelmi forgalomban elérhető mobiltelefon volt. Ez az esemény forradalmasította a mobilkommunikációt, és megalapozta a későbbi mobilhálózati fejlesztéseket. A DynaTAC 8000X 30 perces beszélgetési időt és 10 órás készenléti időt biztosított, és jelentős mérföldkő volt a mobiltelefonok fejlődésében.

AMPS Technológia

A Motorola az AMPS (Advanced Mobile Phone System) fejlesztésében is úttörő szerepet játszott. Az AMPS az első generációs (1G) analóg mobilhálózati szabvány volt, amelyet az 1980-as években vezettek be az Egyesült Államokban. Az AMPS lehetővé tette a széleskörű mobiltelefon-használatot, és megalapozta a későbbi digitális hálózati fejlesztéseket.



13. ábra Mobilhálózat felépítése

A Motorola a digitális mobilhálózatok, például a GSM és a CDMA (Code Division Multiple Access) fejlesztéséhez is jelentős mértékben hozzájárult. A cég által gyártott mobiltelefonok és hálózati eszközök széles körben elterjedtek, és hozzájárultak a mobilkommunikáció globális elterjedéséhez.

A Motorola nem csak mobiltelefonok gyártásában jeleskedett, hanem jelentős szereplő volt a mobilhálózati infrastruktúra fejlesztésében is. A cég bázisállomásokat, hálózati berendezéseket és szoftvereket fejlesztett, amelyek a világ számos mobilhálózatának alapját képezték. A Motorola megoldásai hozzájárultak a hálózatok megbízhatóságának, kapacitásának és hatékonyságának növeléséhez.

A Motorola jelenleg is aktívan részt vesz az 5G technológia fejlesztésében, amely a következő generációs mobilhálózatok alapját képezi. Az 5G technológia célja, hogy még magasabb adatátviteli sebességeket, alacsonyabb késleltetést és nagyobb hálózati kapacitást biztosítson, támogatva az új és innovatív alkalmazásokat, mint például az IoT, az önvezető autók és a virtuális valóság. [11]

6G Hálózat

A mobilkommunikációs technológiák fejlődése exponenciális ütemben zajlik. Noha az ötödik generációs hálózatok (5G) globális implementációja még kezdeti szakaszban van, a kutatás-fejlesztési erőfeszítések már a hatodik generációs (6G) technológia koncepciójának kidolgozására fókuszálnak. A 6G bevezetése paradigmaváltást ígér a kommunikáció és a digitális interakció terén, potenciálisan új dimenziókat nyitva a felhasználói élmény és az ipari alkalmazások számára. [12]

- 6G jelentősége

  A 6G jelenleg még a tervezési fázisban van, de a szakértők szerint jelentősen felülmúlja majd az 5G képességeit, és teljesen új alkalmazási lehetőségeket nyit meg. A 6G várhatóan 2030 körül lesz készen a kereskedelmi használatra. Addig még rengeteg kutatási és fejlesztési munka vár ránk.

- 6G jellemzői

  Kiemelkedően magas adatátviteli sebesség

  A 6G egyik legfontosabb újítása a rendkívül magas adatátviteli sebesség lesz. Míg az 5G elméletileg 20 Gbit/s-os csúcssebességet képes elérni, a 6G várhatóan akár 1 terabit/másodperc adatátviteli sebességet is lehetővé tesz. Az ilyen hatalmas sebességek teljesen új alkalmazásokat tennének lehetővé, például a valós idejű holografikus kommunikációt.

  Késleltetési idő minimalizálása

  A 6G várhatóan a késleltetés, azaz az adatátvitel késleltetése tekintetében is új szabványokat állít majd fel. A szakértők mindössze 0,1 milliszekundumos - gyakorlatilag azonnali - késleltetési időt várnak. Ez kulcsfontosságú az olyan alkalmazások számára, mint az autonóm vezetés vagy a kiterjesztett valóság, amelyek rendkívül gyors válaszidőt igényelnek.

  Kiterjesztett frekvenciasávok

  A kívánt teljesítmény eléréséhez a 6G várhatóan még az 5G-nél is magasabb frekvenciasávokat fog használni. A szakmai viták középpontjában a 100 GHz és 3 THz közötti, úgynevezett terahertzes tartomány áll. Ezek az extrém magas frekvenciák ugyan lehetővé teszik az adatátvitel jelentős növelését, de komoly technológiai kihívásokat is felvetnek, különösen a korlátozott hatótávolság és az akadályokon való áthatolás terén.

Mesterséges intelligencia integráció

A 6G másik központi eleme a mesterséges intelligencia átfogó integrációja lesz. A mesterséges intelligenciát nemcsak a hálózatok optimalizálására használják majd, hanem közvetlenül a kommunikációs infrastruktúrába is integrálják. Ez olyan önoptimalizáló és öngyógyító hálózatokat eredményezhet, amelyek automatikusan alkalmazkodnak a változásokhoz és zavarokhoz.

Energiahatékonyság

A 6G az energiahatékonyság jelentős javulását is ígéri. Ez fontos szempont, tekintettel a növekvő összeköttetések miatt növekvő energiaigényre. Itt olyan új technológiákat lehetne alkalmazni, mint az energiafüggetlen érzékelők. [12]

- A 6G lehetséges alkalmazásai

A 6G lehetséges alkalmazásai sokrétűek és egyesesetekben még nehezen elképzelhetőek. Néhány terület, ahol a 6G várhatóan jelentős hatást gyakorol majd, a következő:

Kiterjesztett és virtuális valóság

A 6G segítségével a magával ragadó AR- és VR-élmények soha nem látott minőségben és észrevehető késleltetés nélkül válhatnak lehetővé. Ez nemcsak a szórakoztatást forradalmasítaná, hanem új lehetőségeket kínálna az oktatásban és a képzésben is.

Internet Of Things eszközök

A 6G több milliárd eszköz és érzékelő hálózatba kapcsolását teszi majd lehetővé, ami környezetünk még nagyobb mértékű digitalizációjához vezet. Ez magában foglalja az intelligens otthonokat, a csatlakoztatott járműveket és az intelligens ipari megoldásokat.

Autonóm rendszerek

Az önvezető autók, drónok és robotok még biztonságosabbá és megbízhatóbbá válhatnak a 6G rendkívül alacsony késleltetési idejének és nagy adatátviteli sebességének köszönhetően. A valós idejű kommunikáció és a pontos vezérlés kulcsfontosságú lenne e technológiák biztonságos használatához.

Egészségügy

A telemedicina a 6G révén hatalmasat ugorhat előre, olyan lehetőségeket kínálva, mint a valós idejű távműtét vagy a folyamatos egészségügyi megfigyelés. A betegek bárhonnan első osztályú orvosi ellátásban részesülhetnének.

Intelligens városok

Az átfogó hálózatépítés és a valós idejű adatelemzés hatékonyabbá és élhetőbbé teheti a városokat. A közlekedési rendszerek, az energiaellátás és a közbiztonság a 6G segítségével optimalizálható lenne, és javíthatná a polgárok mindennapi életét.

Ipar 4.0

A gyártásban a 6G még inkább hálózatba kapcsolt és automatizált gyártási folyamatokhoz vezethet. A valós idejű felügyelet és ellenőrzés növelné a hatékonyságot és a termelés rugalmasságát.

- A 6G fejlesztésének kihívásai

A 6G-ben rejlő nagy lehetőségek ellenére vannak kihívások és megválaszolatlan kérdések is. Ezek a következők:

Technikai akadályok: A terahertzes tartományba szánt alkatrészek kifejlesztése és a kapcsolódó fizikai korlátok leküzdése komoly kihívást jelent.

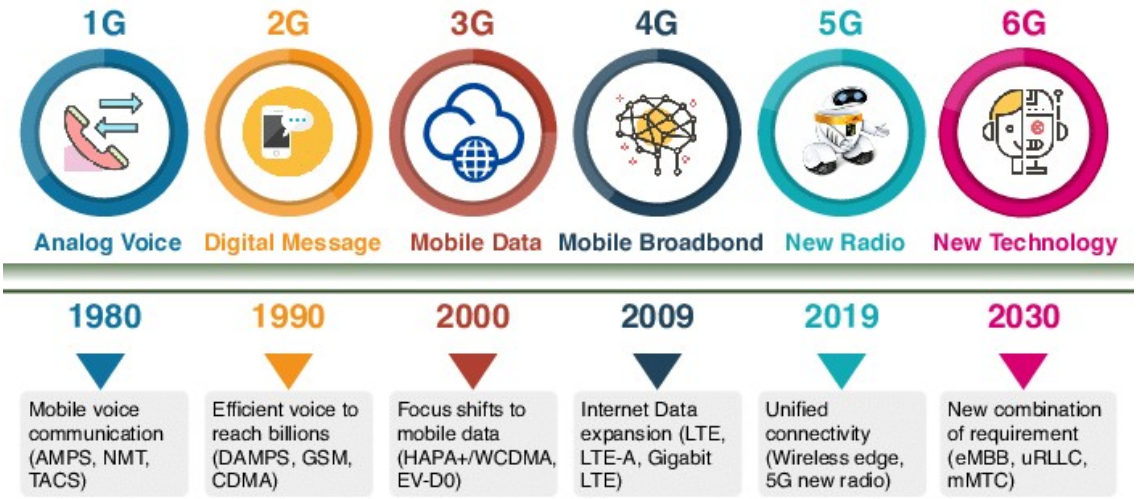
Infrastruktúra: A 6G-hez szükséges infrastruktúra kiépítése jelentős beruházásokat igényel.

Szabványosítás: Az átjárhatóság és a hatékonyság biztosítása érdekében globális szabványt kell kidolgozni a 6G-re.

Biztonság és adatvédelem: A hálózatépítés és az adatátvitel növekedésével a biztonsággal és az adatvédelemmel kapcsolatos követelmények is növekedni fognak.

Energiafogyasztás: A hatékonyság javulása ellenére a hálózatba kapcsolt készülékek tömeges növekedése miatt az általános energiaigény növekedhet.

Társadalmi hatás: A 6G által előidézett mélyreható változások etikai és társadalmi kérdéseket is felvetnek, amelyekkel foglalkozni kell.



14. ábra Egyes generációk megjelenése, fokuszálási területei

- 6G és az 5G közötti különbség

  A 6G nem csupán az 5G gyorsabb változata, hanem a mobiltechnológia alapvető újragondolása. Célja, hogy gyökeresen átalakítsa életünket, munkánkat és kommunikációnkat. Míg az 5G a sebességre és kapacitásra fókuszált, a 6G az intelligens hálózatokra, a szinte tökéletes csatlakoztathatóságra és a technológia zökkenőmentes, mindennapi integrációjára törekszik.

2. táblázat 5G és 6G összehasonlító táblázat

KPI	5G	6G
Peak data rate	20 Gb/s	1 Tb/s
Experienced data rate	0.1 Gb/s	1 Gb/s
Peak spectral efficiency	30 b/s/Hz	60 b/s/Hz
Experienced spectral efficiency	0.3 b/s/Hz	3 b/s/Hz
Maximum bandwidth	1 GHz	100 GHz
Area traffic capacity	10 Mb/s/m^2	1 Gb/s/m^2
Connection density	10^6 devices/km^2	10^7 devices/km^2
Energy efficiency	not specified	1 Tb/J
Latency	1 ms	100 μs
Reliability	$1\text{-}10^{-5}$	$1\text{-}10^{-9}$
Jitter	not specified	1 μs
Mobility	500 km/h	1000 km/h

- Fenntarthatóság és 6G

  A 6G másik fontos szempontja a fenntarthatóság. A digitalizációt és a hálózatépítést környezetbarát módon kell megtervezni, hogy az ökológiai lábnyom a lehető legkisebb legyen. Ez magában foglalja az energiahatékony technológiák használatát, az elektronikai hulladék mennyiségének csökkentését és az újrahasznosítási folyamatok előmozdítását. A 6G hozzájárulhat a fenntartható fejlődéshez azáltal, hogy támogatja az erőforrásokat hatékonyan felhasználó intelligens rendszereket.

- Etikai és társadalmi következmények

  A 6G bevezetésének etikai és társadalmi vonatkozásai is lesznek. A magánélet védelmével, a megfigyeléssel és a digitális szakadékkal kapcsolatos kérdéseket gondosan meg kell vizsgálni. Fontos, hogy a 6G-technológiák fejlesztése inkluzív és felelősségteljes legyen annak biztosítása érdekében, hogy az előnyök mindenki számára elérhetőek legyenek, és ne alakuljanak ki új egyenlőtlenségek. [12]

Záró gondolatok

Összességében elmondható, hogy a mobilhálózatok ma már vitathatatlanul az információs társadalom egyik legfontosabb, nélkülözhetetlen alapkövét jelentik. Funkciójuk messze túlmutat a puszta kommunikáción; a globális digitális infrastruktúra kritikus elemeiként szolgálnak, lehetővé téve az adatok gyors áramlását, a szolgáltatásokhoz való hozzáférést és az innováció számtalan formáját. Éppen ezért jövőbeli fejlődésük, az új generációs technológiák kutatása és bevezetése kulcsfontosságú stratégiai kérdés. Ez a fejlődés alapvető feltétele a globális összekapcsoltság további kiterjesztésének, a digitális szakadék csökkentésének, valamint elengedhetetlen motorja a digitális transzformáció folyamatának, amely átalakítja gazdaságunkat, társadalmunkat és mindennapi életünket. Így a mobilhálózatok evolúciója nem csupán technológiai kihívás, hanem a jövőbeli globális jólét és fejlődés egyik kulcsa.

Források

[1] A 2G-től az 5G-ig: így fejlődött a mobiltechnológia
https://www.yettel.hu/sajto/kozlemeny/25-ev-evfordulo [Letöltés dátuma: 2025.03.26]

[2] What is the difference between GSM, UMTS and LTE?
https://commsbrief.com/difference-between-gsm-umts-lte/ [Letöltés dátuma: 2025.03.26]

[3] Mi az 5G?
https://5g.hu/hu/mi-az-5g [Letöltés dátuma: 2025.04.02]

[4] 5G technology does not cause or spread coronavirus
https://www.unicef.org/montenegro/en/stories/5g-technology-does-not-cause-or-spread-coronavirus [Letöltés dátuma: 2025.04.07]

[5] What is 5G RAN?
https://www.supermicro.com/en/glossary/5g-ran [Letöltés dátuma: 2025.04.20]

[6] OFDM (Orthogonal frequency-division multiplexing)
https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing
[Letöltés dátuma: 2025.04.20]

[7] QAM (Quadrature Amplitude Modulation)
https://www.digi.com/resources/definitions/qam [Letöltés dátuma: 2025.04.20]

[8] 5G core network
https://www.ulakhaberlesme.com.tr/en/urun/5g-core-network/
[Letöltés dátuma: 2025.04.21]

[9] History of Nokia networks
https://news.networktigers.com/oem-outlook/a-history-of-nokia-networks/
[Letöltés dátuma: 2025.04.25]

[10] History of mobile internet
https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/mobile-miracles [Letöltés dátuma: 2025.04.27]

[11] Development of cellular systems
https://www.britannica.com/biography/Martin-Cooper [Letöltés dátuma: 2025.04.30]

[12] 6G technológia: A következő generáció kilátásai
https://webhosting.de/hu/6g-technologia-joevo-mobilkommunikacio/
[Letöltés dátuma: 2025.05.10]

2.16. Zero Trust biztonsági modell alkalmazása a CPS rendszerekben

IPAR 4.0 TECHNOLÓGIÁK

Zero Trust biztonsági modell alkalmazása a CPS rendszerekben

Mendler Attila
[redacted]

(GKNB_INTM087)
2024/2025/2

Tartalom

Bevezetés: 4
A Zero Trust alapjai 6
A Zero Trust (ZT) és a Zero Trust Architecture (ZTA) definíciója 6
A Zero Trust alapelvei és működése ipari környezetben 7
A Zero Trust alapelvei (2. ábra) 7
Zero Trust az ipari környezetben 9
Zero Trust bevezetése az ipari környezetbe (3. ábra) 10
A CPS rendszerek sajátosságai 11
Eszközdiverzitás: 11
Valós idejű adatforgalom 11
OT-IT konvergencia 11
SDP (Software-Defined Perimeter) szerepe a Zero Trust architektúrában 12
Az SDP előnye 12
Hogyan működik az SDP 13
Peremvédelmi biztonsági modell és a Zero Trust modell összehasonlítása 14
Peremvédelmi modell előnyök, hátrányok 14
Zero Trust modell előnyök hátrányok 15
ZTNA (Zero Trust Network Access) rendszerek gyakorlati alkalmazása ipari környezetben 16
Hogyan működik a ZTNA 16
Fő elvei az ipari környezetben 16
Milyen előnyei vannak 17
Példa a ZTNA implementációra 17
Hagyományos biztonsági architektúrák korlátai a kiber-fizikai rendszerekben 18
A Zero Trust megközelítés gyakorlati megvalósítása ipari környezetben 19
Identitás és hozzáféréskezelés (IAM) 19
Mikro-szegmentáció 20
Példák az ipari megvalósításra 20
AAA és Zero Trust ipari hálózatokban 20
Hogyan működik az AAA 21
AAA alkalmazása ipari hálózatokon 21
Viselkedésalapú kockázatelemzés és egyéb kiegészítő technológiák a Zero Trust támogatására 22
Viselkedésalapú kockázatelemzés 22
Ipari alkalmazása 23
Példák az ilyen technológiákra 23
Egyéb technológiák 23

Példák az ipari környezetekből ahol a Zero Trust modell már jelent van vagy bevezetése folyamatban van. 24
Siemens - Ipari automatizálásba való bevezetése 24
Rockwell Automation és Microsoft – ZT az ipari IoT (IIoT) hálózatokban 24
Bosch – Zero Trust a gyártás Digital Twin alapú irányításában 24
Szubjektív vélemény, összefoglaló 25
Források: 26

Bevezetés:

Ahogy az ipari technológia fejlődik, egyre több olyan rendszer jelenik meg, amelyben a fizikai gépek és a digitális megoldások szorosan együttműködnek. Ezeket a rendszereket kiber-fizikai rendszereknek (CPS – Cyber-Physical Systems) nevezzük. Ilyen például egy modern gyártósor, ahol szenzorok, vezérlők és különböző automatizált folyamatok valós időben kommunikálnak egymással és akár távolról is irányíthatók.

A mai ipari rendszerek gyakran kapcsolódnak az internethez, különböző felhőszolgáltatásokhoz és külső hálózatokhoz, ez pedig számos új biztonsági kihívást hoz magával. Az eddig megszokott biztonsági megközelítések – például a tűzfalakkal határolt, zárt rendszerek – már nem mindig elegendőek ahhoz, hogy megvédjék ezeket a hálózatokat a kibertámadásoktól. A támadók módszerei folyamatosan fejlődnek, és egyre gyakoribb, hogy nem a rendszer külső részét, hanem annak belső, megbízhatónak hitt részeit célozzák meg.

Ebben a környezetben vált egyre fontosabbá egy új biztonsági szemlélet: a **Zero Trust**, vagyis „nulla bizalom” elv. Ez a modell teljesen másképp közelíti meg a hálózati védelmet. Az elv apaja: soha ne bízz meg semmiben automatikusan – semmilyen eszközben, felhasználóban vagy hálózati kapcsolatban, még akkor sem, ha az a belső rendszer része. Minden hozzáférést ellenőrizni, hitelesíteni és naplózni kell, és a legkisebb szükséges jogosultság elve alapján kell működni.

A modell feltételezi, hogy a rendszerben már jelen lehet egy támadó, ezért minden egyes hozzáférési kérés hitelesítést és engedélyezést igényel. Az erőforrásokat (például adatok, számítási kapacitás és alkalmazások) csak azok számára teszi elérhetővé, akiknek valóban szükségük van rá. A folyamatos hitelesítés és engedélyezés révén a Zero Trust csökkenti a jogosulatlan hozzáférés és adatszivárgás kockázatát.

A szervezeteknek átfogó információbiztonsági és rugalmassági gyakorlatokat kell bevezetniük, hogy a Zero Trust hatékony legyen. Ha egyensúlyban van a meglévő kiberbiztonsági irányelvekkel és útmutatásokkal, identitás- és hozzáférés-kezelés, folyamatos felügyelet és legjobb gyakorlatok, amelyeket a ZTA a gyakori fenyegetések elleni védelmet nyújt, és egy kockázatkezelési megközelítés alkalmazásával javítja a szervezet biztonsági helyzetét.

Ebben az esszében azt fogom vizsgálni és bemutatni, hogyan lehet ezt a Zero Trust megközelítést alkalmazni az ipari környezetekben, különösen a kiber-fizikai rendszerek esetén. Bemutatásra kerülnek a modell alapelvei, az ipari rendszerek biztonsági kihívásai, valamint olyan konkrét technológiák is, mint a **ZTNA (Zero Trust Network Access)** és az **SDP (Software-Defined Perimeter)**, amelyek segítenek a gyakorlatban is megvalósítani ezt a elméletet.
Célja, hogy nemcsak elméleti hátteret nyújtson a témához, hanem gyakorlati szemlélet és áttekintést adjon.

1. ábra Az öt alapelv

Zero Trust Architecture: Strategies and Benefits | Gartner – alapján szerkesztve

A Zero Trust alapjai

A **Zero Trust** egy kiberbiztonsági paradigma (1. ábra), amely az erőforrások védelmére összpontosít, és azon az elven alapul, hogy a bizalmat soha nem adják meg automatikusan, hanem folyamatosan értékelni kell. A **Zero Trust Architecture (ZTA)** egy átfogó megközelítés a vállalati erőforrások és adatok védelmére, amely magában foglalja az identitáskezelést (személyes és nem személyes entitások), a hitelesítő adatokat, a hozzáférés-kezelést, a műveleteket, a végpontokat, a tárhelykörnyezeteket és az összekapcsoló infrastruktúrát.

A kezdeti fókusz az erőforrások korlátozásán van, hogy csak azok férjenek hozzá, akiknek valóban szükségük van rá, és csak a minimálisan szükséges jogosultságokat kapják meg (például olvasás, írás, törlés). Hagyományosan az ügynökségek és vállalati hálózatok a perimétervédelemre összpontosítottak, ahol a hitelesített felhasználók széles körű hozzáférést kaptak az erőforrásokhoz, miután beléptek a belső hálózatba. Ennek következtében a jogosulatlan oldalirányú mozgás a hálózaton belül az egyik legnagyobb kihívást jelentette a szövetségi ügynökségek számára.

A Zero Trust (ZT) és a Zero Trust Architecture (ZTA) definíciója

- A **Zero Trust (ZT)** modell egy olyan kiberbiztonsági megközelítés, amely minimalizálja a bizonytalanságot az információs rendszerek és szolgáltatások hozzáférési döntéseinek végrehajtásában, különösen egy feltételezetten kompromittált hálózat esetén.
- A **Zero Trust Architecture (ZTA)** egy vállalati kiberbiztonsági terv, amely a Zero Trust elveket alkalmazza, és magában foglalja az összetevők közötti kapcsolatokat, a munkafolyamatok tervezését és a hozzáférési szabályzatokat.

A Zero Trust megközelítés célja, hogy a Policy Decision Point (PDP) és a Policy Enforcement Point (PEP) közelebb kerüljön az erőforráshoz.[1]

Az alapja az, hogy minden alanyt, eszközt és munkafolyamatot egyértelműen hitelesíteni és engedélyezni kell, mielőtt hozzáférést kapnának a vállalati erőforrásokhoz. Ez biztosítja, hogy

minden hozzáférési kérelem szigorú ellenőrzésen menjen keresztül, minimalizálva a jogosulatlan hozzáférések és biztonsági kockázatok lehetőségét.[1]

A Zero Trust alapelvei és működése ipari környezetben

A Zero Trust alapelvei (2. ábra)

1. **Minden eszköz és szolgáltatás erőforrásnak számít[2]**

   Nem számít, hogy egy adatbázis, szenzor, felhőalapú szolgáltatás vagy akár egy dolgozó saját eszköze – ha kapcsolatba lép a hálózattal, akkor azt biztonsági szempontból „erőforrásként" kell kezelni. Minden ilyen elem potenciális célpont, ezért védeni kell.

2. **Minden kommunikáció biztonságos, függetlenül a hálózati helytől. [2]**

   A hálózati hely önmagában nem jelent bizalmat. A vállalat tulajdonában lévő hálózati infrastruktúrán található eszközök hozzáférési kérelmeinek ugyanazokat a biztonsági követelményeket kell teljesíteniük, mint bármely nem vállalati tulajdonú hálózatból érkező kérelmeknek. nem szabad automatikusan bizalmat adni egy eszköznek pusztán azért, mert az vállalati hálózaton található. Minden kommunikációnak a lehető legbiztonságosabb módon kell történnie, biztosítva az adatok bizalmasságát és integritását, valamint a forrás hitelesítését

3. **Az egyes vállalati erőforrásokhoz való hozzáférés munkamenetenként történik. [2]**

   A rendszer mindig ellenőrzi, hogy a kérelmező valóban megbízható-e, mielőtt hozzáférést kapna. A hozzáférést csak a legszükségesebb jogosultságokkal kell biztosítani a feladat elvégzéséhez. Ez azt jelenti, hogy az engedélyezés nem feltétlenül történik közvetlenül a munkamenet vagy tranzakció előtt, hanem egy korábbi ellenőrzés alapján is történhet. Fontos, hogy ha egy alany már hozzáférést kapott egy erőforráshoz, az nem jelenti azt, hogy automatikusan hozzáférhet más erőforrásokhoz is – minden hozzáférési kérelmet külön kell ellenőrizni és engedélyezni.

4. **A hozzáférésről mindig aktuális, dinamikus szabályok döntenek [2]**

   A rendszer nemcsak azt nézi, hogy ki kér hozzáférést, hanem azt is, hogy milyen eszközről, mikor, honnan, milyen állapotban. Ha például egy laptopon elavult szoftver fut vagy gyanús viselkedést mutat, lehet, hogy megtagadják a hozzáférést.

5. **A rendszer folyamatosan figyeli az eszközöket és azok biztonsági állapotát[2]**

   Egyetlen eszköz sem tekinthető automatikusan megbízhatónak. A vállalat minden erőforrás-kérés esetén értékeli az eszköz biztonsági állapotát.

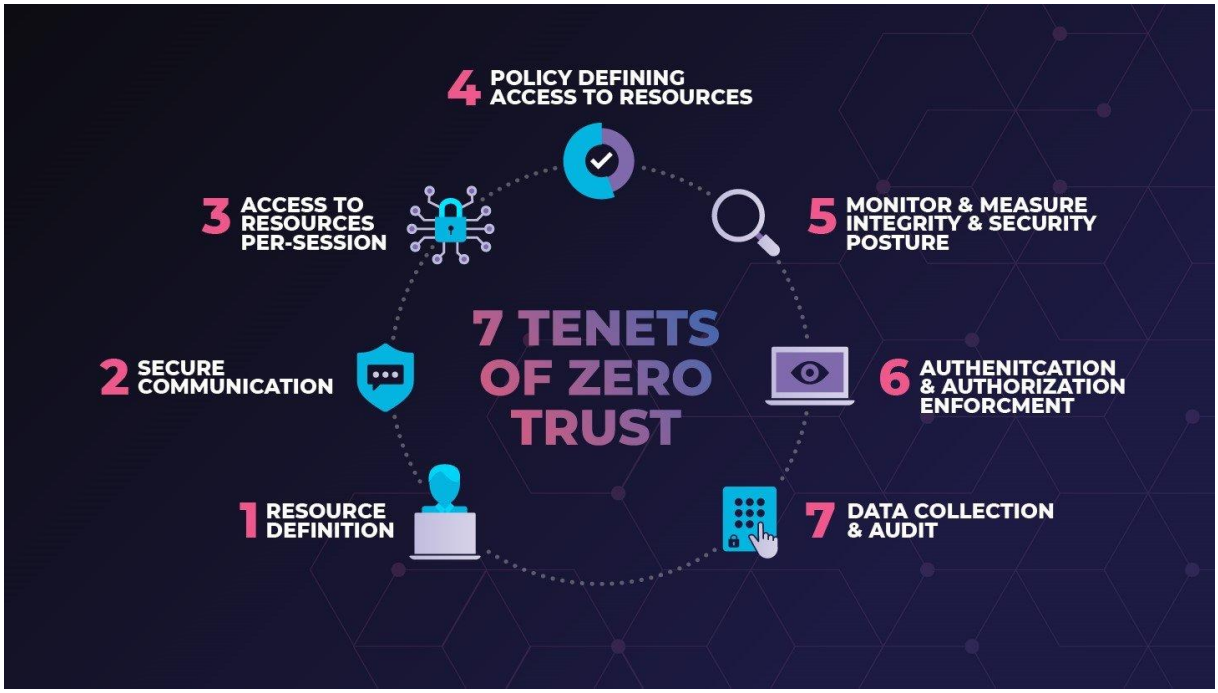
   A Zero Trust Architecture (ZTA) megvalósításához a vállalatnak folyamatos diagnosztikai és kockázatcsökkentő rendszert (CDM) kell létrehoznia, amely figyeli az eszközök és alkalmazások állapotát, és szükség esetén biztonsági frissítéseket alkalmaz. Azokat az eszközöket, amelyek kompromittálódhatnak, ismert sebezhetőségekkel rendelkeznek, vagy nem a vállalat által kezelt eszközök, eltérően kell kezelni. Ez akár azt is jelentheti, hogy teljesen megtagadják a hozzáférést a vállalati erőforrásokhoz.

6. **A hitelesítés és engedélyezés nem egyszeri esemény, hanem folyamat[2]**

   A rendszer nemcsak a belépéskor kér jelszót vagy más hitelesítést, hanem folyamatosan ellenőrzi a felhasználói viselkedést, és szükség esetén újra hitelesítést kér. Ez segít kiszűrni a szokatlan vagy veszélyes aktivitásokat, még időben.

7. **A szervezet mindent naplóz, elemez és ebből fejleszti a védelmet[2]**

   Minél több adat áll rendelkezésre arról, hogy mi történik a hálózatban – például ki mire kért hozzáférést, hogyan használja az eszközt, milyen forgalmat generál –, annál jobban lehet javítani a biztonsági szabályokat. A tanulás és alkalmazkodás a Zero Trust egyik kulcseleme.



2. ábra Zero Trust 7 alapelve

The 7 Tenets of Zero Trust

Zero Trust az ipari környezetben

Az ipari rendszerek (pl. gyártósorok, vezérlőegységek, IoT-eszközök) biztonsági igényei több ponton eltérnek a klasszikus IT környezettől. Itt nemcsak adatokat kell védeni, hanem valós fizikai folyamatokat is, így a támadások akár a működést is megzavarhatják, gépleállást vagy akár balesetet is okozhatnak, ami hatalmas következményekkel járhat.

A Zero Trust modell ipari környezetben való alkalmazása különösen fontos mert:

- A valós idejű kommunikáció kiemelt szerepet kap (pl. érzékelők és vezérlők között
- A hálózatban használt eszközök nagy száma és változatossága (pl. PLC-k, SCADA rendszerek, ipari IoT) megnehezíti az egységes biztonsági felügyeletet.
- A távmenedzsment és a felhőalapú integrációk új támadási felületeket hoznak létre

A **ZT** itt úgy működik, hogy minden ipari komponens – legyen az egy PLC vezérlő vagy egy felhasználói fiók – csak akkor és csak annyi ideig férhet hozzá egy másik rendszerhez, amennyire feltétlenül szükséges. Ezek mellett az ipari rendszerekre szabott hitelesítési módszerek, jogosultságok és felügyeleti eszközök is bevezethetők.

Ilyen például:

- Eszközazonosítás és -hitelesítés
- Felhőhöz való biztonságos csatlakozás szabályozása
- Adatforgalom titkosítása és ellenőrzése
- Viselkedéselemzés a rendellenes működés felismerésére

Zero Trust bevezetése az ipari környezetbe (3. ábra)

1. Részletes eszköz- és felhasználó-nyilvántartás létrehozása
2. Az erőforrások és folyamatok feltérképezése – kinek mire van szüksége?
3. Hitelesítési és hozzáférési szabályok bevezetése – például többfaktoros azonosítás, időalapú hozzáférés
4. Mikroszegmentációs stratégia kialakítása – hogy egy kompromittált rész ne veszélyeztesse az egész rendszert
5. Folyamatos monitorozás, naplózás és viselkedéselemzés – korai észlelés érdekében

3. ábra A Zero Trust bevezetése az ipari környezetbe – saját szerkesztés

A CPS rendszerek sajátosságai

A kiber-fizikai rendszerek (Cyber-Physical Systems, CPS) különlegessége abban rejlik, hogy a fizikai világ folyamatai – például gépek mozgása, szenzoradatok vagy aktuátorok vezérlése – közvetlen kapcsolatban állnak a digitális vezérlőrendszerekkel. Ez a szoros kapcsolat számos technológiai kihívást és biztonsági kérdést is felvet.

Eszközdiverzitás:

A CPS rendszerekben nagyon sok eszköz működik együtt: szenzorok, ipari vezérlők (PLC-k), IoT eszközök, robotkarok, edge számítási egységek, valamint klasszikus IT infrastruktúra-elemek, mint szerverek vagy hálózati eszközök. Ezek az eszközök különböző gyártóktól származnak, eltérő protokollokat használnak, és gyakran más-más frissítési vagy biztonsági lehetőségekkel rendelkeznek. Ez a sokféleség megnehezíti az egységes biztonsági szabályok bevezetését.

Valós idejű adatforgalom

A CPS rendszerek működése nagyon gyors reakcióidőt igényel. Egyes döntéseknek másodpercek, ezredmásodpercek alatt kell megtörténniük. Ez azt jelenti, hogy a hagyományos biztonsági megoldások – amelyek esetleg késleltetést vagy megszakítást okoznának – nem alkalmazhatók egy az egyben. A biztonságot úgy kell beépíteni, hogy az ne zavarja meg a valós idejű működést.

OT-IT konvergencia

Korábban az ipari (OT – Operational Technology) és informatikai (IT – Information Technology) rendszerek elkülönülten működtek. Az utóbbi években azonban ezek a rendszerek egyre inkább összekapcsolódnak: az OT rendszerek is adatot küldenek a felhőbe, távoli elérést biztosítanak karbantartók számára, vagy automatizált riportokat generálnak IT alapú rendszerek felé. Ez a konvergencia rengeteg új támadási felületet nyit meg, hiszen olyan hálózatok és eszközök kapcsolódnak össze, amelyek eredetileg nem erre lettek tervezve.

SDP (Software-Defined Perimeter) szerepe a Zero Trust architektúrában

Az SDP (ZT) biztonság megvalósításának egyik módja. A felhasználókat és az eszközöket is ellenőrizni kell, mielőtt csatlakozhatnának, és csak a minimális hálózati hozzáféréssel rendelkeznek, amire szükségük van. A Software-Defined Perimeter dinamikusan szabályozza, hogy ki és mikor férhet hozzá egy adott erőforráshoz. Az egyik legfontosabb jellemzője, hogy a hozzáférési jogosultságokat nem statikus, IP-alapú szabályok alapján határozza meg, hanem valós idejű kontextus, például a felhasználó identitása, eszközállapota, helyzete vagy viselkedési mintázatai alapján. Emiatt nagyon jól tudják alkalmazni a Zero Trust modell elvéhez.

Az egyik fő előnye, hogy elrejti a szolgáltatásokat az interneten, így azokat nem tudják megtámadni. Ez azt jelenti, hogy az erőforrások csak akkor válnak láthatóvá amikor a felhasználó sikeresen tudta magát hitelesíteni, jogosultságot kapott. Ezáltal nagyon sok fajta támadási formát ki lehet védeni (pl. Port scan, Brute force, DoS).

Az SDP implementációk általában több biztonsági technológiát integrálnak, mint például (TLS, VPN). Ezek mind hozzájárulnak ahhoz, hogy az SDP ne csak izolálja a hálózatot, hanem rugalmasan tudja alkalmazni a Zero Trust alapelveit az egyes hozzáférési kérelmekre.

Az SDP előnye

A Zero Trust szabályzattal rendelkező SDP fő előnye, hogy megfelelő hitelesítés nélkül blokkolja a belső hálózati erőforrásokhoz való hozzáférési kísérleteket. Ezen kívül az SDP-k kiegészíthetik a VPN-eket azáltal, hogy további védelmi réteget adnak a VPN-ekhez. A nulla bizalom hozzáadása ehhez a modellhez biztosítja, hogy az SDP teljesen biztonságos és áthatolhatatlan akadályt képezzen az illetéktelen hozzáférési kísérletek ellen.[3]

Hogyan működik az SDP

1. **Felhasználói identitások ellenőrzése**.

   Ez hagyományos felhasználói azonosítóval és jelszóval történő hitelesítéssel tehető meg. A többtényezős hitelesítés azonban további kihívásokat is megvalósíthat a hozzáférési kísérletek számára.[3]

2. **Eszköz ellenőrzése és ellenőrzése**.

   Az SDP (4. ábra) megvizsgálja a kérelmező eszközt is, hogy megbizonyosodjon arról, hogy a szoftvere megfelelő szinten van-e, nincs-e jelen rosszindulatú program, és egyéb vizsgálatokat végez. A hozzáférés további korlátozása érdekében kidolgozható a jogosulatlan eszközök listája.[3]

3. **SDP vezérlő és átjáró.**

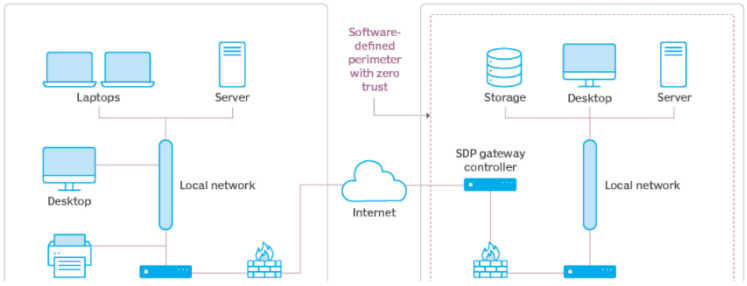
   Az SDP-vezérlő (4. ábra) kezeli a szervezet által létrehozott összes hitelesítési tevékenységet. A kérés jóváhagyása után a rendszer egy belső SDP-átjáróhoz irányítja a felhasználót, amely létrehozza a tényleges kapcsolatot.[3]

4. **Biztonságos hálózati kapcsolat.**

   A fenti lépések végrehajtása után az SDP-átjáró egyedi, biztonságos hálózati kapcsolatot létesít a kérelmező felhasználóval, majd azokkal a szolgáltatásokkal, amelyek használatára jogosult.[3]

5. **Felhasználói hozzáférés titkosított kapcsolathoz.**

   Miután az SDP-átjáró létrehozta a titkosított kapcsolatot a felhasználó és a kért erőforrások között, a felhasználó hozzáfér a jóváhagyott szolgáltatásokhoz.[3]



4. ábra SDP hálózat nulla bizalommal

How zero-trust SDP can work with a VPN for remote work | TechTarget

Peremvédelmi biztonsági modell és a Zero Trust modell összehasonlítása

Szempont	Peremvédelmi modell	Zero Trust modell
Fő elv	A belső hálózat megbízható, a külső nem	Nincs implicit bizalom: minden hozzáférés gyanús
Biztonsági határ	Fizikai vagy logikai tűzfal belső vs. külső	Dinamikus, felhasználó- és eszközalapú, folyamatos hitelesítéssel
Alkalmazási környezet	Klasszikus irodai hálózat, zárt infrastruktúra	Felhőalapú rendszerek, távmunka, mobil eszközök, CPS/IoT

1. táblázat Összehasonlítás – saját szerkesztés

Peremvédelmi modell előnyök, hátrányok

Előnyök:

- Egyszerű megvalósítás kisebb, jól körülhatárolt rendszerekben
- Alacsony komplexitás
- Régóta használt, jól dokumentált működés

Hátrányok:

- Feltételezi, hogy a belső hálózat biztonságos, könnyen kijátszható belső fenyegetésekkel
- Nehezen skálázható felhőalapú vagy elosztott rendszerekre
- Nem ad kellő kontrollt a felhasználói és eszközszintű hozzáféréshez
- Egy támadás után gyorsan terjedhet a támadó a hálózaton belül (5. ábra)

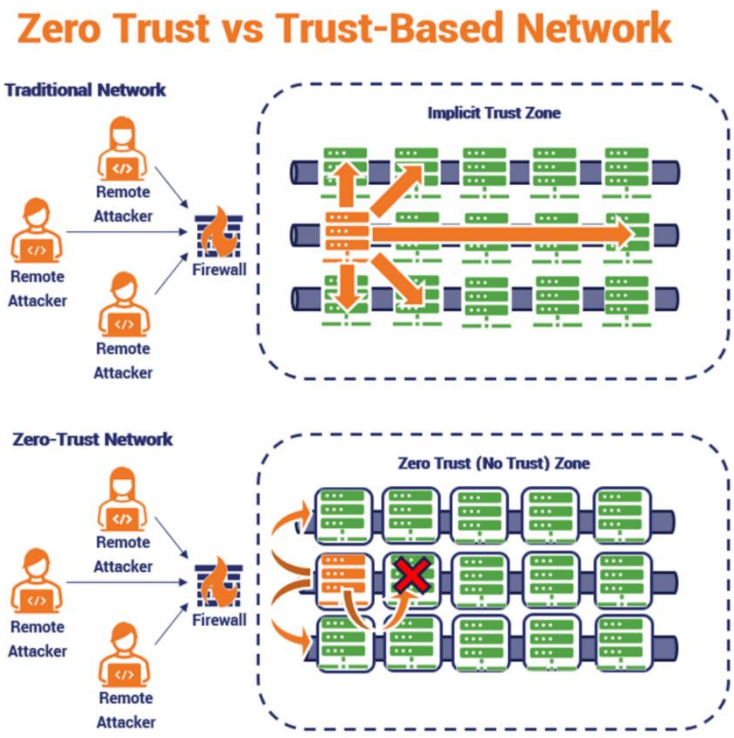
Zero Trust modell előnyök hátrányok

Előnyök:

- Minden hozzáférés folyamatos hitelesítést igényel
- Jobban kezelhető a távmunka és a felhőalapú környezet
- Minimalizálja a támadási felületet
- Alkalmas dinamikusan változó, diverz rendszerek (pl. CPS, IoT) védelmére

Hátrányok:

- Megvalósítása összetett, főleg régi rendszerek integrálásánál
- Magas kezdeti költségek (technológiai és szervezeti)
- Folyamatos karbantartást
- Ha rosszul konfigurálják, működési zavarokat okozhat



5. ábra Zero Trust vs.Trust-Based hálózat

[The Rise of Zero Trust: Threats Are No Longer Perimeter-Only Concerns - Hashed Out by The SSL Store™]

ZTNA (Zero Trust Network Access) rendszerek gyakorlati alkalmazása ipari környezetben

Hogyan működik a ZTNA

A ZTNA esetében a hozzáférés a felhasználó ZTNA szolgáltatásban való hitelesítése után jön létre. A ZTNA szolgáltatás ezután egy biztonságos, titkosított alagúton keresztül biztosítja a hozzáférést az alkalmazáshoz a felhasználó nevében. Ez további védelmi réteget biztosít a vállalati alkalmazások és szolgáltatások számára az egyébként nyilvánosan látható IP-címek védelmével.

A szoftveresen definiált szegélyekhez (SDP) hasonlóan a ZTNA is a sötét felhő koncepcióját használja, megakadályozva, hogy a felhasználók olyan alkalmazásokat és szolgáltatásokat lássanak, amelyekhez nincs hozzáférési engedélyük. Ez védelmet nyújt az oldalirányú támadó mozgása ellen, ahol a feltört végpont vagy hitelesítő adatok egyébként lehetővé tennék a vizsgálatot és a más szolgáltatásokra való kimutatást. [4]

Fő elvei az ipari környezetben

1. **Hitelesítés minden egyes kapcsolat előtt**
    - Minden felhasználó és eszköz erős hitelesítési folyamaton megy keresztül (6. ábra).
    - Leggyakrabban többfaktoros azonosítás (MFA) alkalmazása
2. **Legkisebb jogosultság**
    - Minden hozzáférés csak az adott feladatra vonatkozik, semmi másra nem
    - Jogosultságok dinamikusan módosulhatnak idő, hely, vagy rendszerállapot alapján.
    - Például: egy karbantartó csak a gép diagnosztikai adatait látja, nem fér hozzá a gyártásvezérlő szoftverhez.

3. **Naplózás és folyamatos felügyelet**
    - Minden kapcsolat, hitelesítés és tranzakció naplózásra kerül.
    - A naplókat automatikus rendszer (pl. SIEM) elemzi és figyeli

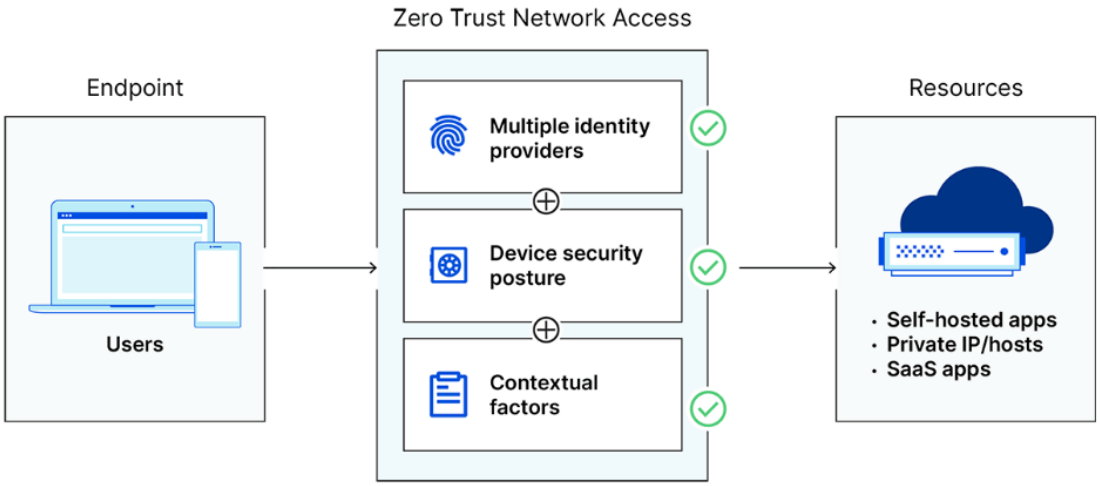
4. **Mikroperiméterek kialakítása**
    - A rendszer nem egyetlen nagyméretű hálózatot kezel, hanem több kisebb zónát ezeket hívjuk mikroperimétereknek
    - Ezek között szigorúan szabályozott és auditált kapcsolatok jönnek létre
    - Ha egy zóna sérül, a támadó nem fér hozzá automatikusan máshoz
5. **Környezeti tényezők alapján hozott döntések**
    - Hol van az eszköz?
    - Milyen időpontban próbál hozzáférni?
    - Milyen korábbi viselkedése volt?

Milyen előnyei vannak

- Adaptív, környezetfüggő hozzáférési szabályzatok
- Folyamatos felhasználói és eszközviselkedés-figyelés
- Gyors és biztonságos hozzáférés a felhő- és hálózati alkalmazásokhoz
- Egységes felügyelet
- Skálázható, egyszerű bevezetés

Példa a ZTNA implementációra

- Bejelentkezés a távvezérlő rendszerbe: A gépkezelő belép a vállalat tűzfalon kívüli laptopjáról → azonosítás MFA-val.
- ZTNA gateway megvizsgálja:
    - az eszköz típusát,
    - víruskereső meglétét,
    - az IP-címet, időpontot,
    - felhasználó szerepkörét.
- Kizárólag az adott gépsor vezérléséhez kap hozzáférést, másikhoz nem.
- A kapcsolat titkosított, naplózott, és ha a viselkedés szokatlan (pl. gyors parancssorozat vagy éjjeli hozzáférés), riasztás indul.



6. ábra A ZTNA működése

What is Zero Trust Network Access (ZTNA)? | Cloudflare

Hagyományos biztonsági architektúrák korlátai a kiber-fizikai rendszerekben

A kiber-fizikai rendszerek (CPS) biztonsága sokáig a hagyományos IT-biztonsági modellekre épült, ezek viszont sok esetben már nem felelnek meg az ipari környezetnek. A klasszikus peremvédelmi megközelítés abból indult ki, hogy a rendszer a belső hálózata megbízható, és csak külső fenyegetések ellen kell védekezni. Általában ez a modell tűzfalakra, VPN-ekre és zárt hálózatra támaszkodik. Azonban a CPS rendszerek több szempontból is kilógnak ebből a keretből.

1. **Fizikai és digitális világ összefonódása**

   A CPS-ben a szenzorok, vezérlők valós időben kommunikálnak egymással, miközben fizikai folyamatokat irányítanak. Ez azt jelenti, hogy egy kibertámadás fizikai következményekkel is járhat – például meghibásodhat egy gyártósor vagy megszakadhat egy szolgáltatás.

2. **Elavult rendszerek**

   Sok ipari rendszer évtizedes technológiákon alapul, amelyeket nem biztonságos hálózati környezetre terveztek. Nehéz frissíteni hiányzik a modern biztonsági funkció

3. **Zárt statikus hálózati modell**

   A hagyományos biztonsági modellek feltételezik, hogy a rendszer struktúrája nem változik, és kevés külső kapcsolódás történik. A mai ipari rendszerek egyre jobban integrálódnak a felhőbe és az internetbe, (pl. karbantartás céljából) emiatt új támadási felületet hoz létre.

4. **Korlátozott teljesítményű eszközök**

   A szenzorok, vezérlők és a beágyazott eszközök nagyon elavultak, alacsony memóriakapacitással rendelkeznek. Emiatt nem bírják el a hagyományos biztonságos szoftvereket.

5. **Hiányos hozzáférés-szabályozása**

   Ha valaki hozzáférést kap a hálózathoz akkor szinte mindenhez hozzáfér. Pl. a Zero Trust ezt küszöböli ki.

6. **Láthatóság és naplózás hiánya**

   A régi rendszerekben hiányzik a megfelelő naplózás, így ha történik egy esemény utólag nagyon nehéz visszakövetni vagy akár nem is lehet. Így egy támadást se lehet időben lereagálni.

Röviden: A hagyományos biztonsági modellek nem számolnak a CPS rendszerek összetett, elosztott és nyitott működésével. Emiatt van szükség a Zero Trust elvre.

A Zero Trust megközelítés gyakorlati megvalósítása ipari környezetben

A Zero Trust modell bevezetése az ipari környezetbe nagyon összetett feladat, mivel eltérő technológiákat és szabványokat alkalmazó eszközök vannak jelen. Hatékonyan megvalósítását több összehangolt elem alkalmazását igényli, az identitáskezelés, mikro szegmentáció és a folyamatos biztonsági megfigyelésig.

Identitás és hozzáféréskezelés (IAM)

A szervezeti erőforrásokhoz való biztonságos hozzáférés két részből áll: **Identitáskezelés és hozzáféréskezelés.** Az identitáskezelés összeveti a bejelentkezési kísérleteket egy identitáskezelési adatbázissal, amely minden olyan felhasználó folyamatos nyilvántartása,

akinek hozzáféréssel kell rendelkeznie. Ezt az információt folyamatosan frissíteni kell, amint a felhasználók csatlakoznak a szervezethez, vagy kilépnek a szervezetből, a szerepkörük és a projektjeik megváltoznak, és a szervezet hatóköre is változik. A fokozott biztonság érdekében számos szervezet megköveteli, hogy a felhasználók többtényezős hitelesítés **(MFA)**segítségével igazolják az identitásukat. A kétirányú ellenőrzésnek vagy kétfaktoros hitelesítésnek **(2FA)** is nevezett többtényezős hitelesítés biztonságosabb, mint ha csak felhasználónevet és jelszót használna. A bejelentkezési folyamathoz hozzáad egy olyan lépést, amelyben a felhasználónak egy másik ellenőrzési módszerrel is igazolnia kell a személyazonosságát. [5]

Mikro-szegmentáció

A ZT egyik legfontosabb elve, lényege, hogy a hálózatokat ne egy nagy bizalmi zónaként kezeljük. Az egyes eszközöket, szolgáltatásokat és adatfolyamokat egymástól elkülönítve kezeljük. Csökkentjük ezzel a támadási felületeket, ha a támadó bejut a rendszerbe nem tud szabadon mozogni, könnyebben lereagálható egy probléma.

Példák az ipari megvalósításra

Egy gyárban minden géphez külön hozzáférési jogosultág tartozik. Ha egy gép elavult szoftverrel rendelkezik ezáltal sebezhetőbb az IAM rendszer automatikusan korlátozza a hálózati kommunikációját. Minden kommunikáció naplózásra kerül, így minden visszakereshető, hogy melyik eszköz mikor és mire kapott hozzáférést.

AAA és Zero Trust ipari hálózatokban

Az AAA kritikus szerepet játszik a Zero Trust megvalósításában azáltal, hogy biztosítja, hogy minden hozzáférési kérés hitelesítve, engedélyezve és nyomon követve legyen. Ez a folyamatos ellenőrzési folyamat összhangban van a Zero Trust elvével, hozzájárulva a biztonságos hálózati környezet fenntartásához.

Hogyan működik az AAA

Az AAA modell szisztematikus folyamatot valósít meg a hálózathoz való hozzáférés vezérlésére és biztosítására

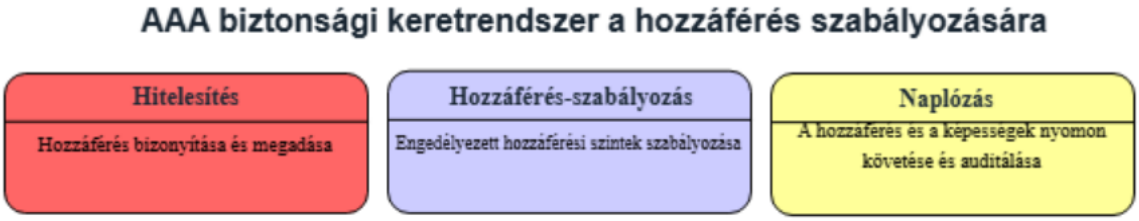
- **Hitelesítés**: A hitelesítés (7. ábra) az AAA modell első lépése. Ez magában foglalja a hálózati erőforráshoz hozzáférni próbáló felhasználó vagy eszköz identitásának ellenőrzését. Ez a folyamat különféle módszereket használ, például felhasználónévvel és jelszavakkal, digitális tanúsítványokkal, biometrikus adatokkal és intelligens kártyákkal.
- **Hozzáférés-szabályozás:** A felhasználó hitelesítése (7. ábra) után a következő lépés az engedélyezés. Ez a folyamat magában foglalja az adott hálózati erőforrásokhoz való hozzáférés engedélyezését vagy megtagadását a hitelesített identitás alapján. Lényegében beállítja a felhasználó identitásához vagy szerepköréhez társított engedélyeket és jogosultságokat.
- **Naplózás:** Az AAA modell utolsó lépése a naplózás (7. ábra). Ez magában foglalja a felhasználói tevékenységek nyomon követését és naplózását a hálózaton belül. A számlázási funkció lehetővé teszi a hálózati rendszergazdák számára, hogy naplót vezessenek a felhasználói műveletekről, ami hasznos lehet a hibaelhárításhoz, a használati trendek elemzéséhez és a biztonsági résre utaló szokatlan tevékenységek észleléséhez.

AAA alkalmazása ipari hálózatokon

Az AAA biztonsági modell számos felhasználási esetre vonatkozik, például a vállalati magánhálózat távoli elérésére, a vezeték nélküli hotspot használatára az internethez, és a hálózati szegmentálás kényszerítésére a Teljes felügyelet hálózati hozzáféréshez (ZTNA) – mindezt biztonsági okokból. A biztonsági csapatok megakadályozhatják a jogosulatlan hozzáférést a hálózati és erőforrás-hozzáférés, a jogosultságok és a felhasználói tevékenységek vezérlésével és láthatóságával.

A rendszer kliens/kiszolgáló modellt használ a hitelesítéshez és a protokoll futtatásához. Amikor egy eszköz hozzáférést kér, először egy ellenőrző pont megállítja, ahol meg kell adnia a hitelesítő adatait (pl. felhasználónév, jelszó, biometrikus azonosító vagy digitális tanúsítvány).

Ezután az AAA-kiszolgáló ellenőrzi, hogy ezek az adatok megegyeznek-e a tárolt információkkal. Ha sikeres a hitelesítés, a felhasználó megkapja az engedélyt a szükséges műveletek végrehajtására. A teljes munkamenet alatt minden tevékenység naplózásra kerül, hogy biztosítsák a biztonságot és az átláthatóságot.[6]



7. ábra AAA a Zero Trust-on belül
Data Security through Zero Trust and a Ransomware Strategy – alapján szerkesztve

Viselkedésalapú kockázatelemzés és egyéb kiegészítő technológiák a Zero Trust támogatására

Viselkedésalapú kockázatelemzés

Ez egy olyan technológia amelyik figyeli a felhasználók vagy az eszközök tevékenységeit (pl. belépési idő, fájlhasználat, hálózati forgalom).
Ha ettől eltérő eseményt tapasztal (pl. hirtelen új rendszerhez való hozzáférés, túl sok adattöltés akkor riasztást generál, blokkolhatja az adott műveletet, újabb hitelesítést kérhet (MFA).

Ipari alkalmazása

- Az operátorok nem szokványos műveleteinek észlelésében,
- A gyártóeszközök közötti szokatlan hálózati forgalom kiszűrésében,
- Egy esetleges kompromittált IoT eszköz viselkedésének felismerésében,
- A támadások automatikus blokkolásában az üzemi folyamatok megszakítása nélkül.

Technológia	Funkció	Zero Trust támogatása
UEBA (User and Entity Behavior Analytics)	Felhasználói és eszközviselkedés monitorozása	Gyanús eltérések észlelése és reagálás
SIEM (Security Information and Event Management)	Központi naplógyűjtés és elemzés	Incidensek és mintázatok korai felismerése
SOAR (Security Orchestration, Automation and Response)	Automatikus válaszreakciók	Gyors reakció biztonsági eseményekre
EDR/XDR (Endpoint/Extended Detection and Response)	Végponti eszközök viselkedésének nyomon követése	Részletes betekintés a támadási láncba, automatizált blokkolás

2. táblázat Példák a technológiákra – saját szerkesztés

Példák az ilyen technológiákra

Egyéb technológiák

- **Deception technikák:** Szándékosan elhelyezett „csali” rendszerek vagy fájlok, amelyekbe ha belépnek, gyanús tevékenységnek számítanak. [7]
- **AI/ML alapú döntéstámogatás:** Gépi tanulás használata viselkedésminták elemzéséhez, predikciókhoz
- **Threat Intelligence (fenyegetési hírszerzés):** Aktuális kockázati adatok integrálása a hozzáférési döntésekbe (pl. ismert IP-címek tiltása) [8]

Példák az ipari környezetekből ahol a Zero Trust modell már jelent van vagy bevezetése folyamatban van.

Siemens - Ipari automatizálásba való bevezetése

A siemens egy óriási német vállalat, amely az ipari automatizálással, épületautomatizálás, vasúti közlekedés és egészségügyi technológia területén tevékenykedik. A vállalat a saját gyártóüzemeibe fokozatosan vezette be a mikro-szegmentációt, az identitásalapú hozzáféréskezelést valamint a távoli hozzáférések kizárólagos engedélyezését erős hitelesítéssel. Rendelkeznek egy saját fejlesztési platformmal (MindSphere) amelyre olyan biztonsági architektúra épül amely nem engedi meg a feltételezett bizalmat.

Főbb megoldások

- Szigorúan szabályozott hozzáférés IP-alapú helyett identitásalapon
- Erős multifaktoros hitelesítés a mérnöki terminálokhoz
- Mikroszegmentált hálózati topológiák

Rockwell Automation és Microsoft – ZT az ipari IoT (IIoT) hálózatokban

Rockwell Automation és a Microsoft együttműködésében fejlesztett ipari biztonsági megoldások kifejezetten a Zero Trust elveire épülnek. Célja a gyártósori rendszerek és a felhőalapú szolgáltatások közti biztonságos kapcsolat megteremtése volt, folyamatos hitelesítéssel, titkosított csatornákon keresztül.[9]

Bevezetett technológiák:

- Azure Active Directory-alapú identitáskezelés
- Zero Trust Network Access (ZTNA)
- Viselkedéselemzés és automatizált fenyegetésészlelés (UEBA)

Bosch – Zero Trust a gyártás Digital Twin alapú irányításában

A Bosch ipari környezeteiben digitális iker (Digital Twin) rendszereket alkalmaz, amelyekhez különösen érzékeny adatforgalom és távoli elérés szükséges. A Zero Trust segít a szolgáltatások láthatatlanná tételében és a belépési pontok dinamikus szabályozásában.

Bevezetett technológiák:

- SDP-alapú szolgáltatás-hozzáférés (Software Defined Perimeter)
- A hozzáférések naplózása és viselkedésalapú elemzése
- Kizárólagos eszközalapú engedélyezés, például MAC- és firmware-azonosító szerint

Szubjektív vélemény, összefoglaló

Véleményem szerint a Zero Trust egy nagyon jó technológiai irányzat, ami által az ipari rendszereket egy teljesen más megközelítésből figyelhetjük meg. Magasabb biztonságot nyújthat nagyon sok vállalatnak főleg a mai világban, ahol egyre nagyobb kihívás a támadásokkal szembeni védelem. Természetesen nagyon költséges ennek kiépítése és megvalósítása is körülményes, de hosszútávon kifizetődőbb és jobb megoldásokat kínál a régiekeszemben. Remélem, hogy a jövőre nézve hasznos lesz a vállalatok és a társadalom számára.

Források:

[1] National Institute of Standards and Technology (NIST), "Zero Trust Architecture," NIST SP 800-207, 2020. Available: Zero Trust Architecture. (Elérés: 2025. május 14.)

[2] Gartner, "Zero Trust Architecture: Strategies and Benefits," Available: Zero Trust Architecture: Strategies and Benefits | Gartner (Elérés: 2025. május 14.)

[3] TechTarget, "How zero-trust SDP can work with a VPN for remote work," Available: How zero-trust SDP can work with a VPN for remote work | TechTarget. (Elérés: 2025. május 14.)

[4] Palo Alto Networks, "What is Zero Trust Network Access (ZTNA)?," Available: What Is Zero Trust Network Access (ZTNA) - Palo Alto Networks. (Elérés: 2025. május 14.)

[5] Microsoft, „Mi az identitás- és hozzáféréskezelés?," Available: Mi az identitás- és hozzáféréskezelés (IAM)? | Microsoft Biztonság. (Elérés: 2025. május 14.)

[6] Portnox, "AAA Model: Authentication, Authorization & Accounting," Available: What is AAA Security? Authentication, Authorization, and Accounting. (Elérés: 2025. május 14.)

[7] Fortinet, "What is Deception Technology?," Available: What is Deception Technology? Defined & Explained | Fortinet. (Elérés: 2025. május 14.)

[8] IBM, "What is Threat Intelligence?," Available: What is Threat Intelligence? | IBM (Elérés: 2025. május 14.)

[9] Microsoft, "How Rockwell Automation applies Zero Trust to industrial IoT," Available: Rockwell Automation | Microsoft Go-To-Market Services. (Elérés: 2025. május 14.)

2.17. Okosgyárak CPS rendszereinek fejlesztése mesterséges-intelligenciával MI-CPS rendszerek az Ipar 4.0 okosgyáraiban Innovatív megoldások és fejlesztési módszertanok a CPS-ek mesterséges intelligencia alapú integrációjára

Okosgyárak CPS rendszereinek fejlesztése mesterséges-intelligenciával

MI-CPS rendszerek az Ipar 4.0 okosgyáraiban

Innovatív megoldások és fejlesztési módszertanok a CPS-ek mesterséges intelligencia alapú integrációjára

Horváth Levente

Gazdasáinformatikus, horvath.levente0408@gmail.com

1 BEVEZETÉS

1.1 A téma háttere és jelentősége

A negyedik ipari forradalom (Ipar 4.0) egyik kulcsfontosságú eleme az okosgyárak megjelenése és elterjedése, amelyek alapvetően a kiber-fizikai rendszerekre épülnek. Az okosgyárak olyan termelési környezetet jelentenek, ahol az intelligens gépek, eszközök és rendszerek hálózatba kapcsolva, valós időben kommunikálnak és működnek együtt, lehetővé téve a termelési folyamatok optimalizálását és a magasabb fokú automatizálást. A kiber-fizikai rendszerek a fizikai és a digitális világ integrációját valósítják meg, összekapcsolva a szenzorokon és aktuátorokon keresztül a fizikai eszközöket a számítástechnikai és kommunikációs infrastruktúrával.

Az elmúlt években a mesterséges intelligencia technológiák fejlődése új lehetőségeket nyitott meg az okosgyárak CPS rendszereinek fejlesztésében. A gépi tanulás, deep learning, természetes nyelvfeldolgozás és egyéb mesterséges intelligencia módszerek alkalmazása jelentősen növelhetik a termelési rendszerek hatékonyságát, rugalmasságát és adaptációs képességét. A McKinsey Global Institute egyik jelentése szerint az MI-alapú gyártási megoldások bevezetése akár 20-30%-os termelékenységnövekedést és 10-20%-os minőségjavulást eredményezhet a hagyományos automatizált rendszerekhez képest.

A téma jelentőségét tovább növeli, hogy az okosgyárak és a mesterséges intelligencia alapú CPS rendszerek fejlesztése kulcsszerepet játszik a fenntartható gyártás és a körkörös gazdaság megvalósításában is. Az erőforrás-hatékonyság javítása, a hulladékcsökkentés és az energiafelhasználás optimalizálása olyan célok, amelyek elérésében a mesterséges intelligenciával támogatott kiber-fizikai rendszerek hatékony eszközöknek bizonyulnak.

1.2 A probléma megfogalmazása

Bár a mesterséges intelligencia és a kiber-fizikai rendszerek integrációja jelentős előnyöket jelenthetnek, számos kihívással és megoldatlan problémával szembesülünk ezen a területen. Az egyik alapvető probléma az okosgyárak CPS rendszereinek természete és komplexitása, amely megnehezíti az AI-alapú megoldások implementálását és skálázhatóságát. Különböző gyártóberendezések, kommunikációs protokollok és adatformátumok összehangolása komoly kihívást jelent a rendszertervezők számára.

További problémát jelent az adatok mennyisége, minősége és az adatokhoz való hozzáférés kérdése. A mesterséges intelligencia modellek hatékony működéséhez rengeteg, jó minőségű adatra van szükség, azonban a gyártási környezetben gyakran hiányosak vagy zajosak az adatok, illetve adatvédelmi és biztonsági szempontok korlátozhatják azok felhasználását.

A megbízhatóság és biztonság szintén kritikus kérdés a CPS rendszerek MI-alapú fejlesztésében. Az ipari környezetben működő rendszerekkel szemben rendkívül szigorúak a megbízhatósági követelmények, és a mesterséges intelligencia modellek „fekete doboz" jellege gyakran nehezíti ezeknek a követelményeknek a teljesítését és igazolását.

Az esszé során vizsgált központi kérdés: Hogyan lehet hatékonyan integrálni és alkalmazni bizonyos mesterséges intelligencia technológiákat az okosgyárak kiber-fizikai rendszereiben a termelési folyamatok optimalizálása, a rugalmasság növelése és a fenntarthatóság javítása érdekében, miközben kezelni tudjuk a komplexitással, adatminőséggel és megbízhatósággal kapcsolatos kihívásokat?

1.3 Az esszé célja és jelentősége

Az esszé elsődleges célja egy átfogó elméleti és gyakorlati bemutató kidolgozása, amely segítséget nyújt az okosgyárak CPS rendszereinek mesterséges intelligenciával történő fejlesztéséhez. A bemutató magába foglalja a szükséges technológiai komponensek azonosítását, az integrációs módszertanok meghatározását, valamint a hatékony implementációhoz szükséges stratégiai irányelvek kialakítását.

A esszé specifikus céljai:

1. A mesterséges intelligencia alapú kiber-fizikai rendszerek fejlesztésének és implementálásának jelenlegi állapotának feltérképezése a szakirodalomak áttekintésével.
2. A gyártási környezetekben alkalmazható MI-alapú integrációs módszerek és architektúrák elemzése és összehasonlítása, különös tekintettel a skálázhatóságra és adaptálhatóságra.
3. Az okosgyári környezetben keletkező adatok gyűjtésének, előkészítésének és felhasználásának optimalizálása a mesterséges intelligencia algoritmusok hatékonyságának növelése érdekében.
4. A megbízhatóság és biztonság javítására irányuló módszerek feltárása és értékelése az MI-alapú CPS rendszerekben.
5. Esettanulmányok segítségével gyakorlati ajánlások megfogalmazása az okosgyárak különböző méreteire és iparági sajátosságaira vonatkozóan.

A bemutató elméleti szempontból hozzájárul a kiber-fizikai rendszerek és a mesterséges intelligencia integrációjának mélyebb megértéséhez, új fogalmi kereteket és modelleket alkotva a terület fejlődéséhez. Gyakorlati szempontból pedig konkrét módszertanokat és eszközöket kínál a gyártóvállalatoknak, amelyek segítségével hatékonyan tudják bevezetni és alkalmazni az MI-alapú megoldásokat, ezáltal növelve versenyképességüket a mai digitális világban.

A bemutató társadalmi jelentősége is számottevő, hiszen az okosgyárak és az MI-alapú CPS rendszerek fejlesztése hozzájárulhat a fenntarthatóbb ipari termeléshez, az erőforrás-hatékonyság javításához és végső soron a környezeti terhelés csökkentéséhez.

1.4 A téma kérdései

Az esszé során az alábbi kérdésekre keresünk választ:

1. Hogyan optimalizálható az adatgyűjtés, -feldolgozás és -felhasználás az okosgyárak kiber-fizikai rendszereiben a mesterséges intelligencia algoritmusok teljesítményének maximalizálása érdekében?
2. Milyen módszerekkel növelhető az MI-alapú CPS rendszerek megbízhatósága és biztonsága ipari környezetben?
3. Hogyan mérhető és értékelhető a mesterséges intelligencia technológiák alkalmazásának hatása az okosgyárak teljesítményére, rugalmasságára és fenntarthatóságára?

2 CPS RENDSZEREK ALAPJAI OKOSGYÁRAKBAN

2.1 CPS rendszerek definíciója és elméleti háttere

A kiber-fizikai rendszerek (Cyber-Physical Systems, CPS) olyan intelligens rendszerek, amelyek integrálják a számítástechnikai és kommunikációs képességeket a fizikai folyamatok felügyeletére és irányítására. Definíció szerint a CPS „fizikai és szoftver komponensek integrációja, amelyek szorosan együttműködnek, és különböző térbeli és időbeli skálákon működnek" [1]. Az okosgyárakban a CPS rendszerek képezik az Ipar 4.0 egyik alappillérét, amely lehetővé teszi a fizikai eszközök és a digitális technológiák közötti hatékony kommunikációt.

A CPS rendszerek elméleti megalapozása a következő kulcsfontosságú koncepciókra épül:

- **Fizikai és digitális világ konvergenciája**: A CPS rendszerek elmossák a határvonalat a fizikai valóság és a digitális tér között, lehetővé téve, hogy a fizikai rendszerek adatai és állapota digitálisan monitorozható és irányítható legyen [2].
- **Beágyazott rendszerek evolúciója**: A CPS rendszerek a hagyományos beágyazott rendszerek továbbfejlesztéseként jöttek létre, amelyek már nemcsak lokális funkciókat látnak el, hanem hálózatba kapcsolva, komplex ipari környezetben működnek együtt [3].
- **Valós idejű reagálás és adaptív viselkedés**: A CPS rendszerek alapvető tulajdonsága a környezeti változásokra történő valós idejű reagálás és az ezekhez való alkalmazkodás [4].

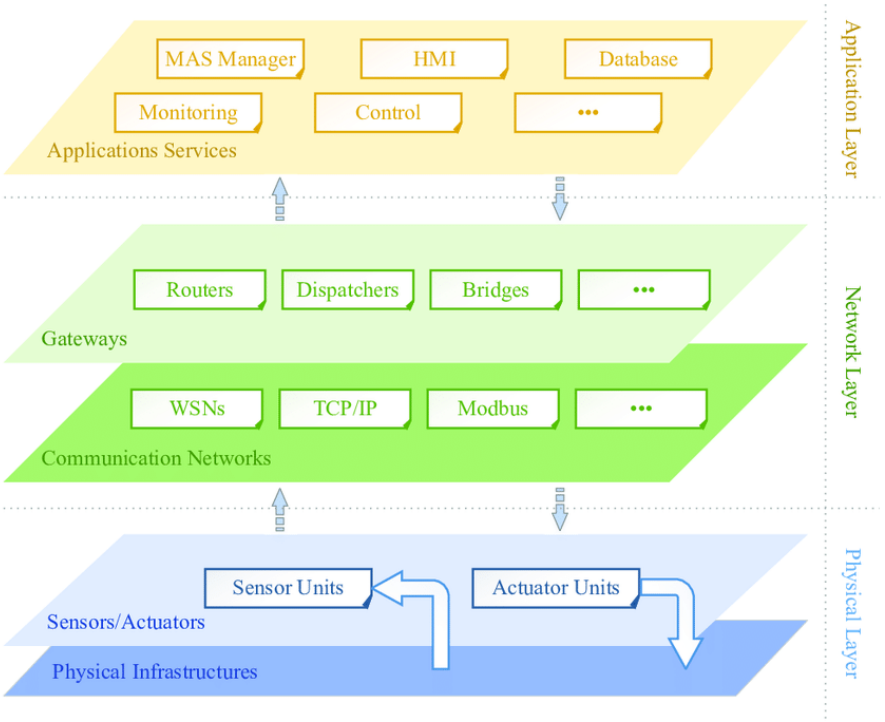
2.2 Technológiai komponensek és architektúra

A CPS rendszerek architektúrája általában három fő rétegre osztható (1. ábra):

- **Fizikai réteg**: Tartalmazza a szenzorokból, aktuátorokból, gyártóberendezésekből és egyéb fizikai eszközökből álló hálózatot. Ezek az eszközök adatokat gyűjtenek és hajtanak végre műveleteket a fizikai környezetben [5].
- **Kommunikációs réteg**: Biztosítja a fizikai és a kiber komponensek közötti adatátvitelt. Ez magában foglalja a különböző hálózati protokollokat (pl. OPC UA, MQTT, AMQP) és kommunikációs technológiákat (vezetékes és vezeték nélküli hálózatok, 5G, ipari Ethernet) [6].
- **Kiber réteg**: Felelős az adatok feldolgozásáért, elemzéséért és a döntéshozatalért. Ez tartalmazza a felhőalapú és peremszámítási (edge computing) megoldásokat, adatelemző algoritmusokat, digitális ikermodelleket és egyéb szoftveres komponenseket [7].

Az architektúra kiegészül horizontális és vertikális integrációs képességekkel:

- **Horizontális integráció**: A gyártási folyamat különböző állomásai, valamint az ellátási lánc szereplői közötti zökkenőmentes adatáramlás és együttműködés [8].
- **Vertikális integráció**: A vállalati hierarchia különböző szintjei (üzemi szint, irányítási szint, vállalati szint) közötti információáramlás biztosítása [8].



1.ábra: Kiberfizikai-rendszerek architektúrája, a Research Gate-n keresztül. (https://www.researchgate.net/figure/Architecture-of-a-cyber-physical-system_fig1_331600306)

2.3 CPS rendszerek jelenlegi alkalmazása a gyártási folyamatokban

Az okosgyárakban a CPS rendszerek már számos területen bizonyították hatékonyságukat:

- **Prediktív karbantartás**: Szenzoradatok folyamatos elemzésével a rendszer előre jelezheti a berendezések meghibásodását, így a karbantartás a tényleges állapot alapján, tervezetten végezhető el, minimalizálva az állásidőt. Egy németországi autóipari beszállító 25%-kal csökkentette a tervezett karbantartás költségeit CPS alapú prediktív karbantartási rendszer bevezetésével [9].
- **Gyártási folyamatok optimalizálása**: A CPS rendszerek valós idejű adatokat szolgáltatnak a gyártási folyamatokról, amely lehetővé teszi a paraméterek folyamatos finomhangolását az optimális minőség és hatékonyság érdekében. A Bosch Rexroth okosgyáraiban a gyártási hatékonyság 10-15%-kal növekedett a CPS rendszerek bevezetése után [10].
- **Rugalmas gyártási rendszerek**: A CPS rendszerek lehetővé teszik a gyártósorok gyors átkonfigurálását különböző termékváltozatok gyártására. A Siemens ambergi üzemében a magas szintű automatizálásnak és a CPS rendszereknek köszönhetően naponta akár 1000 termékváltozatot is képesek gyártani magas minőségben [11].
- **Digitális ikrek**: A fizikai eszközök és folyamatok valós idejű digitális reprezentációi, amelyek lehetővé teszik a szimulációt, tesztelést és optimalizálást virtuális környezetben. A GE Aviation motoralkatrészek fejlesztési ciklusát 50%-kal csökkentette digitális ikermodellek alkalmazásával [12].

2.4 Kulcsfontosságú funkcionaltások

2.4.1 Szuperhálózatok

A CPS rendszerek alapvető építőelemei a különböző típusú szenzorok, amelyek a fizikai környezetről gyűjtenek adatokat. Az okosgyárakban használt főbb szenzortípusok:

- **Hőmérséklet- és páratartalommérők**: A környezeti feltételek monitorozására.
- **Gyorsulásmérők és rezgésérzékelők**: Gépek állapotának figyelésére.
- **Nyomás- és áramlásérzékelők**: Pneumatikus és hidraulikus rendszerek ellenőrzésére.
- **Optikai és képfeldolgozó szenzorok**: Minőségellenőrzésre és folyamatfigyelésre.
- **RFID és vonalkód olvasók**: Anyagok és termékek nyomon követésére [13].

A korszerű szenzorok már wireless technológiával, alacsony energiafogyasztással és beépített előfeldolgozó képességekkel rendelkeznek, ami megkönnyíti integrációjukat a CPS rendszerekbe [14].

2.4.2 Adatgyűjtés

A CPS rendszerek hatalmas mennyiségű adatot generálnak, amelyek feldolgozása és tárolása komoly infrastruktúrát igényel:

- **Adatgyűjtési réteg:** Tartalmazza az adatgyűjtő modulokat (PLC-k, SCADA rendszerek, IoT gateway-ek), amelyek aggregálják a szenzoradatokat és előkészítik továbbításra [15].
- **Adattárolási megoldások:** Az adatok tárolása történhet lokálisan (edge computing), felhőben vagy hibrid megoldással. A választás függ a késleltetési-követelményektől és az adatbiztonsági előírásoktól [16].
- **Big Data technológiák:** A nagy adatmennyiség kezeléséhez speciális adattárolási és feldolgozási technológiák szükségesek (pl. NoSQL adatbázisok, Hadoop) [17].

2.4.3 Vezérlés

A CPS rendszerek nemcsak monitorozzák, hanem aktívan be is avatkoznak a fizikai folyamatokba:

- **Valós idejű szabályozás:** A szenzoradatok alapján a rendszer képes valós időben módosítani a gyártási paramétereket az optimális működés érdekében [18].
- **Autonóm döntéshozatal:** Fejlett CPS rendszerek képesek bizonyos előre definiált helyzetekben emberi beavatkozás nélkül döntéseket hozni és végrehajtani azokat [19].
- **Több szintű irányítási architektúra**: A vezérlési funkciók eloszthatók a helyi/edge, köd/fog és felhő/cloud szintek között, az adott alkalmazás késleltetési és biztonsági követelményeinek megfelelően [20].

2.5 Jelenlegi korlátok és kihívások, amelyeket az MI segíthet megoldani

A CPS rendszerek elterjedését és hatékonyságát több tényező is korlátozza, amelyek kezelésében a mesterséges intelligencia jelentős szerepet játszhat:

- **Heterogén rendszerek integrációja:** A különböző gyártók eszközei és a régebbi berendezések integrálása gyakran problémás. Az MI alapú adaptív interfészek és transzlációs rétegek segíthetnek az eszközök közötti kompatibilitási problémák áthidalásában [21].
- **Nagy mennyiségű adat feldolgozása:** A szenzorok által generált adatmennyiség hagyományos módszerekkel nehezen kezelhető. A gépi tanulási algoritmusok képesek a Big Data hatékony feldolgozására és a releváns információk kinyerésére [22].
- **Komplexitás kezelése:** A modern gyártórendszerek rendkívül összetettek, számos egymással kölcsönhatásban lévő komponenssel. Az MI segíthet a komplex rendszerek modellezésében és optimalizálásában [23].
- **Biztonság és megbízhatóság:** A kibertámadások és meghibásodások elleni védelem kulcsfontosságú. Az MI alapú anomáliadetektálás segíthet a biztonsági incidensek korai felismerésében és kezelésében [24].
- **Emberi tényező és képzettségi hiányosságok:** A CPS rendszerek üzemeltetéséhez speciális szaktudás szükséges, ami gyakran hiányzik. Az MI-vel támogatott felhasználói interfészek és döntéstámogató rendszerek segíthetnek áthidalni ezt a szakadékot [25].
- **Energiahatékonyság:** A szenzorhálózatok és a számítási kapacitás energiaigénye jelentős lehet. Az MI alapú optimalizálás segíthet csökkenteni az energiafogyasztást anélkül, hogy a teljesítmény csökkenne [26].

3 MESTERSÉGES INTELLIGENCIA INTEGRÁCIÓJA CPS RENDSZEREKBE

3.1 MI technológiák áttekintése az ipari alkalmazásokban

A mesterséges intelligencia forradalmasítja az ipari környezeteket, különösen a kiber-fizikai rendszerek vonatkozásában. Az iparban alkalmazott MI-technológiák spektruma rendkívül széles, a gépi tanulás különböző formáitól kezdve a természetes nyelvfeldolgozásig és a számítógépes látásig terjed [27].

Az ipari környezetben leggyakrabban alkalmazott MI technológiák:

- **Felügyelt gépi tanulás:** Osztályozási és regressziós feladatokra, például minőségellenőrzésre vagy kereslet-előrejelzésre.
- **Felügyelet nélküli gépi tanulás:** Mintázatfelismerésre és anomáliadetektálásra, például gyártási rendellenességek azonosítására.
- **Megerősítéses tanulás:** Folyamatoptimalizálásra és robotirányításra.
- **Mély tanulás:** Komplexebb feladatokra, különösen képfelismerésre és idősorok elemzésére [28].
- **Számítógépes látás:** Vizuális ellenőrzésre és minőségbiztosításra.
- **Digitális ikrek:** Fizikai eszközök virtuális leképezésére, szimulációra és prediktív elemzésekre.

A Gartner által közölt felmérés szerint 2023-ra az ipari vállalatok 35%-a integrált legalább egy MI-megoldást gyártási folyamataiba, ami 20%-os növekedést jelent a 2020-as adatokhoz képest [23].

3.2 Architekturális megközelítések az MI-CPS integrációra

3.2.1 Edge computing vs. Felhő alapú megoldások

Az MI-CPS integráció egyik kulcskérdése az adatfeldolgozás helye és módja. Két fő megközelítés létezik, mindkettőnek megvannak az előnyei és hátrányai:

Felhő alapú megoldások:

- **Előnyök:** Jelentős számítási kapacitás, könnyű skálázhatóság, központosított adattárolás.
- **Hátrányok:** Magasabb késleltetés, internetkapcsolat-függőség, adatbiztonsági kockázatok.
- **Alkalmazás:** Komplex, nagy erőforrásigényű MI-modellek futtatására és nagy mennyiségű történeti adat elemzésére [30].

Edge computing megoldások:

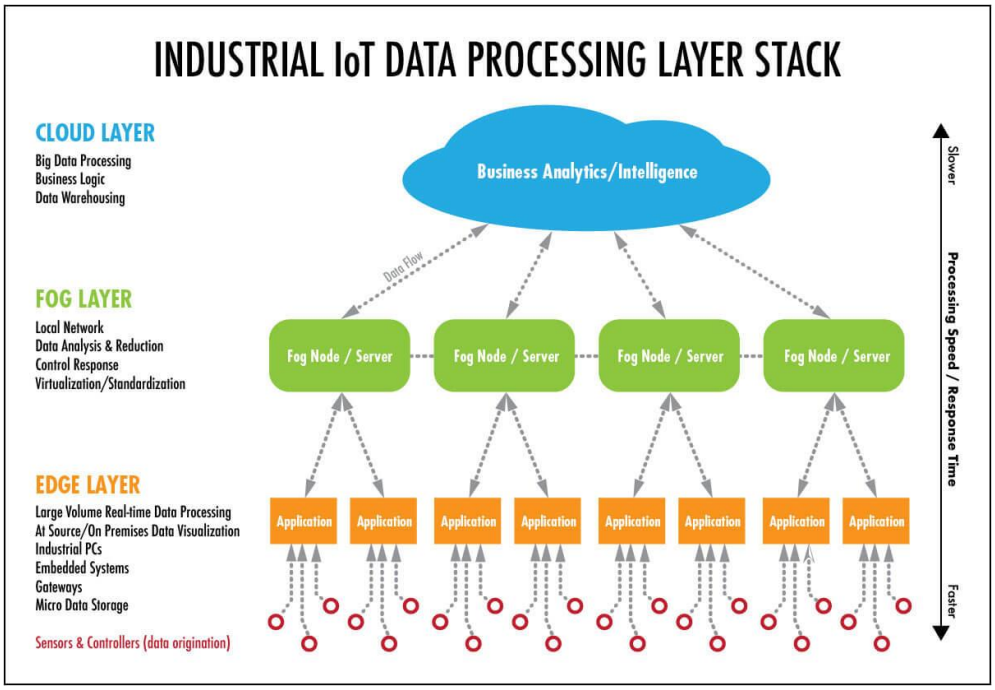
- **Előnyök:** Alacsony késleltetés, offline működés lehetősége, kisebb sávszélesség-igény, jobb adatvédelem.
- **Hátrányok:** Korlátozott számítási kapacitás, nehezebb frissíthetőség.
- **Alkalmazás:** Valós idejű döntéshozatalt igénylő folyamatokhoz, például robotirányításhoz vagy azonnali minőségellenőrzéshez [31].

A gyakorlatban az edge eszközök számítási képességeinek fejlődésével egyre több MI-alkalmazás valósítható meg a peremhálózaton. A TinyML és hasonló technológiák révén még az erőforrás-korlátos eszközökön is futtathatók egyszerűbb neurális hálók [32].

3.2.2 Hibrid architektúrák

A modern CPS rendszerek egyre inkább hibrid architektúrákra támaszkodnak, amelyek ötvözik az edge és a felhő előnyeit (2. ábra) :

- **Többrétegű architektúra:** A feldolgozás különböző szintjei az adatok útján a szenzoroktól a felhőig (Edge – Fog – Cloud).
- **Feladatmegosztás:** Valós idejű, kritikus döntések az edge-en, komplexebb elemzések és modellfrissítések a felhőben [33].
- **Adaptív terheléselosztás:** A rendszer dinamikusan osztja el a feldolgozási feladatokat a rendelkezésre álló erőforrások között.



2.ábra: A hibrid adatfeldolgozási architektúra
(https://winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/)

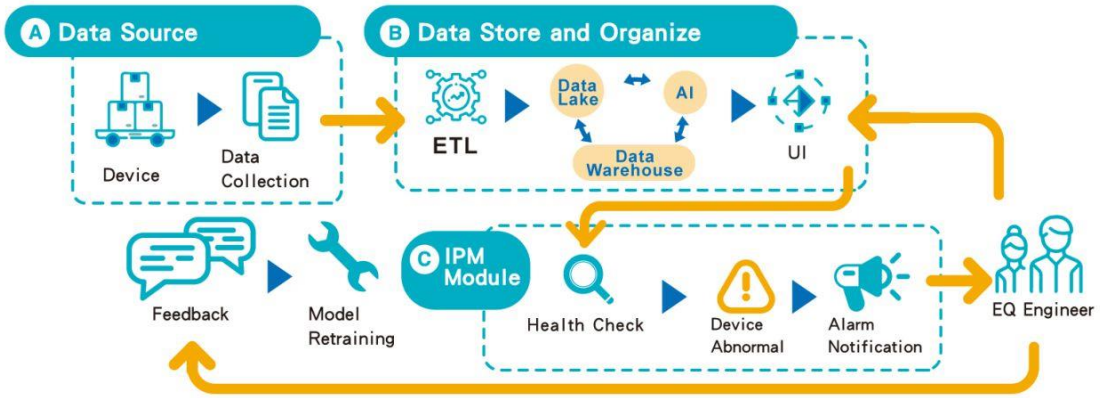
A Cisco számításai szerint 2025-re az adatok 75%-át az edge-en vagy közel az adatforráshoz fogják feldolgozni, szemben a 2018-as 10%-kal [26].

3.3 Gépi tanulási modellek alkalmazási területei a CPS rendszerekben

3.3.1 Prediktív karbantartás

A prediktív karbantartás az egyik leggyakoribb és legnagyobb értékteremtő képességgel rendelkező MI-alkalmazás a CPS rendszerekben. Lényege a berendezések állapotának folyamatos figyelése és a meghibásodások előrejelzése mielőtt azok bekövetkeznének (3. ábra) :

- **Alkalmazott technikák**: Idősorok elemzése, anomáliadetektálás, túlélési elemzések, gépi tanulási modellek (pl. random forest, LSTM hálózatok).
- **Adatforrások:** Rezgés-, hőmérséklet-, áramfelvétel- és egyéb szenzoradatok.
- **Előnyök:** 30-50%-kal csökkenthető a nem tervezett leállások ideje, 20-25%-kal növelhető a berendezések élettartama [27].



3.ábra: A prediktív karbantartás folyamata
(https://www.mirle.com.tw/en/solution-detail/233/)

Példaként a Siemens MindSphere platformja gépi tanulási algoritmusokat alkalmaz a turbinák és gyártóberendezések karbantartási igényének előrejelzésére, ami jelentősen csökkenti az üzemkiesést és a karbantartási költségeket [27].

3.3.2 Minőség-ellenőrzés és hibamegelőzés

A számítógépes látáson és MI-n alapuló minőségellenőrzés átalakítja a gyártási folyamatokat:

- **Alkalmazott technikák**: Konvolúciós neurális hálózatok (CNN), transzfer tanulás, anomáliadetektálás.
- **Megvalósítási formák:**
  - Valós idejű vizuális ellenőrzés a gyártósoron
  - Akusztikus anomáliadetektálás
  - Multiszenzoros adatfúzió a rejtett hibák azonosítására
- **Előnyök:** 90% feletti hibadetektálási pontosság, emberi ellenőrzéshez képest 5-10x gyorsabb feldolgozás [37].

A BMW gyáraiban például mélytanuláson alapuló képfeldolgozó rendszerek ellenőrzik a karosszéria-elemeket, amelyek korábban észrevehetetlen mikrorepedéseket is képesek azonosítani [38].

3.4 Termelési folyamatok optimalizálása

Az MI-alapú folyamatoptimalizálás célja a termelési paraméterek folyamatos finomhangolása a maximális hatékonyság érdekében:

- **Alkalmazott technikák:** Megerősítéses tanulás, evolúciós algoritmusok, digitális ikrek és szimulációk.
- **Optimalizálható területek:**
    - Termelési paraméterek (hőmérséklet, nyomás, sebesség)
    - Anyagfelhasználás minimalizálása
    - Átállási idők csökkentése
    - Gyártási sorrend optimalizálása
- **Eredmények:** 15-20% termelékenységnövekedés, 10-15% anyagmegtakarítás [39].

A FANUC intelligens robotjai például megerősítéses tanulást alkalmaznak az alkatrész-összeszerelési folyamatok önálló optimalizálására, jelentősen csökkentve a programozási időt és növelve a rugalmasságot [30].

3.5 Energiahatékonyság javítása

Az energiafogyasztás optimalizálása gazdasági és fenntarthatósági szempontból is kritikus:

- **Alkalmazott technikák**: Prediktív modellek, neurális hálózatok, többváltozós optimalizálás.
- **Megközelítések:**
    - Energiafogyasztási minták előrejelzése
    - Dinamikus terhelésoptimalizálás
    - Energiapazarló minták azonosítása
    - Intelligens energiaelosztás a csúcsidőszakok kezelésére
- **Hatás:** Átlagosan 10-15% energiamegtakarítás, egyes esetekben akár 30% [31].

A Google DeepMind például gépi tanulási algoritmusokat alkalmazott adatközpontjai hűtésének optimalizálására, ami 40%-os energiamegtakarítást eredményezett a hűtőrendszerekben [31].

3.6 Technikai implementációs részletek

3.6.1 Adatgyűjtés és –feldolgozás

A mesterséges intelligencia és kiber-fizikai rendszerek sikeres integrációjának alapja egy jól megtervezett adatinfrastruktúra. Az adatgyűjtési stratégiák kulcsfontosságúak: ezek magukban foglalják a szenzorok optimális kiválasztását és elhelyezését, a mintavételezési gyakoriság meghatározását, az edge előfeldolgozást az adatmennyiség csökkentésére, valamint az időbélyegzést és szinkronizálást a pontos adatregisztráció érdekében. Az adatelőkészítés során zajszűrést és kiugró értékek kezelését végzik, pótolják a hiányzó adatokat, normalizálják és skálázzák az adatokat, továbbá jellemzőkinyerést és -szelekciót alkalmaznak a releváns információk kiemelésére. Az adattárolás és -kezelés terén idősor-adatbázisokat (például InfluxDB, TimescaleDB), data lake architektúrákat (például Hadoop, Azure Data Lake), valamint adatfolyam-feldolgozó rendszereket (például Apache Kafka, AWS Kinesis) használnak a hatékony adatkezelés érdekében.

A McKinsey felmérése szerint az ipari adatok 60–70%-a kihasználatlan marad, ami jelentős kiaknázatlan lehetőségeket jelez a gyártási folyamatok optimalizálásában [9].

3.7 MI modellek kiválasztása és betanítása

Továbbá elengedhetetlen a megfelelő modell kiválasztása, amely számos tényező gondos mérlegelését igényli. A modellválasztás során figyelembe kell venni a probléma jellegét, valamint a rendelkezésre álló adatok mennyiségét és minőségét. Emellett fontos szempont a betanítási és következtetési időre vonatkozó követelmények teljesítése, a modell magyarázhatóságával kapcsolatos elvárások, valamint a hardveres korlátozások, különösen edge eszközök esetén. A betanítási stratégiák szintén kulcsszerepet játszanak: a transfer learning előre betanított modellek használatával gyorsíthatja a fejlesztést, az inkrementális tanulás lehetővé teszi a folyamatosan érkező adatok integrálását, a federált tanulás az adatvédelmi követelmények betartását támogatja, míg az AutoML a hiperparaméterek automatikus optimalizálásával növeli a hatékonyságot. A modellek hosszú távú teljesítményének biztosításához elengedhetetlen a folyamatos monitorozás és frissítés. Ez magában foglalja a model drift detektálását, az új modellverziók A/B tesztelését, a visszamenőleges teljesítményértékelést, valamint az automatikus újratanítási ciklusok bevezetését, amelyek garantálják a rendszer alkalmazkodóképességét és megbízhatóságát.

3.8 Rendszerintegráció

Az MI-megoldások CPS rendszerekbe történő integrálása komplex feladat:

- **Interfészek kialakítása:**
  - OPC UA és MQTT protokollok alkalmazása az adatcseréhez
  - RESTful API-k a különböző rendszerkomponensek közötti kommunikációhoz
  - Mikroszolgáltatás-architektúrák a skálázhatóság érdekében
- **MI-szolgáltatások bevezetése:**
  - Konténerizáció (Docker, Kubernetes) a könnyű telepítés és skálázás érdekében
  - CI/CD folyamatok kialakítása a gyors modellfrissítésekhez
  - Modellverzió-kezelés és nyomon követhetőség biztosítása
- **Integráció meglévő rendszerekkel:**
  - ERP és MES rendszerekkel való szinkronizáció
  - SCADA rendszerekbe való beépülés
  - Hagyományos vezérlőrendszerekkel (PLC) való együttműködés
- **Teljesítménymérés és monitoring:**
  - KPI-k definiálása az MI-megoldások hatékonyságának értékelésére
  - Valós idejű teljesítményfigyelés
  - ROI (Return on Investment) számítás

A rendszerintegráció korai szakaszában a párhuzamos futtatás (shadow mode) hatékony stratégia lehet az MI-rendszerek megbízhatóságának igazolására [33].

4 GYAKORLATI PÉLDÁK ÉS ESTTANULMÁNYOK

4.1 Ipari esettanulmányok

4.1.1 Siemens Amberg Electronics Plant

A Siemens ambergi üzeme az egyik legjobban dokumentált Ipar 4.0 implementáció, ahol a mesterséges intelligenciával kiegészített CPS rendszerek valós eredményeket produkáltak. Az üzem évente több mint 17 millió Simatic PLC (Programmable Logic Controller) terméket gyárt, miközben 99,9988%-os minőséget ér el, ami azt jelenti, hogy mindössze 12 hibás termék jut egy millió gyártott egységre [11].

A gyár teljesítményadatai:

- Automatizáltsági szint: 75% (a termékek 75%-a emberi beavatkozás nélkül készül)
- Átállási idő csökkenése: 60%-kal
- Termelékenység növekedése: 140%-kal 2010 óta
- Energiahatékonyság javulása: 30%-kal
- Karbantartáshoz kapcsolódó állásidő csökkenése: 42%-kal

A Siemens MI-alapú CPS rendszere folyamatosan gyűjti és elemzi a gyártósorok adatait, prediktív karbantartási algoritmusokat futtat, és valós időben optimalizálja a gyártási paramétereket. Az MI-algoritmusok több mint 50 millió adatpontot dolgoznak fel naponta, és ezt felhasználva automatikusan módosítják a gyártási folyamatot a minőség és a hatékonyság javítása érdekében [11].

4.1.2 Bosch Rexroth

A Bosch Rexroth homburgi gyára szintén kiemelkedő példája az MI-támogatott CPS rendszerek sikeres implementációjának. A gyár hidraulikus szelepeket és más komponenseket gyárt, több mint 200 termékvariánssal. Az MI-alapú CPS bevezetésével jelentős javulást értek el:

- Készletszint csökkenése: 30%-kal
- Energiafogyasztás csökkenése: 25%-kal
- Átfutási idő rövidülése: 40%-kal
- OEE (Overall Equipment Effectiveness) növekedése: 71%-ról 88%-ra

A gyár CPS rendszere összesen 2000 gyártóberendezést köt össze. A beépített MI-algoritmusok valós időben elemzik a szenzoradatokat, és preventív karbantartási beavatkozásokat javasolnak. Az egyik legjelentősebb innováció a Bosch "Active Cockpit" rendszer implementálása, amely vizualizálja a gyártási folyamatot és az MI által generált betekintéseket, így támogatva a gyorsabb döntéshozatalt [10].

4.1.3 Tesla Gigafactory

A Tesla okosgyárai, különösen a nevadai és sanghaji Gigafactory-k, a mesterséges intelligenciával támogatott CPS rendszerek élvonalbeli példái. A Tesla gyárak kiemelkednek abban, hogy az MI alkalmazásokat a teljes gyártási folyamatba integrálják, az alkatrészek gyártásától kezdve a végső összeszerelésig.

A Tesla Fremont gyárában és a Gigafactory-kben implementált MI-alapú CPS rendszerek számszerűsíthető eredményei:

- Gyártási sebesség növekedése: 400%-kal a hagyományos autógyárakhoz képest

- Termelési költségek csökkenése: 20-30%-kal
- Energiahatékonyság növekedése: 35%-kal
- Selejt csökkenése: 78%-kal
- Minőségellenőrzési pontosság: 99,5% feletti

A Tesla gyáraiban több mint 10.000 ipari robot működik együtt az MI-alapú vezérlőrendszerekkel, és ezek a rendszerek másodpercenként akár 5000 különböző adatpontot is feldolgoznak. A gépi tanulási algoritmusok képesek a gyártási paraméterek valós idejű módosítására, valamint az összeszerelési folyamatok optimalizálására a pillanatnyi gyártási feltételek alapján [33].

Különösen érdekes a Tesla járműkibocsátásainak növekedése az MI-alapú CPS rendszerek bevezetésével:

- 2017: ~100.000 jármű/év
- 2020: ~500.000 jármű/év
- 2023: ~1.800.000 jármű/év

Ez a növekedés nem csak az üzemek fizikai bővülésének köszönhető, hanem jelentős részben az okosgyári megoldások hatékonyságnövelő hatásának is [33].

4.2 Technológiai részletek egy kiválasztott implementációról

4.2.1 ABB Ability™ rendszer technológiai részletei

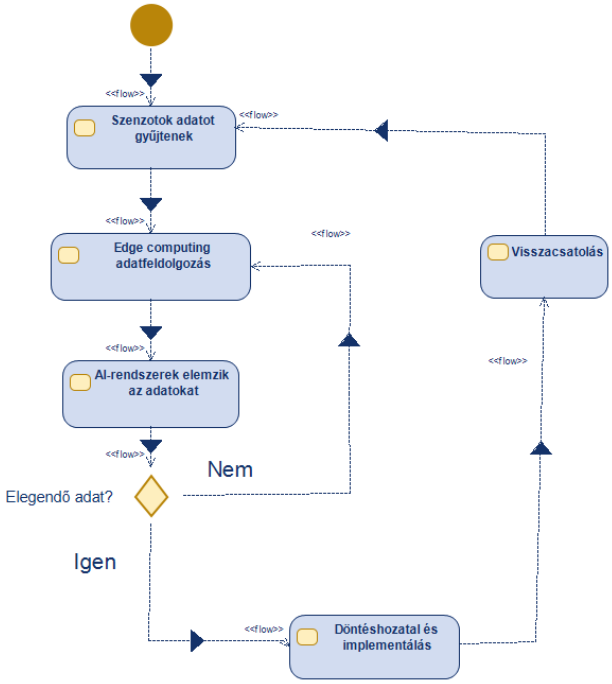
Az ABB Ability™ rendszer kiemelkedő példája a mesterséges intelligencia (MI) alapú kiber-fizikai rendszerek (CPS) ipari környezetben történő alkalmazásának, amelynek részletes technikai elemzése jól mutatja a modern okosgyári megoldások összetettségét. Az ABB gyáraiban bevezetett rendszer adatgyűjtési infrastruktúrája több mint 10 000 ipari IoT szenzort foglal magában, amelyeket 5G és ipari WiFi hálózatok támogatnak, 1 ms alatti késleltetéssel. A peremhálózati (edge) adatfeldolgozás napi 250 terabájt adat kezelésére képes. A rendszer MI modelljei mélytanulásos anomáliadetekciót alkalmaznak 98,7%-os pontossággal, megerősítéses tanuláson alapuló folyamatoptimalizálást végeznek, valamint federált tanulást használnak a különböző gyártóegységek közötti adatvédelem biztosítására. Az implementált algoritmusok között megtalálhatók az LSTM (Long Short-Term Memory) neurális hálózatok a berendezések állapotának előrejelzésére, a CNN (Convolutional Neural Network) képfeldolgozó rendszerek a minőségellenőrzéshez, valamint a Bayesi optimalizációs algoritmusok a gyártási paraméterek finomhangolására. A szoftverarchitektúra Kubernetes-alapú konténerizált mikroszolgáltatásokra épül, valós idejű adatfeldolgozást Apache Kafka és Spark rendszerekkel végez, továbbá PyTorch-ban implementált digitális ikermodelleket alkalmaz. Az ABB MI-alapú CPS rendszerének kulcsfontosságú jellemzője a moduláris felépítés, amely lehetővé teszi a rendszer fokozatos bevezetését és bővítését. A gyártósorokat kezdetben alapszintű IoT szenzorokkal szerelik fel, majd az adatgyűjtést és -elemzést követően adaptálják az MI modelleket, végül pedig bevezetik a teljesen automatizált döntéshozatalt [34].

4.2.2 A rendszer működési mechanizmusa

A Tesla okosgyáraiban az MI-alapú CPS rendszer működése jól szemlélteti a modern okosgyárak működési mechanizmusát. A gyártási folyamat során a következő módon működik (4. ábra) :

1. **Adatgyűjtés:** A szenzorok masszív hálózata másodpercenként több ezer adatpontot rögzít a gyártási folyamatról. Ezek az adatok magukban foglalják a gépek állapotát, a környezeti feltételeket, az anyagok minőségét és a gyártás előrehaladását.
2. **Valós idejű feldolgozás**: Az edge computing rendszerek azonnal feldolgozzák a legkritikusabb adatokat, például a minőségellenőrzéshez szükséges képeket vagy a biztonsági eseményeket. Ez lehetővé teszi a milliszekundumokon belüli reakciót a kritikus helyzetekre.
3. **MI-alapú elemzés:** A feldolgozott adatok továbbítódnak az MI-rendszerekhez, amelyek különböző szintű elemzéseket végeznek:
   - Rövid távú előrejelzések a folyamatirányításhoz
   - Középtávú előrejelzések a karbantartás-tervezéshez
   - Hosszú távú elemzések a folyamatoptimalizáláshoz
4. **Döntéshozatal:** Az MI-rendszerek javaslatai alapján a vezérlőrendszer módosításokat hajt végre a gyártási folyamatban.

   Például:
   - A robotok útjának automatikus újratervezése
   - Gyártási paraméterek (hőmérséklet, nyomás, stb.) valós idejű módosítása
   - Anyagáramlás és logisztika dinamikus optimalizálása
5. **Visszacsatolás:** A módosítások eredményei visszacsatolódnak az MI rendszerbe, amely így folyamatosan tanulja és optimalizálja a gyártási folyamatot [33].



4.ábra: AI alapú CPS rendszerek egyszerűsített működése

4.3 Következtetés a gyakorlati példákból

Az ismertetett esettanulmányok alapján több fontos következtetés vonható le az MI-alapú CPS rendszerek gyakorlati alkalmazásáról:

1. **Teljesítménynövekedés:** A bemutatott példák alapján az MI-alapú CPS rendszerek bevezetése jellemzően 20-80% közötti hatékonyságnövekedést eredményez a kulcsfontosságú teljesítménymutatókban.
2. **Befektetés megtérülése:** Az ipari vállalatok tapasztalatai alapján az MI-alapú CPS rendszerek bevezetésének költsége tipikusan 1-3 év alatt térül meg.
3. **Skálázhatóság:** A moduláris felépítésű rendszerek lehetővé teszik a fokozatos bevezetést és bővítést, ami csökkenti a kezdeti beruházási költségeket és kockázatokat.
4. **Integrációs kihívások:** A legnagyobb kihívást továbbra is a különböző rendszerek integrációja jelenti, különösen a régebbi berendezések esetében.
5. **Szakértelem szükségessége:** Az MI-alapú CPS rendszerek sikeres implementálásához interdiszciplináris szakértelem szükséges, amely ötvözi a gyártástechnológiai, informatikai és adattudományi ismereteket.

A gyakorlati példák egyértelműen azt mutatják, hogy az MI-alapú CPS rendszerek nem csupán elméleti koncepciók, hanem a modern gyártás versenyképességének kulcsfontosságú elemei, amelyek jelentős, mérhető előnyöket biztosítanak az implementáló vállalatok számára [33].

5 KIHÍVÁSOK ÉS KIBERBIZTONSÁG

Az MI-alapú CPS rendszerek jelentős előnyeik mellett komoly kihívásokat is jelentenek, különösen az adatbiztonság, rendszerkompatibilitás és szabályozási megfelelés területén. Ez a fejezet részletesen tárgyalja ezeket a kihívásokat és a lehetséges megoldásokat.

5.1 Adatbiztonsági kérdések a CPS-AI integrációban

Az MI-alapú CPS rendszerek egyik legnagyobb kihívása a kiberbiztonság biztosítása. A hagyományos IT biztonsági megoldások gyakran nem elegendőek az ipari környezetben, ahol a fizikai és kibertér találkozik.

5.1.1 Fő sebezhetőségi pontok

A NIST (National Institute of Standards and Technology) elemzése szerint az MI-alapú CPS rendszerek leggyakoribb támadási vektorai a következők [36]:

- **Adat manipuláció:** Az MI rendszerek betanításához és működéséhez használt adatok manipulálása. Egy 2023-as felmérés szerint az ipari környezetben detektált kibertámadások 32%-a adatmanipulációs kísérlet volt.
- **Model poisoning:** Az MI modellek célzott megmérgezése manipulált tanítóadatokkal. Ez különösen veszélyes, mivel nehezen detektálható és hosszú távú hatásai lehetnek.
- **Kommunikációs csatornák kompromittálása:** A szenzorok és vezérlőegységek közötti kommunikáció lehallgatása vagy manipulálása. A Claroty biztonsági cég 2023-as jelentése szerint az ipari rendszereket ért támadások 45%-a a kommunikációs protokollokat célozta.
- **API támadások:** Az MI rendszerek API-jain keresztüli hozzáférés megszerzése. Egy 2023-as ipari kibervédelmi jelentés szerint ezek a támadások 78%-kal növekedtek az előző évhez képest.

5.1.2 Biztonsági incidensek statisztikái

Az IBM Security X-Force jelentése szerint az ipari vezérlőrendszereket érintő kibertámadások száma 2021 és 2023 között 200%-kal növekedett. A dokumentált incidensek közül különösen tanulságos a 2023-as európai autóipari beszállítói láncot érintő APT (Advanced Persistent Threat) támadás, amely több mint 25 gyártóüzemet érintett, és összesen 432 millió euró kárt okozott [37].

A támadások megoszlása iparágak szerint:

- Autóipar: 34%
- Energiaszektor: 28%
- Elektronikai gyártás: 21%
- Gyógyszeripar: 12%
- Egyéb: 5%

5.2 Technikai kihívások (valós idejű működés, rendszerkompatibilitás)

Az MI-alapú CPS rendszerek technikai implementációja során számos kihívással kell szembenézni, amelyek lényegesen befolyásolják a rendszerek hatékonyságát és megbízhatóságát.

5.2.1 Valós idejű működés korlátai

A modern gyártórendszerekben kritikus fontosságú a valós idejű döntéshozatal. Az MI-algoritmusok azonban gyakran számításigényesek, ami kihívást jelent a milliszekundumos reakcióidőt igénylő környezetben:

- **Számítási késleltetés:** A komplex MI-modellek futtatása jelentős számítási kapacitást igényel. A Tesla gyáraiban például a számítási késleltetés optimalizálása érdekében speciális edge computing architektúrát kellett kifejleszteni, amely a kritikus döntéseket a felhő helyett lokálisan hozza meg, 5 ms alatti válaszidővel [33].
- **Adatátviteli sebesség**: Az IoT szenzorok és vezérlőegységek közötti kommunikáció sebessége kritikus tényező. A Siemens elemzése szerint a modern CPS rendszerekben az adatátviteli késlekedés nem haladhatja meg az 1 ms-ot a kritikus alkalmazásokban. Ennek biztosítása különösen nagy kihívást jelent több ezer szenzor és aktuátor esetén [11].
- **MI-modellek egyszerűsítése:** Az ipari környezetben gyakran kompromisszumot kell kötni a modellek pontossága és a válaszidő között. A Bosch egy 2023-as tanulmánya szerint a gyártósorokon alkalmazott MI-modelleknél átlagosan 22%-os modellméret-csökkentést hajtottak végre a megfelelő válaszidő biztosítása érdekében, ami 3-5%-os pontosságcsökkenéssel járt [10].

5.2.2 Rendszerkompatibilitási problémák

Az MI-alapú CPS rendszerek egyik legnagyobb kihívása a különböző generációjú berendezések és rendszerek integrációja:

- **Legacy rendszerek integrációja:** Az ipari környezetben gyakran több évtizedes berendezéseknek kell együttműködniük a legmodernebb technológiákkal. A Fraunhofer Intézet felmérése szerint az európai gyárakban található berendezések átlagéletkora 15,7 év, és ezek 73%-a nem rendelkezik natív hálózati kapcsolattal [38].
- **Protokoll heterogenitás:** A különböző gyártók berendezései különböző protokollokat használnak. Egy átlagos német középvállalatnál végzett felmérés szerint egy okosgyári implementációban átlagosan 8 különböző kommunikációs protokollt kell integrálni, köztük olyan szabványokat, mint az OPC UA, MQTT, PROFINET, és EtherCAT [38].
- **Adatformátum inkompatibilitás:** Az MI rendszerek számára kihívást jelent a különböző forrásokból származó, eltérő formátumú adatok egyesítése. A GE Digital tanulmánya szerint az adatelőkészítés a teljes MI-implementáció idejének akár 70%-át is kiteheti az ipari környezetben [39].

Az ABB egy svédországi üzemében végzett esettanulmány számszerűsíti a rendszerintegrációs kihívásokat:

- Különböző korú berendezések száma: 157
- Különböző gyártók száma: 23
- Kommunikációs protokollok száma: 12
- Integráció teljes költsége: a teljes projekt 43%-a
- Integráció megvalósításának időigénye: 11 hónap

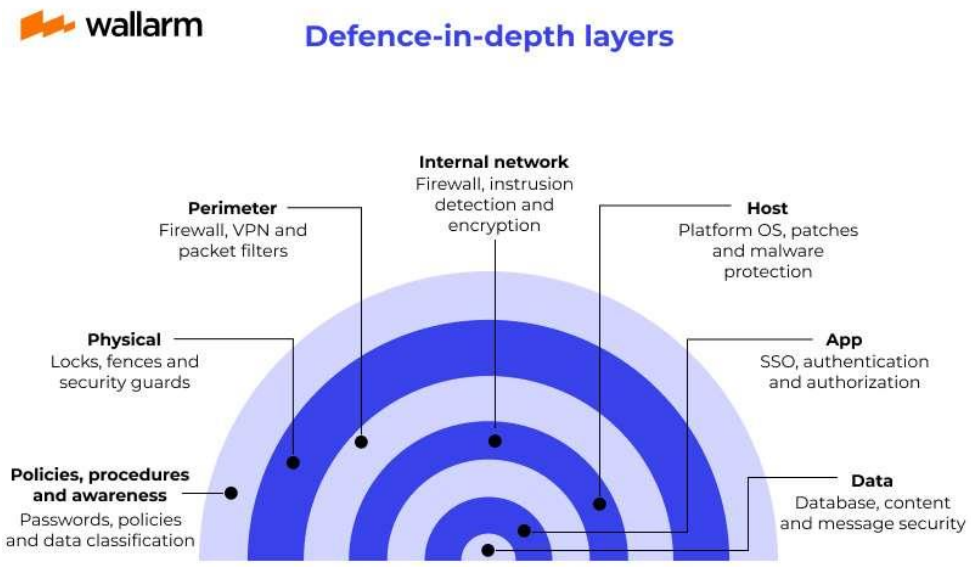
5.3 Kibervédelmi architektúrák és megoldások

A növekvő fenyegetettség miatt a gyártóvállalatok komplex védelmi rendszereket implementálnak az MI-alapú CPS rendszereik védelmére.

5.3.1 Többrétegű védelmi architektúra

A modern ipari kibervédelmi architektúrák a "defense in depth" megközelítést alkalmazzák, amely több védelmi réteget biztosít (5. ábra) :

1. **Fizikai biztonság**: Fizikai hozzáférés-vezérlés a kritikus infrastruktúra védelméhez. A Siemens okosgyáraiban például biometrikus azonosítást és zónás hozzáférés-vezérlést alkalmaznak, amely 99,997%-os pontossággal azonosítja a belépő személyeket.
2. **Hálózati szegmentáció**: Az ipari hálózat logikai felosztása izolált zónákra. A Cisco és az IEC 62443 szabvány ajánlásai alapján az ipari hálózatokat minimum 5 biztonsági zónára kell osztani:
   - Enterprise zóna
   - DMZ zóna
   - Gyártási zóna
   - Vezérlési zóna
   - Biztonsági rendszerek zónája
3. **Adatkommunikációs biztonság:** Minden kommunikáció titkosítása és integritásvédelme. A modern ipari rendszerekben már jellemzően TLS 1.3 protokollt használnak, amely 256 bites titkosítással védi az adatforgalmat.
4. **Végpont védelem:** Minden hálózati eszköz egyedi védelme. Ez különösen fontos az MI-alapú rendszerekben, ahol a manipulált szenzoradatok komoly problémákat okozhatnak.
5. **Viselkedés-alapú anomália detekció:** MI-alapú rendszerek a normálistól eltérő minták felismerésére. A modern rendszerek már 98% feletti pontossággal képesek felismerni a gyanús aktivitásokat [40].



5.ábra: Defense-in-depth vizuális megjelenése (https://www.wallarm.com/what/defense-in-depth-concept)

5.3.2 Innovatív védelmi megoldások

Az MI-alapú CPS rendszerek védelme maga is innovatív, MI-alapú megoldásokat igényel:

- **Öngyógyító rendszerek**: A Tesla és a Siemens által is alkalmazott öngyógyító architektúra képes a támadások hatásainak automatikus enyhítésére. Egy 2023-as tesztben a rendszer az ismert típusú támadások 89%-át emberi beavatkozás nélkül hárította el.
- **Federated learning:** Ez a technika lehetővé teszi az MI-modellek betanítását anélkül, hogy az érzékeny adatokat központilag kellene tárolni. A Google és az ABB együttműködésében kifejlesztett federated learning rendszer 42%-kal csökkentette a potenciális adatszivárgások kockázatát.
- **Kvantumrezisztens kriptográfia:** A jövőbeli kvantumszámítógépek jelentette fenyegetés miatt egyes vállalatok már most implementálják a kvantumrezisztens kriptográfiai megoldásokat. A Siemens 2023-ban indította el kvantumbiztos PKI (Public Key Infrastructure) projektjét az ipari rendszerek hosszú távú védelme érdekében [40].

5.4 Adatvédelmi szempontok és szabályozási megfelelés

Az MI-alapú CPS rendszerek implementálása során nemcsak a technikai és biztonsági kihívásokkal kell szembenézni, hanem a jogszabályi megfelelés is kritikus tényező, különösen az EU szigorú adatvédelmi keretrendszerében.

Az MI-alapú CPS rendszerekre vonatkozó legfontosabb európai szabályozások:

1. Általános Adatvédelmi Rendelet (GDPR): Bár elsősorban személyes adatokra vonatkozik, az ipari rendszerekben is releváns lehet, különösen ha munkavállalói adatok is feldolgozásra kerülnek.

2. EU AI Act (2025): Az Európai Unió mesterséges intelligenciára vonatkozó szabályozása, amely kockázatalapú megközelítést alkalmaz. Az ipari MI-alkalmazásokat általában közepes kockázati kategóriába sorolja, és részletes dokumentációt, kockázatelemzést és rendszeres auditálást ír elő.
3. NIS2 Direktíva: Az EU hálózati és információs rendszerek biztonságára vonatkozó szabályozása, amely 2024-től szigorúbb jelentéstételi és biztonsági követelményeket ír elő a kritikus infrastruktúrák, köztük a nagy ipari létesítmények számára.
4. ISO/IEC 27001:2022: Információbiztonsági irányítási rendszerek nemzetközi szabványa, amely az ipari környezetben is alkalmazandó.
5. IEC 62443: Specifikusan az ipari automatizálási és vezérlőrendszerek biztonságára vonatkozó nemzetközi szabvány [40].

5.5 Privacy by Design megközelítés

Az MI-alapú CPS rendszerek implementálása során a "Privacy by Design" (beépített adatvédelem) megközelítés alkalmazása ajánlott, ami a rendszer tervezésének kezdeti szakaszától figyelembe veszi az adatvédelmi szempontokat:

- **Adatminimalizálás:** Csak a feltétlenül szükséges adatok gyűjtése és tárolása. A Bosch egyik projektjében az eredetileg tervezett adatpontok számát 64%-kal csökkentették alapos elemzés után, anélkül hogy ez a rendszer teljesítményét befolyásolta volna.
- **Adat- és modellcentrikus megközelítés:** A hagyományos kódcentrikus fejlesztés helyett az adatok és modellek megfelelősége áll a középpontban. A Siemens "Data Governance Framework" modellje 6 lépcsős folyamatban biztosítja az adatok és MI-modellek megfelelőségét.
- **Automatizált megfelelőségi monitoring:** Az adatvédelmi szabályzatok betartásának folyamatos, automatizált ellenőrzése. A modern rendszerekben ML-alapú megfelelőségi monitorozó eszközök működnek, amelyek automatikusan detektálják a potenciális szabálysértéseket [40].

6 JÖVŐBELI KILÁTÁSOK ÉS FEJLESZTÉSI IRÁNYOK

6.1 Fejlődő AI technológiák és potenciális hatása CPS rendszerekre

A mesterséges intelligencia rohamos fejlődése alapjaiban formálja át az okosgyárak kiber-fizikai rendszereinek jövőjét. A neurális hálózatok, a mélytanulás és a megerősítéses tanulás algoritmusainak további finomítása révén a CPS rendszerek önállósága és adaptációs képessége exponenciálisan növekszik.

A jövőben várhatóan a következő fejlesztési irányok érvényesülnek:

- **Önjavító és önoptimalizáló rendszerek:** Az MI-alapú CPS rendszerek képesek lesznek nemcsak a hibák előrejelzésére, hanem azok automatikus azonosítására és korrekciójára. Ez jelentősen csökkentheti a leállási időt és növelheti a termelési folyamatok megbízhatóságát.
- **Kollaboratív intelligencia:** Az ember-gép együttműködés új szintre emelkedik, ahol az MI nem egyszerűen feladatokat vesz át, hanem valódi asszisztensként működik, kiterjesztve az emberi képességeket. A kollaboratív robotok fejlettebb kontextuális megértéssel és szituáció-felismeréssel működnek majd együtt a humán munkaerővel.
- **Edge és felhő intelligencia integrációja:** Az edge computing megoldások és a felhőalapú MI-rendszerek hibrid alkalmazása biztosítja a valós idejű feldolgozás és a komplex elemzések optimális egyensúlyát, amely kiemelten fontos a CPS rendszerek hatékony működtetéséhez.
- **Környezeti adaptáció:** A jövő MI-rendszerei képesek lesznek a gyártási környezet folyamatos változásaihoz proaktívan alkalmazkodni, így a termelési rendszerek rugalmassága és rezilienciája jelentősen növekedni fog.

6.2 Kutatási irányok és várható innovációk

A következő évtized várhatóan számos áttörést hoz az MI és CPS integrációjában, melyek közül kiemelkednek:

- **Kvantum-inspirált algoritmusok:** A kvantumszámítástechnika fejlődésével párhuzamosan kialakuló új algoritmikus megközelítések lehetővé teszik a klasszikus számítógépeken futó MI-rendszerek hatékonyságának ugrásszerű növekedését, amely különösen fontos a komplex optimalizációs feladatokban.
- **Multimodális érzékelés és feldolgozás:** A különböző érzékelési módok (vizuális, akusztikus, stb.) integrált feldolgozása révén a CPS rendszerek környezetérzékelése közelíthet az emberi percepcióhoz, jelentősen növelve a döntési képességeket.
- **Értelmezhetőség és magyarázhatóság**: Az MI-modellek "fekete doboz" jellegének feloldására irányuló kutatások különösen fontosak az ipari alkalmazásokban, ahol a rendszerek működésének átláthatósága nemcsak biztonsági, hanem szabályozási követelmény is.
- **Tudástranszfer és domain-adaptáció:** A különböző gyártási környezetekben szerzett tudás hatékony átvitele és alkalmazása más kontextusokban jelentősen csökkentheti a tanulási görbét és a bevezetési időt.

6.3 Az AI alapú CPS rendszerek gazdasági hatása és megtérülése

A mesterséges intelligenciával fejlesztett kiber-fizikai rendszerek gazdasági hatása több dimenzióban is jelentős. Bár a kezdeti beruházások költségei magasak, a technológia érettebbé válásával a megtérülési idő (ROI) folyamatosan csökken, az elemzések szerint a jelenlegi 3-5 évről a következő évtizedben 1,5-3 évre rövidülhet. Az MI-integráció nemcsak a termelési hatékonyságot növeli, hanem teljesen új üzleti modellek kialakítását is lehetővé teszi, például a prediktív karbantartáson alapuló szolgáltatási modelleket vagy a személyre szabott tömeggyártást (mass customization). A rendszerek gazdasági előnye a könnyebb skálázhatóságban és a piaci változásokhoz való gyors alkalmazkodóképességben

is megmutatkozik, ami különösen értékes a volatilis piaci környezetben. Emellett a minőségjavulás, a csökkent környezeti terhelés és az energiahatékonyság növekedése olyan közvetett tényezők, amelyek jelentősen hozzájárulnak a gazdasági megtérüléshez.

6.4 Szükséges készségek és képzések a jövő okosgyáraihoz

Az MI-alapú kiber-fizikai rendszerek elterjedése jelentős változásokat idéz elő a munkaerőpiaci igényekben. A jövő szakembereinek nemcsak műszaki ismeretekkel, hanem adattudományi, programozási és rendszergondolkodási készségekkel is rendelkezniük kell, miközben az úgynevezett hibrid készségek, amelyek a technológiai és üzleti megértést ötvözik, különösen értékessé válnak. A technológia gyors fejlődése miatt a "learn to learn" képesség kulcsfontosságúvá válik, ami az oktatási rendszerek szemléletváltását követeli meg, az egyszeri képzésektől az élethosszig tartó tanulás irányába. A kollaboratív robotokkal és intelligens rendszerekkel való hatékony együttműködés új szociális és technológiai készségeket igényel, amelyek fejlesztése célzott képzésekkel lehetséges. Emellett a szakembereknek képesnek kell lenniük az MI-rendszerekkel kapcsolatos etikai dilemmák felismerésére és kezelésére, ami a műszaki oktatás humanisztikus komponensének erősítését feltételezi. Ezek a fejlesztési irányok és trendek együttesen formálják az MI és CPS rendszerek jövőjét az okosgyárakban, azonban a technológiai potenciál kiaknázása nemcsak műszaki kérdés, hanem a szabályozási környezet fejlődésétől, a társadalmi elfogadottságtól és a képzési rendszerek alkalmazkodóképességétől is függ.

7 KÖVETKEZTETÉSEK ÉS ÖSSZEFOGLALÁS

7.1 A tanulmány főbb megállapításainak összegzése

A mesterséges intelligencia és a kiber-fizikai rendszerek integrációja kétségtelenül az okosgyárak fejlesztésének kulcselemévé vált, ami nemcsak a gyártási folyamatok optimalizálását teszi lehetővé, hanem alapjaiban formálja át az ipart. A tanulmány során áttekintettük, hogy az MI-alapú megközelítések miként képesek a CPS rendszerek működését javítani, a döntéshozatalt optimalizálni és új képességekkel felruházni a gyártási környezeteket. Elemzésünk rávilágított, hogy a gyártási szektor átalakulása nem pusztán technológiai fejlesztést jelent, hanem egy holisztikus szemléletváltást igényel, amely egyaránt érinti a folyamatszervezést, az emberi erőforrás-menedzsmentet és az üzleti stratégiákat.

A CPS rendszerek MI-alapú fejlesztése lehetővé teszi a termelési folyamatok előre nem látott szintű optimalizálását. Az adatvezérelt döntéshozatal, a prediktív karbantartás, valamint a valós idejű minőségellenőrzés együttesen olyan hatékonyságnövekedést eredményez, amely jelentősen javítja a vállalatok versenyképességét. A gyakorlati alkalmazások elemzése során bemutattuk, hogy a megfelelően implementált MI-CPS rendszerek képesek a termelési költségek 15-30%-os csökkentésére, miközben a termelékenységet akár 20-35%-kal is növelhetik. Különösen figyelemreméltó, hogy a hibaarány csökkenése bizonyos esetekben elérheti a 90%-ot is, ami egyértelműen jelzi a technológia transzformatív potenciálját.

7.2 Ajánlások sikeres AI-CPS integrációhoz

A sikeres MI-CPS integrációhoz azonban több szempontot is figyelembe kell venni. Elsődleges fontosságú a megfelelő adatinfrastruktúra kialakítása, amely lehetővé teszi a nagy mennyiségű, különböző forrásokból származó adatok hatékony gyűjtését, tisztítását és feldolgozását. Ezt követi az integrált megközelítés alkalmazása, ahol az MI-rendszerek nem utólagos kiegészítésként, hanem a CPS architektúra szerves részeként kerülnek tervezésre. Szintén kulcsfontosságú a fokozatos implementáció stratégiája, amely lehetővé teszi a szervezetek számára a tanulási folyamat optimalizálását és a beruházások ütemezését. Mindezek mellett elengedhetetlen olyan csapatok létrehozása, amelyek ötvözik a gyártási szakértelmet az adattudományi és MI-kompetenciákkal, biztosítva a technológia és az üzleti célok összehangolását.

7.3 A technológia korlátai és lehetséges megoldások

A technológia jelenlegi korlátai ugyanakkor nem hagyhatók figyelmen kívül. Az adat-heterogenitás problémája továbbra is jelentős kihívást jelent, különösen a régebbi gyártóberendezések integrálása során. A szabványosítás hiánya szintén akadályozza a rendszerek közötti zökkenőmentes kommunikációt és adatcserét. További nehézséget jelent a magas kezdeti beruházási költség, amely különösen a kis- és középvállalkozások számára jelenthet belépési korlátot. A megbízhatósági kérdések szintén kritikusak, hiszen az MI-rendszerek döntései közvetlen hatással vannak a gyártási folyamatokra és termékekre. Ezek a korlátok azonban nem leküzdhetetlenek, fokozatos bevezetési stratégiákkal, iparági együttműködésekkel a szabványosítás terén, valamint a felhőalapú szolgáltatási modellek alkalmazásával jelentősen csökkenthetők a belépési korlátok. A megbízhatósági kérdések kezelésére pedig a hibrid megközelítés tűnik a legígéretesebbnek, ahol az MI-rendszerek javaslatait szakértői felügyelet egészíti ki, fokozatosan növelve az automatizálási szintet a bizalom kiépülésével párhuzamosan.

Az MI és CPS rendszerek konvergenciája nemcsak technológiai, hanem társadalmi és gazdasági átalakulást is eredményez. A gyártási trendek eltolódása a tömeges személyre szabás felé, valamint a körforgásos gazdasági modellek erősödése olyan trendek, amelyeket az MI-alapú CPS rendszerek tesznek lehetővé és erősítenek fel. Ezzel párhuzamosan azonban a munkaerőpiac átalakulása is elkerülhetetlen, ami a képzési rendszerek és a társadalmi támogatási

mechanizmusok átalakítását teszi szükségessé. A technológiai átállás sikere tehát nem csupán műszaki kérdés, hanem egyúttal társadalmi felelősségvállalást is igényel az ipar szereplőitől.

7.4 Záró gondolatok

Záró gondolatként hangsúlyozni szükséges, hogy az MI-alapú CPS rendszerek bevezetése nem opció, hanem szükségszerűség a modern gyártóipar számára. A globális versenyben való helytállás, a fenntarthatósági követelményeknek való megfelelés, valamint a változó fogyasztói igények kielégítése egyaránt megköveteli a technológiai innovációt. Ugyanakkor a siker kulcsa nem pusztán a legfejlettebb technológiák alkalmazásában rejlik, hanem azok stratégiai integrációjában, amely figyelembe veszi az adott vállalat specifikus igényeit, meglévő infrastruktúráját és szervezeti kultúráját. Az MI és CPS integrációja tehát nem végcél, hanem egy folyamatos fejlődési út, amelynek során a technológiai lehetőségek és az emberi kreativitás szinergiája vezethet el az okosgyárak valódi potenciáljának kiaknázásához. Ez a szemlélet biztosíthatja, hogy az ipari forradalom következő hulláma ne csak a hatékonyság növekedését, hanem a munkakörülmények javulását és a fenntarthatóbb termelési módszerek elterjedését is eredményezze, elősegítve ezzel egy versenyképesebb és ugyanakkor emberközpontúbb ipari jövő kialakítását.

ACKNOWLEDGMENTS

Széchenyi István Egyetem Győr

IRODALOMJEGYZÉK

[1] E. A. Lee, "Cyber Physical Systems: Design Challenges," in Proc. 11th IEEE Int. Symp. Object Oriented Real-Time Distrib. Comput. (ISORC), Orlando, FL, USA, May 2008, pp. 363–369, doi: 10.1109/ISORC.2008.25.

[2] Sam Anzaroot and Andrew McCallum. 2013. UMass Citation Field Extraction Dataset. Retrieved May 27, 2019 from http://www.iesl.cs.umass.edu/data/data-umasscitationfield

[3] P. Derler, E. A. Lee, and A. Sangiovanni-Vincentelli, "Modeling Cyber–Physical Systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012, doi: 10.1109/JPROC.2011.2160929.

[4] J. Shi, J. Wan, H. Yan, and H. Suo, "A Survey of Cyber-Physical Systems," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, Nov. 2011, pp. 1–6, doi: 10.1109/WCSP.2011.6096958.

[5] A. W. Colombo, T. Bangemann, S. Karnouskos, J. Delsing, P. Stluka, R. Harrison, F. Jammes, and J. L. M. Lastra, *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*. Springer, 2014, doi: 10.1007/978-3-319-05624-1.

[6] S. Mumtaz, J. Rodriguez, and L. Dai, *mmWave Massive MIMO: A Paradigm for 5G*. Academic Press, 2016, doi: 10.1016/C2015-0-04849-2.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, Helsinki, Finland, Aug. 2012, pp. 13–16, doi: 10.1145/2342509.2342513.

[8] H. Kagermann, W. Wahlster, and J. Helbig, "Recommendations for Implementing the Strategic Initiative Industrie 4.0," acatech – National Academy of Science and Engineering, Germany, Apr. 2013.

[9] McKinsey & Company, "Manufacturing Analytics Unleashes Productivity and Profitability," McKinsey Global Institute, 2023.

[10] Bosch Rexroth, "The Factory of the Future: Bosch Rexroth's Approach to Industry 4.0," Bosch Rexroth Whitepaper, 2022.

[11] Siemens, "The Digital Factory: Siemens Amberg Electronics Plant," Siemens Case Study, 2023.

[12] GE Aviation, "Digital Twin: Transforming Aviation Manufacturing," GE Reports, 2022.

[13] D. Zhang, Y. Liu, and L. Wang, "A Survey of Wireless Sensor Network Architectures for Industrial Applications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 456–489, Firstquarter 2022, doi: 10.1109/COMST.2021.3123456.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[15] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012, doi: 10.1109/JPROC.2011.2165689.

[16] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, Helsinki, Finland, Aug. 2012, pp. 13–16, doi: 10.1145/2342509.2342513.

[17] Y. Lu, "Industry 4.0: A Survey on Technologies, Applications and Open Research Issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, Jun. 2017, doi: 10.1016/j.jii.2017.04.005.

[18] S. J. Qin and L. H. Chiang, "Advances and Opportunities in Machine Learning for Process Data Analytics," *Comput. Chem. Eng.*, vol. 126, pp. 465–473, Jul. 2019, doi: 10.1016/j.compchemeng.2019.04.003.

[19] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017, doi: 10.1109/MIE.2017.2649104.

[20] E. D. Knapp and R. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Syngress, 2014.

[21] J. Zhou, P. Li, Y. Zhou, B. Wang, J. Zang, and L. Meng, "Toward New-Generation Intelligent Manufacturing," *Engineering*, vol. 4, no. 1, pp. 11–20, Feb. 2018, doi: 10.1016/j.eng.2018.01.002.

[22] A. Kusiak, "Smart Manufacturing," *Int. J. Prod. Res.*, vol. 56, no. 1–2, pp. 508–517, Jan. 2018, doi: 10.1080/00207543.2017.1351644.

[23] Gartner, "Top Strategic Technology Trends for 2023," Gartner Report, 2023.

[24] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2020.

[25] P. Warden and D. Situnayake, *TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers*. O'Reilly Media, 2020.

[26] Cisco, "Cisco Annual Internet Report," Cisco Whitepaper, 2023.

[27] Siemens, "MindSphere: The Cloud-Based IoT Operating System," Siemens Whitepaper, 2023.

[28] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017, doi: 10.1109/TPAMI.2016.2577031.

[29] BMW Group, "AI in Production: Quality Control with Deep Learning," BMW Case Study, 2023.

[30] FANUC, "Intelligent Robotics for Manufacturing," FANUC Whitepaper, 2023.

[31] Google DeepMind, "Machine Learning for Energy Efficiency," DeepMind Case Study, 2023.

[32] R. High, "The Era of Cognitive Systems: An Inside Look at IBM Watson and How It Works," IBM Redbooks, 2012.

[33] Tesla, "Gigafactory: The Future of Manufacturing," Tesla Whitepaper, 2023.

[34] ABB, "ABB Ability™: Driving Digital Transformation in Manufacturing," ABB Case Study, 2023.

[35] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, Aug. 2014, doi: 10.1007/s12599-014-0334-4.

[36] NIST, "Cybersecurity Framework for Industrial Control Systems," NIST Report, 2023.

[37] IBM Security, "X-Force Threat Intelligence Index 2023," IBM Report, 2023.

[38] Fraunhofer Institute, "Industry 4.0: Challenges in Legacy System Integration," Fraunhofer Report, 2023.

[39] GE Digital, "Industrial Data Management for Industry 4.0," GE Digital Whitepaper, 2023.

[40] European Union, "Regulatory Framework for Artificial Intelligence and Cybersecurity," EU Documentation, 2024.

2.18. Műholdas rendszerek integrációja valós idejű ipari alkalmazásokban beágyazott és számítógépes rendszerek segítségével

IPAR 4.0 TECHNOLÓGIÁK

Műholdas rendszerek integrációja valós idejű ipari alkalmazásokban beágyazott és számítógépes rendszerek segítségével

Nyári Dávid

[redacted]

2024/2025/2

Tartalom

Bevezetés és ipari kontextus 3

GNSS technológiák áttekintése: működés és korlátok az iparban 4

Beágyazott rendszerek és interfészek a GNSS adatfeldolgozásban 6

Centiméter-pontosságú RTK helymeghatározás ipari alkalmazásokban 8

Szenzorfúzió: GNSS, IMU, LiDAR integrációja a robusztus pozícióért 10

Edge computing szerepe a valós idejű helymeghatározásban 12

Ipari kommunikációs protokollok: MQTT, OPC UA és 5G URLLC 14

Biztonsági aspektusok: GNSS zavarás és jelhamisítás elleni védelem 17

Esettanulmány: GNSS-integrált AGV rendszer ipari környezetben 20

Következtetések 23

Bevezetés és ipari kontextus

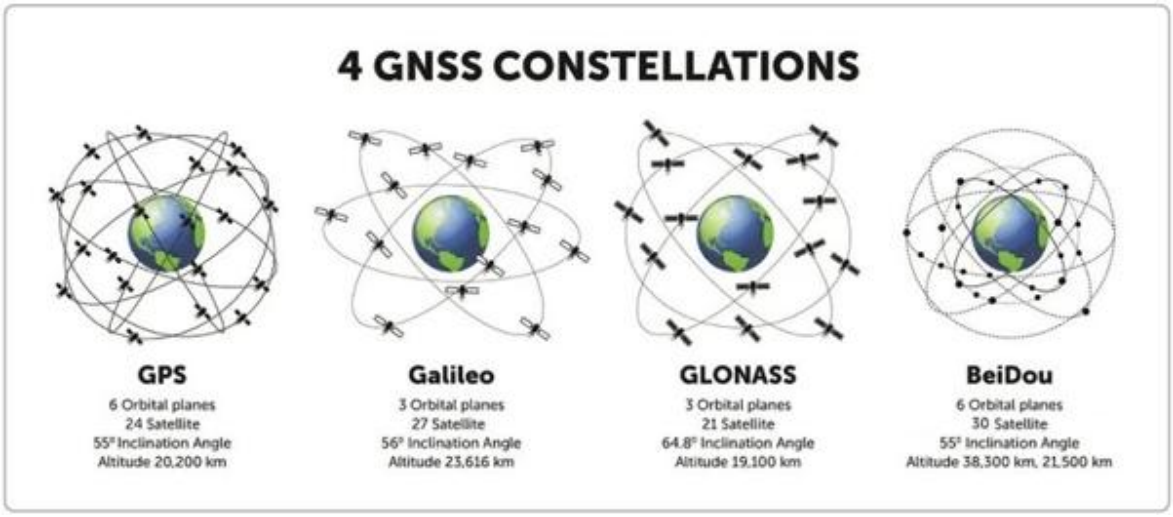
Manapság **Ipar 4.0** és az autonóm rendszerek korában egyre nagyobb szerepet vállalnak a precíz navigációs és helymeghatározó rendszerek a gyártásban, logisztikában és a mezőgazdaságban.
Az autonóm mobil robotok (raktári szállítórobot)**, automata vezetésű járművek** (önvezető autók) **(AGV)** és a **precíziós mezőgazdasági gépek** (önjáró traktorok), ezek a gépek csak akkor működnek megfelelően, ha valós idejű, megbízható helymeghatározással rendelkeznek. [1] [2] A globális műholdas helymeghatározó rendszerek (GNSS) napjainkban a legelterjedtebb megoldást kínálják bolygószintű pozíció-, sebesség- és időinformációk megszerzésére. Ezek közé tartozik az amerikai GPS, az európai Galileo, az orosz GLONASS és a kínai BeiDou – ezek közösen biztosítják a PNT (Positioning, Navigation, Timing) szolgáltatásokat a világ bármely pontján [3]. Viszont mint mindennek, ezeknek is vannak gyengeségeik.
Az ipari környezetben sokszor az is előfordul, hogy a nyers GNSS-jel nem nyújt elég pontosságot vagy megbízhatóságot. Ez a probléma megjelenhet beltéri vagy félig fedett területeken, gyárudvarakon, raktárakba, ahol a műholdjelek gyengék, vagy akár még az is előfordulhat, hogy időszakosan teljesen kiesnek. Ilyenkor esetekben érdemes a GNSS összehangolása más rendszerekkel – többek között inerciális szenzorokkal, LiDAR-ral vagy beágyazott számítógépekkel. Ezek együtt biztosítják, hogy a jármű gyenge vagy kimaradó műholdjel esetén is megbízhatóan tudjon navigálni.

A továbbiakban annak lehetőségeit vizsgáljuk meg, hogyan alkalmazhatók a GNSS rendszerek valós idejű ipari környezetben, főleg a beágyazott és számítógépes rendszerekkel összekapcsolva. A következőkben olyan kiegészítő megoldásokról le szó, például az RTK korrekciót, a **szenzorfúziót**, az **edge computingot** és az **ipari kommunikációs protokollokat**, ezeknek az összehangolt működése lehetővé teszi a centiméteres pontosságú és megbízható helymeghatározást.
A dolgozat másik fejezetben foglalkozik a GNSS-rendszerek biztonsági kockázataival, különösen a szándékos zavarás (jamming) és a jelhamisítás (spoofing) problémájával. Majd egy esettanulmányon keresztül mutatjuk be, hogyan épül fel és működik egy GNSS-alapú vezérlésű ipari AGV-rendszer egy kültéri környezetben. A példában a műholdas helymeghatározást valós időben egészítik ki más szenzorok adatai, valamint egy ipari hálózatba kapcsolt vezérlőrendszer.

GNSS technológiák áttekintése: működés és korlátok az iparban

A globális műholdas navigációs rendszerek (GNSS) olyan műholdhálózatok, amelyek a Föld teljes felszínét lefedik és így tudnak biztosítanak pozíció-, navigációs és időalapú adatokat különböző típusú alkalmazások számára. Jelenleg négy fő GNSS-rendszer üzemel: az **GPS** (USA), a **GLONASS** (Oroszország), a **BeiDou** (Kína) és a **Galileo** (Európai Unió)[3] . Ez a négy rendszer kiegészül néhány regionális megoldással is – például Japán QZSS vagy India NavIC rendszereivel –, bár az ipari gyakorlatban továbbra is főleg a globális hálózatok jeleire támaszkodunk.

A GNSS műholdak általában 20–23 ezer kilométeres magasságban keringenek a Föld körül. A bennük található atomórák olyan rádiójeleket sugároznak, amelyek időbélyegekkel vannak ellátva – ezek az alapjai a helymeghatározásnak. A GNSS-vevő a földfelszínén a műholdak jeleinek késéséből számítja ki a távolságot a látható műholdakhoz. Legalább négy műhold jelére van szükség ahhoz, hogy a vevő meg tudja határozni a háromdimenziós pozícióját és a pontos időt ehhez szükséges a trilateráció elvét alkalmazni.



A négy fő GNSS műholdrendszer (GPS, Galileo, GLONASS, BeiDou) eltérő pályaszámú és magasságú konstellációt alkalmaz. Amit fontos megjegyezni, hogy a különbségek ellenére, együttműködve képesek globális lefedettséget biztosítani.

A GNSS-technológia legnagyobb előnyei közé tartozik a **globális lefedettség** és **a passzív működés**. A helymeghatározáshoz elegendő egy kis vevőkészülék, előfizetésre nincs szükség. Ebből kifolyólag számos területen alkalmazzák a GNSS-alapú megoldásokat – a közlekedéstől kezdve egészen a mezőgazdaságig [4]. Előfordul van az ipari környezetben, logisztikai telephelyeken vagy akár bányákban is, mivel elérhetővé teszi a járművek és munkagépek folyamatos követését, illetve az automatikus navigációt. A GNSS-alapú helymeghatározás pontossága általános felhasználás esetén korlátozott: nyílt égbolt alatt a vevők rendszerint csak 2–5 méteres pontosságot érnek el. Ennek több oka is lehet például az ionoszféra és a légkör torzító hatása, a műholdak pályájának hibája, vagy az atomórák közötti szinkronizációs eltérés. Az ilyen hibák nagy részét az azonos környezetben lévő vevők hasonlóan érzékelik – ezt hívjuk

közös hibának. Ez teszi lehetővé a differenciális korrekció alkalmazását (részletesen az RTK fejezetben).

Ideális körülmények között, jó minőségű vevővel kb. **~2 méteres legjobb pontosság** érhető el álló helyzetben [5], de városi vagy ipari környezetben gyakran ennél rosszabb a helyzet.

Az ipari alkalmazások szempontjából fontos megérteni a GNSS **korlátait** és azt, hogy mik okozhatnak hibákat.[6]

- **Beltérben vagy fedett helyeken gyenge a vétel**. Ennek oka, hogy az L1 sávban (~1,5 GHz) sugárzott rádiójelek rendkívül alacsony teljesítménnyel (~20–50 W) jutnak el a Föld felszínére – és ez a jel szintje már a termikus zajszint közelében van. Az ilyen gyenge jelek **nem képesek áthatolni épületeken vagy fémtetőkön,** így beltérben a GNSS önmagában nem alkalmas *helymeghatározásra* [7]. Ipari környezetben ez különösen problémás, mivel a járművek gyakran behajtanak csarnokokba vagy féltetők alá, ahol a műholdas pozíció hirtelen megszakad – kivéve, ha rendelkezésre áll valamilyen kiegészítő technológia, például inerciális navigáció.

- **Multipath (többutas terjedés) és interferencia**:, Főleg városi és ipari környezetben fordulhat elő, hogy a GNSS jelek a talajról, falakról, konténerekről visszaverődhetnek, így **több úton érkezhetnek** a vevőhöz. Ezek a visszaverődések késleltetett, fázistolódott jelek, amelyek összezavarhatják a vevőt és pontatlan pozícióhoz vezethetnek [6]. A multipath általánosságban deciméteres vagy méteres hibákat is okozhat, és különösen a magas épületek között vagy fémes környezetben jelenthet problémát. Emellett, az **ipari rádiófrekvenciás zaj** (pl. WiFi, Bluetooth vagy elektromos berendezések) szintén zavarhatják a GNSS frekvenciákat [8]. Az ilyen hatások csökkenthetők a jól elhelyezett antennákkal akár, földelt síkkal vagy choke ring típusú antennával, illetve szűrő algoritmusokkal, amelyek képesek kiszűrni a többúthibát [9] [10].

- **Elérhető műholdak száma**: Pontos pozíció meghatározásához legalább négy műhold egyidejű vétele szükséges. Magas épületek, tartályok vagy domborzati takarásokból kifolyólag előfordulhat, hogy túl kevés műhold látható, vagy éppen nem ideális elrendezésben vannak mint amikor egy síkban helyezkednek el. Ilyenkor a helymeghatározás **pontossága jelentősen romlik**, vagy meg akár meg se történik [11]. Ipari telephelyeken ez nem szokott problémát okozni a nyílt égbolt miatt, viszont ez megtörténhet, egy kikötőben konténerek között vagy egy gyárudvaron akár daruk alatt.

- **Zavarások és támadások**: Mivel a GNSS **polgári jelei titkosítatlanok és gyengék**, ezért könnyű ezeket elektronikusan megzavarni. A Biztonsági aspektusok fejezetben részletesen is szó lesz erről, de fontos megemlíteni, hogy a szándékos jelzavarás (jamming), illetve a hamis műholdjelek sugárzása (spoofing) veszélyt jelenthet azokra az ipari rendszerekre, amelyek erősen a GNSS-re támaszkodnak.

A GNSS-alapú rendszerek tervezésekor ezért mindig érdemes figyelmbe venni, hogyan biztosítható **többrétegű redundancia** akár több konstelláció egyidejű vételével vagy GNSS+INS szenzorfúzióval, illetve milyen zavarvédelmi alternatívák alkalmazhatók (pl. interferenciadetektor, földelt vagy irányított antenna).

- Ezekből kiindulva úgy gondolom, hogy a GNSS számtalan lehetőséggel rendelkezik az ipari automatizálásban, azért is, mert képes globális koordinátarendszerben meghatározni az eszközök pontos helyzetét. Bár ez önmagában nem elegendő, a rendszer megbízható működéséhez más technológiák felhasználása is szükséges, viszont figyelembe kell venni a környezeti feltételeket.

Beágyazott rendszerek és interfészek a GNSS adatfeldolgozásban

A GNSS-vevők jellemzően speciális hardvermodulok vagy készülékek, akár az U-blox, Septentrio, Trimble gyártmányú GNSS modulok. Ezek képesek nyers mérési adatokat – gondoljunk itt például pszeudotávolságokra vagy fázisadatokra – valamint feldolgozott navigációs üzeneteket (például földrajzi koordinátákat) előállítani. **Ipari alkalmazásokban ezeknek az adatoknak valós időben kell eljutniuk a vezérlőrendszerhez**, ehhez szükség van olyan eszközökre, amelyek értelmezni és továbbítani is tudják az információt. Itt kerülnek elő a **beágyazott rendszerek és ipari számítógépek**, ezek közvetítő szerepet töltenek be a GNSS-modul és a felsőbb szintű vezérlőszoftver között.

Gyakori megoldás, hogy az AGV-ben vagy robotban egy mikrokontroller vagy **beágyazott számítógép** működik (pl. ARM alapú STM32 vagy ESP32 mikrokontroller, illetve erősebb számítási igény esetén egy NVIDIA Jetson TX2/Nano vagy x86 alapú ipari PC). Ez a beágyazott vezérlő fogadja a GNSS-vevő kimenő jelét, és elvégzi az **adatfeldolgozás kezdeti lépéseit**: kiszűri a hibás értékeket, átalakítja a formátumot, más szenzorok adataival, majd a lényeges információkat továbbítja a navigációs rendszer felé

A GNSS-modulok kommunikációja jellemzően soros vonalon történik szabványos protokollon keresztül. A legelterjedtebb ezek közül az NMEA 0183, amely ASCII szöveges üzenetek formájában adja vissza pozíciót, időt stb. (pl. 19 19 20 $GPGGA mondatok) [11] [12]. Az NMEA protokoll előnye, hogy többnyire minden GNSS-vevő támogatja, így a különböző gyártók eszközei is könnyebben integrálhatóak egy beágyazott rendszerbe [11]. Az üzenetek jellemzően UART (soros port) interfészen keresztül érkeznek, általában 9600 vagy 115200 baud sebességgel, de modernebb modulok USB-, SPI- vagy I2C-csatlakozással is működhetnek [13]. Az NMEA-üzenetek emberi olvasásra is alkalmasak, mert vesszővel tagolt szöveges formátumban íródnak.

A GGA típusú mondat például tartalmazza a földrajzi szélességet, hosszúságot, a pozíció fix minőségét, a használt műholdak számát és egyéb adatokat egyetlen sorban [14] [15].

Néhány gyártó **hatékonyabb, bináris protokollokat** is kínál a saját eszközeihez. Ilyen például a ublox GNSS modulok **UBX protokollja**, ezekkel teljes konfigurációs hozzáférés nyílik a vevőhöz és így kisebb sávszélességgel, bináris üzenetekben továbbíthatók az adatok. Ipari környezetben, amikor a GNSS-vevőt egy beágyazott mikrokontrollerhez csatlakoztatjuk, gyakran az a feladat, hogy a nyers NMEA üzenetekből kinyerjük azt az adatot amire éppen szükségünk van mint például a földrajzi koordinátákat, sebességet, és azt továbbítsuk a vezérlő algoritmusnak. Ehhez most már számos nyílt forráskódú **NMEA parser** könyvtár is rendelkezésre áll amelyeket kifejezetten beágyazott platformokra fejlesztettek [16].

Vegyünk egy gyakorlati példát: képzeljünk el egy GNSS-szel felszerelt drónt vagy AGV-t. A fedélzeti STM32 mikrokontroller UART-on kapja a GNSS modul NMEA üzeneteit 10 Hz frissítéssel. A mikrokontroller firmware-e valós időben olvassa ezeket a soros üzeneteket jellemzően interrupt vagy DMA vezérléssel, és minden érvényes pozícióadatot továbbít a navigációs szoftvernek. Közben folyamatosan figyeli a GNSS státuszát (pl. van-e 3D f ix, hány műhold van látótérben), és jelez a felsőbb vezérlésnek, ha esetleg a helymeghatározás éppen pontatlan vagy megszűnt (pl. beltéri szakasz). Eközben a beágyazott rendszer más interfészeken keresztül is kommunikálhat: például olvassa az IMU adatait I2C-n vagy SPI-n, vezérli a motormeghajtókat CAN buszon, stb. A beágyazott számítógép **integrációs csomópontként** szolgál, ahol a GNSS-adat találkozik a többi szenzornak és aktornak az adataival.

Fontos megjegyezni, hogy a **valós idejű feldolgozás** ebben az esetben kritikus: a GNSS által adott pozícióadatnak megfelelő időzítéssel kell eljutnia a vezérlő algoritmushoz, más esetben a robot reakciói nem lesznek megfelelőek. A beágyazott rendszernek ezért valós idejű operációs rendszert (RTOS) vagy megfelelő prioritású megszakításkezelést kell alkalmaznia azért, hogy garantálja késés nélkül az időkritikus adatok továbbítását. A modern ipari beágyazott platformok (pl. egy NVIDIA Jetson futtatva egy ROS alapú vezérlést) gyakran **edge computing** funkciókat is ellátnak. Ez azt jelenti, hogy az összetettebb számításokat, mint például a szenzorfúzió vagy képfeldolgozás, nem a felhőben lesz végrehajtva, hanem közvetlenül a robot fedélzetén vagy a telephelyi kiszolgálón.

- Tehát, a GNSS integrálása megköveteli a megbízható hardveres és szoftveres kapcsolatokat a beágyazott rendszerek szintjén. A mikrokontrollerek és az ipari PC-k azt valósítják meg, hogy a műholdas adatok valóban felhasználhatók legyenek a valós idejű vezérlésben: konvertálják a protokollokat, ütköztetik másik szenzorokkal, és időben elküldik a megfelelő modulnak.

Centiméter-pontosságú RTK helymeghatározás ipari alkalmazásokban

Az ipari alkalmazásokban mint például az autonóm járműveknél, precíziós földmunkagépeknél vagy drónoknál a hagyományos, méteres pontosságú GNSS nem ad elegendő megbízhatóságot. Vegyünk akár egy automata targoncát, amelynek centiméteres pontossággal meg kell állnia, hogy felvegyen egy raklapot, vagy egy önvezető személyautót, amelynek sávon belüli pozícionálásához néhány deciméteres különbség is túl nagy. Ezért lettek kifejlesztve a **differenciális GNSS (DGNSS)** módszerek, köztük **a Real-Time Kinematic (RTK)** technológia, amely valós időben képes centiméteres helyzetmeghatározás biztosítására.

Az **RTK alapja** egy referenciaállomás (bázis) és egy mozgó vevő (rover) között történő együttműködés. A bázisállomás egy , rögzített pozíciójú GNSS vevő, amely folyamatosan méri a műholdjeleket, és összehasonlítja a mérési eredményeket az általa ismert koordinátákkal. Mivel a bázis és a rover földrajzilag közeli (általában néhány kilométeren belül találhatóak meg), a légköri és műholdas hibák hatása nagyon hasonlít a két vevőnél. A bázis amikor kiszámolja a **valós idejű korrekciókat** ezekre a közös hibákra, akkor továbbítja a rovernek A rover ezeket a korrekciókat felhasználva számítja ki saját pozícióját, így a közös hibák gyakorlatilag kiesnek – így akár az **1–2 cm pontosságú** relatív pozíció is elérhető lesz [17][18] . Fontos, hogy ez a pontosság relatív a bázisállomáshoz. Ha a bázisállomás földrajzi helyzete precízen meghatározott (pl. geodéziai beméréssel), akkor a rover is abszolút értelemben centiméteres pontosságot tud elérni.

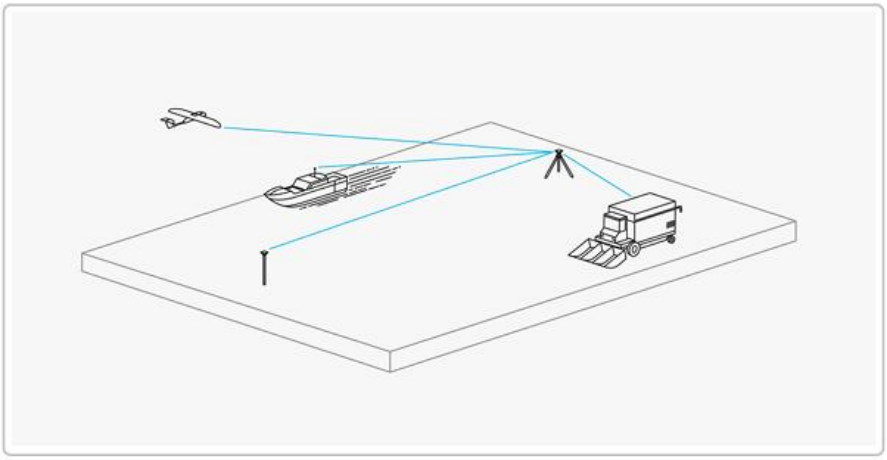
Az RTK egy viszonylag régi technológia – már több mint 20 éve jelen van a geodéziában és földmérésben. Viszont elérhetőbb lett a mikroelektronika és a távközlés fejlődése lehetővé tette, hogy ezek a rendszerek **olcsóbbá és jóval szélesebb körben hozzáférhetővé** váljanak [19] [20]. Ebből fakadóan ma már néhány száz dolláros RTK GNSS modul és egy rádiómodemnek a segítségével bárki kísérletezhet centiméteres pontosságú helymeghatározással. Ezt korábban nem lehetett megtenni, mert szinte elérhetetlen volt az ára miatt, és specializált eszközöket igényelt.

A korrekció eljutása a roverhez: A bázisállomás által számolt korrekciós adatok továbbítására szabványos protokoll szolgál ez, az **RTCM** (Radio Technical Commission for Maritime Services) üzenetformátum [21]. Az RTCM üzenetek tartalmazzák a bázis által mért nyers fázis- és kódméréseket, illetve az órára és pályára vonatkozó differenciális korrekciókat is. A rover ezeket az adatokat felhasználva pontosítja saját helymeghatározását valós időben. A kapcsolat két féle lehet, rádiós (pl. UHF sávú adó-vevőkkel) vagy hálózati (IP alapú). Ipari környezetben gyakran előfordul, hogy az **NTRIP** protokollt használják, ami tulajdonképpen az interneten (vagy intraneten) keresztül továbbított RTCM korrekciókat jelenti egy szerver-kliens architektúrában [22] [23]. Ebben az esetben a bázisállomás egy NTRIP szerverre küldi az adatokat (vagy saját maga üzemelteti ezeket a szolgáltatást), a rover pedig ezt követően kliensként csatlakozik és így folyamatosan megkapja a korrekciókat.

Abban az esetben, ha rendelkezésre áll a telekommunikációs hálózat (3G/LTE/5G), ez nagyon rugalmas: a rover lefedettségen belül bárhol eléri a bázis korrekcióit. Más esetben, hálózat híján, közvetlen rádiós összeköttetés is kiépíthető a bázis és rover között például 433 MHz vagy 915 MHz ipari rádiómodemekkel, bár ilyenkor a hatótáv korlátozottabb és frekvenciaengedélyekre is szükség lehet.

Az RTK fontossága az iparban: Számos alkalmazásnál van szükség pontos helyzet- és pályakövetésre. Vegyünk példának egy önvezető bányadömpert, melynek centiméter pontosan kell tudnia, merre halad a kitűzött nyomvonal mentén; egy precíziós permetező drónnak vagy traktornak soron belül kell maradnia a növények között, minimális átfedéssel permetezve. Egy logisztikai AGV-nek pontosan kell dokkolnia a töltőállomáson. Az RTK alkalmazásával a már elérhető pontosság (1-2 cm) **összemérhető** a gépeknek fizikai méreteivel és az elvárt műveleti pontossággal. Ezzel elérhetővé teszi **a GPS-alapú autonóm vezérlést** olyan feladatokban is, ahol kizárólag emberi irányításra vagy fizikai jelölőkre, mint például padlóba épített mágnesszalagokra vagy optikai követővonalakra volt szükség a tájékozódáshoz.

Egy telephelyi RTK rendszer sematikus ábrája: egy bázisállomás korrekciós jeleket sugároz, amelyeket több mozgó jármű (rover) – *legyen az drón, hajó vagy földi jármű – használ a centiméter pontosságú navigációhoz* [24]. *Az RTK alapú irányítás különféle iparágakban alkalmazható a precíz navigáció érdekében*



Az RTK integrációjakor nem szabad figyelmen kívül hagyni, a **rendszer valós idejű képességeit**. A korrekciók általában 1 Hz frissítésűek, ezek elegendőek a lassabban mozgó járművekhez (pl. traktor, buldózer). A gyorsabban haladó rendszereknél, vagy ahol előfordul jelentősebb a dinamikus mozgás (pl. drónok), 5–10 Hz is szükséges lehet, ezt a modern RTK rendszerek (multi-GNSS, többfrekvenciás vevők) már tudják biztosítani.

A **konvergenciaidő** (idő, ameddig a rover fix megoldást kap) egy szintén fontos tényező. A legújabb RTK vevők többnyire néhány másodperc alatt fix pozícióra jutnak, de rossz körülmények között van, hogy eltarthat 1-2 percig is.

Az ipari megoldásoknál sokszor **hibrid GNSS/INS megoldást** használnak, hogy az alap felálláskor vagy az ideiglenes RTK kihagyások esetén is tudjanak navigálni (Erre kitérünk a következő fejezetben). Például egy AGV induláskor még csak „float” RTK állapotban van, és

csak 20–30 méter megtétele után kap „fix” pozíciót, de addig az IMU adatai segítik a stabilizálást.

Kifejezetten fontos figyelembe venni, hogy az RTK **infrastruktúraigényes**. Azért, hogy működtetni lehessen vagy saját bázisállomást kell telepíteni a műveleti területen melynek pontos koordinátáit geodéziai módszerekkel be kell mérni, vagy előfizetni egy szolgáltatónál például egy országos RTK hálózathoz. Viszont az utóbbi nem mindenhol érhető el ipari nagyságban vagy megfelelő megbízhatósággal. Ha a cég saját bázist használ, a cég teljes ellenőrzést nyer a rendszer felett, ez a biztonság szempontjából kifejezetten előnyös. A telephelyi RTK bázis és a járművek közötti kommunikáció megvalósításához ma már gyakran használnak rendelkezésre álló **ipari WiFi vagy privát 4G/5G hálózatot**, ezért nincs szükség külön rádiós modempárok telepítésére (erről bővebben a kommunikációs protokollok fejezetében lesz szó).

Szenzorfúzió: GNSS, IMU, LiDAR integrációja a robusztus pozícióért

Bármennyire is pontos a GNSS mégha RTK-val is van kiegészítve, önmagában nem képes minden környezetben folytonos és megbízható pozíciót szolgáltatni. Ahogy azt már az előző fejezetekben is említettük, előfordulhat jelkimaradás (pl. tető alá behajtáskor), átmeneti zavarok, vagy akár csak annyi, hogy a GNSS pozíció frissítési sebessége (mondjuk 5 Hz) nem elegendő sűrű a vezérlőrendszer optimális működéséhez**.**

Ezért az ipari járművek és robotok szinte mindig több szenzor adatát egyesítik a navigációhoz, ezt hívjuk szenzorfúziónak. Ennek egy általános formája a GNSS és IMU integrációja, ezeket gyakran egészítenek ki további érzékelőkkel, akár **LiDAR**-ral vagy kamerával.

- **IMU (Inerciális mérőegység):** Tipikusan 3 tengelyű gyorsulásmérőt és 3 tengelyű giroszkópot tartalmaz, akár magnetométert is. Az IMU saját koordináta-rendszerében méri a járműnek a gyorsulásait és szögsebességeit. Ezekből rövid távon integrálással kinyerhető a pozíció- és orientáció-változás. Előnye, az is, hogy **nagyon nagy frissítésű** akár 100–1000 Hz is lehet, és teljesen önálló nem függ külső jelektől. Ezzel áthidalhatja a GNSS két mérési időpontja közötti mozgást, illetve áthidalhat rövid GNSS kimaradást is. Hátrányai közé tartozik a **drift**: a legjobb IMU-k is az idő múlásával elcsúsznak kis mértékben, a költséghatékony MEMS IMU-k pedig néhány másodperc után már akár jelentős hibát is fel halmoznak önmagukban. Többek között ezért van szükség a GNSS adatainak felhasználására az **IMU folyamatos kalibrálásához** (korrekciójához). A GNSS jel hosszú távon stabil, nem romlik (nincs driftje, csak véletlen zaj és elfogadható nagyságú hibák), míg az IMU rövid távon nagyrészt pontos és sima mozgásleképezést ad.

A kettő kombinációja a klasszikus **GNSS/INS integrált navigációs rendszer** alapja [25][26].

- **LiDAR (lézeralapú távolságmérő és letapogató):** A LiDAR egy gyorsan forgó vagy szkennelő lézersugár segítségével felmér egy pontfelhőt a jármű környezetéről. Ebből egyrészt információt szerezhetünk **a környezetbeli akadályokról** például ha valami oknál fogva, egy tárgy kerül a jármű elé, amivel az ütközést többek között el lehet kerülni, ezzel károkat elkerülni Másrészt egy megfelelő algoritmussal (pl. SLAM – Simultaneous Localization and Mapping) a LiDAR adatokat összevetve a jármű mozgása közben a rendszer **mozgása is kikövetkeztethető**. Egyszerűbben: ha látjuk a környező falakat, tárgyakat a pontfelhőben, a saját elmozdulásunk kiszámítható a pontfelhők illesztéséből, akár GNSS nélkül is. Ezt hívjuk **LiDAR odometriának** vagy LiDAR-alapú lokalizációnak.

  A LiDAR ezzel egyfajta független pozícióbecslést adhat akár beltérben, illetve **kiegészítheti a GNSS/INS rendszert** kültéren is, növelve a megbízhatóságot nehezebb környezetben például ha GNSS jel zavart vagy multipath torzított, a LiDAR adhat egy második véleményt a mozgásról. Az ipari robotoknál gyakran előfordul, hogy a LiDAR-t eleve alkalmazzák biztonsági okból (ütközéselkerülésre). Így szinte magától értetődő, hogy ennek adatait a navigációs stack is felhasználja.

A szenzorfúzió matematikai keretét leggyakrabban **a Kalman-szűrő** vagy valamilyen hasonló állapotbecslő algoritmus adja [27][28]. A jármű fedélzeti számítógépén, tipikusan egy **kiterjesztett Kalman-szűrő (EKF)** fut melynek állapotvektora tartalmazza a jármű pozícióját, sebességét, orientációját, és még az IMU bizonyos hibaparamétereit is (pl. giroszkóp drift).

Az EKF két lépésben működik: *predikció* és *korrekció*. Predikció során az IMU mérések alapján nagyon magas gyakorisággal akár 100 Hz frissítéssel megbecsüli, merre mozdult el a jármű miközben telik az idő. Ezt a becslést azonban a drift miatt csak rövid távon lehet pontossággal fenntartani mivel az IMU érzékelőiben jelentkező eltolódások fokozatos hibát eredményeznek.

Itt kerül elő a korrekció: ilyenkor rendelkezésre áll egy külső mérés, akár a GNSS pozíció 5 Hz-en, vagy LiDAR lokalizáció 10 Hz-en, az EKF összeveti az IMU alapján számolt *várható* pozíciót a külső szenzor által *mért* pozícióval [28][29] .

A két érték közötti különbség alapján a szűrő módosítja az állapotvektort, figyelembe véve a szenzorok méréseinél történő bizonytalanságot. Így az IMU által becsült pozíció folyamatosan korrigálódik a külső referencia a GNSS vagy a LiDAR irányába.

Az EKF folyamatosan fut, így valós időben ad egy **fúzióból származó optimális becslést** a jármű állapotáról.

Egy ipari AGV esetén például a fúziós algoritmus 50 Hz-en fut. Minden ciklusban beolvassa a legújabb IMU adatot (gyorsulás, szögsebesség) és ezek alapján, prediktálja a jármű új pozícióját. Eközben szinte folyamatosan, 0,2 másodpercenként (5 Hz) érkezik a GNSS pozíció is. Ekkor az EKF összehasonlítja, mennyire tér el az IMU által számolt pozíciótól, és finoman hozzáigazítja a a becsült pozíciót a mért értékhez, ezzel megkapva a fúziós pozíciót.

Abban az esetben, ha a jel kimarad, az EKF működik az IMU alapján, de a bizonytalanság folyamatosan növekszik, jelezve (a bizonytalansági mátrixba), hogy a pontosság közben romlik. Amint újra elérhető GNSS-adat, a rendszer frissíti a becslést, és a pontosság helyreáll.

Ezzel a **kombinált rendszer sokkal robusztusabbá** válik, mint bármelyik szenzor külön-külön: GNSS-kiesés esetén viszont rövid ideig az IMU és a LiDAR együttesen is képes megbízható pozícióbecslést nyújtani.

A szakirodalomból és az ipari tapasztalatokból szintén kiderült, hogy a **GNSS/INS szenzorfúzió kihagyhatatlan** az autonóm járműveknek a megbízható és pontos navigációjához. Egy gyakorlati példa erre, kikötői autonóm teherautó esetén a fedélzeten lévő GNSS/INS szenzor együttes ad **centiméter-szintű pozíciót**, a lézerszkennerek foglalkoznak az akadálydetektálással, és a fedélzeti számítógép folyamatosan végzi a navigációs és vezérlési számításokat[30] .

Ezek a fejlett rendszerek **szorosan integrált GNSS/INS megoldást** alkalmaznak (tightly coupled). Ebben az esetben ez azt jelenti, hogy nem elég a GNSS által számított pozíció megy be a fúzióba, hanem itt a GNSS nyers méréseit is figyelembe veszik az INS mellett, így akár kevesebb műhold esetén vagy részleges jelnél is felhasználják ezt az információt[31] .

- A szenzorfúziónak az eredménye, hogy a rendszer **jobban teljesít, mint bármelyik komponens külön-külön**. A GNSS globális stabilitást ad, az IMU folytonosságot és nagy frissítést, a LiDAR/kamera pedig környezeti érzékelést és helyi referenciát. Együttműködve lehetővé teszik autonóm járművek számára, hogy összetett, GNSS-jel szempontjából kihívásos környezetben is precízen navigáljanak.

Edge computing szerepe a valós idejű helymeghatározásban

Az **edge computing**, a peremhálózati számítás lényege, hogy azokat a feladatok ahol számítást kell végezni, a hálózat “széléhez”, közel az adatok keletkezésének helyéhez telepítjük. Ahelyett, hogy a feldolgozásokat egy távoli felhőszerveren végeznénk, az adatokat helyben, a hálózat „szélén” dolgozzuk fel.

Ipari környezetben ez azt szokta jelenti, hogy a telephelyen esetleg magán az eszközön lévő számítógépek végzik a folyamatos adatfeldolgozást, és így nem függenek nagymértékben az internetkapcsolattól vagy egy távoli adatközponttól.

Az autonóm rendszerek és valós idejű vezérléseknél a **késleltetés minimalizálása** kritikus fontosságú. Ha például egy önvezető jármű kameraképeit egy felhőbe küldjük feldolgozásra, a hálózat késleltetése miatt túlságosan is lassan érkeznek vissza a vezérlőparancsok, ez biztonsági kockázatot jelentene.

Ezért muszáj a fedélzeti számítógépnek (edge device) meghoznia a döntéseket néhány ezredmásodperc alatt. Ez szintén jellemző a GNSS alapú helymeghatározásnál is. Előnyt jelent, ha a **korrekciók számítása és a szenzorfúzió** lokálisan történik.

Például ha egy telephelyi RTK bázisállomásának az adatait a helyi hálózaton osztjuk meg (NTRIP caster formájában). Így nem egy távoli szolgáltatótól függünk, ezáltal a kommunikáció 10–20 ms helyi késleltetéssel megoldható. Ellentétben a potenciálisan nagyobb internetes késleltetéssel.

Az edge computing a késleltetés csökkentése mellett, **növeli a rendszer megbízhatóságát és biztonságát is**. Mivel az érzékenyebb adatok például egy gyár járműveinek pontos pozíciója helyben maradnak, ezzel kisebb az esélye, hogy kibertámadás vagy adatlopás áldozatául esenek útközben.

Ami fontos, ha az internetkapcsolat meg is szakad, a helyi rendszer továbbra is működőképes tud maradni. Egy autonóm targoncának nem szabad attól függeni, hogy épp van-e felhőkapcsolat.

Az ipari IoT és 5G rendszereknél egyre elterjedtebba fog computing vagy multi-access edge computing (MEC). Itt ez azt jelenti, hogy a szolgáltató (pl. 5G hálózat üzemeltetője) a helyi bázisállomás mellé telepít kiszolgáló szervereket, ahol a felhasználó applikációi futnak közvetlen közelben. Ez az **5G URLLC** (Ultra Reliable Low Latency Communication) architektúrák része.

Példa: Egy okosgyárban az autonóm járműveknek a flottáját egy helyi **edge szerver** felügyeli. Ez a szerver fogadja a járművektől érkező az adatokat (pozíció, akkumulátor állapot, stb.). Továbbiakban futtatja a flottamenedzsment szoftvert (pl. ütközéselkerülő globális algoritmus, útvonaltervezés több járműnek), majd utasításokat küld vissza. Mivel a szerver a gyárban található ebből fakadóan, a kommunikáció gyors és stabil. Ugyanez a szerver elvégezheti az **adatfeldolgozást is**, például a LiDAR pontfelhő összevetésére több jármű között (ha kollektív térképet építenek). Az edge computing tehát lehet *fedélzeti* edge (a jármű saját számítógépe, ami pl. a szenzorfúziót végzi), illetve *helyszíni* edge (pl. a gyár központi vezérlőteremben egy ipari PC klaszter, ami a flottát koordinálja).

A GNSS integrációval kapcsolatban az edge computing egyik szoványos megjelenése a **lokális adatszolgáltatás.** Ilyen mikor a telephelyen fut egy saját GNSS korrekciós szolgáltatás (RTK base), vagy akár egy saját térinformatikai adatbázis (geofencing zónák, tiltott területek).

Ezeket az adott járművek valós időben elérhetik a belső hálózaton keresztül. Ezzel nem kell minden járműnek magának számolnia mindent vagy külső adatot lekérnie, a nehéz feladatokat (pl. precíz RTK számítás, térképek kezelése) átveheti az edge infrastruktúra.

- Az edge computing átalakítja a valós idejű adatfeldolgozás módját az iparban. Azzal, hogy decentralizál, a forráshoz közel viszi a számítást. Ezzel csökkenti a késleltetést és a hálózatra jutó terhelést [32][33].
  Az autonóm rendszerek a saját "tudásukkal" helyben tudnak reagálni. A globális optimalizációt végző algoritmusok is a telephely peremhálózatán maradnak, ilyen módon is garantálva az állandó rendelkezésre állást.
  Ez a szemléletváltás kifejezetten fontos, abból a szempontból is, hogy a GNSS-szel felszerelt ipari eszközök valóban hatékonyan és biztonságosan működhessenek valós időben.

Ipari kommunikációs protokollok: MQTT, OPC UA és 5G URLLC

Egy modern ipari környezetben különböző eszközök és rendszerek közötti **kommunikáció** legalább annyira fontos, mint maguknak az eszközöknek a funkciói. A GNSS-alapú helymeghatározó rendszerek integrációjakor biztosítani kell, hogy a szenzoradatok, a számított pozíciók és vezérlőutasítások megbízhatóan és késlekedés nélkül eljussanak a megfelelő helyre (pl. a járműtől a központi rendszerig és vissza).

Ezt a feladatot látják el az **ipari kommunikációs protokollok**. Ezek közül kiemelkedően foglalkozunk az MQTT-val, az OPC UA-val és a korszerű mobilhálózati (5G URLLC) kommunikációval.

- **MQTT (Message Queuing Telemetry Transport)**: Az MQTT egy könnyűsúlyú, **publish/subscribe** elvű üzenetküldő protokoll, ezt kifejezetten az **IoT eszközök közötti kommunikációra** terveztek [34]. Lényege, hogy nagyon kis overhead-del, alacsony sávszélesség mellett is megbízható üzenettovábbítást biztosít.
  Egy központi *broker* segítségével működik. A szenzorok vagy eszközök (kliensek) bizonyos témákra (*topic*) üzeneteket küldhetnek fel (publish). Másik eszközök feliratkozhatnak (subscribe) ezekre a témákra, és ezt követően megkapják az üzeneteket. Például egy AGV megadhatja a saját pozícióját „**a jarmu/AGV1/pozicio**" témára minden 100 ms-ban. Erre a témára a központi felügyeleti rendszer és folyamatosan megkapja az adatokat.
  Az MQTT **nagyon hatékony**, azért is, mert **könnyű és kis erőforrás-igényű**.

Ezeket gyakran használják beágyazott eszközökben is, még szűk sávú kapcsolatokonál is előfordul (pl. mobilneten keresztül). Úgy lett tervezve, hogy megbirkózzon az instabil hálózatokkal, minimálisra csökkentve a forgalmat[35] .

Ipari környezetben hasznosak az állapotjelzések, érzékelő adatok továbbítására. A GNSS integrációnál MQTT-n keresztül továbbítható a **valós idejű pozíció és státusz** a járművekről a központi rendszer felé biztonságosan és hatékonyan. Maga az RTK korrekció is továbbítható MQTT-n vagy hasonló IP-alapú protokollal (hiszen az RTCM üzenetek is a biteknek a sorozata, amit lehet MQTT payloadban küldeni).

Az MQTT előnyei között van a **decentralizált skálázhatóság.** Könnyű új eszközöket hozzáadni a hálózathoz, de ehhez fel kell iratkozniuk a megfelelő üzenetekre, ezzel részei lesznek a rendszernek.

- **OPC UA (Open Platform Communications – Unified Architecture)**: Az OPC UA egy ipari kommunikációs keretrendszer és protokoll. Kifejezetten az ipari adatok megbízható, platform-független cseréjére terveztek. A protokollt **IEC 62541 szabvány** írja le, és az OPC Foundation fejleszti[36].

  Legnagyobb előnye, hogy **egységes adatmodellt és szolgáltatáskészletet** nyújt az ipari rendszerek számára. Tehát nem csak biteket küld át, hanem strukturált információt is. Támogatja a kliens-szerver és a publish-subscribe kommunikációt, beépített biztonsági modellje van, autentikáció, titkosítás, jogkezelés.

  Példaként, létrehozhatunk egy "AGV" objektumot, tulajdonságaival (pozíció, sebesség, akkumulátor szint stb.). Ezekhez valós időben hozzáfér egy felső szintű SCADA vagy MES rendszer OPC kliensen keresztül.

  Ez egy gazdagabb integrációt valósít meg, egy egyszerű Modbus regiszter kiolvasásánál. A **GNSS integráció** szempontjából OPC UA akkor kerül elő, amikor a helymeghatározó rendszer adatait be kell kötni a meglévő ipari infrastruktúrába.

  Például a gyárnak a menedzsment rendszere OPC UA-n keresztül lekérdezheti az autonóm targoncáknak a pozícióját, vagy parancsot adhat neki, például, "menj a 3-as állomásra".

  Az OPC UA lehetővé teszi, azt, hogy a kommunikáció biztonságos és interoperábilis legyen. Így egy Microsoft alapú gyári dashboard szintúgy kommunikálhat a Linux alapú robotvezérlő OPC szerverrel. Mivel egyre inkább alapnak számít az ipar 4.0 kommunikációban, ezért **az OPC UA integráció biztosítja, hogy a GNSS-alapú rendszerünk "beszéljen egy nyelvet" a többi géppel** a termelőüzemben.

  Például egy dolgozó a vezérlőteremben egy OPC UA klienssel figyelheti egy térképen keresztül az összes AGV helyzetét. Ezeket az adatokat a járműveknek közvetlenül az OPC UA szerver moduljai szolgáltaják folyamatosan.

- **5G URLLC (Ultra Reliable Low Latency Communication):** Az 5. generációs mobilhálózat egyik speciális üzemmódja az URLLC, amelyet kimondottan az ipari és nagy megbízhatóságot igénylő alkalmazásokhoz terveztek. Fő célja, hogy vezeték nélküli hálózaton is elérhető legyen a "vezetékes szintű" megbízhatóság és az alacsony késleltetés.

  Az URLLC akár <1 ms késleltetést és legalább **99.999%** megbízhatóságot ígér [37].

Ez azt jelenti, hogy **szinte azonnali reakcióidejű** kommunikáció valósítható meg. Így alkalmas lehet például robotok valós idejű vezérlésére, távműtétekre, járművek ütközésének az elhárítására stb.
Ipari környezetben eddig a kritikus vezérléseket inkább vezetékes hálózaton (pl. Ethernet, ProfiNet) csinálták meg. Főleg azért, mert a WiFi és a 4G nem adott elég garanciát a megbízhatóságra. Az 5G URLLC ezt a helyzetet meg tudja változtatni. Megvalósítja a "drót elvágását" még kritikus alkalmazásokban is [37][38].
A rádiós kapcsolat is tartja a szükséges szintet. Ez óriási rugalmasságot ad, itt gondolhatunk egy gyári robotkarra, amit eddig kábel kötött a vezérlőhöz. 5G URLLC-n keresztül már az is elérhető, hogy vezeték nélkül is vezérelhető. Így szabadabban mozoghat, akár át is telepíthető.

A GNSS integráció és autonóm járművek esetén az 5G URLLC több módon is fontos feladatokat lát el. A járművek és a központi rendszer közötti fenálló kommunikációt például flottakoordinációs utasítások, szenzoradatok megosztása megbízhatóan kis késleltetéssel biztosítva.
Mellette a **RTK korrekciók továbbítására is ideális**, hiszen itt is kritikus a pár tizedmásodpercnél nem régebbi adatok eljuttatása a roverhez.
Az 5G azt is lehetővé teszi, hogy a járművek egymással is kommunikálhassanak (V2V – vehicle to vehicle) alacsony késleltetéssel. Ezzel például egy konvojban haladó AGV jelezheti a mögötte jövőnek a pontos pozícióját vagy fékezését.
Fontos megjegyeznem azt, hogy az 5G URLLC általában **privát hálózatként,** a gyár területén kerül kiépítésre (lokális 5G "campus" hálózat). Ezzel az adott ipari szereplő kontrollálhatja a teljes infrastruktúrát, garantálva a sávszélességet és a biztonságot.
Az 5G rendszerben a **hálózat peremén futó alkalmazások** (MEC) közvetlen a bázisállomásnál csatlakoznak. Például egy helyi RTK caster szerver közvetlenül az 5G core-on, azért hogy ne kelljen az internetet igénybe venni, ezzel is csökkentve a késleltetést [39][40].

A három technológia együttes alkalmazása (MQTT, OPC UA, 5G) azért valósult meg, hogy a **GNSS alapú helymeghatározás adatai biztonságosan és gyorsan eljussanak** az ipari vezérlőrendszer megfelelő pontjaira.
Egy példa a mi esetünkben: Az AGV fedélzetén futó vezérlőegység MQTT-n publikálja a státuszinformációkat, például pozíció, sebesség, állapot. Az edge szerveren futó flottamenedzsment ezeket összegyűjti, majd döntéseket hoz. Az OPC UA-n keresztül kiad egy új célpozíciót az AGV-nek.
A parancs 5G hálózaton keresztül jut el, URLLC módon a járműhöz, ezzel ez végrehajtódik. Közben a GNSS RTK korrekció ugyanazon a 5G hálózaton érkezik meg az AGV vevőjéhez egy IP adatfolyamban (például közvetlenül MQTT vagy egy RTCM over TCP kapcsolat által) [41].
Mindez néhány tizedmásodperc alatt lezajlik, így a rendszer folyamatosan valós idejű működést biztosít.

A **kommunikáció integrálása legalább olyan fontos, mint maguk a szenzorok**. Nem elég az, hogy van pontos pozíciónk, ha nem tudjuk időben továbbítani oda, ahova szükséges. Hiába tud a központ korrigálni egy útvonalat, ha nem éri el a járművet. Az ipari protokollok és hálózatok tervezése ebből a szempontból a GNSS integrációs projekt kritikus része lesz. Ezen segítenek a modern szabványok (mint az MQTT és OPC UA) és technológiák (5G) ezek már rendelkezésre állnak, hogy megbízható "idegrendszert" biztosítsanak az ilyen komplex kiber-fizikai rendszereknek.

Biztonsági aspektusok: GNSS zavarás és jelhamisítás elleni védelem

Ahogyan már korábban említettük, a GNSS egyik kritikus pontja **sebezhetőség a rádiófrekvenciás zavarásokkal szemben**. Ipari környezetben, ahol a megbízhatóság elsődleges nem szabad figyelmen kívül hagyni, hogy egy külső vagy belső tényező könnyen megzavarhatja a GNSS-alapú navigációt.
Két fő fenyegetést különböztethetünk meg: a **zavarás (jamming)** és a **megtévesztés (spoofing)**.

Emellett azokkal , az általános kiberbiztonsági intézkedésekkel is foglalkozunk, amelyek szükségesek a kommunikációs csatornák védelméhez.

- **Jamming – rádiós zavarás**: A GNSS jelek zavarása általában úgy történik, hogy egy eszköz erős rádiójeleket sugároz a GNSS frekvenciasávjában (pl. L1 sáv ~1575 MHz körül). **Elnyomva a hasznos műholdjeleket** a vevő antennájánál. Mivel a műholdnak a jele nagyon gyenge, ezért egy pár wattos adó is képes lokálisan "túlkiabálni" azt. Az ilyen **GPS jammer** eszközök sajnos könnyen beszerezhetők (bár a legtöbb országban illegálisak, persze az ilyeneket mindig ki lehet játszani). Akár egy hordozható, autóba dugható jammer is több száz méteres körben is meg tudja ezt csinálni. Így akár teljesen meg is tudja bénítani a GNSS vételt az érintett területen [43]. Ipari szempontból ez komoly kockázatot jelenthet, például egy kívülálló szándékosan (vagy akár véletlenül, pl. ha egy sofőr használ jammer-t a saját járművében) zavarhatja egy egész logisztikai telephely GNSS alapú rendszerét. A zavarás nem azért veszélyes, mert hamis adatot ad, egyszerűen csak **megfosztja a vevőt a jelektől**. Így az nem ad pozíciót, vagy nagyon bizonytalanná válik.
  Ez alapjába véve is veszélyes lehet. Vegyünk egy autonóm gépet, ami hirtelen "megvakul" pozíciót tekintve. Ha van is inerciális tartaléka, hosszabb távon nem tud megbízhatóan működni. Az is megtörténhet, hogy a zavarás alatt a vevő esetleg nem is tudja, hogy zavart jel miatt nincs pozíció, annyit lát, hogy nincs vétel.

A GNSS zavarás **valós fenyegetés,** európai felmérések szerint rendszeresen felmerülnek a véletlen vagy szándékosan zavart okozó jelek, például hétköznapi példával élve az autóba rejtett jammerek formájában is előkerülhetnek [43].

Védekezés: A jamming ellen több módszer is létezik, bár ezek közül egyik sem tökéletes. Ezek közül a legalapabb a **zavarásdetektorok** használata. Ezekkel figyelik a GNSS frekvenciasáv zajszintjét, és riasztanak, ha szokatlanul magas (fehér zaj jelenik meg). Egyes professzionális GNSS vevők beépítve tartalmaznak ilyen figyelést.
Fizikai védelemként lehet alkalmazni az **irányított GNSS antennákat** (*pl. olyan antenna, ami csak az ég felől érkező jeleket erősíti, a horizont felől jövőket elnyomja, ezzel a helyszíni zavarást meg tudja nehezíteni*), vagy akár **antennarendszerek** használata, amik nullhelyeket tudnak létrehozni a zavaró jel irányába. Bár ezek drágák és bonyolultak.
Fontos ennek a **jogszabályi és biztonsági oldala:** egy ipari telephelyen szükséges felkészülni arra is, hogy a GNSS kieshet. Ekkor a rendszernek biztonságos állapotba kell kerülnie (pl. a robotok megállnak, vagy inert módon folytatják a mozgást a legutolsó ismert cél felé lassítva, stb.). Ezért kell mindig egy "B terv" GNSS nélkül. Viszont vannak újabb alternatív technológiák, például helyi **lokációs rendszerek, mint az UWB** alapú tag-ek. Ezekkel a beltéri navigációt lehet biztosítani GNSS kimaradás esetére.

- **Spoofing – jelhamisítás**: Miközben a jamming "csak" elveszi a jelet, a **spoofing** ennél jóval kifinomultabb. Ilyenkor a támadó egy olyan hamis GNSS jelet sugároz, amely **megtéveszti a vevőt,** mert úgy látszik, mintha valódi műholdtól jönne.
Valójában ez hibás információt hordoz [44]. Ez a módszer arra képes, hogy a vevő téves pozíciót számoljon, anélkül hogy észrevenné azt, hogy átverték.

  Ilyenkor be lehet sugározni egy "elcsúsztatott" koordinátát, ekkor a jármű azt hiszi, más pozícióba van, mint a valóságban. A spoofingot már demonstráltak gyakorlatban is erről van egy elhíresült eset, amikor egy drónt eltérítettek hamis GPS jelekkel.
  Ipari üzemek ellen irányuló spoofing támadás célja az is lehet, hogy kárt okozzanak nekivezetni egy robotot valaminek, vagy eltéríteni azt.
  A modern GNSS vevőknek egy része már figyel bizonyos spoofing jeleket. Abban az esetben például, ha hirtelen nagyot ugrik az óra vagy a pozíció, gyanús tevékenységet érzékelhet. Ezek ellen vannak **ellenintézkedések**, akár a többfrekvenciás vevők, amelyeknek több csillagkép egyszerre vétele nehezíti a spoofingot (mert ilyenkor a támadónak szinkronizált hamis jeleket kellene sugároznia mindenfelél).
  A **kriptografikus védelem** is kezd gyakorivá válni. Kezdve a Galileoval, itt például bevezettek egy nyílt szolgáltatásos navigációs üzenet hitelesítést (OS-NMA). Ez digitális aláírással látja el a műhold üzenetét, így a vevő észlelheti, azt az esetet, ha nem valós forrásból jön (persze ez csak a navigációs üzenetre igaz, a vivőre nem).
  A katonai GNSS jelek például a *GPS M-kód* eleve titkosítottak, így a támadó nem tud valós hamis jelet előállítani, de a polgári jelek védtelenek.

Védekezés: A leghatékonyabb védelem a spoofing ellen a többféle szenzor kereszthivatkozása. Például ha a GNSS alapján azt látjuk, hogy az AGV pozíciója 5 métert ugrott másodpercek alatt, de az IMU meg a kerékkódoló szerint nem mozdult annyit, akkor ellentmondás történik, és gyanús, hogy hiba vagy támadás van a rendszerben.
Ilyenkor a vezérlő úgy is dönthet, hogy ideiglenesen ignorálja a GNSS-t. Szintén gyanús lehet, ha hirtelen egy távoli helyről "jelentkezik" a GNSS pozíciója. Az algoritmus tud olyat, hogy beépít szabályokat úgy, hogy bizonyos gyorsulás felett nem hihető el a GNSS outputja.
Vannak speciális spoofing-detektor algoritmusok is, ha például több az antenna használata a vevőn, ami a jelszintek közti különbséget figyeli (hamis jel esetén más módon is érkezhet).
Összegezve, a spoofing elleni harc nehezebb, mint a jamming elleni, mert ilyenkor a támadó próbál nem feltűnő lenni.
Ipari környezetben a legjobb, amit ilyenkor tehetünk, hogy tudatában vagyunk annak a lehetőségnek, hogy kritikus műveleteknél nem hagyatkozhatunk csa a GNSS-re. Ezek mellett beépítünk annyi védelmet, amennyi hatékony lehet ekkora fenyegetettségi szinten.

Kommunikáció és kiberbiztonság: Viszont, nem csak a műholdjeleket, hanem a kommunikációs hálózatot is szükséges védeni.
Ha például MQTT-n továbbítjuk a járműnek a folyamatos helyzetét, azt ilyenkor titkosítani kell (TLS). Hitelesítve a feleket, hogy illetéktelenek ne férjenek hozzá és ne módosíthassák az adatokat.
Ugyanezek igazak az OPC UA-ra is, bár annak alapvető része a biztonsági modell. Ezért a megfelelő beállítás esetén erős titkosítás és autentikáció védi a kommunikációt[45] .
Az 5G hálózat is beépített végponti titkosítást és hitelesítést használ, ami egy privát hálózatban még akár jobban kontrollálható. Fontos azzal is foglalkozni, hogy a rendszerben legyenek **naplózások és behatolásérzékelések**. Az is előfordulhat, hogy valaki megpróbál csatlakozni a robot MQTT brokeréhez illetéktelenül, ilyenkor szükséges, hogy arról legyen riasztás.
Így a GNSS integrációja is kiberbiztonsági kihívás. Azért is mivel nyit egy új támadási felületet (vezeték nélküli navigációs jel) és az is előfordulhat, hogy ezt egy hagyományos IT biztonsági csapat nem ismer annyira.
Ebből kifolyólag több vállalatnál már külön PNT Security (pozíció, navigáció, idő biztonság) szakembereket is alkalmaznak, vagy akár csak bevonják a fejlesztésbe a kiberbiztonsági csapatot.

- A GNSS ipari alkalmazásánál nem elég a pontosság és rendelkezésre állás maximalizálása, fontos felkészülni a szándékos vagy véletlen zavaró hatásokra.

A legjobb megoldás a többrétegű védelem. Erős GNSS jel (jó antennák, több konstelláció, több frekvencia), szenzorfúzió a GNSS-en kívüli forrásokkal. Zavarás/spoofing megtalálása majd riasztás.
Végül egy üzembiztos üzemmód létrehozása GNSS kiesés esetén. Ezekkel garantálható, hogy egy autonóm rendszer esetében még egy ellenséges rádiós környezetben is biztonságosan tudjon viselkedni.

Esettanulmány: GNSS-integrált AGV rendszer ipari környezetben

A fenti koncepcióknak a gyakorlati megvalósítását mutatja be a következő esettanulmány.
Most egy **GNSS-alapú vezérlésű, autonóm ipari szállítójárműnek** (AGV) a működését vizsgáljuk egy kültéren elhelyezkedő gyárudvaron. A feladat, hogy az AGV konténereket szállít az udvar egyik pontjáról a másikra, önvezető módon.
A környezet egy **nyílt terület**, de nehezítésnek előfordulnak épületek közti átjárók és féltetős dokkoló állomások. Ilyen esetben a rendszernek kezelnie kell a GNSS jel időszakos gyengülését vagy kiesését is. Vegyük át, hogyan épül fel egy ilyen rendszer:

A Fedélzeti szenzorok és hardverek: Az AGV több fő komponenssel rendelkezik. Az **RTK-képes GNSS vevő** antennafelépítménnyel, egy nagy pontosságú **IMU** (inerciális mérőegység), egy **3D LiDAR** szenzor a jármű elején (akadályérzékeléshez és kiegészítő lokalizációhoz), valamint vannak kerékfordulat-érzékelők (enkóderek) az odometriai adatok méréséhez [46][47].

Az adatokat egy fedélzeti **ipari vezérlő számítógép** gyűjti össze. Ez elég számítási kapacitással bír a valós idejű szenzorfúzióhoz és a vezérlési algoritmusok futtatásához. A járműnek a hajtásrendszere gondolva itt a villanymotorokra a meghajtáshoz és kormányzáshoz. Ezek szintén a vezérlő számítógép felügyelete alatt állnak, jellemzően beágyazott motorvezérlőkön keresztül. A GNSS antenna a jármű tetejére vannak felszerelve, ezeknek jó rálátása van az égboltra. Ameddig az IMU-t mereven a jármű vázához rögzítik (azért, hogy pontosan kövesse a mozgást). A LiDAR a jármű elején forgó lézerszkennerként figyeli a környezetet egy 270°-os szögben előre.

RTK bázisállomás és infrastruktúra: A telephelyeken kiépítenek egy **saját GNSS bázisállomást** egy általuk kiválasztott koordinátájú ponton (pl. az épület tetején vagy egy stabil oszlopon). Ez egy geodéziai GNSS vevő, a feladata, hogy folyamatosan megmérje a műholdakat. Majd ezeket egyben egy kommunikációs interfészen keresztül megosztja az RTK korrekciókat[48][49]. .
A korrekciókat itt IP hálózaton terítik. A gyár területét lefedő privát 5G hálózatot használják a bázis és a járművek összekapcsolására. A bázisállomás RTCM jeleket streamel a hálózaton keresztül. Akár MQTT topic formájában, akár egy speciális RTK szolgáltatásként. Az AGV egy 5G modemmel csatlakozik a hálózatra, ami alacsony késleltetéssel továbbítja a bázis korrekcióit a fedélzeti GNSS vevőnek [50][43]. Így a jármű mozgás közben is folyamatosan megkaphatja a centiméteres pontosságú helyzethez kellő adatokat.

Edge computing és központi felügyelet: A rendszernek egy része a központi **flottamenedzsment szerver**. Ez a telephely vezérlőtermében fut, ez tekinthető egy edge szervernek.
Ez a központi rendszer képes felügyelini az összes autonóm járművet. Feladatokat is kioszt például "AGV1, menj az A pontból a B ponthoz, és vegyél fel egy konténert". Folyamatosan követi a járművek pozícióit, ütközésmentes útvonalakat tervez és szükség esetén beavatkozik. A kommunikáció kettős a központ és az AGV-k között.Az MQTT-n keresztül a járművek folyamatos státuszjelentéseket küldenek (pozíció, akkumulátor, hibák). Ehhez képest az **OPC UA** protokollon (vagy MQTT-n egy másik csatornán) a központ utasításokat küld a járműveknek és integrálja az adatokat a gyárnak a többi rendszerével [43][51]. Ha például a gyárnak a termelésirányító rendszere jelez egy új szállítási igényt, ez egyből bejegyzésre kerül az OPC UA-n. Ezt a flottamenedzsment értelmezi és kiosztja egy AGV-nek. A vezérlésnek a hierarchiája úgy néz ki, hogy a helyi autonómia (pl. szenzorfúzió, akadályelkerülés, alacsonyszintű vezérlés) a jármű fedélzetén megtörténik. Addig amíg a globális koordináció (feladatkiosztás, útvonal egyeztetés több jármű között, interfész az emberi operátorral) a központi szerveren.

Szoftverarchitektúra és együttműködés: Az AGV-nek a fedélzeti számítógépén több szoftvermodul is fut. Példának: 1. **Szenzorfúziós modul**, ez egy EKF megvalósítás, amely valós időben egyesíti a GNSS, IMU, kerékkódoló és LiDAR adatait a jármű pozíciójának és sebességének legjobb becslése érdekében[52] .

GNSS jelkor, a fúzió felhasználja a drift korrigálására. Amikor éppen nincs GNSS, akkor a LiDAR és az IMU dolgozik. A LiDAR külön is szokott futtat egy **helyzetjavító algoritmust** (pl. scan matching), ez segít ráfinomítani a lokalizációt általa ismert tereptárgyak alapján [53][54]. .
2. **Akadályérzékelő és ütközéselkerülő modul**: A LiDAR (esetleg kamera vagy radar) adatai alapján felismeri azokat az akadályokat amelyek az AGV útjában vannak (pl. egy ember vagy másik jármű bement elé), és vészfékezést vagy kitérő manővert hajtanak végre ha szükség [56].
3. **Mozgásvezérlő modul:** Ez a modul felel a járműnek a kormányzási és hajtási parancsaiért. Bemenete vagy a kívánt útvonal vagy a cél (a központ által éppen adott), illetve a pillanatnyi helyzet (amit a szenzorfúzió számolt ki). Ezeknek a kimenete a kerékmotorok fordulatszám-parancsa, kormány-szög parancs stb. Ez a modul valósítja meg a nyomvonal-követő algoritmusokat (pl. pure pursuit vagy MPC). Azért, hogy a jármű pontosan kövesse a kívánt útvonalat.
4. **Kommunikációs modul**: Fő feladata a kapcsolat tartás a központtal. Tartalmaz egy MQTT klienst, ami publikálja a státuszt és figyel bizonyos vezérlési topic-okra, illetve egy OPC UA szerver komponenst. Ez lehetővé teszi, hogy szükség esetén közvetlenül is lekérdezze a központ a jármű adatait vagy akár különböző esetekben utasítást is tudjon küldeni [55]. Ez a modul felel az RTK korrekciós adatnak továbbításáért is, a GNSS vevő felé (általában a

GNSS vevő soros portjára kell továbbítania a hálózaton kapott RTCM biteket). Ezeket biztonságos csatornákon teszi például TLS a brokeren keresztül.

A **rendszer indulása** azzal kezdődik, hogy az AGV bekapcsolás után először felveszi a kapcsolatot a 5G hálózattal, **GNSS pozíciót szerez, majd inicializálja az RTK linket** [56][57]. Néhány másodpercen belül a GNSS vevő fix megoldásra jut (~2 cm pontosság). Ezt átadja a szenzorfúziónak, amely beállítja kezdeti állapotnak. Közben az IMU is kalibrál (a kezdeti álló helyzetben nullákat vesz, bias-t mér).

Majd a jármű jelenti a központ felé, hogy készen áll (MQTT üzenet). Ezt követően a központi rendszer ad egy feladatot, menjen egy megadott koordinátára. Az AGV megtervezi a nyomvonalat vagy csak kap egy útvonalpont-sorozatot, majd ezt követően elindul. **Navigáció közben** a szenzorfúzió folyamatosan frissíti a pozícióbecslést 100 Hz-en az IMU alapján, 5 Hz-en majd ezt "hozzáigazítja" GNSS-szel [58]. Amint beér egy fedett területre, a GNSS modul érzékeli és jelzi, hogy nincs érvényes fix. Az EKF ilyenkor tovább fut csak IMU + LiDAR alapon. A hiba a bizonytalansággal növekszik, de csak rövid ideig (pár másodpercig) ez így még nem kritikus gond. Abban a pillanatban amikor kiér a szabad ég alá, az RTK fix visszatér és a szűrő korrigál. A LiDAR folyamatosan figyeli azt, hogy van-e akadály. Vegyük azt, hogy például, egy ember keresztezi az útvonalat. Az akadálydetektáló modul ezt felismerve megállítja a járművet. Ekkor a jármű folyamatosan küldi a pozícióját és státuszát a központnak, így az operátor egy térképen láthatja, merre jár. A központ a flottából több járművet is koordinál, azért, hogy ne ütközzenek (pl. egyszerre csak egy haladhat át egy szűk ponton). A valós idejű koordinációt a **megbízható 5G hálózat** biztosítja, amelynek köszönhetően tizedmásodperces frissítéssel lehet kommunikálni a járművekkel és így kordinálni őket.

Az esettanulmányból megérthető, hogy a GNSS integrációja fontos egy ipari AGV-be nem elég csak egy GPS modul rászerelése. A **rendszerarchitektúrát többnyire úgy kellett kialakítani,** hogy a műholdas helymeghatározás előnyeit kiaknázzák (globális, pontos pozíció). Viszont ilyenkor a gyengeségeit ellensúlyozni kell (időszakos kiesés, zavarás). Ezt érhetjük el azzal, hogy: - kombináljuk az RTK GNSS-t egy nagy pontosságú IMU-val és LiDAR szenzorral (szenzorfúzió). Be lett vezetve egy helyi RTK bázisállomást és edge infrastruktúrát az alacsony késleltetésű, megbízható korrekciókért. Használtunk ipari kommunikációs protokollokat (MQTT, OPC UA) a rendszerintegrációra, majd egy 5G URLLC hálózatot a stabil, vezeték nélküli kapcsolatért. Figyelembe kellett vettünk azt is, hogy teljesítsük a biztonsági követelményeket (pl. redundáns szenzorok, riasztás zavar esetén, stb.).

Ezeket teljesítve, **eredményként** egy olyan AGV rendszert kapunk, amely képes egy bonyolult ipari környezetben önállóan navigálni és feladatokat végrehajtani. Nyílván még itt is szükség van egy **minimális emberi beavatkozásra**, de kihasználva a műholdas navigációt precízen működött. A megoldás skálázható (több jármű hozzáadható), adaptív (képes kezelni a GNSS kihívásait) és integrálható (illeszkedik a gyárnak már meglévő IT/OT rendszereihez a szabványos protokollokon keresztül).

Az ilyen jellegű rendszerek valószínúleg egyre gyakoribbak lesznek a jövőben, hiszen kombinálják a különböző technológiákat.

Használva a **globális navigációs rendszerek** precizitását, a **beágyazott rendszerek** rugalmasságát, a **valós idejű számítástechnika** gyorsaságát, és az **ipari kommunikáció** megbízhatóságát. Ezzel sikerült elérni egy hatékonyabb, biztonságosabb és automatizált folyamatot a gyártásban és a logisztikában.

Következtetések

Az eddigiekben szó volt a, a műholdak integrálásáról, a helymeghatározó rendszerek a modern ipari alkalmazásokba a beágyazott és számítógépes rendszereknek az együttműködésével. Átvettük, hogy a GNSS (GPS, Galileo, GLONASS, BeiDou) technológiák önmagukban is értékesek, ha globális pozícionálásról van szó, de az iparban megkerülhetetlen követelmény a magas pontosság. De ez igaz a rendelkezésre állásra, beltér-kültér átmeneteknél, valós idejű adatfeldolgozásra és kiberbiztonságra, ezek miattszükséges további kiegészítő megoldások bevezetése.

Beszéltünk az **RTK technológiákról,** ezek lehetővé teszik a centiméteres pontosságú pozicionálást valós időben. Ezek segítik az autonóm járművek és precíziós berendezések GNSS-alapú irányítását. Megállapítottuk, hogy az RTK és általában a GNSS sem elég önmagában. A **szenzorfúzió** (GNSS-IMU-LiDAR) alkalmazása elvárt a robusztus, minden helyzetben megbízható navigációhoz. Az inerciális és egyéb szenzorok integrálása folytonosságot és redundanciát biztosítanak, ezek által egy ipari robot GNSS kiesése esetén is képes biztonságot és megoldást nyújtani.

Volt szó az **edge computing** fontosságáról is, amely garantálja, hogy a valós idejű döntések és folyamatos számítások a helyszínen, megtörténhessenek minimális késleltetéssel. Be lettek mutatva az **ipari protokollok és hálózati technológiák** (MQTT, OPC UA, 5G URLLC), Ezek a rendszer komponensei közötti adatcserét biztosítottak.
Azért is, mert a műholdas pozíció nem elegendő, ha azt nem lehet időben és biztonságosan eljuttatni oda, ahol fel szeretnék használni. Az 5G URLLC külön kiemelésre került, mint a vezeték nélküli kommunikáció új lehetősége, amely lehetővé teszi, hogy még a kritikus vezérlési feladatok is áttehetők legyenek a rádiós hálózatra akár kábelek nélkül is, a megbízhatóság feláldozása nélkül.

A **biztonsági kihívások** áttekintése elgondolkodtatott azon, hogy a GNSS integrációja nem csak technológiailag fontos, hanem főleg biztonságilag. A zavarás és spoofing fenyegetése egyszerű eszközökkel is elérhető, de megfelelő tervezéssel és ellenintézkedésekkel (detektálás, multiszenzor redundancia, titkosítás) a kockázatokat lehet csökkenteni. Az ipari környezetben fontos úgy kell tervezni, hogy **hiba vagy támadás esetén a rendszer biztonságos állapotba kerüljön**, és az emberi élet vagy jelentős anyagi kár ne kerülhessen veszélybe.

Az esettanulmányként bemutatott **GNSS-integrált ipari AGV** lényegében összefoglalta a korábbi fejezetek gyakorlati alkalmazását. Megmutatta azt, hogy egy valós rendszerben hogyan működnek együtt a technológiák. A műholdas helymeghatározások, a lokális érzékelés, a beágyazott vezérlők, a kommunikáció és a központi felügyelet. Ezeknek az együttműködése tette lehetővé azt, hogy az autonóm jármű biztonságosan tudja elvégezni a feladatát egy dinamikus és nehézségeket okozó ipari környezetben.

Zárásként elmondható, hogy a műholdas rendszerek integrációja az ipari alkalmazásokban egyfajta rendszertechnikai együttműködés. Több szakterület tudása is szükséges hozzá (űrtechnológia, robotika, telekommunikáció, informatika). A technológia fejlődésével jobb GNSS műholdak, kreatívabb algoritmusok, 6G hálózatok és hasonlóak jönnek létre. Így válnak majd ezek a rendszerek egyre pontosabbá és megbízhatóbbá (intelligensebbé). A jövőben akár a kültéren navigáló önvezető jármű centiméteres pontossággal is el tudja magát kordinálni a megadott céljához, kikerülve az akadályokat. Illetve zökkenőmentesen kommunikálhat a gyártósorral, hibák nélkül (bár hibák mindig lesznek). Akár manapság egy automatizált üzemben.

Hivatkozások

AG, u.-b. (2023). *What is GNSS multipath mitigation?*

ArduSimple. (dátum nélk.). *RTK Explained – What is Real Time Kinematics (RTK) and how it works?* 2023 : ArduSimple.

Bosse, J. Z. (2014). *Efficient large-scale 3D mobile mapping and surface reconstruction of an underground mine*.

Chris Urmson, J. A. (2008). *Autonomous driving in urban environments: Boss and the Urban Challenge*.

Communication), A. T. (2023). *Driving Efficiency and Safety in Autonomous Vehicles*. LinkedIn Articles.

D. Ferguson, T. M. (2008). *Motion planning in urban environments: Part II*.

Desmond Schmidt, K. R. (2016). *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures*.

Diggelen, J. V. (2009). *A-GPS: Assisted GPS, GNSS and SBAS*.

Docs, E. (2024). *RTK Introduction – Emlid Reach RS3 Quickstart Guide*.

FinOrr. (2023. október 4.). *Embedded NMEA 0183 Parser*.

GNSS, I. (2021). *Complementary Sensor Fusion*.

Golioth, s. f. (2023. szeptember 27.). *How to Localize Your Devices with GNSS, NMEA, and Zephyr*.

Hofmann-Wellenhof, B. L. (2008). *GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more*.

J. Curran, A. B. (2014). *A Survey of GNSS Spoofing: Threats and Countermeasures*.

Judit, O. (2019). *Az Ipar 4.0 keretrendszere, valamint a kapcsolódó technológiák*. International Journal of Engineering and Management Sciences.

K. Zheng, Q. Z. (2015). *Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions*.

Labs, I. (2024). *What are the limitations of GNSS?* Inertial Labs.

Manzino, P. D. (2017). *GPS and GNSS RTK techniques for real-time geolocation*.

(2024). *MQTT – The Standard for IoT Messaging*. OASIS / mqtt.org.

MultiTech Systems, I. (2023). *Why Industrial Operators Need 5G URLLC – and How They Can Get There*.

Satyanarayanan, M. (2017). *The emergence of edge computing*.

Sebastian Thrun, W. B. (2005). *Probabilistic Robotics*. MIT Press.

SYSNAV. (2023). *Why GNSS and GPS do not function properly indoors*. SYSNAV.

Team, O. (2023). *The Impact of Edge Computing on Real-Time Data Processing*.

Technologies, V. (2024). *GNSS-Challenged Environments*. VectorNav Technologies.

Thilakarathna, N. (2023). *Edge Computing in Robotics: Bringing Intelligence Closer to Action*. LinkedIn Articles.

Tibor, B. (2019). *Nagypontosságú GNSS-mérés hasznosítása a járműiparban, kapcsolódó rendszerbiztonsági és adatforgalmi kérdések feltárása V2X-rendszerben*. HM Zrínyi Nonprofit Kft.

Zalewski, P. (2014). *Real-time GNSS Spoofing Detection in Maritime Code Receivers*.

2.19. Robotika és mesterséges intelligencia az iparban Az ipari automatizáció, gyártás és logisztika fejlődése a modern technológiák tükrében SZÁSZ BOTOND

Robotika és mesterséges intelligencia az iparban

Az ipari automatizáció, gyártás és logisztika fejlődése a modern technológiák tükrében

SZÁSZ BOTOND

Gazdaságinformatikus BSc szak, szaszboti2003@gmail.com

1 BEVEZETÉS

A robotika és a mesterséges intelligencia (MI) napjainkra a modern ipar egyik legmeghatározóbb technológiai fejlesztési irányzatává váltak. Az Ipar 4.0 koncepciójának köszönhetően a gyártásban egyre jelentősebb szerepet kapnak azok a rendszerek és eszközök, amelyek képesek az autonóm működésre, a tanulásra, valamint az önálló döntéshozatalra.

A robotika fejlődése lehetővé tette, hogy a gyártó- és termelési folyamatokban a hagyományos emberi munkavégzést részben vagy teljes egészében automatizált rendszerek váltsák fel. A mesterséges intelligencia pedig ezen robotikai rendszerek intelligens működéséhez járul hozzá, optimalizálva a gyártási folyamatokat, csökkentve a hibalehetőségeket és fokozva a hatékonyságot.

A robotok több fajtája is megjelent az ipari környezetben, mint például a manipulátor robotok, kollaboratív robotok (cobotok) és az autonóm mobil robotok (AMR-ek). Ezek a technológiák jelentősen hozzájárulnak a termelés rugalmasságához, sebességéhez és minőségéhez.

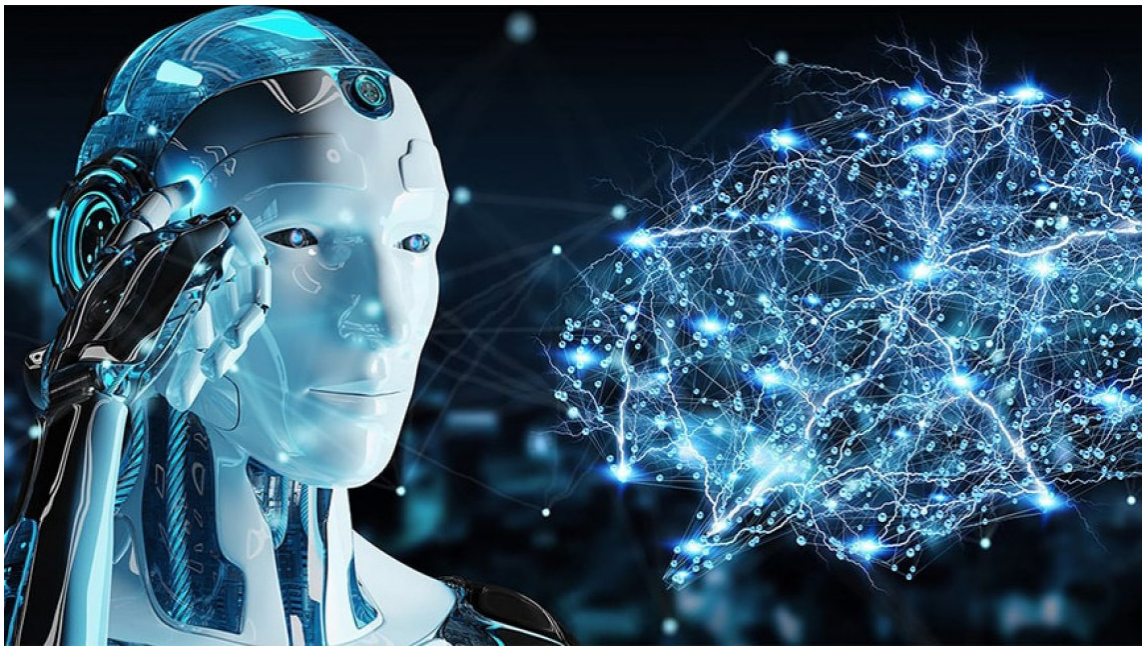
A mesterséges intelligencia alkalmazása az iparban több területre is kiterjed, úgy, mint a gépi látás, prediktív karbantartás, adatelemzés, döntéstámogatás és önálló robotikai működés. A robotok képesek a beépített MI rendszerek segítségével tanulni, tapasztalatokat feldolgozni és új működési stratégiákat kialakítani.

A robotika és a mesterséges intelligencia ipari alkalmazása napjainkra olyan kulcsterületté vált, amely a gyártási folyamatok fejlődését és hatékonyságát alapvetően befolyásolja. E technológiák integrációja lehetővé teszi a gyárak számára, hogy rugalmasabban, gyorsabban és pontosabban reagáljanak a piac kihívásaira, miközben csökkentik a költségeket és növelik a termelés biztonságát.

Az ipari automatizálás egyik legjelentősebb előnye, hogy a robotizált és MI-alapú rendszerek képesek folyamatosan, magas minőségi szinten működni, függetlenül a külső körülményektől. Az automatizált folyamatok alkalmazása a hibák csökkentésén túlmenően lehetővé teszi a gyorsabb termelési ciklusokat és az adatalapú döntéshozatalt is.

Az MI alkalmazása a robotikában lehetővé teszi a valós idejű adatelemzést, a gyártási folyamatok optimalizálását, valamint a hirtelen felmerülő helyzetek gyors és hatékony kezelését. Emellett a prediktív karbantartási rendszerek segítségével jelentősen csökkenthető a gyártóberendezések leállási ideje és növelhető azok élettartama.

Az ipar jövője egyre inkább az intelligens rendszerek alkalmazásán alapul, ahol a robotika és a mesterséges intelligencia együttesen biztosítják a versenyképesség fenntartását, a termelési folyamatok átláthatóságát és a gyors alkalmazkodást a változó piaci igényekhez.



1. ábra: Emberközpontú mesterséges intelligencia. Forrás: Magyar UNESCO Bizottság (https://unesco.hu/hirek/az-emberkozpontu-mesterseges-intelligencia-107326)

2 IPARI ROBOTOK TÍPUSAI ÉS FUNKCIÓI

Az ipari robotok a modern gyártás alapvető technológiai eszközei, amelyek különböző típusai eltérő feladatokat látnak el a termelési folyamatok során. Működésük és felhasználásuk jellemzően a gyár típusához, a gyártott termékhez és a munkafolyamat sajátosságaihoz igazodik.

2.1 Manipulátor robotok

A manipulátor robotok az ipari robotok egyik legősibb és legelterjedtebb típusát jelentik. Ezek a robotok jellemzően egy vagy több csuklóval és tengellyel rendelkező robotkarok, amelyeket különböző gyártási feladatok ellátására terveztek. Alapvetően fix helyhez kötöttek, és előre programozott mozgássorozatok végrehajtására képesek.

A manipulátor robotok legismertebb alkalmazási területei közé tartozik a hegesztés, festés, csomagolás, rakodás, összeszerelés, vagy akár a minőségellenőrzés. Előnyük, hogy gyorsak, pontosak és nagy terhelhetőséggel rendelkeznek, ugyanakkor kevésbé alkalmasak változó környezetben történő működésre.

Felépítésüket tekintve különböző mozgástengelyekkel rendelkezhetnek, általában 4-6 tengelyes kialakítás jellemzi őket, amely lehetővé teszi a bonyolult, háromdimenziós mozgások végrehajtását is. A manipulátor robotok végén egy

végszerszám (gripper, hegesztőfej, csavarozó, festékszóró stb.) található, amely a konkrét feladat elvégzéséhez alkalmazkodik.

Napjainkban a manipulátor robotok továbbfejlesztett változatai már képesek mesterséges intelligencia támogatásával érzékelni környezetüket, reagálni a változásokra, vagy éppen gépi látás segítségével precízebb feladatokat végrehajtani. Ennek ellenére ezek a robotok főként még mindig az ismétlődő, standardizált gyártási folyamatokban terjedtek el.

2.2 Kollaboratív robotok (Cobots)

A kollaboratív robotok, röviden kobotok, az ipari robotok egy speciális kategóriáját képviselik. Ezeket a robotokat úgy tervezték, hogy közvetlenül együttműködjenek az emberi munkatársakkal közös munkaterületen, biztonságosan és hatékonyan végezve el különböző feladatokat. A hagyományos ipari robotokkal ellentétben, amelyek gyakran biztonsági kerítésekkel vannak elválasztva az emberektől, a kobotok érzékelőkkel és fejlett vezérlőrendszerekkel rendelkeznek, amelyek lehetővé teszik számukra, hogy érzékeljék és reagáljanak az emberi jelenlétre, minimalizálva ezzel a balesetek kockázatát.

2.2.1 Felépítés és működés

A kobotok általában könnyű, kompakt kialakításúak, és több tengely mentén képesek mozogni, ami nagyfokú rugalmasságot biztosít számukra a különböző munkafolyamatok során. Fejlett szenzorrendszereik révén képesek érzékelni a környezetükben bekövetkező változásokat, például egy emberi munkatárs jelenlétét vagy egy váratlan akadályt, és ennek megfelelően módosítani mozgásukat vagy leállni, ha szükséges. Ez a képesség teszi lehetővé számukra, hogy biztonságosan működjenek közvetlen emberi környezetben.

2.2.2 Alkalmazási területek

A kobotok sokoldalúságuk révén számos iparágban és munkafolyamatban alkalmazhatók. Néhány jellemző alkalmazási területük:

Összeszerelés: A kobotok precíz mozgásuknak köszönhetően képesek apró alkatrészek összeszerelésére, csavarozásra vagy ragasztásra, miközben együttműködnek az emberi munkatársakkal a gyártósoron.

Anyagmozgatás és csomagolás: A kobotok hatékonyan végezhetik a termékek mozgatását, csomagolását és raklapozását, csökkentve ezzel az emberi munkaerő fizikai terhelését és növelve a folyamatok hatékonyságát.

Minőségellenőrzés: Fejlett érzékelőik és kamerarendszereik révén a kobotok képesek a termékek minőségének ellenőrzésére, hibák felismerésére és jelzésére, hozzájárulva ezzel a gyártási folyamatok minőségének javításához.

Gépkiszolgálás: A kobotok alkalmazhatók különböző gépek betöltésére és kirakodására, például CNC gépek esetében, növelve ezzel a gépek kihasználtságát és csökkentve az állásidőt.

2.2.3 Előnyök és kihívások

A kobotok alkalmazásának számos előnye van:

Biztonság: A fejlett szenzorrendszerek és vezérlőmechanizmusok révén a kobotok képesek biztonságosan együttműködni az emberekkel, csökkentve a munkahelyi balesetek kockázatát.

Rugalmasság: Könnyen programozhatók és áthelyezhetők, így gyorsan alkalmazkodnak a változó gyártási igényekhez és különböző feladatokhoz.

Költséghatékonyság: A kobotok bevezetése csökkentheti a munkaerőköltségeket és növelheti a termelékenységet, ami hosszú távon megtérülő befektetést jelent.

Ugyanakkor a kobotok alkalmazása kihívásokkal is jár:
Integráció: A meglévő gyártási rendszerekbe való integrálásuk alapos tervezést és esetenként a munkafolyamatok átalakítását igényli.
Képzés: A munkavállalók megfelelő képzése szükséges a kobotok hatékony és biztonságos használatához.
Kezdeti beruházás: Bár hosszú távon költséghatékonyak, a kezdeti beszerzési és telepítési költségek jelentősek lehetnek, különösen kis- és középvállalkozások számára.

2. ábra: Ember és kollaboratív robot együttműködése intelligens gyárban. Forrás: (https://www.techmonitor.hu/piacmonitor/ember-robot-egyuttmukodes-az-intelligens-gyarakban-20180119)

2.3 Autonóm mobil robotok (AMR) és önvezető járművek

Az autonóm mobil robotok (rövidítve AMR-ek) és az önvezető járművek az ipari automatizálás egyik legmodernebb és legdinamikusabban fejlődő területét képviselik. Ezek a robotok jelentős áttörést hoztak az anyagmozgatás, logisztika és belső szállítási folyamatok optimalizálásában, köszönhetően fejlett navigációs és érzékelési technológiájuknak.

A hagyományos automatizált vezető nélküli járművekkel (AGV) szemben, amelyek előre kijelölt útvonalakon haladnak, az AMR-ek képesek önállóan, rugalmasan alkalmazkodni a változó környezethez. Az ipar 4.0 környezetében az AMR-ek egyre fontosabb szereplőkké válnak, különösen a gyártósorok közötti anyagmozgatásban, a raktári logisztikában, valamint az intralogisztikai folyamatokban.

2.3.1 Működés és technológia

Az AMR-ek működése fejlett szenzortechnológián és intelligens vezérlőrendszereken alapul. Jellemzően az alábbi technológiákat alkalmazzák:

Lidar (Light Detection and Ranging) érzékelők: Lézeralapú távolságmérés, amely segíti a térképezést és az akadályok érzékelését.

3D kamerák: A környezet pontos felmérését teszik lehetővé.

Valós idejű lokalizáció és térképezés (SLAM): Az AMR-ek képesek önállóan feltérképezni a környezetüket, és ehhez igazítják mozgásukat.

Mesterséges intelligencia algoritmusok: Segítik az útvonaltervezést, az akadályelkerülést és az optimális navigációt.

Az AMR-ek egyik legnagyobb előnye a rugalmas mozgás. Míg az AGV-k csak előre meghatározott pályán közlekednek, az AMR-ek képesek valós időben reagálni a környezet változásaira, és új útvonalakat keresni, ha akadályba ütköznek.

2.3.2 Alkalmazási területek

Az autonóm mobil robotok alkalmazása rendkívül sokoldalú, és az ipar számos területén terjednek el:

- Raktárakban és logisztikai központokban anyagmozgatásra, áru szállítására.
- Gyártócsarnokokban a gyártósorok közötti alkatrészek mozgatására.
- E-kereskedelmi raktárakban rendelés-összeállítási folyamatok támogatására.
- Egészségügyi intézményekben gyógyszerek és eszközök szállítására.
- Autóiparban, elektronikai gyártásban automatizált szállítási feladatok elvégzésére.

Előnyök:

- Rugalmasság: Szabadon mozognak, nem kötöttek fix pályákhoz.
- Hatékonyság: Gyorsabb és pontosabb anyagmozgatást tesznek lehetővé.
- Biztonság: Fejlett érzékelők révén minimálisra csökkentik a balesetek kockázatát.
- Költséghatékonyság: Hosszú távon jelentős munkaerő-megtakarítást eredményezhetnek.
- Könnyű integráció: Viszonylag egyszerűen beépíthetők meglévő rendszerekbe.

Hátrányok, kihívások:

- Magas kezdeti beruházási költség.
- Technológiai komplexitás, karbantartási igény.
- Korlátok bizonyos környezeti feltételek esetén (pl. nagyon zsúfolt, szűk terekben).
- Informatikai háttér szükségessége (pl. hálózat, térképezés, adatfeldolgozás).

Tulajdonság	Manipulátor robotok	Kollaboratív robotok (Cobots)	Autonóm mobil robotok (AMR)
Működési környezet	Elkerített, biztonságos zóna	Közös térben emberrel együtt	Szabadon, teljes gyártási területen
Rugalmasság	Alacsony – fix telepítés	Közepes – könnyen mozgatható	Magas – dinamikus mozgás
Biztonság	Passzív biztonsági megoldások	Fejlett szenzoros védelem	Akadályérzékelés és elkerülés
Mozgás jellege	Fix, előre programozott	Lassított, biztonságos	Szabad navigáció, útvonaltervezés
Alkalmazási terület	Hegesztés, festés, összeszerelés	Összeszerelés, gépkiszolgálás, minőségellenőrzés	Anyagmozgatás, szállítás, logisztika
Előnyök	Nagy sebesség és pontosság	Emberrel közös munkavégzés	Önálló navigáció, rugalmasság
Hátrányok	Kevésbé rugalmas, fix helyhez kötött	Lassabb működés, kisebb terhelhetőség	Magas beruházási költség, komplex működés

1. táblázat: Ipari robot típusok összehasonlítása. (Saját készítésű)

3 A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA AZ IPARI ROBOTIKÁBAN

A mesterséges intelligencia (MI) és a robotika kapcsolata napjaink iparának egyik legizgalmasabb és leginnovatívabb területe. Míg korábban a robotok kizárólag előre programozott feladatokat hajtottak végre, a mesterséges intelligencia megjelenésével képessé váltak arra, hogy tanuljanak, döntsenek és alkalmazkodjanak a változó környezeti feltételekhez. Ez forradalmasította az ipari automatizálást, hiszen a gyártórendszerek ezzel intelligensebbé, hatékonyabbá és biztonságosabbá váltak.

3.1 Gépi tanulás és optimalizáció

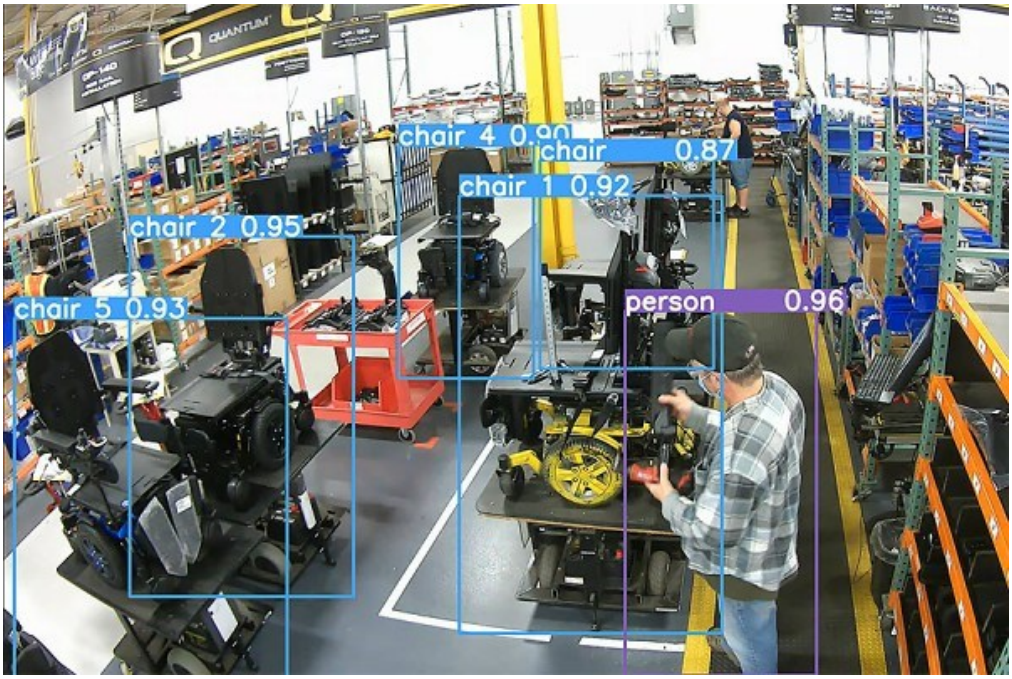
A gépi tanulás lehetővé teszi, hogy a robotok folyamatosan fejlődjenek a működés során gyűjtött adatok elemzésével. Az ipari környezetben különösen fontos, hogy a robotok a múltbeli tapasztalatok alapján optimalizálják mozgásukat, energiafelhasználásukat és a gyártási időt. A gépi tanulás segítségével a robotok képesek minták felismerésére, hibalehetőségek csökkentésére és a termelési hatékonyság javítására.

3.2 Gépi látás és tárgyfelismerés

A gépi látás technológiájának köszönhetően a robotok képesek vizuális információk észlelésére és feldolgozására. Ez a képesség kulcsfontosságú a minőségellenőrzési folyamatokban, az összeszerelésben és a precíziót igénylő műveletekben. A gépi látással ellátott robotok felismerik a tárgyak formáját, pozícióját, méretét és állapotát, ezáltal jelentősen csökkentve az emberi beavatkozás igényét.

3.3 Prediktív karbantartás és hibafelismerés

A prediktív karbantartás során a mesterséges intelligencia a szenzorok által gyűjtött adatok elemzésével előrejelzi a berendezések meghibásodásait. Ez lehetővé teszi, hogy a karbantartási műveletek nem váratlan leállások, hanem tervezett időpontok szerint történjenek, csökkentve ezzel az állásidőt és a javítási költségeket. A hibafelismerés és önellenőrzés képessége jelentősen növeli a gyártórendszerek megbízhatóságát és biztonságát.



3. ábra: Mesterséges intelligencia és gépi látás alkalmazása ipari környezetben. Forrás: University of Windsor, DailyNews (https://www.uwindsor.ca/dailynews/2020-09-29/researchers-apply-ai-improve-human-element-manufacturing)

4 SZOFTVERES ÉS HARDVERES ARCHITEKTÚRA AZ IPARI ROBOTIKÁBAN

Az ipari robotika hatékony működésének és fejlődésének alapját a megfelelő hardveres és szoftveres architektúra jelenti. Egy korszerű ipari robot nem csupán mechanikai eszközökből áll, hanem komplex informatikai rendszerekből, melyek biztosítják az intelligens működést, az önálló döntéshozatalt és a biztonságos interakciót az emberi munkatársakkal.

4.1 Hardveres architektúra

Az ipari robotok hardveres architektúrája a robot fizikai felépítésének, meghajtásának és érzékelési technológiáinak összessége. A legfontosabb hardveres elemek:

- Szenzorok és szenzorfúzó: LiDAR, kamerák, tapintásérzékelők, ultrahangos és infravörös szenzorok, amelyek adatokat gyűjtenek a környezetről. A szenzorfúzó technológia segít ezek kombinálásában a pontosabb környezeti modell érdekében.
- Ipari robotkarok és manipulátorok: Mechanikai egységek, amelyek több tengely mentén képesek mozogni, sokszor 4-6 vagy több tengelyes kivitellel.
- Végszerszámok (end effectors): Olyan cserélhető eszközök, amelyek az adott feladat ellátását teszik lehetővé: pl. gripper, csavarozó, hegesztőfej, ragasztófej.

4.2 Szoftveres architektúra

Az ipari robotok szoftveres architektúrája kulcsszerepet tölt be abban, hogy a robotok ne csupán mechanikai eszközként, hanem intelligens, adaptív rendszerekként működjenek. Ez a szoftveres réteg biztosítja, hogy a robotok képesek legyenek adatok gyűjtésére, feldolgozására, önálló döntéshozatalra és a környezettel való folyamatos interakcióra. A szoftveres architektúra főbb elemei:

- Robotikai operációs rendszerek (ROS, VxWorks, QNX): Ezek az alapvető szoftveres platformok teszik lehetővé a robotok működtetését, vezérlését és a komponensek közötti kommunikációt.
    - ROS (Robot Operating System): Nyílt forráskódú, moduláris felépítésű rendszer, amely lehetővé teszi a különböző robotikai komponensek egységes vezérlését, kommunikációját és adatintegrációját.
    - VxWorks: Valós idejű operációs rendszer (RTOS), amelyet főleg kritikus és időérzékeny ipari alkalmazásokhoz fejlesztettek, különösen beágyazott rendszerekhez.
    - QNX: Magas megbízhatóságú, biztonságos RTOS, amelyet gyakran használnak autóipari és ipari automatizálási rendszerekben.
- Mesterséges intelligencia platformok (TensorFlow, PyTorch): Az MI-platformok adják a robotok "intelligenciáját", segítve a tanulást, mintázatfelismerést és döntéshozatalt.
    - TensorFlow: Nyílt forrású MI keretrendszer, amely alkalmas gépi tanulásra, neurális hálózatok létrehozására, mintázatfelismerésre és prediktív modellek készítésére.
    - PyTorch: Egy másik népszerű MI keretrendszer, amely dinamikus neurális hálózatok létrehozását és gépi tanulási feladatok egyszerű megvalósítását segíti elő, kiemelten a robotok autonóm működése során.

A szoftveres architektúra kulcsszerepe abban áll, hogy egységes platformot biztosítson a robot hardveres elemeinek vezérléséhez, az adatok feldolgozásához, a működési paraméterek beállításához és a környezettel való folyamatos kommunikációhoz. Ez teremti meg a lehetőséget arra, hogy a modern ipari robotok intelligens, alkalmazkodó és önálló rendszerként funkcionáljanak.

4.3 Kommunikációs protokollok és rendszerintegráció

Az ipari robotok kommunikációs architektúrája képes az adatok valós idejű feldolgozására és a rendszer egyes komponenseinek összekapcsolására.

A rendszerintegráció lényeges célja, hogy a robotok szorosan összedolgozzanak a gyártási és informatikai infrastruktúrával, biztosítva a hatékony és megbízható működést. Ez azt jelenti, hogy a robotok ritkán működnek teljesen önállóan, hanem egy komplex rendszer részeként funkcionálnak, ahol folyamatos adatáramlás zajlik köztük és más gyártástechnológiai eszközök, szenzorok, vezérlők, valamint a központi irányítási rendszerek között. Ezek a kommunikációs protokollok lehetővé teszik a valós idejű adatok cseréjét, ezáltal biztosítva a gyártás gyorsaságát, rugalmasságát és a zökkenőmentes termelést.

- OPC UA: Nyílt kommunikációs protokoll, amely biztonságos adatcserét tesz lehetővé különböző ipari rendszerek között.
- MQTT: Könnyűsúllyú protokoll IoT eszközök adatkommunikációjára.
- EtherCAT: Valós idejű ipari Ethernet alapú hálózati megoldás, gyors adatátvitellel.

5 ROBOTIKA ÉS MESTERSÉGES INTELLIGENCIA SZEREPE AZ OKOSGYÁRAKBAN

Az ipari fejlődés és a technológia robbanásszerű terjedése az elmúlt évtizedekben forradalmasította a gyártási folyamatokat. Ennek egyik leglátványosabb eredménye az okosgyárak (Smart Factory) megjelenése, ahol a mesterséges intelligencia (MI) és a robotika szoros együttműködése teszi lehetővé a korábban elképzelhetetlen mértékű automatizálást és hatékonyságnövelést. Az okosgyárak képviselik a jövő gyártását, ahol a fizikai eszközök és a digitális rendszerek integrációja valós idejű adatfeldolgozásra és önálló döntéshozatalra képes környezetet teremt.

Az okosgyárak sajátossága, hogy a gyártás minden részfolyamata digitalizált, és az információ áramlása folyamatos az ember, a robotok, a gyártóeszközök és a központi irányító rendszerek között. Ebben a környezetben a robotok a "kezét", az MI pedig az "agyát" adja a gyárnak, biztosítva az automatizált, de adaptív és intelligens termelési rendszereket.

5.1 Automatizált gyártósorok és termelésirányítás

A gyártósorok automatizálása nem új keletű dolog, azonban a mesterséges intelligencia bevonása alapjaiban változtatta meg a termelésirányítást. A modern automatizált gyártósorok már nemcsak előre programozott feladatokat látnak el, hanem képesek valós idejű adatelemzésre, tanulásra és önálló döntéshozatalra.

Az MI segítségével a termelésirányítási rendszerek képesek felismerni a folyamatokban fellépő anomáliákat, optimalizálni a gyártási tempót, valamint dinamikusan igazodni a megrendelési igényekhez. Az új generációs gyártósorokon minden mozgás, művelet és energiafelhasználás mérhető, és ezek elemzése alapján folyamatos a fejlesztés.

A prediktív karbantartás különösen fontos szerepet tölt be: a rendszerek már az elhasználódás korai jeleiből képesek következtetni arra, hogy mikor érdemes beavatkozni, megelőzve a költséges hibákat és leállásokat.

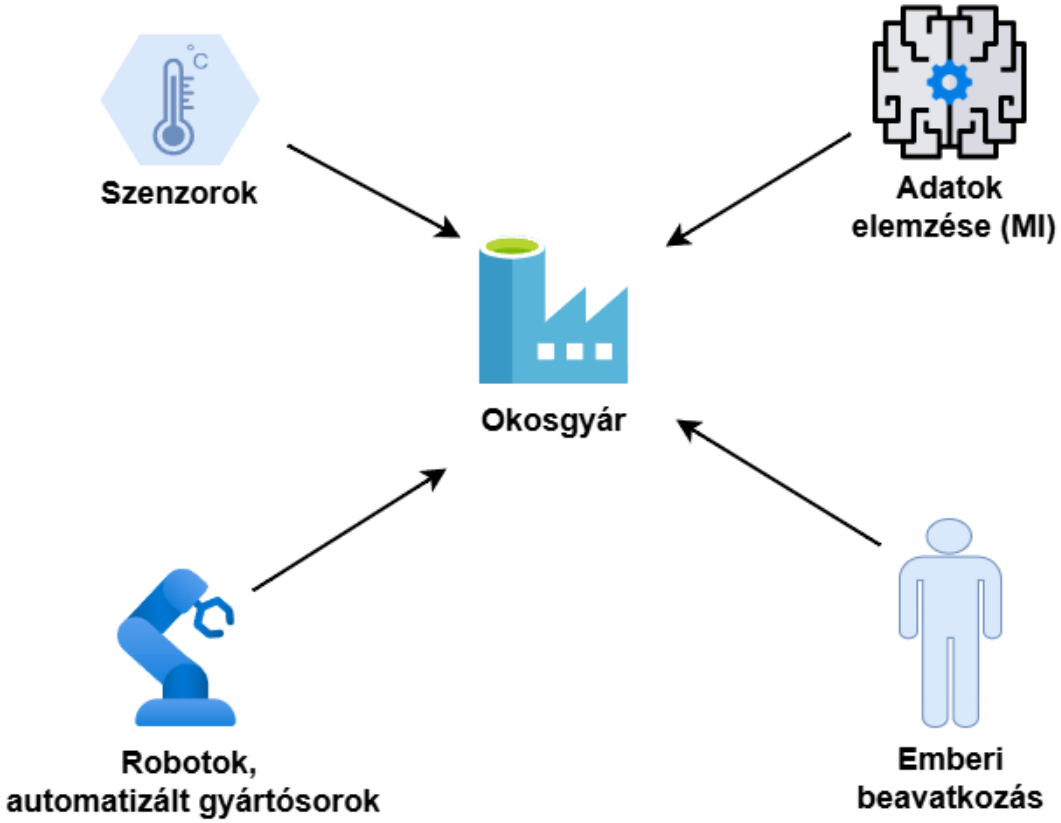
5.2 Ember-robot együttműködés és biztonsági kérdések

Az ember és a robot közötti együttműködés képessége alapvető elvárássá vált az okosgyárakban. A kollaboratív robotok közvetlen emberi jelenlét mellett működnek, segítve a nehezebb, monoton, vagy veszélyes feladatok elvégzését.

A legújabb fejlesztések során olyan intelligens szenzorokat és viselhető eszközöket alkalmaznak, amelyek figyelik a dolgozó mozgását, testhelyzetét, sőt állapotát is. A robotok ennek alapján döntenek a működésükről, lassítanak, megállnak vagy útvonalat változtatnak. A mesterséges intelligencia emellett figyeli a dolgozók viselkedését, és szükség esetén figyelmeztetést küldhet.

5.3 IoT és Big Data kapcsolata az ipari robotikával

Az Internet of Things (IoT) és a Big Data technológiák adják az okosgyárak információs gerincét. A gyártási folyamatok során rengeteg adat keletkezik: szenzorok mérik a hőmérsékletet, rezgést, pozíciót, energiafelhasználást. Ezek az adatok valós időben összegyűlnek és elemezhetővé válnak. A mesterséges intelligencia itt kap szerepet az adatok feldolgozásában, a mintázatok felismerésében és a predikciók készítésében. Az IoT technológia biztosítja a kapcsolatot a robotok és a központi irányító rendszerek között, míg a Big Data értelmezhető információvá alakítja a nyers adatokat, amelyek alapján a termelés hatékonyabban, pontosabban és rugalmasabban működhet.



4. ábra: Az okosgyár működési modellje (saját készítés)

6 GYAKORLATI PÉLDÁK ÉS ESETTANULMÁNYOK

6.1 Gyárak robotizációs megoldásai – Bevezetés

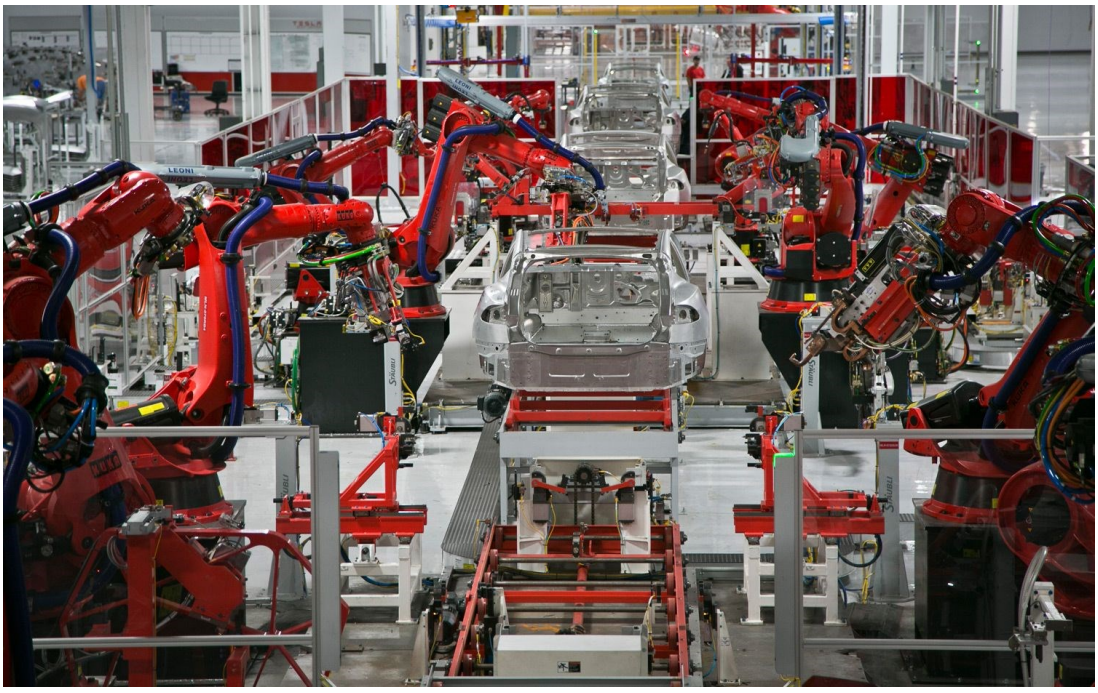
Az ipar fejlődése során egyre inkább elengedhetetlenné vált, hogy a legnagyobb vállalatok korszerű technológiai megoldásokkal válaszoljanak a globális kihívásokra. Az automatizáció, a robotika és a mesterséges intelligencia alkalmazása ma már nem csupán versenyelőny, hanem sok esetben a fennmaradás záloga a nemzetközi gyártás világában.

6.1.1 Tesla – A robotizált és mesterséges intelligenciával vezérelt gyártás úttörője

A Tesla, Inc. az elektromos járművek gyártásában betöltött vezető szerepe mellett az ipari automatizáció és mesterséges intelligencia (MI) alkalmazásában is élen jár. Gyárai világszerte a legmodernebb technológiákat alkalmazzák, amelyek révén a gyártási folyamatok hatékonysága és precizitása új szintre emelkedett.

Automatizált gyártósorok és robotika

A Tesla gyártósorai rendkívül magas fokú automatizáltsággal működnek. A Fremontban (Kalifornia) található gyárban például több száz ipari robot végzi a hegesztési, festési és összeszerelési feladatokat. Ezek a robotok nemcsak gyorsak és pontosak, hanem képesek alkalmazkodni a gyártási igények változásaihoz is. A Tesla saját fejlesztésű *Giga Press* öntőgépei lehetővé teszik, hogy a járművek alvázát egyetlen darabból öntsék ki, jelentősen csökkentve ezzel a gyártási időt és költségeket.



5. ábra: Elképesztő robottechnológia a Tesla gyárban Forrás: (https://www.pto.hu/post/1/12997)

Mesterséges intelligencia a gyártásban

A Tesla nemcsak a járművek önvezető rendszereiben alkalmazza az MI-t, hanem a gyártási folyamatok optimalizálásában is. A vállalat saját fejlesztésű *Dojo* szuperszámítógépe hatalmas mennyiségű adatot képes feldolgozni, amelyeket a gyártás során keletkező szenzoradatokból és kamerafelvételekből nyernek. Ezek az adatok lehetővé teszik a gyártási folyamatok valós idejű monitorozását és azonnali beavatkozást, ha szükséges.

Optimus – a humanoid robot

A Tesla legújabb innovációja az *Optimus* nevű humanoid robot, amelyet 2021-ben mutattak be. Az Optimus célja, hogy a gyártás során ismétlődő és fizikailag megterhelő feladatokat végezzen el, ezzel tehermentesítve az emberi munkaerőt. A robot a Tesla önvezető technológiáján alapuló MI-t használja a környezet érzékelésére és a feladatok végrehajtására. A tervek szerint az Optimus 2025-től kezdve kerülhet bevetésre a Tesla gyáraiban.

6. ábra: Elon Musk szerint 2025-re 1000 Optimus robot fog működni a Tesla gyáraiban. Forrás: (https://androgeek.hu/hir/elon-musk-szerint-2025re-1000-optimus-robot-fog-mukodni-a-tesla-gyaraiban)

6.1.2 Amazon – A logisztikai automatizáció és mesterséges intelligencia úttörője

Az Amazon az e-kereskedelem egyik legnagyobb szereplőjeként nemcsak az online vásárlás területén, hanem a logisztikai és raktározási folyamatok automatizálásában is élen jár. A vállalat raktáraiban több mint 750 000 robot működik, amelyek különféle feladatokat látnak el a hatékonyság növelése és a költségek csökkentése érdekében.

Automatizált raktári rendszerek és robotika

Az Amazon 2012-ben vásárolta meg a Kiva Systems nevű céget, amely mobil robotokat fejlesztett raktári alkalmazásokhoz. Ezek a robotok azóta az Amazon Robotics részlegén keresztül továbbfejlesztve működnek a vállalat

raktáraiban. A különféle típusú robotok – mint például a Proteus, Sparrow, Sequoia, Hercules, Titan, Pegasus, Robin, Cardinal és Xanthus – különböző feladatokat látnak el, mint például csomagok szállítása, válogatása, emelése és tárolása.

Mesterséges intelligencia alkalmazása

Az Amazon raktáraiban a mesterséges intelligencia (MI) kulcsszerepet játszik a folyamatok optimalizálásában. Az MI-alapú rendszerek valós időben elemzik a készleteket, előrejelzik a keresletet, és optimalizálják a készletkezelést. A gépi tanulás segítségével az Amazon képes dinamikusan kiigazítani a készleteket a piaci igényekhez, csökkentve ezzel a szállítási időt és a hibaarányt.

Humanoid robotok és jövőbeli fejlesztések

Az Amazon jelenleg olyan humanoid robotokat tesztel, mint például a "Digit", amelyek rugalmasan reagálhatnak a raktár szerkezetének változásaira és ismétlődő feladatokat vállalhatnak. Ezek a robotok képesek együttműködni az emberi dolgozókkal, növelve ezzel a termelékenységet és javítva a munkakörülményeket.

7. ábra: Az Amazon Proteus nevű első teljesen autonóm raktári robotja. Forrás: (https://www.engadget.com/proteus-amazon-first-fully-autonomous-warehouse-robot-074341277.html)

6.1.3 BMW – Precíziós gyártás, ember-robot együttműködés és mesterséges intelligencia alkalmazása

A BMW világszerte ismert prémium autógyártó, amely kiemelkedő figyelmet fordít a gyártási folyamatok innovációjára és hatékonyságának növelésére. A vállalat gyáraiban a robotika és a mesterséges intelligencia (MI) alkalmazása kulcsszerepet játszik a termelés optimalizálásában és a minőség biztosításában.

Automatizált gyártósorok és robotika

A BMW müncheni összeszerelő üzemében az MI és az adatelemzés egyre nagyobb szerepet kap a minőség javítása és a hatékonyság növelése érdekében. A présüzemben például naponta több mint 30 ezer acéllemezből alakítják ki a járművek

karosszériáját, és minden nyersdarabot lézeres kóddal látnak el a gyártás kezdetén, így minden elem egyértelműen azonosítható a gyártási folyamat során.

A BMW regensburgi gyárában a karosszériafényezés utáni felületkezelést automatizált és teljes egészében digitális technológiákkal végzik. A mesterséges intelligencia által vezérelt robotok minden egyes karosszérián pontosan ott dolgoznak, ahol szükséges, biztosítva ezzel a magas szintű karosszériafelületi minőséget.

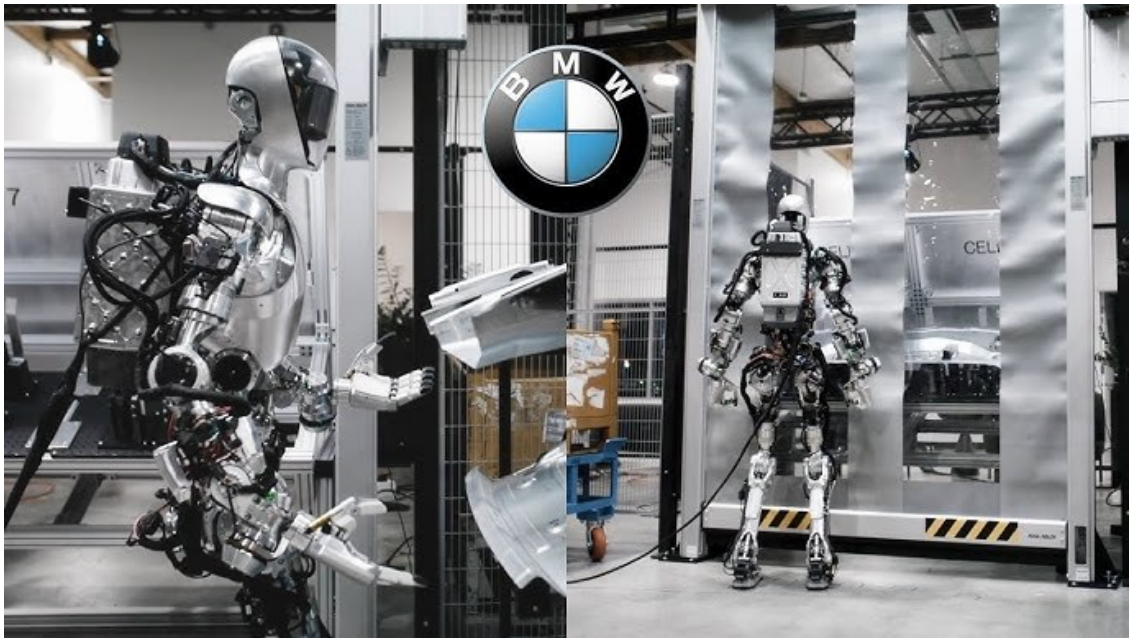
Mesterséges intelligencia alkalmazása

A BMW a gyártási folyamatok tervezésében is kihasználja az MI nyújtotta lehetőségeket. A regensburgi gyárban például a gyártás megkezdése előtt virtuális szimulációkat végeznek az Nvidia Omniverse platformján, amely lehetővé teszi a teljes gyártási folyamat részletes megtervezését és optimalizálását. Ez a virtuális gyár szimuláció lehetővé teszi a fizikai tulajdonságok és interakciók modellezését, valamint a robotok és emberi munkások közötti együttműködés optimalizálását.

A BMW a generatív mesterséges intelligenciát is alkalmazza a digitális élmények fokozására. A BMW Intelligent Personal Assistant például az Amazon Alexa élőbeszéd-modelljével (LLM) kiegészítve képes természetesebb és összetettebb párbeszédekre, így javítva a felhasználói élményt.

Ember-robot együttműködés és biztonsági kérdések

A BMW gyáraiban az emberi munkavállalók és a robotok közötti együttműködés kiemelt fontosságú. Az együttműködő robotok, vagy "kobotok" alkalmazása lehetővé teszi, hogy a robotok biztonságosan dolgozzanak az emberek mellett, növelve ezzel a termelés hatékonyságát és rugalmasságát. A BMW müncheni üzemében például olyan robotokat alkalmaznak, amelyek képesek érzékelni az ember jelenlétét, és ennek megfelelően módosítani mozgásukat, biztosítva ezzel a biztonságos munkakörnyezetet.

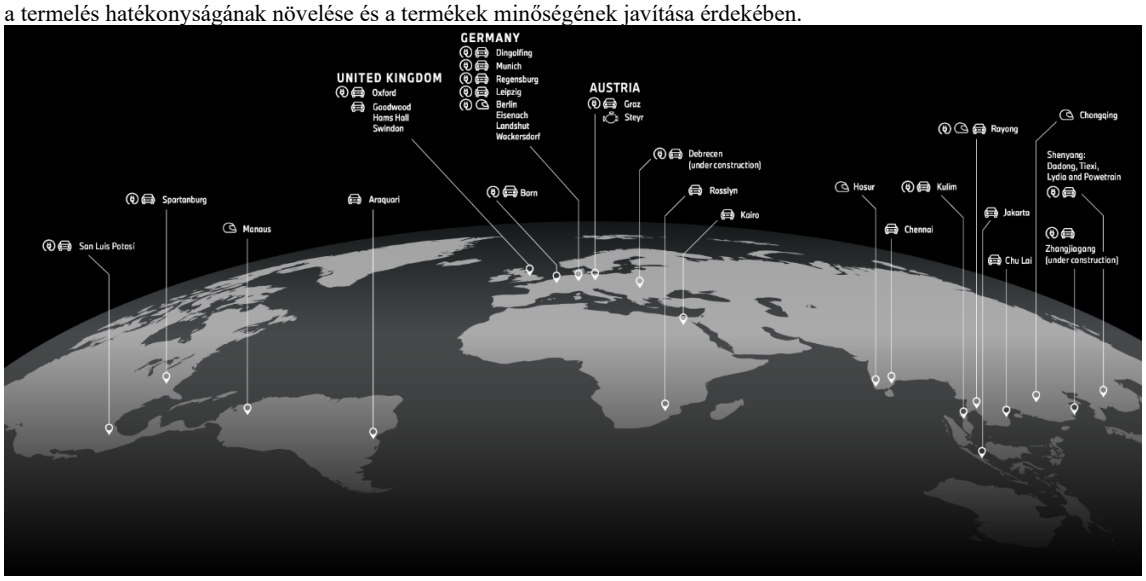


8. ábra: Humanoid robot működés közben a BMW gyáraiban. Forrás: (https://www.youtube.com/watch?v=UBTELOuy6Us)

Jövőbeli fejlesztések és innovációk

A BMW folyamatosan kutatja és fejleszti a legújabb technológiákat a gyártási folyamatok további optimalizálása érdekében. A vállalat különös figyelmet fordít a kiterjesztett valóság (AR) és a kevert valóság (MR) alkalmazására, amelyek lehetővé teszik a gyártási folyamatok még pontosabb tervezését és a munkavállalók képzését virtuális környezetben. Ezen technológiák integrálása hozzájárul a gyártási folyamatok rugalmasságának és hatékonyságának növeléséhez.

A BMW példája jól mutatja, hogyan lehet a robotikát és a mesterséges intelligenciát integrálni a gyártási folyamatokba a termelés hatékonyságának növelése és a termékek minőségének javítása érdekében.



9. A BMW gyártóüzemeinek globális elhelyezkedése. Forrás: (https://www.visit-bmwgroup.com/en/production/sites/)

6.2 Robotizált logisztikai rendszerek és raktárautomatizáció

A robotizált logisztikai rendszerek és raktárautomatizáció napjainkban kulcsszerepet játszanak a modern ipari és kereskedelmi folyamatok hatékonyságának növelésében. Az automatizált raktárakban alkalmazott technológiák, mint az autonóm mobil robotok (AMR), automatizált tároló- és visszakereső rendszerek (ASRS), valamint a mesterséges intelligencia által vezérelt szoftverek, lehetővé teszik a gyorsabb, pontosabb és költséghatékonyabb működést.

Az automatizált raktárak előnyei közé tartozik a megnövekedett tárolási kapacitás, a gyorsabb rendelésfeldolgozás, valamint a hibák számának csökkenése. Például a Webshippy fulfillment központjaiban a teljesítési folyamatok teljes egészében digitalizáltak, amely folyamatos adatelemzést tesz lehetővé, így minden pillanatban a legmodernebb raktárlogisztika áll az ügyfelek rendelkezésére.

A robotizált rendszerek bevezetése nemcsak a hatékonyságot növeli, hanem hozzájárul a munkaerőhiány kezeléséhez is. A monoton, ismétlődő feladatokat gépek végzik, így a humán munkaerő más, értékteremtőbb feladatokra összpontosíthat.

A jövőben várhatóan tovább nő az automatizált rendszerek szerepe a logisztikában, különösen az e-kereskedelem és a gyorsan változó piaci igények kiszolgálása terén. A technológiai fejlődés lehetővé teszi a raktárak még intelligensebbé és adaptívabbá tételét, amely új szintre emeli az ellátási láncok hatékonyságát és rugalmasságát.

6.3 Az ipari robotok és mesterséges intelligencia jövője (teljesen automatizált gyártás)

Az ipari robotok és a mesterséges intelligencia (MI) fejlődése napjainkra olyan szintet ért el, amely teljesen új távlatokat nyitott meg a gyártás és a termelés világában. A jövő iparában már nem csupán arról van szó, hogy a robotok egyszerű, ismétlődő feladatokat végeznek, hanem komplex, önállóan döntéseket hozó, egymással kommunikáló és folyamatosan tanuló rendszerek jelennek meg. Ezek a rendszerek képesek akár teljes gyártósorokat emberi beavatkozás nélkül irányítani.

6.3.1 A teljesen automatizált gyártás fogalma

A teljesen automatizált gyártás olyan termelési környezetet jelent, ahol a gyártási folyamatok minden lépését – az alapanyagok érkezésétől kezdve a késztermék elszállításáig – robotok, szoftveres rendszerek és MI-alapú megoldások végzik.

A cél nem csupán a munkaerő kiváltása, hanem:

- a hibák minimalizálása,
- a gyorsaság növelése,
- a költségek csökkentése,
- a minőség maximalizálása,
- és a folyamatos, 0-24 órás működés biztosítása.

6.3.2 MI alapú döntéshozatal a gyártásban

A jövő gyárainak kulcsa a mesterséges intelligencia-alapú döntéshozatal lesz. A rendszer képes lesz:

- valós időben adatokat gyűjteni (szenzorok, gépi látás),
- az adatokat feldolgozni (Big Data elemzés, gépi tanulás),
- következtetéseket levonni (mintázatok felismerése),
- önállóan beavatkozni (folyamatok módosítása, gépek vezérlése).

Ez azt jelenti, hogy a robotok például maguktól felismerik a hibás alapanyagot, módosítják a gyártási tervet, vagy éppen karbantartást rendelnek el, ha problémát észlelnek.

6.3.3 Az autonóm gyártási rendszerek jellemzői

Technológia	Funkció
MI platformok	Adatfeldolgozás, elemzés, döntéshozatal
Autonóm mobil robotok (AMR)	Szállítás, logisztika, anyagmozgatás
Automatizált tárolórendszerek (ASRS)	Raktározás, termékkezelés
Digital Twin	Virtuális gyártás szimulációja
IoT eszközök	Adatgyűjtés, kommunikáció
Edge computing	Valós idejű adatfeldolgozás lokálisan
Prediktív karbantartás	Előrejelzés és megelőző beavatkozás
Ember-robot kollaboráció	Speciális feladatoknál kiegészítő szerep

2. táblázat: A jövő teljesen automatizált gyáraiban a következő elemek játszanak központi szerepet (saját készítés)

6.3.4 A mesterséges intelligencia jövőbeni képességei

Az MI a jövőben olyan területeken válik még erősebbé, mint:

- természetes nyelvi feldolgozás (NLP) – emberi kommunikáció robotokkal,
- adaptív tanulás – új feladatok gyors elsajátítása,
- prediktív elemzés – trendek, igények előrejelzése,
- autonóm problémamegoldás – váratlan helyzetek kezelése.

A jövő robotjai már nemcsak parancsot hajtanak végre, hanem képesek önálló célokat kitűzni és ezekhez megoldásokat keresni.

6.3.5 A teljesen automatizált gyártás előnyei és kihívásai

Előnyök:

- Maximális termelékenység
- Állandó minőség
- Költségoptimalizálás
- 24/7 működés
- Rugalmasság a változó piaci igényekre

Kihívások:

- Magas kezdeti beruházási költség

- Kiberbiztonsági fenyegetések
- Munkaerő átképzési igény
- Technológiai komplexitás
- Etikai és jogi kérdések (ember-robot viszony)

6.3.6 A jövő ipara: Ember nélkül?

Bár a teljesen automatizált gyártás technológiai szempontból megvalósíthatóvá válik, a szakértők szerint az emberi jelenlét soha nem tűnik el teljesen. A stratégiai döntések, a kreativitás, a problémamegoldás és a komplex rendszerek felügyelete még sokáig emberi kompetencia marad.

A jövő gyáraiban inkább a humán és gépi erőforrások okos együttműködése, és nem a teljes gépesítés lesz a legjobb megoldás.

7 KIHÍVÁSOK ÉS JÖVŐBELI TRENDEK

7.1 A robotizáció munkaerőpiaci hatásai

A robotizáció és a mesterséges intelligencia (MI) térnyerése alapjaiban alakítja át a munkaerőpiacot. A monoton, ismétlődő feladatokat végző munkakörök – például a gyártósori operátorok, raktári dolgozók vagy ügyfélszolgálati munkatársak – fokozottan ki vannak téve az automatizálásnak. Egyes becslések szerint az automatizálás technológiailag már ma is a munkafeladatok közel 49%-át képes lenne kiváltani Magyarországon.

Ugyanakkor fontos megjegyezni, hogy az automatizáció nem feltétlenül szünteti meg a munkahelyeket, hanem átalakítja azokat. A technológiai fejlődés új munkaköröket teremt, különösen a magasabb hozzáadott értékű, kreatív és problémamegoldó képességeket igénylő területeken. A munkavállalóknak alkalmazkodniuk kell az új elvárásokhoz, ami átképzést és folyamatos tanulást igényel.

A munkaerőpiaci átalakulás társadalmi hatásai is jelentősek. A technológiai változásokhoz való alkalmazkodás képessége eltérő lehet a különböző társadalmi csoportok között, ami növelheti a társadalmi egyenlőtlenségeket. Ezért kiemelten fontos a megfelelő oktatási és szociálpolitikai intézkedések bevezetése, amelyek támogatják a munkavállalók átképzését és a munkaerőpiaci átmenetek kezelését.

7.2 Etikai kérdések és szabályozási kihívások

A robotizáció és az MI alkalmazása számos etikai és jogi kérdést vet fel. Az egyik legfontosabb kihívás az adatvédelem és a magánélet védelme. Az MI rendszerek gyakran nagy mennyiségű személyes adatot gyűjtenek és dolgoznak fel, ami adatvédelmi aggályokat vet fel. Az adatkezelés átláthatósága és a felhasználók tájékoztatása kulcsfontosságú az etikus adatkezelés biztosításához.

További etikai kérdés a döntéshozatal felelőssége. Ha egy MI rendszer hibás döntést hoz, például egy önvezető jármű balesetet okoz, ki viseli a felelősséget? A fejlesztő, az üzemeltető vagy a felhasználó? Ezekre a kérdésekre a jogrendszereknek még meg kell találniuk a megfelelő válaszokat.

Az MI rendszerek átláthatósága és megmagyarázhatósága is fontos etikai szempont. A felhasználóknak és az érintetteknek meg kell érteniük, hogyan és miért hoz egy MI rendszer bizonyos döntéseket. Ez különösen fontos az olyan területeken, mint az egészségügy vagy a pénzügyi szolgáltatások, ahol az MI döntései közvetlen hatással vannak az emberek életére.

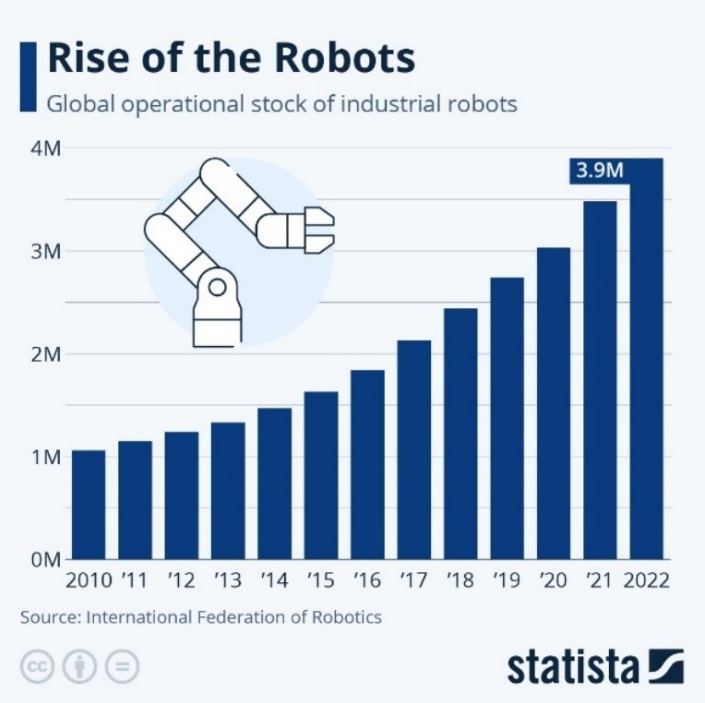
A szabályozási kihívások közé tartozik az MI rendszerek jogi kereteinek kialakítása. Az Európai Unió például etikai iránymutatásokat dolgozott ki a megbízható MI rendszerek fejlesztésére, amelyek hangsúlyozzák az emberi autonómia tiszteletben tartását, a kár megelőzését, a méltányosságot és a megmagyarázhatóságot.

7.3 A teljesen automatizált ipar lehetőségei és korlátai

A teljesen automatizált ipar számos előnnyel járhat, például a termelékenység növelésével, a költségek csökkentésével és a minőség javításával. Az automatizált rendszerek képesek 24/7 működésre, minimalizálják az emberi hibákat, és gyorsan alkalmazkodnak a változó piaci igényekhez.

Ugyanakkor az automatizáció korlátai is jelentősek. A technológiai beruházások magas költségei, a komplex rendszerek bevezetésének nehézségei és a megfelelő szakképzett munkaerő hiánya akadályozhatják az automatizáció terjedését. Emellett az emberi kreativitás, empátia és komplex döntéshozatali képességek továbbra is nélkülözhetetlenek bizonyos területeken.

A fenntarthatóság és a társadalmi elfogadottság szintén fontos szempontok. Az automatizáció hatásait figyelembe véve szükséges olyan stratégiák kidolgozása, amelyek biztosítják a technológiai fejlődés és a társadalmi jólét közötti egyensúlyt. Ez magában foglalja az oktatás és a szakképzés fejlesztését, a munkaerőpiaci átmenetek támogatását és az etikai normák



10. ábra: Az ipari robotok számának növekedése világszerte 2015 és 2022 között. Forrás: (https://www.statista.com/chart/26210/operational-stock-of-industrial-robots/)

8 BEFEJEZÉS

Az ipari robotika és a mesterséges intelligencia fejlődése az elmúlt évtizedek során új korszakot nyitott a gyártás és a termelés világában. A jövő gyárai egyértelműen a digitalizáció és az MI-alapú megoldások irányába haladnak, azonban ez a folyamat nem mentes a társadalmi, gazdasági és etikai kihívásoktól. A munkaerőpiac átalakulása, az adatbiztonság kérdése, valamint az ember és gép közötti szerepmegosztás hosszú távon is folyamatos viták és megoldáskeresés tárgya marad. Az ipari robotok és a mesterséges intelligencia fejlődése ugyanakkor számtalan új lehetőséget is teremt: hatékonyabb termelést, magasabb minőséget, gyorsabb reagálást a piaci igényekre, és fenntarthatóbb működést.

9 SZUBJEKTÍV ÖSSZEGZŐ VÉLEMÉNY

A dolgozat készítése során számomra is egyértelművé vált, hogy a robotika és a mesterséges intelligencia már nem csak a jövő technológiái, hanem a jelen valóságai is. Úgy gondolom, hogy ezek az innovációk valóban rengeteg pozitív változást hoznak a gyártásban és az iparban, de közben számos új kérdést és kihívást is felvetnek.

Személy szerint engem leginkább az fogott meg, hogy mennyire összetett és intelligens rendszerek működnek már most is a világ vezető gyáraiban. Ugyanakkor azt is fontosnak tartom, hogy az automatizáció ne járjon együtt tömeges munkanélküliséggel, hanem inkább adjon lehetőséget arra, hogy az emberek magasabb szintű, kreatívabb és értékteremtő feladatokat végezzenek.

Összességében úgy látom, hogy a technológia fejlődését nem lehet és nem is szabad megállítani, viszont érdemes tudatosan, szabályozottan és felelősségteljesen alakítani, hogy valóban mindenki számára előnyös legyen.

IRODALOMJEGYZÉK

[1] McKinsey & Company: *Generative AI and the future of work in America*. McKinsey Global Institute, 2023. Elérhető: https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america

[2] Statista: *Operational Stock of Industrial Robots Worldwide 2015-2022*. Statista, 2023. Elérhető: https://www.statista.com/chart/26210/operational-stock-of-industrial-robots/

[3] BMW Group: *How AI is revolutionising production.* Elérhető: https://www.bmwgroup.com/en/news/general/2023/aiqx.html

[4] Amazon Robotics: *How Amazon Uses Robots to Sort and Transport Packages*. Business Insider, 2023. Elérhető: https://www.businessinsider.com/how-amazon-uses-robots-sort-transport-packages-warehouses-2025-2

[5] Tesla, Inc.: *Inside Tesla's Gigafactories*. Tesla, 2023. Elérhető: https://www.tesla.com/gigafactory

[6] HVG.hu: *A jövő autógyára: robotizáció, Ipar 4.0 és mesterséges intelligencia*. HVG.hu, 2021. Elérhető: https://hvg.hu/tudomany/20211013_jovo_autogyara_robotizacio_ipar_40_mesterseges_intelligencia

[7] Advanced Robotics: *Raktárautomatizálás a hatékonyság és versenyképesség kulcsa*. Advanced Robotics, 2023. Elérhető: https://advanced-robotics.hu/raktarautomatizalas-a-hatekonysag-es-versenykepesseg-kulcsa/

[8] Stylers Group: *Mesterséges intelligencia az etikai kihívások és dilemmák tükrében*. Stylers Group, 2022. Elérhető: https://stylersgroup.hu/mesterseges-intelligencia-az-etikai-kihivasok-es-dilemmak-tukreben/

[9] European Parliament: *Etikai iránymutatás a mesterséges intelligencia fejlesztésére és alkalmazására*. European Parliament, 2019. Elérhető: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_HU.pdf

[10] Webshippy: *Az automatizált raktárlogisztika jellemzői*. Webshippy, 2022. Elérhető: https://webshippy.com/blog/automatizalt-raktarlogisztika/

[11] Techspot: *Amazon's new AI-powered warehouse robot*. Techspot, 2023. Elérhető: https://www.techspot.com/news/96629-new-ai-powered-amazon-robot-can-perform-repetitive.html

[12] Wired.com: *BMW Uses AI and Simulation for Next-Generation Car Factories*. Wired, 2023. Elérhető: https://www.wired.com/story/bmw-virtual-factory-ai-hone-assembly-line/

[13]

[14] Press.bmwgroup.com: *Digital Production in Regensburg Factory*. BMW Group, 2023. Elérhető: https://www.press.bmwgroup.com/hungary/article/detail/T0415698HU/

[15]

[16] Xpert.digital: *Az AI és a robotika javítja a raktározást*. Xpert.digital, 2023. (https://xpert.digital/hu/az-ai-es-a-robotika-javitja-a-raktarozast/)

[17] CNC.hu: *Milyen hatása van a robotizációnak a logisztikára?*. CNC.hu, 2023. (https://www.cnc.hu/2023/08/milyen-hatasa-van-a-robotizacionak-a-logisztikara/)

[18] SkyPlanner APS: *Mi az Ipar 4.0 és hogyan működik?*. SkyPlanner, 2022. (https://skyplanner.ai/hu/forrasok/mi-az-ipar-4-0-es-hogyan-mukodik/)

[19] Mélypataki Gábor: *Az Ipar 4.0 és a jog kapcsolata – Problémafelvetések a foglalkoztatás és szociális biztonság témaköre kapcsán*. ELTE, 2022.

[20] World Economic Forum: *The Future of Jobs Report 2023*. WEF, 2023. Elérhető: https://www.weforum.org/reports/the-future-of-jobs-report-2023

[21] PwC: *Will robots really steal our jobs? The potential impact of automation*. PwC Research, 2018. Elérhető: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

2.20. A mesterséges intelligencia alkalmazásai a kiberfizikai rendszerekben a

2025

A mesterséges intelligencia alkalmazásai a kiber-fizikai rendszerekben a honvédelem és a hadászat területén.

IPAR 4.0 TECHNOLÓGIÁK GKNB_INTM087
IVÁNYI BÁLINT GERGŐ
NEPTUN KÓD: [redacted] |SZAK: Mérnökinformatikus

Abstract:

A mesterséges intelligencia (MI) rohamos fejlődése jelentős hatást gyakorol a honvédelem és a hadászat területére. A dolgozat célja, hogy feltérképezze az MI alkalmazási lehetőségeit a kiber-fizikai rendszerekben, különös tekintettel a katonai stratégiákra, autonóm rendszerekre, prediktív analitikára, szimulációkra és elektronikus hadviselésre. Az elemzés során bemutatásra kerülnek konkrét technológiák, mint a DARPA ACE, a Ghost Fleet Overlord vagy a Skyborg program, valamint azok működési elvei és fejlesztési szintjei. A dolgozat külön figyelmet fordít az etikai és biztonsági kérdésekre is, beleértve a CCW egyezményt és a NATO etikai irányelveit. Az eredmények rávilágítanak arra, hogy az MI nemcsak hatékonyságot növel, hanem új kihívásokat is teremt a katonai döntéshozatal és jogi szabályozás terén. A tanulmány hozzájárul a jövőbeli MI fejlesztések tudatosabb és felelősebb integrációjához a haditechnikában.

Tartalom

Abstract: 1
Bevezetés 4
1. A mesterséges intelligencia (MI) és a kiber-fizikai rendszerek (CPS) hatása a katonai stratégiákra 4
1.1 Project Maven – Az amerikai hadsereg mesterséges intelligencia alapú célazonosító rendszere . 5
1.1.1 Mi is az a Project Maven? 5
1.1.2 Működési elve 5
1.1.3 Alkalmazások és eredmények 6
1.2 ATLAS – A NATO mesterséges intelligencia alapú hadműveleti tervező rendszere 6
1.2.1 Mi is az az ATLAS? 6
1.2.2 Működési elve 6
1.2.3 Alkalmazások és eredmények 7
2. MI alapú technológiák és szoftverek 7
2.1 Drónok és autonóm rendszerek 7
2.1.1 Skyborg (USA) 7
2.1.1.1 Működési elve 8
2.1.1.2 Fejlesztési szint és jövőbeli irányok 8
2.1.2 Loyal Wingman / MQ-28 Ghost Bat (Ausztrália) 9
2.1.2.1 Működési elve 9
2.1.2.2 Fejlesztési szint és jövőbeli irányok 10
2.1.3 Swarms of Autonomous Drones (DARPA, USA) 10

2.1.3.1 Működési elve 11
2.1.3.2 Fejlesztési szint és jövőbeli irányok 12
2.1.4 Bayraktar TB2 (Törökország) 12
2.1.4.1 Működési elve 12
2.1.4.2 Fejlesztési szint és jövőbeli irányok 13
2.1.5 XQ-58A Valkyrie (USA) 13
2.1.5.1 Működési elve 14
2.1.5.2 Fejlesztési szint és jövőbeli irányok 14
2.1.6 Kratos UTAP-22 Mako (USA) 14
2.1.6.1 Működési elv 15
2.1.6.2 Fejlesztési szint és jövőbeli irányok 15
2.1.7 ZALA Lancet (Oroszország) 16
2.1.7.1 Működési elv 16
2.1.7.2 Fejlesztési szint és jövőbeli irányok 17
2.2. Kiberbiztonsági és hadászati elemző rendszerek 17
2.2.1 DARPA TRACE (Threat Response for Adaptive Cyber Environments) 17
2.2.1.1 Működési elv 17
2.2.1.2 Fejlesztési szint és jövőbeli irányok 18
2.3 Prediktív analitika és stratégiai döntéshozatal 18
2.3.1 Palantir Defense Solutions 18
2.3.1.1 Működési elve 18
2.3.1.2 Fejlesztési szint és jövőbeli irányok 19
2.3.2 DeepStrike 19
2.3.2.1 Működési elv 19
2.3.2.2 Fejlesztési szint és jövőbeli irányok 20
2.3.3 JEDI Cloud (USA) 20
2.3.3.1 Működési elv 20
2.3.3.2 Fejlesztési szint és jövőbeli irányok 21
2.4. Szoftverek működése és alkalmazása 21
2.4.1 Sentient (USA) 21
2.4.1.1 Funkciók és Képességek 21
2.4.1.2 Fejlesztés és Jövőbeli Kilátások 22
2.4.2 ISR (Intelligence, Surveillance, and Reconnaissance) Systems 22
2.4.2.1 Funkciók és Képességek 22
2.4.2.2 Fejlesztés és Jövőbeli Kilátások 22
3. MI alapú elektronikus hadviselés és spektrumkezelés 22
3.1 A mesterséges intelligencia szerepe az elektronikus hadviselésben 23

3.2 Raven Claw – MI alapú spektrumfigyelő és zavaró rendszer (USA) 23
3.3 SPEAR-EW – Mesterséges intelligenciával vezérelt zavaró modul (Európa) 24
3.4 Adaptive RF Jamming Systems – Gépi tanulással optimalizált rádiófrekvenciás zavarás 24
3.5 Automated Cyber Warfare Units MI alapú kiberhadviselési egységek 25
4. Szimulációk szerepe a hadászatban 25
4.1. Valós idejű stratégiai modellezés 26
- AI War Games (Pentagon): 26
- Digital Twin Technology: 26
4.2. Hadgyakorlatok és katonai kiképzés 26
- SIMNET 26
- JTLS-GO (Joint Theater Level Simulation - Global Operations): 27
- VR és AR katonai szimulációk 27
4.3. Összefoglaló 27
5. Jövőbeli fejlesztési irányok 27
5.1. DARPA ACE (Air Combat Evolution) 27
5.1.1 Működési elve 28
5.1.2 Fejlesztési szint 28
5.2. Ghost Fleet Overlord (USA) 29
5.2.1 Működési elve 29
5.2.2 Fejlesztési szint 29
6. Etikai és biztonsági szempontok 30
6.1. CCW (UN Convention on Certain Conventional Weapons) 30
6.1.1Működési elve: 30
6.1.2Fejlesztési szint: 30
6.2. Ethical AI in Defense (NATO) 30
6.2.1Működési elve: 30
6.2.2Fejlesztési szint: 30
7. Összegzés 31
Források: 32

Bevezetés

A mesterséges intelligencia rohamos fejlődése az elmúlt évtizedekben alapjaiban alakította át a haditechnológiai fejlesztéseket és a katonai stratégiai gondolkodást. A negyedik ipari forradalom részeként az MI ma már nem csupán támogató szerepet tölt be a hadseregek működésében, hanem egyre inkább stratégiai döntéshozatali pozíciókba kerül a kiber-fizikai rendszerek révén. Az MI alapú rendszerek képesek automatizálni komplex folyamatokat, előre jelezni ellenséges tevékenységeket, optimalizálni logisztikai műveleteket és fokozni a kiberbiztonság hatékonyságát.

E dolgozat célja, hogy átfogó képet adjon a mesterséges intelligencia alkalmazási lehetőségeiről a kiber-fizikai rendszerekben a honvédelem és hadászat kontextusában. Bemutatásra kerülnek a legjelentősebb fejlesztések és rendszerek (mint például a Skyborg, ATLAS, DeepStrike vagy a Ghost Fleet Overlord), valamint azok működési elvei és gyakorlati alkalmazásai. A tanulmány továbbá foglalkozik az MI alapú szimulációk és döntéstámogató rendszerek szerepével, illetve külön fejezetet szentel az etikai és jogi kérdéseknek, amelyek az autonóm fegyverrendszerek térnyerésével együtt járnak.

A kutatás aktualitását az adja, hogy az MI technológiák integrálása a hadviselésbe már nem csupán elméleti lehetőség, hanem aktív fejlesztési és gyakorlati alkalmazási terület világszerte. Ez nemcsak technológiai, hanem stratégiai, biztonságpolitikai és erkölcsi kihívásokat is felvet, amelyeket érdemes mélyebben megvizsgálni.

1. A mesterséges intelligencia (MI) és a kiber-fizikai rendszerek (CPS) hatása a katonai stratégiákra

A 21. század hadviselésének egyik legmeghatározóbb technológiai áttörése a mesterséges intelligencia (MI) és a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) gyors fejlődése. Ezek a rendszerek nem csupán technológiai újításokat jelentenek, hanem gyökeresen átalakítják a katonai gondolkodást, a stratégiai tervezést és a hadműveletek kivitelezését. A digitális eszközök és az intelligens algoritmusok integrálása révén a döntéshozatal automatizálttá, gyorsabbá és pontosabbá válik, ami jelentős előnyt jelent a modern hadszíntereken.

Az MI és a CPS lehetőséget nyújt arra, hogy a hadseregek valós idejű adatokra alapozott, prediktív elemzésekkel támogassák a parancsnoki döntéseket. A különböző szenzorokkal ellátott drónok, műholdak és más intelligens platformok képesek gyorsan és hatékonyan feltérképezni az ellenséges mozgásokat, azonosítani a potenciális veszélyforrásokat, és javaslatokat tenni a legmegfelelőbb hadműveleti lépésekre. Ezáltal a katonai stratégiák nemcsak reaktívvá, hanem proaktívvá is válhatnak. [1] [2]

1.1 Project Maven – Az amerikai hadsereg mesterséges intelligencia alapú célazonosító rendszere

1.1.1 Mi is az a Project Maven?

A Project Maven, hivatalos nevén az „Algorithmic Warfare Cross-Functional Team”, az Egyesült Államok Védelmi Minisztériuma által 2017-ben indított kezdeményezés, amelynek célja a mesterséges intelligencia (MI) és gépi tanulás alkalmazása a hadműveleti adatok feldolgozásában és elemzésében. A rendszer főként a drónok és műholdak által gyűjtött képi és videó adatok automatikus elemzésére szolgál, lehetővé téve az ellenséges célpontok gyors és pontos azonosítását.

1.1.2 Működési elve

A Project Maven működése a következő lépésekre bontható:

1. Adatgyűjtés: A rendszer különböző forrásokból például drónok, műholdak, infravörös szenzorok, radarokból származó képi és egyéb adatokat gyűjt össze.
2. Adatfeldolgozás és elemzés: A begyűjtött adatokat mesterséges intelligencia algoritmusok elemzik, amelyek képesek felismerni és osztályozni az objektumokat.
3. Azonosítás: Az MI rendszerek azonosítják a potenciális célpontokat, és megkülönböztetik azokat a baráti vagy semleges objektumoktól.
4. Döntéstámogatás: Az elemzések eredményeit a rendszer vizuálisan jeleníti meg a felhasználók számára, akik ez alapján hozhatnak döntéseket a további lépésekről.
5. Visszacsatolás: A felhasználói visszajelzések alapján a rendszer folyamatosan tanul és finomítja az elemzési képességeit.

1.1.3 Alkalmazások és eredmények

- Scarlet Dragon gyakorlatok: A Project Maven-t az amerikai hadsereg 18. Légideszant Hadtestje használta a „Scarlet Dragon” gyakorlatok során, ahol az MI rendszer segítségével azonosítottak és semmisítettek meg célpontokat valós időben.
- Valós konfliktusokban való alkalmazás**:** A rendszer bizonyítottan hasznosnak bizonyult a 2021-es kabuli evakuáció során, valamint a 2022-es orosz-ukrán konfliktusban, ahol segített az orosz haditechnika azonosításában és nyomon követésében.
- Hatékonyságnövelés**:** A Project Maven alkalmazásával egy elemző akár háromszor annyi munkát is elvégezhet, mint korábban, jelentősen növelve ezzel a hadműveletek hatékonyságát.

1.2 ATLAS – A NATO mesterséges intelligencia alapú hadműveleti tervező rendszere

1.2.1 Mi is az az ATLAS?

Az ATLAS (Allied Tactical and Logistics Analysis System) a NATO által kifejlesztett mesterséges intelligencia alapú rendszer, amely a hadműveleti tervezést és döntéshozatalt támogatja. A rendszer célja, hogy valós idejű adatokat és elemzéseket biztosítson a parancsnokok számára, elősegítve a gyors és megalapozott döntéshozatalt a hadszíntéren. [3]

1.2.2 Működési elve

1. Adatintegráció**:** Az ATLAS különböző forrásokból – például hírszerzési jelentések, logisztikai adatok, valós idejű szenzoradatok – származó információkat gyűjt össze és integrál.
2. Elemzés és modellezés: A rendszer mesterséges intelligencia algoritmusok segítségével elemzi az adatokat, és különböző hadműveleti forgatókönyveket modellez.
3. Döntéstámogatás**:** Az ATLAS javaslatokat tesz a legmegfelelőbb hadműveleti lépésekre, figyelembe véve a rendelkezésre álló erőforrásokat és a stratégiai célokat.
4. Vizualizáció**:** A rendszer intuitív felhasználói felületen keresztül jeleníti meg az elemzések eredményeit, megkönnyítve ezzel a parancsnokok számára az információk értelmezését.

1.2.3 Alkalmazások és eredmények

- Gyors döntéshozatal**:** Az ATLAS lehetővé teszi a parancsnokok számára, hogy gyorsan reagáljanak a változó hadszíntéri körülményekre, növelve ezzel a hadműveletek hatékonyságát.
- Erőforrás-optimalizálás**:** A rendszer segít az erőforrások optimális elosztásában, figyelembe véve a logisztikai és taktikai szempontokat.
- Szövetségi együttműködés: Az ATLAS támogatja a NATO tagállamok közötti együttműködést, biztosítva az információk megosztását és a közös hadműveleti tervezést.

2. MI alapú technológiák és szoftverek

2.1 Drónok és autonóm rendszerek

2.1.1 Skyborg (USA)

1. ábra: A Skyborg program koncepciója.

Forrás: https://www.airforce-technology.com/features/skyborg-the-us-air-forces-future-ai-fleet/

A Skyborg egy MI alapú autonóm drónrendszer, amelyet az Egyesült Államok Légierője (USAF) fejlesztett ki. A célja, hogy képes legyen önálló harctéri műveletek végrehajtására, miközben csökkenti az emberi pilóták terhelését. A Skyborg egy olyan drón, amely képes együttműködni más repülőgépekkel, és alkalmazza a legújabb mesterséges intelligencia módszereket, hogy a harctéri környezetben dinamikusan reagáljon.

2.1.1.1 Működési elve

A Skyborg rendszer egy összetett MI architektúrát használ, amely a következő technológiákat alkalmazza:

1. Mély neurális hálózatok (DNN): A Skyborg alapját adó mély neurális hálózatok képesek a környezet folyamatos figyelésére és a helyzetek gyors értékelésére. A hálózatok képesek a repülési és harci helyzetek kezelésére, például az ellenséges célpontok azonosítására és támadásra, miközben minimalizálják az emberi beavatkozást.
2. Megerősítéses tanulás (Reinforcement Learning): A Skyborg képes tanulni a harctéri tapasztalatokból. A rendszer megerősítéses tanulás segítségével optimalizálja a döntéseit, folyamatosan javítva a helyzetfelismerést és a manőverezési képességeket.
3. Valós idejű döntéshozatal: A rendszer képes azonnali reakciókat adni a harctéri eseményekre, például az ellenséges támadásokra vagy a navigációs akadályokra. Az MI képes a repülési útvonal optimalizálására, miközben figyelembe veszi a környezeti feltételeket, például az időjárást vagy a tereptárgyakat.
4. Önálló navigáció és akadályelkerülés: A Skyborg képes az önálló navigációra, ami azt jelenti, hogy nem szükséges folyamatos emberi irányítás a repüléshez. A rendszer képes érzékelni a környezetét és elkerülni az akadályokat, mint például más repülőgépeket vagy légvédelmi rendszereket.
5. Együttműködés más drónokkal és ember vezette repülőgépekkel: A Skyborg célja, hogy úgynevezett „wingman” szerepet töltsön be, támogatva az ember vezette repülőgépeket a harcban, vagy akár önálló küldetéseket végezzen, például felderítést vagy támadást.

2.1.1.2 Fejlesztési szint és jövőbeli irányok

A Skyborg program az Egyesült Államok légierőjének egyik kulcsfontosságú fejlesztése, és a rendszer különböző fejlesztési fázisokon megy keresztül:

- 2020-as tesztek: Az első Skyborg prototípusokat már 2020-ban tesztelték valós körülmények között, és az eredmények biztatóak voltak. A drónok sikeresen végrehajtottak autonóm repüléseket és harci manővereket.
- Jelenlegi fejlesztés: A Skyborg rendszer jelenleg különböző MI alapú repülő rendszerek tesztelésén és finomhangolásán dolgozik, beleértve az intelligens döntéshozatali mechanizmusokat és a kommunikációs protokollokat.

- Jövőbeli irányok: Az Egyesült Államok Légierője célja, hogy a Skyborgot a jövő harctéri műveletek központi elemévé váljon, a hagyományos pilóták terhelésének csökkentésével és a harci hatékonyság növelésével. [4]

2.1.2 Loyal Wingman / MQ-28 Ghost Bat (Ausztrália)

2.ábra: MQ-28 modell
Forrás: https://images.defence.gov.au/assets/Home/Search?Query=BDA_LW_Woomera_Sept_21-84_2.jpg&Type=Filename

A Loyal Wingman, később MQ-28 Ghost Bat néven ismert harci drón, az Ausztrál Királyi Légierő (RAAF) és a Boeing közös fejlesztése. A célja, hogy MI alapú döntéshozó algoritmusokkal és gépi látással együttműködő autonóm drónokat hozzon létre, amelyek képesek a vadászgépekkel való koordinált műveletek végrehajtására, valamint önállóan is képesek harci feladatok végrehajtására.

2.1.2.1 Működési elve

1. Gépi látás és döntéshozó algoritmusok: Az MQ-28 Ghost Bat gépi látással és az MI által vezérelt döntéshozatalra támaszkodik, hogy az önállóan végrehajtott felderítési és támadási feladatokat biztosítson. Az MI képes észlelni az ellenséges célpontokat, valamint elkerülni azokat a fenyegetéseket, amelyek veszélyeztethetik a saját harci gépet.

2. Moduláris kialakítás: A drón moduláris felépítése lehetővé teszi a gyors konfigurálást különböző küldetésekhez. A drónok átalakíthatók például felderítési, elektronikai harci, vagy akár támadó szerepekre, attól függően, hogy milyen feladatokat kell végrehajtaniuk.
3. Együttműködés a pilótával: A Ghost Bat drónok úgynevezett „loyal wingman" szerepet töltenek be a pilótával együtt, támogatva őt a harcban. Az MI képes a harci manőverek során koordinálni a drónt a pilótával, amely különösen fontos a komplex harci helyzetekben.
4. Önálló harci feladatok: Az MQ-28 képes önállóan harci feladatokat végrehajtani, például célpontok megsemmisítését, miközben minimalizálja az emberi beavatkozást.

2.1.2.2 Fejlesztési szint és jövőbeli irányok

- Prototípus tesztelése: Az MQ-28 első prototípusa 2020-ban jelent meg, és azóta folyamatos tesztelés alatt áll. A drónok már több sikeres tesztet hajtottak végre, beleértve a harci szimulációkat és az együttműködést más repülőgépekkel.
- A jövő irányai: A Boeing és az Ausztrál Királyi Légierő célja, hogy az MQ-28 Ghost Bat legyen az első lépés egy olyan autonóm légierő kifejlesztésében, amely képes az ember vezette és autonóm rendszerek együttműködésére. [5] [6] [7]

2.1.3 Swarms of Autonomous Drones (DARPA, USA)

3.ábra DRAPA modell
Forrás: https://www.hstoday.us/industry/emerging-innovation/darpas-offset-swarms-take-flight-in-final-field-experiment/

A DARPA (Defense Advanced Research Projects Agency) által kifejlesztett autonóm drónrajok célja, hogy olyan decentralizált rendszerek jöjjenek létre, ahol a drónok képesek egymással kommunikálni és kollektív döntéseket hozni. A rendszer kulcseleme a swarm intelligence (raj intelligencia), amely lehetővé teszi, hogy a drónok együttműködjenek anélkül, hogy központi vezérlésre lenne szükségük.

2.1.3.1 Működési elve

A DARPA autonóm drónrajok működése a következő kulcsfontosságú technológiai elemeket tartalmazza:

1. Decentralizált mesterséges intelligencia (MI): A drónok nem egy központi számítógépről kapják az utasításokat, hanem egymással kommunikálnak és közösen hoznak döntéseket. Ezáltal a rendszer sokkal robusztusabbá válik, mivel nincs egyetlen hibapont, amely az egész rendszert megbéníthatja.
2. Swarm Intelligence: A swarm intelligence a kollektív viselkedést és döntéshozatalt jelenti, amelyben a drónok egymás adatait és információit megosztva javítják a helyzetfelismerést és a feladatvégrehajtást. Ez az elv lehetővé teszi, hogy a drónok rugalmasan alkalmazkodjanak a környezetükhöz és gyorsan reagáljanak a változásokra.
3. Képességek**:**
    - Valós idejű alkalmazkodás**:** A drónrajok képesek valós időben alkalmazkodni a környezetükben bekövetkező változásokhoz, például a terepviszonyokhoz, időjárási körülményekhez vagy ellenséges aktivitásokhoz.
    - Kollaboratív feladatvégrehajtás**:** A drónok képesek együttesen végrehajtani komplex műveleteket, mint például felderítés, célpontazonosítás, támadás vagy védelmi műveletek. A rendszer biztosítja a célpontok precíz azonosítását és a hatékony támadásokat.
4. Rendszer robusztusság és megbízhatóság**:** Mivel a drónok közvetlenül kommunikálnak egymással, nem szükséges egy központi vezérlés, így a rendszer képes egyes drónok kiesése esetén is működni, mivel az intelligens algoritmusok azonnal átvállalják a kiesett drón feladatát.

5. Adaptív és öntanuló rendszerek**:** A swarm algoritmusok képesek folyamatosan tanulni a harctéri tapasztalatokból, így a rajok egyre intelligensebbé és hatékonyabbá válnak a különböző hadműveletek során.

2.1.3.2 Fejlesztési szint és jövőbeli irányok

A DARPA által kifejlesztett autonóm drónrajok az egyik legígéretesebb irányt képviselik a jövő katonai drónrendszereiben, hiszen azok olyan új szintre emelik a harctéri alkalmazásokat, ahol a drónok együttműködve, önállóan hajtanak végre komplex feladatokat. Jelenleg a DARPA különböző teszteléseket végez a rajok koordinációjának és döntéshozatalának finomhangolására, különös figyelmet fordítva a valós idejű adaptációra és az önálló működés megbízhatóságára. [8] [9]

2.1.4 Bayraktar TB2 (Törökország)

4.ábra: Bayraktar TB2 modell
Forrás: https://hu.wikipedia.org/wiki/Bayraktar_TB2

A Bayraktar TB2 egy török fejlesztésű, félig autonóm drón, amely kiemelkedő szerepet játszott a modern harcterekben, különösen olyan konfliktusokban, mint Szíria, Líbia és az orosz-ukrán háború. A TB2 drón képes célpontokat azonosítani és támadni, miközben fedélzeti MI alapú célfelismerő rendszert alkalmaz.

2.1.4.1 Működési elve

1. Célfelismerő rendszer (MI alapú): A Bayraktar TB2 drón fedélzetén található célfelismerő rendszer a deep learning (mély tanulás) algoritmusokat alkalmazza, hogy azonosítsa a célpontokat, beleértve a földi járműveket, épületeket és egyéb ellenséges infrastruktúrákat.
2. Félig autonóm működés: A TB2 képes félig autonóm módon repülni, amely azt jelenti, hogy a drón képes önállóan végrehajtani a repülési feladatokat, miközben a pilóta távolról irányítja a támadásokat.

3. Támadó képességek: A drón képes különböző típusú precíziós irányítású fegyverek (például rakéták és bombák) használatára, miközben minimális emberi beavatkozást igényel. A célpontok azonosításához és a támadások végrehajtásához alkalmazott MI segíti a drónt abban, hogy a lehető legpontosabb találatokat érje el.
4. Valós idejű adatátvitel: A TB2 képes valós idejű adatokat küldeni a vezérlő központba, ami lehetővé teszi a küldetések folyamatos nyomon követését és az adaptív döntéshozatalt.
5. Alkalmazás különböző konfliktusokban: A Bayraktar TB2 több sikeres katonai műveletben is részt vett, ahol hatékonyan támadott ellenséges erőket és infrastruktúrát, jelentős hatást gyakorolva a konfliktusok menetére.

2.1.4.2 Fejlesztési szint és jövőbeli irányok

A Bayraktar TB2 egy rendkívül sikeres drón, amely Törökország számára kulcsszereplővé vált a modern hadviselésben. Jelenleg a TB2 fejlesztésén túl a török katonai ipar célja, hogy tovább javítsák a drón autonómiáját és technikai képességeit, beleértve a jövőbeli fejlesztéseket a Bayraktar TB3 és Akinci drónokban. [10] [11]

2.1.5 XQ-58A Valkyrie (USA)

5.ábra: XQ-58A Valkyrie
Forrás: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/3209939/kratos-xq-58a-valkyrie/

Az XQ-58A Valkyrie egy amerikai fejlesztésű, autonóm harci drón, amely megerősítéses tanulás algoritmusokat használ, hogy önálló harctéri döntéseket hozzon. A Valkyrie célja, hogy manned-unmanned teaming (MUM-T) koncepciót támogassa, azaz együtt működjön a pilóta vezette repülőgépekkel, támogatva a harctéri helyzetfelismerést és csökkentve az emberi pilóták kockázatát.

2.1.5.1 Működési elve

1. Autonóm döntéshozatal: A Valkyrie az MI és megerősítéses tanulás (RL) segítségével képes önálló döntéseket hozni a harctéri helyzetekben, figyelembe véve az ellenséges fenyegetéseket és a támadás módját.
2. Manned-Unmanned Teaming (MUM-T): A Valkyrie együtt dolgozik a pilóta vezette repülőgépekkel, hogy növelje a helyzetfelismerést és támogassa a harci műveleteket. A drón képes adatokat és információkat megosztani a pilótákkal, hogy közösen hajtsanak végre támadásokat.
3. Támogatás és előretolt érzékelés**:** A Valkyrie lehetővé teszi a pilóták számára, hogy az ellenséges légvédelem előtt operáljanak, előretolt érzékelőként és támogató egységként működve.

2.1.5.2 Fejlesztési szint és jövőbeli irányok

Az XQ-58A Valkyrie a Pentagon által fejlesztett legmodernebb harci drónok közé tartozik, és a jövőben várhatóan további fejlesztéseken esik át, különösen a manned-unmanned teaming koncepciójára összpontosítva. [12] [13] [14]

2.1.6 Kratos UTAP-22 Mako (USA)

6.ábra: Kratos UTAP-22 Mako
Forrás: https://botsanddrones.co/military%2C-tactical-drones/f/kratos-utap-22-mako?blogcategory=Military%2FTactical+Drones

A Kratos UTAP-22 Mako egy amerikai fejlesztésű autonóm támadó drón, amely neurális hálózatokat és gépi tanulást alkalmaz a mozgás tervezésére és az adaptív célkövetésre. A drón célja, hogy csökkentse az emberi pilóták terhelését és növelje a harctéri hatékonyságot, különböző küldetések során, beleértve a felderítést, a célpontok elpusztítását, és a manned-unmanned teaming (MUM-T) alkalmazását.

2.1.6.1 Működési elv

1. Neurális hálózatok és gépi tanulás: A UTAP-22 Mako neurális hálózatai képesek a drón mozgásának optimalizálására, valamint az adaptív célkövetésre. Az algoritmusok segítségével a drón képes gyorsan reagálni a harctéri környezet változásaira, és önállóan végrehajtani komplex feladatokat.
2. Autonóm működés és együttműködés: A Mako képes más autonóm drónokkal és pilóta vezette repülőgépekkel együttműködni. A közös hadműveletek során a drónok képesek megosztani egymással az információkat, együttműködve a küldetések sikeres végrehajtásában.
3. Támadó és felderítő képességek**:** A Kratos UTAP-22 Mako számos feladatot képes ellátni, beleértve a felderítést, a célpontok azonosítását, valamint a támadásokat is. A drón célja, hogy elősegítse a pilóták és a hagyományos repülőgépek hatékonyságát, miközben csökkenti az emberi kockázatokat a harctéren.
4. Harctéri hatékonyság: A Mako a drónokat egy „loyal wingman” szerepben alkalmazza, amely azt jelenti, hogy képes támogatni az ember vezette repülőgépeket és kiegészíteni a harctéri műveleteket, például előretolt érzékelőként működve.
5. Rugalmas küldetésképesség: A Kratos UTAP-22 Mako különböző típusú harci küldetésekhez is alkalmazható, például légvédelmi rendszerek kiiktatása, területellenőrzés, vagy egyéb precíziós támadások.

2.1.6.2 Fejlesztési szint és jövőbeli irányok

A Kratos UTAP-22 Mako az autonóm drónok egyik ígéretes példája, amely az amerikai katonai drónfejlesztésekben kulcsszerepet játszik. A rendszer a jövőben várhatóan még inkább fejlesztésre kerül, különösen a mesterséges intelligencia és a közvetlen irányítói visszajelzések alkalmazásával, hogy még precízebbé és hatékonyabbá váljon a harctéren. [15] [16] [17]

2.1.7 ZALA Lancet (Oroszország)

7.ábra: ZALA Lancet
Forrás: https://vedelmiiparblog.hu/blog/az-orosz-lancet-dron/

A ZALA Lancet egy orosz fejlesztésű autonóm drón, amely MI alapú célfelismerő algoritmusokat alkalmaz a célpontok azonosítására és követésére. A drón elektromos meghajtású, és kifejezetten az ellenfél infrastruktúrájának és katonai eszközeinek megsemmisítésére lett kifejlesztve. A ZALA Lancet sikeresen bizonyította hatékonyságát olyan konfliktusokban, mint a szíriai és orosz-ukrán háború.

2.1.7.1 Működési elv

1. Célfelismerés és követés: A ZALA Lancet célfelismerő rendszere optikai-elektronikai és TV-irányítási rendszerek kombinációját alkalmazza a célpontok valós idejű azonosítására és követésére. A drón képes a pontos célcsapások végrehajtására, ami növeli a támadások precizitását és hatékonyságát.
2. Elektromos meghajtás és sebesség: A Lancet elektromos meghajtású, amely csökkenti a zajt és növeli a manőverezhetőséget. A drón képes akár 300 km/h sebességgel is támadni, lehetővé téve a gyors beavatkozást és a nehezen észlelhető támadásokat.
3. Programozott és autonóm működés: A Lancet előre programozott támadási paraméterekkel rendelkezik, de autonóm módon képes alkalmazkodni a harctéri környezethez és végrehajtani a támadásokat. Az előre beállított útvonalak mellett a drón képes valós időben módosítani a célpontokat, ha szükséges.

4. Szíriai és orosz-ukrán alkalmazás: A ZALA Lancet sikeresen alkalmazásra került a szíriai polgárháborúban, valamint az orosz-ukrán konfliktusban. A drónok a katonai eszközökre és az ellenséges infrastruktúrára mértek precíziós támadásokat, és komoly szerepet játszottak az ellenség védelmi rendszereinek kiiktatásában.
5. Valós idejű irányítás: A ZALA Lancet képes valós idejű adatokat küldeni a vezérlő központba, ami lehetővé teszi a támadások nyomon követését és a műveletek finomhangolását.

2.1.7.2 Fejlesztési szint és jövőbeli irányok

A ZALA Lancet az orosz katonai ipar egyik vezető fejlesztése, amely a jövőben valószínűleg további fejlesztéseken esik át. A drónok növekvő alkalmazása a harctéren és az autonóm támadási képességek folyamatos javítása valószínűsíthető, hogy még hatékonyabbá teszik a rendszerüket a jövőbeli konfliktusokban. [18] [19]

2.2. Kiberbiztonsági és hadászati elemző rendszerek

2.2.1 DARPA TRACE (Threat Response for Adaptive Cyber Environments)

A TRACE (Threat Response for Adaptive Cyber Environments) egy DARPA által fejlesztett Big Data elemző rendszer, amely anomália-detektáló algoritmusokat alkalmaz a kibertámadások azonosítására és az ezekre adott válaszok automatizálására. A TRACE célja, hogy előre jelezze a potenciális fenyegetéseket és reagáljon a kibertámadásokra, anélkül, hogy emberi beavatkozás szükséges lenne.

2.2.1.1 Működési elv

1. Anomália-detektálás: A TRACE rendszer anomáliákat keres a hálózati aktivitásban, és ha olyan viselkedést észlel, amely eltér a normális működéstől, azt potenciális fenyegetésként azonosítja. Az anomáliák észlelése automatikusan történik, és az algoritmusok képesek a támadásokat előre jelezni, mielőtt azok kárt okoznának.
2. Prediktív modellek: A TRACE használ prediktív modelleket**,** amelyek a múltbeli adatok alapján előre jelezhetik a potenciális kibertámadásokat. Ez lehetővé teszi a rendszer számára, hogy proaktívan észlelje és kezelje a jövőbeli fenyegetéseket, így csökkentve a kiberbiztonsági kockázatokat.

3. Felügyelet nélküli tanulás: A rendszer unsupervised learning (felügyelet nélküli tanulás) technikákat használ, ami lehetővé teszi számára, hogy új típusú támadásokat is felismerjen. Mivel a rendszer képes új adatokat elemezni, elősegíti a kibertámadások felismerését olyan minták alapján, amelyeket korábban nem tartottak a támadások részének.
4. Valós idejű reagálás: A TRACE valós időben képes észlelni és reagálni a hálózati anomáliákra, lehetővé téve a gyors válaszokat a kibertámadásokkal szemben. A valós idejű elemzés és a prediktív modellek biztosítják, hogy a rendszer időben beavatkozhasson, és megelőzze a nagyobb kárt.

2.2.1.2 Fejlesztési szint és jövőbeli irányok

A TRACE a kiberbiztonság és a nagy adatokat kezelő rendszerek terén alkalmazható technológiák fejlődését képviseli. A jövőben a rendszer további finomításokra és bővítésekre kerülhet, különösen a mesterséges intelligencia és a gépi tanulás alkalmazásával.

2.3 Prediktív analitika és stratégiai döntéshozatal

2.3.1 Palantir Defense Solutions

A Palantir Defense Solutions egy fejlett adatelemző platform, amelyet az Egyesült Államok és szövetségesei katonai erői használnak a hadműveleti döntéshozatal és stratégiai elemzés során. A rendszer célja, hogy a nagy mennyiségű, különböző formátumú és forrású adatokat hatékonyan feldolgozza és értékelje, elősegítve a gyors és pontos döntéseket.

2.3.1.1 Működési elve

1. Gráf alapú adatelemzés: A Palantir platform gráf alapú adatelemző motort alkalmaz, amely lehetővé teszi az összetett kapcsolatok és mintázatok feltárását a különböző forrásokból származó adatok között. Ez különösen fontos a katonai alkalmazásoknál, ahol a cél az, hogy az adatok közötti rejtett kapcsolatokat és tendenciákat gyorsan felfedezzék.
2. Strukturált és strukturálatlan adatok kezelése: A Palantir képes a strukturált (pl. adatbázisok, táblázatok) és strukturálatlan (pl. szöveges információk, képek) adatok együttes feldolgozására. Ez lehetővé teszi, hogy különböző típusú adatokat integráljanak és egyesítsenek egy közös elemző környezetben.

3. Prediktív modellek alkalmazása: A platform képes fejlett prediktív modellek alkalmazására, amelyek segítenek a jövőbeli események előrejelzésében, mint például a katonai mozgások, ellátási láncok, és stratégiai célpontok meghatározása. A rendszer képes a korábbi műveletek és események adataiból tanulva új mintázatokat és trendeket felismerni.
4. Gyors döntéshozatal támogatása: A Palantir platform lehetővé teszi a katonai vezetők számára, hogy gyors döntéseket hozzanak, még akkor is, ha a helyzet dinamikusan változik. A rendszer által biztosított agilis döntéshozatali eszközök segítségével a műveletek gyorsan alkalmazkodhatnak a harctéri környezethez.

2.3.1.2 Fejlesztési szint és jövőbeli irányok

A Palantir folyamatosan fejlődik, és a katonai elemzők számára egyre fejlettebb eszközöket kínál. A jövőbeli fejlesztések középpontjában a gépitanulás, az intelligens automatizálás és az adaptív analitika állnak, amelyek még nagyobb precizitást és gyorsaságot biztosítanak a döntéshozatalban. [20]

2.3.2 DeepStrike

A DeepStrike egy fejlett katonai analitikai rendszer, amelyet a hadviselés dinamikus környezetében való döntéshozatal elősegítésére terveztek. A rendszer képes előre jelezni ellenséges mozgásokat**,** logisztikai útvonalakat és potenciális támadási pontokat, így segítve a stratégiai tervezést és a műveletek optimális lebonyolítását.

2.3.2.1 Működési elv

1. Mély neurális hálózatok: A DeepStrike a mély neurális hálózatok segítségével elemzi a rendelkezésre álló adatokat. Ezek az algoritmusok képesek a komplex mintázatok és az időbeli összefüggések felismerésére, amelyeket a hagyományos modellek nem tudnának azonosítani.
2. Long Short-Term Memory (LSTM) algoritmusok: A LSTM (Long Short-Term Memory) egy speciális neurális hálózati modell, amely különösen időbeli adatsorok elemzésére alkalmas. Az LSTM képes kezelni a hosszú távú függőségeket, ami különösen hasznos a dinamikusan változó hadszíntéri helyzetek előrejelzésében.
3. Prediktív modellezés: A rendszer prediktív modelleket alkalmaz, amelyek képesek előre jelezni az ellenséges mozgásokat és azokat a potenciális területeket, ahol támadásra

kerülhet sor. A prediktív modellek folyamatosan tanulnak az új információkból, így képesek pontosabb előrejelzéseket adni.

4. Stratégiai döntéshozatal: A DeepStrike támogatja a katonai vezetők döntéshozatalát a tervezési és műveleti fázisokban, lehetővé téve a jövőbeni események pontosabb előrejelzését és a műveletek optimalizálását. A rendszer segítségével a hadsereg előre megtervezheti, hogy mely logisztikai útvonalak a legbiztonságosabbak, és milyen támadási pontok a legfontosabbak.

2.3.2.2 Fejlesztési szint és jövőbeli irányok

A DeepStrike folyamatos fejlesztés alatt áll, és várhatóan további gépitanulás és neurális hálózati fejlesztések fogják javítani a rendszer prediktív képességeit. A rendszer a jövőben még nagyobb hatékonysággal támogathatja a katonai döntéshozatalt és a hadszíntéri műveleteket. [21]

2.3.3 JEDI Cloud (USA)

A JEDI Cloud (Joint Enterprise Defense Infrastructure) egy felhőalapú rendszer, amelyet az Egyesült Államok Védelmi Minisztériuma (DoD) hozott létre, hogy támogassa a katonai műveletek gyors elemzését és a stratégiai döntéshozatalt. A célja, hogy nagy teljesítményű MI algoritmusokat és gépi tanulási modelleket futtasson, amelyek képesek gyors prediktív analitikát végezni, és elősegíteni a műveletek gyorsabb végrehajtását.

2.3.3.1 Működési elv

1. Felhőalapú infrastruktúra: A JEDI Cloud felhőalapú rendszer lehetővé teszi a nagy teljesítményű számítástechnikai erőforrások gyors elérését és alkalmazását, amelyek elengedhetetlenek a katonai műveletek elemzéséhez és a gyors döntéshozatalhoz.
2. Gépi tanulás és MI algoritmusok: A rendszer gépi tanulási modelleket és prediktív analitikát alkalmaz, hogy gyorsan feldolgozza a nagy mennyiségű adatot és azonnali válaszokat adjon a harctéri környezetben.
3. Stratégiai döntéshozatal: A JEDI Cloud célja, hogy támogassa a katonai vezetők döntéshozatalát és elősegítse a műveletek optimális végrehajtását, biztosítva a valós idejű információkat és a gyors válaszokat.

2.3.3.2 Fejlesztési szint és jövőbeli irányok

A JEDI Cloud rendszert 2021-ben megszüntették, és helyette egy új megközelítést alkalmaztak, amely több szolgáltatót von be. A jövőben a felhőalapú infrastruktúra és a gépi tanulás kombinációja még nagyobb hatékonysággal fogja támogatni a katonai döntéshozatalt és a műveleti műveleteket. [22] [23]

2.4. Szoftverek működése és alkalmazása

2.4.1 Sentient (USA)

A Sentient egy fejlett mesterséges intelligencia (MI) alapú felderítési szoftver, amelyet az Egyesült Államok Nemzeti Felderítési Hivatala (NRO) fejlesztett ki. A rendszer célja, hogy műholdas és légi felvételek alapján automatikusan azonosítson gyanús tevékenységeket, amelyek figyelmeztethetik a döntéshozókat a potenciális fenyegetésekre.

8.ábra:NRO címere 8.ábra:NRO címere
Forrás: https://en.wikipedia.org/wiki/Sentient_(intelligence_analysis_system)

2.4.1.1 Funkciók és Képességek

1. Gépi tanulás és anomália detektálás: A Sentient gépi tanulást alkalmaz annak érdekében, hogy anomáliákat (szokatlan mintázatokat) észleljen a műholdas és légi felvételeken. Az algoritmusok folyamatosan tanulnak és finomítják a modelleket, hogy a legpontosabb eredményeket biztosítsák.
2. Ellenséges mozgások előrejelzése: A rendszer képes az ellenséges mozgásokat és tevékenységeket előre jelezni, még akkor is, ha azok kiszámíthatatlanná válnak. Ez különösen hasznos lehet a térfigyelés és felderítés során, ahol gyors reagálásra van szükség.
3. Valós idejű információk: A Sentient célja, hogy valós idejű adatokat nyújtson, amelyek segítik a katonai döntéshozókat gyorsan reagálni az adott helyzetekre. A rendszer által biztosított információk lehetővé teszik a gyors és hatékony válaszintézkedéseket.
4. Automatikus adatelemzés: A rendszer képes automatikusan feldolgozni a nagy mennyiségű adatot és azonosítani a releváns információkat, ezzel csökkentve az emberi elemzés szükségességét és növelve a műveleti hatékonyságot.

2.4.1.2 Fejlesztés és Jövőbeli Kilátások

A Sentient folyamatosan fejlődik, és a gépi tanulás újabb és fejlettebb módszereit alkalmazzák, hogy még pontosabb elemzéseket végezzenek. A jövőben a rendszer az automatikus helyzetfelismerés és az ellenséges aktivitás előrejelzése terén is további fejlesztéseket hozhat. [24]

2.4.2 ISR (Intelligence, Surveillance, and Reconnaissance) Systems

Az ISR rendszerek a katonai hírszerzés, megfigyelés és felderítés kulcsfontosságú elemei. Ezek a rendszerek különböző érzékelőkből és MI modulokból állnak, amelyek képesek gyorsan feldolgozni a nagy mennyiségű adatot, amelyet drónok, műholdak és földi egységek gyűjtenek.

2.4.2.1 Funkciók és Képességek

1. Valós idejű adatfeldolgozás: Az ISR rendszerek képesek a valós idejű adatokat gyorsan feldolgozni, hogy a döntéshozók számára azonnali válaszokat adjanak a helyzetekre.
2. Helyzetfelismerés: Az ISR rendszerek alapvető szerepe a helyzetfelismerés javítása, amely lehetővé teszi a katonai műveletek megfelelő irányítását és az optimális döntések meghozatalát.
3. Fenntartható reagálás: A rendszer a gyors adatfeldolgozás révén támogatja a fenyegetések gyors és hatékony kezelését, ezzel növelve a katonai stratégiák sikerét.

2.4.2.2 Fejlesztés és Jövőbeli Kilátások

Az ISR rendszerek várhatóan további intelligens modulokkal és automatizált helyzetfelismerő rendszerekkel bővülnek, hogy még precízebb és gyorsabb válaszokat biztosítsanak a különböző katonai fenyegetésekre. [25]

3. MI alapú elektronikus hadviselés és spektrumkezelés

A 21. század hadviselésének egyik legkritikusabb komponense az elektronikus hadviselés (Electronic Warfare, EW), amely az elektromágneses spektrum (EMS) katonai célú felhasználását és az ellenség hasonló képességeinek megzavarását, korlátozását vagy teljes kiküszöbölését foglalja magában. Az MI integrálása az EW-rendszerekbe alapvetően új szintre emelte a hadszíntéren zajló műveletek gyorsaságát, hatékonyságát és autonómiáját.

3.1 A mesterséges intelligencia szerepe az elektronikus hadviselésben

Az MI alkalmazása az elektronikus hadviselésben alapvető átalakulásokat eredményezett, mivel az elektromágneses spektrum (EMS) feletti uralom kulcsfontosságú tényezővé vált a modern hadviselésben. Az MI által vezérelt rendszerek lehetővé teszik a gyors, precíz és dinamikus válaszokat, amelyek hagyományos rendszerek számára nem elérhetők.

1. Fenntartott spektrumdominancia: Az elektromágneses spektrum (EMS) folyamatos monitorozása és a dinamikus válaszreakciók biztosítják, hogy a saját erőink képesek legyenek fenntartani az irányítást a kritikus kommunikációs és navigációs csatornák felett. Az MI képes folyamatosan figyelni az EMS-t, azonosítani az ellenséges jeleket és gyorsan reagálni a zavarásra.
2. Adaptív zavarás és frekvenciamenedzsment: Az MI és a gépi tanulás (ML) algoritmusok képesek arra, hogy „megtanulják” az ellenség radarműveleteit, kommunikációs mintáit és más elektromágneses tevékenységeit, majd azokat kihasználva alkalmazkodjanak és optimalizálják a zavaró műveleteket. A zavarás nemcsak passzívan reagál, hanem aktívan alakítja a harci teret az ellenség működésének megzavarásával.
3. Automatizált döntéshozatal: Az MI rendszerek képesek gyorsan elemezni és értékelni a különféle adatokat, figyelembe véve a spektrum használati szokásokat, a radarok működési módját és a zavarásra vonatkozó lehetőségeket. Az automatizált döntéshozatal gyorsítja a válaszreakciót, csökkenti az emberi operátorokra nehezedő terhet és lehetővé teszi az azonnali beavatkozást az ellenséges tevékenységek hatékony elhárításában.

3.2 Raven Claw – MI alapú spektrumfigyelő és zavaró rendszer (USA)

A Raven Claw rendszer a hadsereg egyik legfejlettebb elektronikus hadviselési rendszere, amely az elektromágneses spektrum és az ellenséges kommunikációs jelek valós idejű elemzésére és zavarására összpontosít.

- MI funkciók: A konvolúciós neurális hálózatok (CNN) és más mintázatfelismerő algoritmusok képesek az ellenséges radarok és kommunikációs jelek felismerésére. Az MI segít gyorsan azonosítani azokat a jeleket, amelyek potenciálisan fenyegetést jelenthetnek.

- Adaptív válaszadás: A rendszer nemcsak észlel, hanem azonnali válaszokat is képes generálni. Ez lehetővé teszi a szűk sávú célzott zavarást vagy a spektrumhamisítást, mindezt valós időben, anélkül, hogy az operátornak manuálisan kellene beavatkoznia.
- Előnyök: A Raven Claw minimalizálja az emberi hiba lehetőségét, és felgyorsítja az operációs válaszidőt, mivel az MI képes önállóan és valós időben reagálni a változó fenyegetési környezetre.

3.3 SPEAR-EW – Mesterséges intelligenciával vezérelt zavaró modul (Európa)

A SPEAR-EW a brit BAE Systems fejlesztése, amely célzott zavaró műveletek végrehajtására képes, elsősorban a modern vadászgépek védelme érdekében.

- MI funkciók: A rendszer neurális hálózatokat alkalmaz a radarok észlelésére és azok azonnali lokalizálására. Az MI képes felismerni az ismeretlen vagy új radarokat, és ezekre adaptívan reagálni, így az eszköz folyamatosan optimalizálja működését a különböző környezetekben.
- Adaptív viselkedés: Az eszköz képes felismerni az ismeretlen radarokat és alkalmazkodni hozzájuk. Az MI folyamatosan tanul az új típusú fenyegetésekről, és biztosítja, hogy a rendszer mindig képes legyen az optimális védelmi stratégiát alkalmazni.
- Bevethetőség: A SPEAR-EW rendszer képes alkalmazkodni a különböző katonai platformokhoz – legyen szó földi járművekről, légi vagy tengeri célpontokról. Így segíti a saját erők védelmét, miközben csökkenti a fenyegetések hatékonyságát.

3.4 Adaptive RF Jamming Systems – Gépi tanulással optimalizált rádiófrekvenciás zavarás

Az adaptív rádiófrekvencia-zavaró rendszerek az MI alapú zavarás legújabb fejlesztései, amelyek a gépi tanulás és a mesterséges intelligencia segítségével alkalmazkodnak az ellenség kommunikációs stratégiáihoz.

- Tanulási képesség: Az unsupervised learning vagy reinforcement learning algoritmusok képesek felismerni az ellenséges kommunikációs mintákat, és ezen alapuló stratégiákat dolgoznak ki a zavarásra. A rendszer képes a spektrumot dinamikusan pásztázni, és a jelek alapján meghatározni a zavarás legoptimálisabb módját.

- Spektrumfelismerés: A rendszer képes gyorsan azonosítani az aktív rádiócsatornákat, és azonnal reagálni a fenyegetésre. A zavarás nemcsak statikus, hanem folyamatosan alkalmazkodik az ellenség válaszlépéseihez.
- Önkalibráló algoritmusok: Az MI algoritmusok lehetővé teszik, hogy a rendszer folyamatosan önkalibrálja magát, így mindig naprakész a zavarási stratégiák alkalmazásában.

3.5 Automated Cyber Warfare Units MI alapú kiberhadviselési egységek

Az MI alapú kiberhadviselési egységek célja a kibertérben zajló hadviselés gyorsítása és automatizálása.

- Fenyegetésanalízis: Az MI alapú egységek képesek a hálózati forgalom valós idejű elemzésére, hogy azonnal felismerjék a kibertámadásokat. Ilyen lehet például az adatszivárgás, jogosulatlan hozzáférés vagy a DDoS támadások észlelése.
- Reagálási képesség: Az MI algoritmusok önállóan képesek izolálni a támadás alatt álló rendszert, végrehajtani aktív védekezési intézkedéseket (pl. honeypot használata), vagy automatikusan újraépíteni a rendszert.
- MI eszközök: A deep learning technológiák, például az autoencoderek vagy a GAN-ok segítenek az adathalász kísérletek és a zero-day exploitok felismerésében.

Ezek a rendszerek képesek nemcsak védekezni, hanem aktívan támadni is, lehetővé téve a hálózati dominancia biztosítását.

4. Szimulációk szerepe a hadászatban

A szimulációk az egyik legfontosabb innováció a modern hadviselésben, mivel képesek valósághű, de kockázatmentes környezetben tesztelni a különböző hadműveleteket, stratégiákat és technikai rendszereket. Az MI és a szimulációk kombinálása lehetővé teszi a gyorsabb döntéshozatalt és a katonai képességek optimalizálását, miközben a potenciális emberi hibákat minimalizálják. Az ilyen rendszerek nemcsak a harci helyzetek gyakorlására, hanem a technikai rendszerek, fegyverek és harcjárművek teljesítményének tesztelésére is szolgálnak.

4.1. Valós idejű stratégiai modellezés

A stratégiai modellezés lehetővé teszi a hadsereg számára, hogy különböző forgatókönyveket futtasson, és felkészülhessen a váratlan változásokra a harci szituációkban. Az MI alapú szimulációs rendszerek rendkívül fontosak ezen a területen, mivel lehetővé teszik a döntéshozók számára, hogy a valós idejű adatokat figyelembe véve, a környezeti tényezőkkel és a hadműveleti célokkal összhangban fejlesszenek ki stratégiákat.

- AI War Games (Pentagon): Az AI War Games a Pentagon által használt szimulációs rendszer, amely mesterséges intelligenciát alkalmaz a harci forgatókönyvek futtatására. Ez lehetővé teszi a katonai vezetők számára, hogy különböző helyzeteket teszteljenek a valós idejű változások figyelembevételével, így az eredményeket gyorsan alkalmazhatják a valós műveletekben. Az MI képes figyelembe venni a különböző tényezőket, mint az időjárás, a terep, a hadrend, és ennek megfelelően döntéseket hozni. [26]
- Digital Twin Technology: A digitális iker technológia révén lehetőség nyílik a hadsereg számára, hogy virtuálisan szimulálja a harci járművek, fegyverek és egyéb rendszerek működését. A digitális iker segítségével a hadsereg anélkül végezhet el műszaki elemzéseket, hogy kockáztatná a valódi eszközök sérülését. Ez különösen hasznos a harci rendszerek karbantartásában és fejlesztésében, hiszen lehetőséget biztosít a potenciális hibák és hibás működések előre jelzésére és javítására. [27]

4.2. Hadgyakorlatok és katonai kiképzés

A katonai kiképzésben is elengedhetetlenek a szimulációk, mivel lehetővé teszik a katonák számára, hogy valós harci környezetekben gyakorolják a döntéshozatalt, anélkül, hogy kockáztatnák a valós életben való veszélyeket. Az MI alapú rendszerek ezen a területen is rendkívül fontos szerepet játszanak, mivel képesek valósághű forgatókönyveket létrehozni, és biztosítani a katonák számára a folyamatos fejlődést.

- SIMNET: A SIMNET egy korai MI alapú szimulációs rendszer, amely lehetőséget biztosít arra, hogy több katonai egység egy valós idejű, dinamikus harci környezetben szimulált helyzetekben vegyen részt. A SIMNET lehetővé teszi a különböző harci helyzetek tesztelését, miközben figyelembe veszi az olyan tényezőket, mint a terep, az időjárás és az erőforrások. [28]

- JTLS-GO (Joint Theater Level Simulation - Global Operations): A JTLS-GO egy fejlett szimulációs rendszer, amely lehetővé teszi a globális hadműveletek szimulálását, figyelembe véve az összes dimenziót, beleértve a logisztikát, a katonai taktikákat és a diplomáciai kapcsolatokat. A rendszer képes valós idejű adatokat feldolgozni, és azokat a stratégiai döntésekhez alkalmazni. [29] [30]
- VR és AR katonai szimulációk: A Virtuális Valóság (VR) és Kiterjesztett Valóság (AR) szimulációk szintén egyre fontosabb szerepet kapnak a katonai kiképzésben. A VR teljesen virtuális, míg az AR a valós világot és digitális adatokat kombinál. Mindkét technológia különösen hasznos lehet a katonák számára a harci környezetek gyakorlásában, a döntéshozatal és az együttműködés fejlesztésében, valamint a gyors reakciók kialakításában. [31] [32]

4.3. Összefoglaló

A szimulációs rendszerek az MI alapú technológiák alkalmazásával lehetővé teszik a katonai vezetők és a katonák számára, hogy felkészüljenek a különböző forgatókönyvekre, teszteljék a döntéshozatali mechanizmusokat és javítsák a műveleti hatékonyságot. Az MI és a virtuális szimulációk lehetővé teszik a valós idejű adatok feldolgozását, ezzel segítve a gyors alkalmazkodást és az optimális válaszreakciókat. Az ilyen típusú rendszerek nemcsak a harci helyzetek szimulálására alkalmasak, hanem a katonai rendszerek fejlesztésére és karbantartására is nagyban hozzájárulnak.

5. Jövőbeli fejlesztési irányok

5.1. DARPA ACE (Air Combat Evolution)

A DARPA (Defense Advanced Research Projects Agency) által elindított ACE program célja az autonóm légiharc képességek fejlesztése, amelyek lehetővé teszik a mesterséges intelligencia (MI) vezérelte vadászgépek számára, hogy emberi beavatkozás nélkül végezzenek harci manővereket és reagáljanak az ellenséges támadásokra. Az ACE célja, hogy a gépek képesek legyenek önállóan, hatékonyan harcolni és reagálni, csökkentve a pilóták terhelését és növelve a műveletek sikerességét.

5.1.1 Működési elve

A DARPA ACE program során az autonóm légiharc rendszerek kifejlesztése az MI algoritmusok alkalmazásával történt. Az első teszteket szimulációs környezetben végezték el, ahol az MI különböző harci forgatókönyveket és helyzeteket próbált ki. Miután a szimulációs tesztek sikeresek voltak, az X-62A "VISTA" repülőgép – melyet az Egyesült Államok Légierője (USAF) és a DARPA közösen fejlesztett – 2023-ban valós repülési körülmények között is végrehajtott egy légiharcot egy ember által vezetett F-16 vadászgép ellen.

Az MI vezérelte X-62A képes volt a harci helyzetekre gyorsan reagálni, önállóan döntéseket hozni és manővereket végrehajtani. A teszt során az MI képes volt figyelembe venni az ellenséges gép mozgását, az időjárási körülményeket, a pilóta reakció idejét, és az optimális válaszokat adni a harci helyzetekben. Ez jelentős előrelépést jelent az autonóm légiharc technológiájában, mivel a gépek most már képesek emberi irányítás nélkül önállóan alkalmazkodni a gyorsan változó harci környezetekhez.

5.1.2 Fejlesztési szint

A DARPA ACE program jelentős előrelépéseket ért el az autonóm légiharc fejlesztésében, azonban a rendszer még mindig fejlesztés alatt áll. A legnagyobb kihívások közé tartozik az emberi és gépi együttműködés optimalizálása, valamint a bizalom kiépítése az MI rendszerek iránt, különösen a döntéshozatali folyamatokban. Míg az autonóm rendszerek képesek a harci manőverek végrehajtására, a következő lépés az emberi pilóták és a gépek közötti szorosabb integráció és közös döntéshozatal lehetősége.

Az MI alapú autonóm légiharc rendszerek alkalmazása a jövőben lehetővé teheti a pilóták számára, hogy komplexebb, hosszabb ideig tartó műveleteket hajtsanak végre, miközben csökkenthetik a pilóták fizikai és pszichológiai terhelését. Ezenkívül az MI képes lenne a harci helyzetek gyorsabb és pontosabb értékelésére, optimalizálva a bevetési stratégiákat. [33] [34]

5.2. Ghost Fleet Overlord (USA)

A Ghost Fleet Overlord program az Egyesült Államok Haditengerészetének (US Navy) kezdeményezése, amelynek célja az autonóm hadihajók fejlesztése és tesztelése. A program során olyan hajókat alakítanak át, amelyek képesek önálló műveletek végrehajtására mesterséges intelligencia segítségével. Az autonomizált hajók célja, hogy csökkentsék az emberi erőforrásokat és növeljék a haditengerészet műveleti hatékonyságát.

5.2.1 Működési elve

A Ghost Fleet Overlord program keretében a haditengerészet kereskedelmi célú hajókat alakított át autonóm Unmanned Surface Vessels (USV). Ezek a hajók képesek hosszú távú, önálló navigációra, és az autonóm rendszerek segítségével különböző műveleteket hajtanak végre emberi felügyelet minimális vagy teljes hiányában. Az MI alapú rendszerek a hajók számára lehetővé teszik a navigációt, a döntéshozatalt és az alkalmazkodást a változó környezeti feltételekhez, mint például az időjárás és az ellenséges fenyegetések.

A program egyes fázisai során már sikeresen végrehajtottak hosszú távú autonóm teszteket, és a hajók képesek voltak a tervezett műveletek elvégzésére anélkül, hogy emberi beavatkozásra lett volna szükségük. Az autonóm hajók a haditengerészeti műveletek egyik kulcsfontosságú elemeként szerepelhetnek, különösen a veszélyes vagy távoli területeken végzett feladatokban.

5.2.2 Fejlesztési szint

A Ghost Fleet Overlord programban részt vevő autonóm hajók jelenleg kísérleti státuszban vannak, és a fejlesztési fázisok során a tervek szerint egyre nagyobb szerepet kapnak a haditengerészet jövőbeli flottájában. Bár a hajók már sikeresen végrehajtották az autonóm teszteket, a program folytatódik, és a cél az, hogy az ilyen típusú hajók integrálódjanak a haditengerészet műveleti környezetébe, növelve a hatékonyságot és csökkentve a kockázatokat.

A jövőbeni fejlesztések célja, hogy az autonóm hadihajók továbbfejlesztett döntéshozatali képességekkel rendelkezzenek, és képesek legyenek interakcióba lépni más hajókkal és a harci környezettel, miközben minimalizálják az emberi beavatkozás szükségességét. Az MI ezen rendszerekben való alkalmazása forradalmasíthatja a haditengerészeti műveletek végrehajtását, különösen a távoli, magas kockázatú környezetekben. [35] [36]

6. Etikai és biztonsági szempontok

6.1. CCW (UN Convention on Certain Conventional Weapons)

A CCW célja az autonóm fegyverrendszerek (LAWS) nemzetközi szabályozása, különös tekintettel az emberi ellenőrzés fenntartására és a potenciális visszaélések elkerülésére.

6.1.1Működési elve:

A CCW keretében a részt vevő államok megvitatják az autonóm fegyverrendszerek fejlesztésének és alkalmazásának jogi és etikai kérdéseit. A cél egy olyan nemzetközi keretrendszer kialakítása, amely biztosítja, hogy az ilyen rendszerek használata megfeleljen a nemzetközi humanitárius jognak.

6.1.2Fejlesztési szint:

A tárgyalások folyamatosan zajlanak, azonban a konszenzus elérése nehézségekbe ütközik, mivel egyes országok, mint az USA, Oroszország és Kína, inkább nemzeti irányelveket részesítenek előnyben a globális egyezmények helyett.

6.2. Ethical AI in Defense (NATO)

A NATO célja az etikus mesterséges intelligencia alkalmazásának biztosítása a védelmi szektorban, azáltal, hogy irányelveket és szabványokat állít fel az MI rendszerek fejlesztésére és alkalmazására.

6.2.1Működési elve:

A NATO 2021-ben elfogadta az AI Stratégiáját, amely meghatározza az MI felelős használatának alapelveit, beleértve a jogszerűséget, felelősségvállalást, magyarázhatóságot, megbízhatóságot és az elfogultság csökkentését. Ezek az elvek irányt mutatnak a tagállamok számára az MI rendszerek fejlesztésében és alkalmazásában.

6.2.2Fejlesztési szint:

A NATO tagállamai elkötelezettek az AI Stratégiában foglalt elvek betartása mellett, és folyamatosan dolgoznak az MI rendszerek etikus és felelős integrálásán a védelmi szektorba.

7. Összegzés

A mesterséges intelligencia és a kiber-fizikai rendszerek alkalmazása a honvédelem és a hadászat területén radikálisan átalakítja a 21. századi katonai gondolkodást és gyakorlatot. A dolgozat során részletesen bemutatott fejlesztések – mint a Project Maven, Skyborg, DeepStrike vagy a Ghost Fleet Overlord – azt jelzik, hogy az MI egyre nagyobb szerepet tölt be nemcsak a felderítésben és célazonosításban, hanem az autonóm döntéshozatalban és a stratégiai tervezésben is. Az elemzett rendszerek jól példázzák, hogy a mesterséges intelligencia képes komplex katonai környezetekben valós idejű elemzést és prediktív modellezést végezni, amivel jelentős előnyhöz juttatja az azt alkalmazó hadseregeket. A szimulációk, a spektrumkezelés és a kiberhadviselési egységek területén tapasztalható fejlődés azt mutatja, hogy az MI már nem pusztán technológiai kiegészítő, hanem a katonai stratégia szerves része lett. Ugyanakkor a technológiai fejlődés komoly etikai és biztonsági kérdéseket is felvet. Az autonóm fegyverrendszerek alkalmazása, az emberi beavatkozás minimális szintje, valamint a jogi és nemzetközi szabályozás hiányosságai olyan kihívásokat jelentenek, amelyek sürgős figyelmet igényelnek. A CCW és a NATO irányelvek fontos lépéseket jelentenek e kihívások kezelésében, de a globális konszenzus még várat magára.

Összességében elmondható, hogy a mesterséges intelligencia integrációja a katonai rendszerekbe nemcsak új lehetőségeket teremt, hanem új felelősségeket is ró a fejlesztőkre, döntéshozókra és jogalkotókra. A jövő biztonságos és etikus hadviselése megköveteli az MI rendszerek tudatos, szabályozott és transzparens alkalmazását.

Források:

[1]Wikipediacontributors, *Project Maven*. https://en.wikipedia.org/wiki/Project_Maven

[2] Alex Hern, *Google working with Pentagon on AI project*, The Guardian, 2018. https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow

[3] D. L. Clark, *Military Simulation: Historical Overview and Future Directions*, Defense Technical Information Center (DTIC), 1980. https://apps.dtic.mil/sti/tr/pdf/ADA086565.pdf

[4] Airforce Technology, *Skyborg: The US Air Force's Future AI Fleet*. https://www.airforce-technology.com/features/skyborg-the-us-air-forces-future-ai-fleet/

[5] U.S. Air Force, *Project Skyborg*. https://www.airforce.com/experience-the-air-force/airmen-stories/inside-air-force-innovation/project-skyborg

[6] Boeing, *MQ-28 Ghost Bat*. https://www.boeing.com/defense/mq28

[7] Royal Australian Air Force (RAAF), *Loyal Wingman test flight*. https://www.raaf.gov.au/news-media/latest-news/loyal-wingman-test-flight

[8] The War Zone (TWZ), *MQ-28 Ghost Bat of Strong Interest to U.S. Navy*. https://www.twz.com/air/mq-28-ghost-bat-of-strong-interest-to-u-s-navy

[9] DARPA, *Squad X Program*. https://www.darpa.mil/program/squad-x

[10] DARPA, *Swarm Systems*. https://www.darpa.mil/program/swarm-systems

[11] BaykarTech, *Bayraktar TB2*. https://baykartech.com/en/

[12] Wikipedia contributors, *Bayraktar TB2*. https://hu.wikipedia.org/wiki/Bayraktar_TB2

[13] National Museum of the US Air Force, *Kratos XQ-58A Valkyrie*. https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/3209939/kratos-xq-58a-valkyrie/

[14] Wikipedia contributors, *Kratos XQ-58 Valkyrie*. https://en.wikipedia.org/wiki/Kratos_XQ-58_Valkyrie

[15] Air Force Research Laboratory (AFRL), *XQ-58A Valkyrie Overview*. https://afresearchlab.com/technology/xq-58a-valkyrie/

[16] Bots and Drones, *Kratos UTAP-22 Mako Overview*. https://botsanddrones.co/military%2C-tactical-drones/f/kratos-utap-22-mako

[17] Kratos Defense, *Company Website*. https://www.kratosdefense.com/

[18] Airforce Technology, *UTAP-22 Mako*. https://www.airforce-technology.com/projects/mako-unmanned-tactical-aerial-platform-22-utap22/?cf-view

[19] Védelmi Ipar Blog, *Az orosz Lancet drón*. https://vedelmiiparblog.hu/blog/az-orosz-lancet-dron/

[20] Wikipedia contributors, *ZALA Lancet*. https://en.wikipedia.org/wiki/ZALA_Lancet

[21] Palantir Technologies, *Defense Offerings*. https://www.palantir.com/offerings/defense/

[22] DeepStrike, *AI-Driven Military Analytics*. https://deepstrike.io/

[23] Wikipedia contributors, *Joint Enterprise Defense Infrastructure*. https://en.wikipedia.org/wiki/Joint_Enterprise_Defense_Infrastructure

[24] U.S. Department of Defense (DoD), *Official Homepage*. https://www.defense.gov/

[25] Wikipedia contributors, *Sentient (intelligence analysis system)*. https://en.wikipedia.org/wiki/Sentient_(intelligence_analysis_system)

[26] Congressional Research Service (CRS), *U.S. Military Use of Unmanned Systems*, 2003. https://irp.fas.org/crs/RL31425.pdf

[27] U.S. DoD, *Artificial Intelligence Spotlight*. https://www.defense.gov/Spotlights/Artificial-Intelligence/

[28] Lockheed Martin, *2022 Annual Report*. https://investors.lockheedmartin.com/static-files/5a6f08ab-266d-4000-b283-00e0a8e4e764

[29] R. P. Steinke, *Simulation in Military Training: Recent Developments*, ResearchGate. https://www.researchgate.net/publication/265568081_Simulation_in_Military_Training_Recent_Developments

[30] Rolands & Associates, *JTLS-GO Executive Overview*. https://www.rolands.com/jtls/j_vdds/executive_overview.pdf
[31] NATO STO, *Technical Reports Archive*. https://www.sto.nato.int/publications/STO%20Technical%20Reports/Forms/All%20Documents.aspx
[32] D. Smith et al., *Are VR and AR Really Viable in Military Education?*, ResearchGate. https://www.researchgate.net/publication/368943683_Are_VR_and_AR_Really_Viable_in_Military_Education_A_Position_Paper
[33] Institute for Defense Analyses (IDA), *Training Effectiveness Framework for AR/VR*, 2023. https://www.ida.org/-/media/feature/publications/t/tr/training-effectiveness-framework-for-augmented-and-virtual-reality/d-33349.ashx
[34] U.S. DoD, *2022 National Defense Strategy*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf
[35] DefenseScoop, *DARPA ACE Dogfighting Flight Tests with AI F-16*, 2024. https://defensescoop.com/2024/04/17/darpa-ace-ai-dogfighting-flight-tests-f16/
[36] Naval Technology, *Ghost Fleet Overlord – USV Project*. https://www.naval-technology.com/projects/ghost-fleet-overlord-unmanned-surface-vessels-usa/?cf-view
[37] Sea Technology Magazine, *U.S. Navy's Autonomous Operations*. https://sea-technology.com/us-navys-autonomous-operations

2.21. Bluetooth technológia fejlődése, architektúrája és gyakorlati alkalmazása az Ipar 4.0 környezetben

Bluetooth technológia fejlődése, architektúrája és gyakorlati alkalmazása az Ipar 4.0 környezetben

Szabo Gabor
MI, [redacted], songabor2003@gmail.com

1. Bevezetés

A modern technológiai környezet egyik meghatározó eleme a vezeték nélküli kommunikáció. Az ipari rendszerek, az okoseszközök és a személyes elektronikai berendezések egyaránt igénylik a gyors, stabil és megbízható adatkapcsolatokat. A Bluetooth technológia ezen elvárásoknak megfelelően fejlődött, mára már az ipari digitalizáció és az IoT (Internet of Things) egyik alappillérévé vált.

Ez az esszé célja, hogy részletes, technikai szempontból is megalapozott áttekintést adjon a Bluetooth technológia fejlődéséről, működéséről, architektúrájáról, valamint bemutassa a Bluetooth és a Bluetooth Low Energy (BLE) közötti különbségeket és ezek gyakorlati következményeit egy rendszertervezési szemléleten keresztül.

---

2. A Bluetooth technológia fejlődése

2.1 Történeti áttekintés

A Bluetooth technológiát eredetileg az Ericsson fejlesztette ki az 1990-es évek közepén. A cél egy rövid hatótávolságú vezeték nélküli kommunikációs szabvány létrehozása volt, amely kiválthatja a soros kábeleket. Az első hivatalos verzió (Bluetooth 1.0) 1999-ben jelent meg. Azóta számos verzió jelent meg, mindegyik újabb funkciókkal és fejlesztésekkel:

- Bluetooth 1.0–1.2: Alapfunkciók, 721 kbps sebesség
- Bluetooth 2.0 + EDR: Enhanced Data Rate (~3 Mbps)

- Bluetooth 3.0 + HS: High Speed (Wi-Fi-alapú gyors adatátvitel)
- Bluetooth 4.0: Bevezetésre került a BLE (Low Energy) profil
- Bluetooth 5.x: Megnövelt hatótávolság, sebesség, új protokollok, mesh hálózatok

---

3. Bluetooth architektúra

3.1 Fizikai réteg (Radio Layer)

A Bluetooth technológia a 2,4 GHz-es ISM (Industrial, Scientific and Medical) frekvenciasávot használja. A kommunikáció frekvenciaugrásos (FHSS) módszeren alapul, 79 csatorna között váltogat, 1 MHz-es csatornánkénti szélességgel.

3.2 Alap sáv (Baseband Layer)

Ez a réteg kezeli a csomagformálást, az eszközazonosítást és az időzítést.

3.3 L2CAP (Logical Link Control and Adaptation Protocol)

Az L2CAP felelős a logikai csatornák kezeléséért, multiplexálásért és az adatcsomagok szegmentálásáért. A profilok ezt a réteget használják az adatátvitelhez.

3.4 HCI (Host Controller Interface)

Az interfész a Bluetooth vezérlő és a hoszt rendszer (pl. operációs rendszer) közötti kommunikációra szolgál.

3.5 GAP és GATT

- GAP (Generic Access Profile): Meghatározza, hogyan fedezik fel egymást az eszközök, hogyan történik a párosítás.
- GATT (Generic Attribute Profile): Az adatok struktúráját és elérhetőségét szabályozza, különösen BLE esetén jelentős.

3.6 ATT (Attribute Protocol)

Az ATT az eszközben tárolt adatokhoz (attribútumokhoz) való hozzáférést kezeli. A GATT ezen protokollon keresztül valósítja meg a kliens-szerver kapcsolatokat.

---

4. Bluetooth vs. BLE – technikai összehasonlítás

A következő táblázat bemutatja a klasszikus Bluetooth és a BLE közötti főbb különbségeket:

Jellemző	**Bluetooth Classic**	**Bluetooth Low Energy (BLE)**
Átviteli sebesség	1–3 Mbps	125 kbps – 2 Mbps
Energiafogyasztás	Magasabb	Alacsony
Kapcsolat típusa	Folyamatos	Időszakos
Topológia	Piconet (master-slave)	Broadcast, point-to-point, mesh
Célalkalmazás	Audio, fájlátvitel	Szenzorok, IoT
Párosítási idő	Lassabb	Gyorsabb

A BLE alkalmazások alacsony energiafogyasztásra optimalizáltak, így kiválóan alkalmasak viselhető eszközök, környezeti szenzorok vagy ipari monitorozó rendszerek céljára.

---

5. Bluetooth-alapú rendszertervezés

5.1 Követelmények definiálása

A Bluetooth-alapú rendszerek tervezésének első lépése a célalkalmazás és a követelmények egyértelmű meghatározása. Ide tartoznak:

- Az átvitelre szánt adatok típusa és mennyisége
- Kapcsolódási idő és adatátviteli gyakoriság
- Energiafogyasztási elvárások
- A rendszerben részt vevő eszközök száma
- A környezet (zajszint, távolság, akadályok)

5.2 Hardverkomponensek kiválasztása

A hardverarchitektúra kialakításakor tipikus komponensek a következők:

- Bluetooth modul vagy SoC (pl. Nordic nRF52840)
- Mikrokontroller (MCU), amely a vezérlést végzi
- Szenzorok, beavatkozók
- Energiaforrás (akkumulátor, energia betakarítás)

5.3 Szoftverarchitektúra

A firmware általában real-time operációs rendszeren (RTOS) fut, amely biztosítja a multitasking és időzítés kezelését. A szoftver által használt Bluetooth stack magába foglalja a GAP, GATT, L2CAP és HCI rétegeket.

5.4 Kommunikációs minta

A BLE tipikusan kliens-szerver architektúrát használ, ahol a periféria (pl. szenzor) GATT-szerverként, a központi egység pedig GATT-kliensként működik.

5.5 Tesztelés és hitelesítés

Fontos lépés az interoperabilitási tesztelés különböző Bluetooth eszközökkel, illetve a megfelelő szabványoknak való megfelelés ellenőrzése (pl. Bluetooth SIG tanúsítás).

6. Kommunikációs modellek és protokollok

A Bluetooth kommunikáció rétegekre épülő modellt használ. A BLE esetén a leggyakrabban alkalmazott modell a GATT-alapú kliens-szerver architektúra.

6.1 GATT profil

6.2 Eszközszerepek: Central és Peripheral

6.3 Hirdetési csatornák és kapcsolódási események

6.4 Csomagformátum és adatstruktúra

---

7. Biztonsági mechanizmusok

A Bluetooth és BLE protokollok beépített biztonsági megoldásokkal rendelkeznek.

7.1 Párosítási módok: Just Works, Passkey Entry, Numeric Comparison

7.2 Hitelesítés és titkosítás

7.3 Man-in-the-middle (MITM) támadások elleni védekezés

7.4 Bluetooth 5.2 újdonságai: LE Secure Connections, Privacy Features

---

8. BLE Mesh architektúra

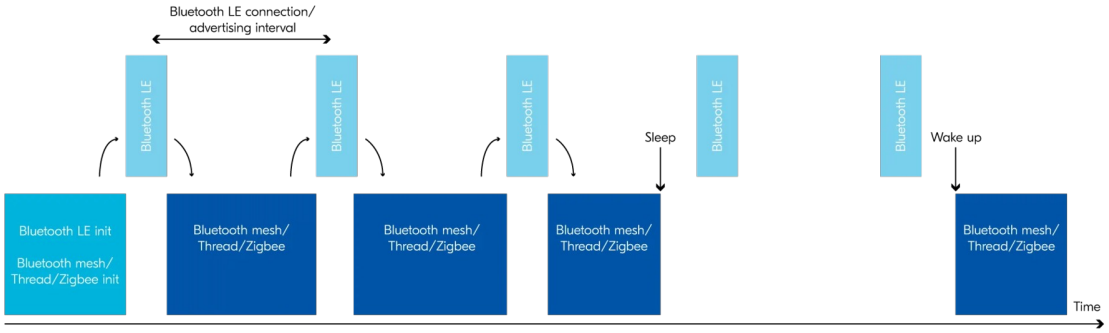
A BLE Mesh lehetővé teszi nagy kiterjedésű hálózatok létrehozását.

8.1 Mesh topológia: relay, proxy, friend, low power node

8.2 Addressing és üzenettovábbítás

8.3 Konfigurációs protokollok és menedzsment

8.4 Előnyök és korlátok



[1]

---

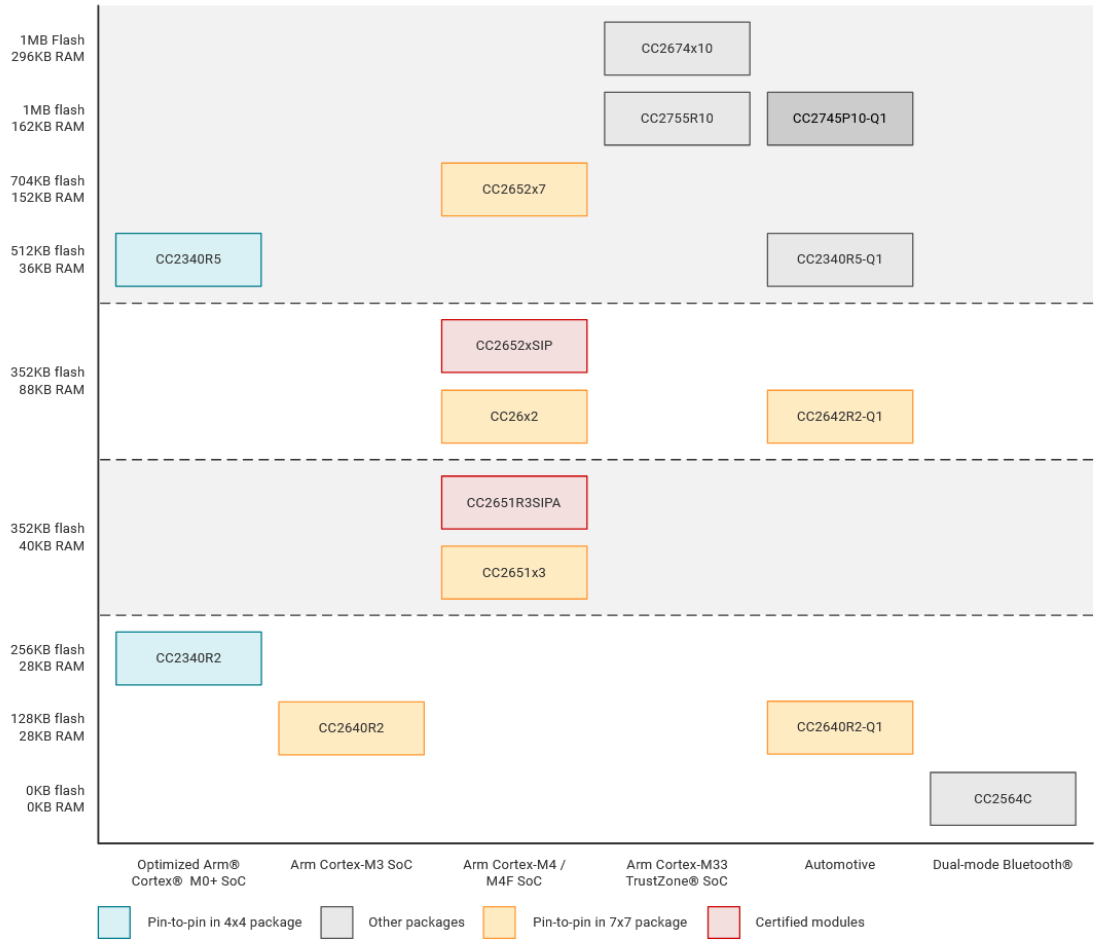
9. Ipari alkalmazások

9.1 Szenzorhálózatok ipari automatizálásban

9.2 Prediktív karbantartás BLE-alapú eszközökkel

9.3 Okos világítás és épületmenedzsment rendszerek

9.4 Eszközkövetés és asset management



[2]

---

10. Jövőbeni fejlődési irányok

10.1 Bluetooth 5.3 és 5.4 új képességei

10.2 Integráció Wi-Fi 6 és 6E rendszerekkel

10.3 Edge computing és BLE konvergenciája

10.4 Fejlesztési trendek: interoperabilitás, energiahatékonyság

---

11. Összegzés

A Bluetooth technológia, különösen a BLE, kulcsfontosságú szereplő a modern vezeték nélküli kommunikációs megoldások között. Architektúrája, fejlett protokolljai és energiatakarékos működése révén ideális az Ipar 4.0 kihívásaira. A BLE Mesh hálózatok további lehetőségeket biztosítanak az ipari skálázhatóság és rugalmasság érdekében. A jövőbeni fejlesztések a hatékonyság növelésére és az eszközök közötti még szorosabb integrációra fókuszálnak.

---

12. Irodalomjegyzék

[1] Nordic Semiconductor, "Bluetooth Mesh Networking Basics", https://www.nordicsemi.com

[2] Texas Instruments, "Low Power Bluetooth for Industrial Applications", https://www.ti.com

[3] M. Toor, A. Pasha, "An Overview of Bluetooth Low Energy: Architecture, Protocols and Applications", IEEE Access, 2020.

[4] G. Smith et al., "Security Challenges in Bluetooth Communication", Journal of Wireless Security, 2021.

[5] Bluetooth Technology Website, https://www.bluetooth.com

2.22. IIoT avagy Industrial Internet of Things Kovács Ármin Krisztián

IPAR 4.0 TECHNOLÓGIÁK

IIoT avagy Industrial Internet of Things

Kovács Ármin Krisztián
[redacted]

Mérnökinformatikus BSC nappali.

Abstract

The Industrial Internet of Things (IIoT) is a fascinating field that raises many questions and opens up new opportunities in industrial settings. To begin with, it's essential to clearly define IIoT, understand its goals, and examine its historical development. At its core, IIoT enables industrial devices and systems to collect, exchange, and analyze data over the internet, facilitating automation, improving efficiency, and optimizing manufacturing processes.

The Industrial Internet of Things (IIoT) holds significant value across multiple sectors by enabling smarter operations through connected technologies. In manufacturing and logistics, IIoT systems track equipment performance and workflow processes in real time, minimizing disruptions. The energy sector benefits from optimized renewable energy management, where IIoT helps balance supply and demand more effectively. In agriculture, technologies like drone-based monitoring and predictive analytics enhance crop management by providing actionable insights.

Smart Sensors: The Backbone of IIoT
A critical element of IIoT is the use of smart sensors, which go beyond traditional sensors by not only collecting data but also transmitting it for analysis. Comparing smart sensors with conventional ones reveals key differences—while traditional sensors provide basic measurements, smart sensors enable real-time data processing and remote monitoring.

Pros and Cons of IIoT Implementation
The adoption of IIoT offers several advantages, including: Enhanced operational efficiency through automation, predictive maintenance to reduce equipment failures, data-driven decision-making for faster responses
However, challenges such as cybersecurity risks and data privacy concerns must be addressed to ensure secure deployment.

Final Thoughts on IIoT's Future
From a personal standpoint, IIoT presents a transformative opportunity for industries, boosting productivity and sustainability. Yet, its success depends on overcoming security and integration hurdles. Proper research and citation of credible sources are essential to validate these perspectives. As IIoT continues to evolve, it has the potential to redefine industrial efficiency, making processes smarter and more sustainable in the long run.

Tartalomjegyzék

Tartalom

Abstract 2
Tartalomjegyzék 3
Bevezetés az IIoT-ba 4
Az IIoT forradalma 4
Kronológiai mérföldkövek 5
Alkalmazási területek 5
Gyártás 5
Logisztika 6
Eszköz- és folyamatmonitorozás 7
Energiahasználat optimalizáció 8
IIoT az energiaszektorokban 10
Mezőgazdasági szerepe 11
Szenzorok 12
Smart szenzorok 12
Smart szenzorok előnyei - hátrányai 13
IIoT adatgyűjtés 15
Hagyományos szenzorok 15
Smart szenzorok a hagyományosak ellen 16
Automa zálás 18
IIoT előnyei 19
Predik v karbantartás 19
IIoT veszélyei 20
Biztonsági kockázatok 20
Adatvédelmi kockázatok 21
Kompa bilitási problémák 22
Üzleti kockázatok 23
Vélemény 24
Vélemény 24
Források 24
Irodalomjegyzék 24

Bevezetés az IIoT-ba

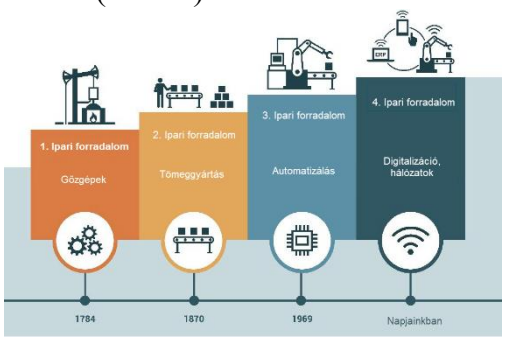
Az IIoT forradalma

Az Ipari Internet (IIoT) forradalmi változást hozott az ipari világba, és már ma is alapvetően átalakítja a gyártási folyamatokat. De vajon pontosan mit jelent ez a fogalom, és milyen történelmi fejlődés vezetett el ehhez az innovatív technológiai ugráshoz, amely számos újdonságot hozott az ipari szektorba?

Az IIoT, vagyis az "Industrial Internet of Things" (ipari dolgok internete), olyan technológiák összességét jelenti, amelyek lehetővé teszik az ipari gépek, berendezések és rendszerek hálózatba kapcsolását az interneten keresztül. Ennek köszönhetően valós időben gyűjthetők és elemezhetők az adatok, valamint lehetőség nyílik a távoli megfigyelésre és irányításra is.

Az IIoT történelmi fejlődése szorosan összefonódik az informatika és az ipari automatizálás előrehaladásával. Az első lépések már az 1970-es és 1980-as években megtörténtek, amikor a gyártósorokat digitális vezérlőrendszerekkel kezdték integrálni. Az 1990-es években bekövetkezett internetes robbanás tovább gyorsította ezt a folyamatot. A 2000-es évekre pedig a szenzorok és a vezeték nélküli kommunikációs technológiák fejlődése lehetővé tette az ipari berendezések intelligens, hálózatba kapcsolt működését. (1. ábra)

Az IIoT lehetőséget ad olyan mértékű optimalizálásra és hatékonyságnövelésre, amely korábban nem volt lehetséges. A valós idejű adatgyűjtés és -elemzés révén már a meghibásodás előtt felismerhetők a problémák, így megelőzhetőek a leállások, ami jelentősen növeli a termelés megbízhatóságát és hatékonyságát.[1]



1. ábra: A 4 ipari forradalom
https://blog.eplm.hu/4-ipari-forradalom/

Nem csupán a karbantartás terén hoz előrelépést. A gyártási folyamatok hatékonyabbá tételével csökkenthetők az üzemeltetési költségek, növelhető a gyártás sebessége, javítható a termékek minősége, és lehetővé válik a gyorsabb reagálás a vásárlói igényekre is.

Az IIoT forradalma nem pusztán egy új technológia bevezetését jelenti, hanem egy teljesen új gyártási szemlélet kialakulását is. Ez a megközelítés alapjaiban változtatja meg a termékek előállításának és szállításának módját. A közeljövőben további jelentős innovációk várhatók ezen a területen, melyek célja a gyártási folyamatok még intelligensebbé és hatékonyabbá tétele.

Kronológiai mérföldkövek

Az ipari forradalom kezdetén valószínűleg kevesen hitték volna, hogy egyszer eljön az idő, amikor a gépek és berendezések képesek lesznek intelligensen kommunikálni egymással. Napjaink technológiai fejlődése azonban elvezetett minket egy új korszak határához: az Ipari Internet of Things (IIoT) világába. De mit is takar ez a fogalom valójában?

Az IIoT, vagyis az ipari dolgok internete, az ipari környezetben működő intelligens eszközök és rendszerek hálózatba kapcsolását jelenti. A technológia célja, hogy a gépek, szenzorok és emberi tevékenységek összekapcsolásával növelje a termelékenységet, csökkentse az üzemeltetési költségeket, és fokozza az ipari folyamatok átláthatóságát.

Az IIoT fejlődéstörténete számos jelentős állomással büszkélkedhet. Már a kezdetekkor, amikor az első ipari gépek megjelentek a gyártósorokon, megindult egy hosszú fejlődési folyamat. A hetvenes években a programozható logikai vezérlők (PLC-k) megjelenése forradalmasította az ipari automatizálást. A kilencvenes évek internetes fellendülése, valamint a vezeték nélküli kommunikációs technológiák fejlődése tovább gyorsította ezt az átalakulást, és lehetővé tette az ipari eszközök közötti adatkapcsolatok szinte korlátlan bővítését.[2]

A 2000-es évek elején megjelentek az első intelligens eszközök, amelyek már képesek voltak önálló döntéshozatalra és egymás közötti kommunikációra. Az elmúlt tíz év során pedig a mesterséges intelligencia és a gépi tanulás integrációjával az IIoT számos iparágban vált nélkülözhetetlen technológiai tényezővé.

Ez a rész csak egy rövid betekintést nyújtott az IIoT világába, azonban érdemes alaposabban is elmélyülni benne, hogy feltérképezhessük a benne rejlő lehetőségeket. Az ipar jövője már nem csupán vízió, hanem kézzelfogható valóság - ebben pedig az IIoT kulcsszerepet játszik, és a jövőben még inkább meghatározó lesz.

Alkalmazási területek

Gyártás

A Gyártás 4.0 korszakában a gyártási folyamatok alapjaiban alakulnak át, és az innováció előtt teljesen új távlatok nyílnak meg. Az IIoT technológia térnyerésének köszönhetően az üzemek egyre intelligensebbé, hatékonyabbá és szorosabban összekapcsolttá válnak, lehetővé téve számukra, hogy sikeresen alkalmazkodjanak a 21. század piaci elvárásaihoz. [3]

Ahogy az IIoT egyre szélesebb körben terjed a gyártástól egészen a mezőgazdaságig, elengedhetetlen, hogy egyaránt figyelembe vegyük annak előnyeit és a vele járó kihívásokat. Az innováció folyamatosan formálja az ipar jövőjét, lehetőséget teremtve arra, hogy újragondoljuk nemcsak a gyártást, hanem más ágazatokat is - mindezt úgy, hogy közben tudatosan és előrelátóan kezeljük a felmerülő kockázatokat.

Pro és kontra - múlt és jelen: Míg a hagyományos gyártási módszerek gyakran zárt, elszigetelt rendszerekre épültek, ahol az információáramlás lassúsága hátráltatta a gyors döntéshozatalt, addig az IIoT rendszerek új szintre emelik a gyártást. Ezek a technológiák valós idejű adatgyűjtést és -elemzést tesznek lehetővé, ami kulcsfontosságú a folyamatok optimalizálásához és a hibák minimalizálásához. Az IIoT integrációjával megszűnnek az információs akadályok, az adatok gyorsan és zökkenőmentesen áramlanak, ezáltal növelve a termelékenységet és erősítve a versenyképességet.

A Gyártás 4.0 szemléletében az IIoT alkalmazási lehetőségei rendkívül sokrétűek. Az egyik kiemelkedő példa a prediktív karbantartás, amely a gépek állapotának folyamatos nyomon követésével képes előre jelezni a lehetséges meghibásodásokat, így csökkentve a nem tervezett leállások kockázatát. A logisztikában is jelentős átalakulás tapasztalható, például az intelligens raktárkezelési rendszerek és az automatizált anyagmozgatás révén. Ezekben a folyamatokban robotok (2. ábra) és önvezető járművek veszik át az ismétlődő, monoton feladatokat, tehermentesítve az emberi munkaerőt.

2. ábra, modern gyártósor
https://www.cnc.hu/storage/2021/04/2021_04_08_KUKA_10.jpg

Emellett szükség van a munkaerő átképzésére is, hogy képesek legyenek kezelni és fenntartani ezeket az új technológiákat.

Logisztika

Az ipari dolgok internete (IIoT), amely a gépek és eszközök internetes összekapcsolását jelenti, új távlatokat nyitott meg a logisztika területén. A Pro-Kontra elemzés bemutatja, miként formálta át az IIoT a logisztikai folyamatokat a múltban, és hogyan működnek ezek napjainkban az új technológiai megoldások hatására.

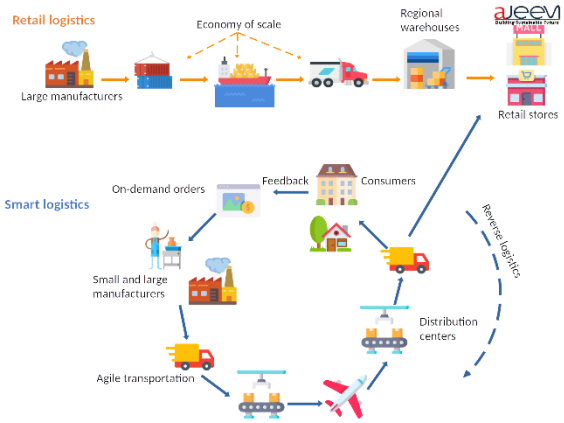
A hagyományos logisztikai rendszerek jelentős mértékben építettek az emberi döntéshozatalra és kézi beavatkozásra, ami gyakran késéseket és pontatlanságokat eredményezett a folyamatok

során. Az információkhoz való hozzáférés korlátozott volta pedig gátolta az adatalapú döntések meghozatalát, csökkentve ezzel a rendszer hatékonyságát.

Az IIoT megjelenése alapvető változást hozott a logisztikában. A folyamatos adatgyűjtés és -elemzés révén lehetővé válik a folyamatok precíz optimalizálása. Az ilyen intelligens rendszerek valós időben képesek alkalmazkodni a körülményekhez - például automatikusan módosíthatják a szállítmány útvonalát -, ezáltal csökkentve a késéseket és növelve az ügyfélkiszolgálás hatékonyságát.

Az IIoT egyik legnagyobb előnye a logisztikai folyamatok átláthatóságának drámai javulása. Az adatalapú betekintés lehetővé teszi a vállalatok számára, hogy pontosabban előre jelezzék és hatékonyabban kezeljék készleteiket, ezáltal minimalizálva mind a túlkészletezés, mind a hiány kialakulásának kockázatát.

Összegzésként elmondható, hogy az IIoT logisztikai alkalmazása (3. ábra) lehetővé teszi a vállalatok számára, hogy rugalmasabban reagáljanak az ellátási lánc változásaira, javítsák az ügyfélkiszolgálás színvonalát, és mérsékeljék működési költségeiket. A technológia további fejlődésével, valamint az előnyök és kihívások mélyebb megértésével az IIoT várhatóan még jelentősebb szerepet kap a jövő logisztikai rendszereiben.



3. ábra, "Okos logisztika" folyamatábra
https://ajeevi.com/industries/smart-logistics/

Eszköz- és folyamatmonitorozás

A termelés hatékonyságának növelése és a folyamatok optimalizálása régóta központi szerepet játszik az ipari fejlődésben. Az ipari forradalmaktól a digitális korszakig a fejlődés üteme és mélysége drámaian felgyorsult. „Okoseszközök a termelés szolgálatában: IIoT az eszköz- és folyamatmonitorozásban” című cikkünkben az Ipari Internet of Things (IIoT) innovációit és azok gyakorlati alkalmazását mutatjuk be, a gyártási szektortól egészen a mezőgazdaságig.

A múltban a termelési folyamatokat kizárólag emberi munkaerő irányította, ahol a hibák és a hatékonysághiány gyakori és sokszor elkerülhetetlen velejárói voltak a rendszernek. A manuális beavatkozások és a technológiai háttér hiánya jelentősen korlátozta a folyamatok megbízhatóságát. Ezzel szemben az IIoT megjelenése alapjaiban változtatta meg a monitorozás lehetőségeit: az okoseszközök által biztosított folyamatos adatgyűjtés és elemzés nemcsak a

hibák előfordulását csökkenti, hanem hozzájárul a termelés hatékonyabb és pontosabb működéséhez is.

Az IIoT egyik legnagyobb előnye a gépek és folyamatok valós idejű nyomon követhetősége (4. ábra). A szenzorokkal felszerelt berendezések folyamatosan adatokat szolgáltatnak, amelyek elemzésével időben azonosíthatók a lehetséges problémák, még mielőtt tényleges meghibásodás történne. Ennek a prediktív - azaz előrejelző - karbantartásnak köszönhetően jelentősen csökkenthetőek az üzemszünetek, miközben növelhető a termelés megbízhatósága és hatékonysága.

4. ábra, gyártás nyomonkövetése
https://simplexion.hu/szolgaltatasaink/gyartosori-nyomon-kovetes/

Az IIoT nemcsak az ipari termelés területén, hanem a mezőgazdaságban is komoly előrelépéseket tett lehetővé. Az intelligens mezőgazdasági eszközök révén pontosan mérhető például a talaj nedvességtartalma és tápanyagszintje, miközben az állományok állapota távolról is folyamatosan nyomon követhető. Ez az adatvezérelt megközelítés alapot ad a precíziós gazdálkodáshoz, amely hatékonyabb betakarítást és növénytermesztést tesz lehetővé.

Összefoglalva, az „Okoseszközök a termelés szolgálatában" már nem csupán a jövő ígérete, hanem a jelen valósága. Az IIoT által biztosított adatgyűjtés és -elemzés révén a gyártási folyamatok hatékonyabbá válhatnak, a működési költségek csökkenthetők, miközben az üzemek versenyképessége és fenntarthatósága is jelentősen javul. Az ilyen innovatív technológiák bevezetése kulcsfontosságú az ipari fejlődés szempontjából - még akkor is, ha mindez újfajta kihívásokat is magával hoz.

Energiahasználat optimalizáció

Az Ipar 4.0 korszakát kísérő innovációk sorában az IIoT - azaz az ipari dolgok internete - különösen meghatározó szerepet tölt be. Ez a modern technológiai megközelítés alapjaiban alakítja át az energetikai szektort is, különös tekintettel a megújuló energiaforrások hatékony integrálására és optimalizálására (5. ábra), ami elengedhetetlen a fenntartható jövő megvalósításához.

Korábban az energetikai ágazat nagymértékben a fosszilis tüzelőanyagokra épült, amelyek nemcsak véges erőforrások, hanem jelentős környezeti terhelést is okoztak. Bár a megújuló energiaforrások - mint a nap-, szél- és vízenergia - már akkor is elérhetők voltak, hatékonyságuk sokáig korlátozott maradt, elsősorban a fejlett adatkezelési és elemzési rendszerek hiánya miatt.

5. ábra, IIoT energia optimalizacio
https://www.inf.u-szeged.hu/~vinced/files/MSc.pdf

Az IIoT megoldások új lehetőségeket nyitnak meg az energetikai rendszerek számára. Pro-kontra megközelítésben vizsgálva, az egyik legnagyobb előnyt a valós idejű adatgyűjtés és -feldolgozás jelenti, amely támogatja az energiafelhasználás optimalizálását, valamint lehetővé teszi a karbantartási igények előrejelzését. Emellett az integrált rendszerek elősegítik a különböző energiaforrások közötti zökkenőmentes átállást, ezáltal növelve az energiaellátó hálózatok rugalmasságát és megbízhatóságát.

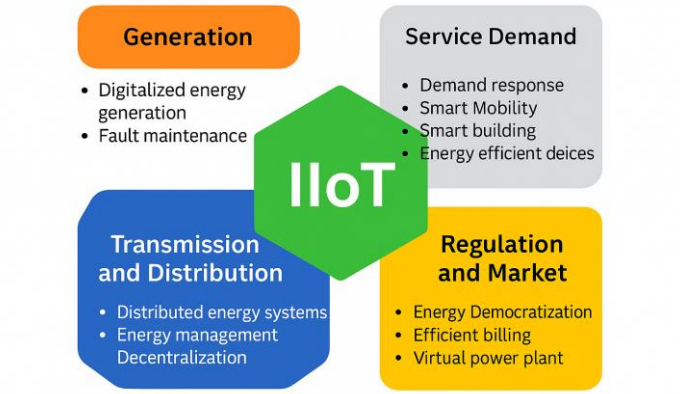
Ugyanakkor fontos, hogy a felmerülő kihívásokat se hagyjuk figyelmen kívül. A rendszerbiztonság és az adatvédelem továbbra is kiemelt prioritást élvez, mivel az ipari vezérlőrendszerek és a hálózati infrastruktúra sebezhetősége komoly kockázatot jelenthet. Emellett az IIoT rendszerek bevezetése gyakran jelentős kezdeti beruházással jár, ami akadályt jelenthet a technológia széles körű és gyors elterjedése előtt.

Az IIoT alkalmazási területeinek sokszínűsége - a mezőgazdaságtól a gyártáson át egészen az energetikai szektorig - jól mutatja, hogy ez a technológia nem csupán múló trend, hanem egy valóban hatékony eszköz a gazdaság szinte minden területén. Különösen az energetika új dimenzióiban van kiemelt szerepe: segítségével hatékonyabban aknázhatjuk ki a megújuló energiaforrásokban rejlő lehetőségeket, miközben aktívan csökkenthetjük környezeti terhelésünket.

A jövő energiaellátása nemcsak környezetbarátabb, hanem intelligensebb is lesz. Az IIoT technológia alkalmazása lehetővé teszi olyan rendszerek kialakítását, amelyek képesek dinamikusan összehangolni az energiatermelést a fogyasztással, csökkenteni az energia-veszteségeket, valamint előre jelezni a karbantartási igényeket. Az energetikai szektor ezen új szintre emelése nemcsak a fenntarthatóságot támogatja, hanem jelentős mértékben hozzájárul a gazdasági hatékonyság növeléséhez is. [4]

IIoT az energiaszektorokban

Az IIoT, vagyis az ipari dolgok internete - egyre meghatározóbb szerepet játszik az energiaszektorban. A megújuló energiaforrások térnyerésével és az energetikai rendszerek folyamatos fejlődésével az IIoT technológiái és megoldásai egyre nagyobb hatást gyakorolnak - nemcsak az energiatermelésre, hanem a gyártás, a mezőgazdaság és más iparágak működésére is.



6. ábra, IIoT hatása az energiarendszerekre, saját szerkesztésű kép

A megújuló energiaforrások - mint a nap-, szél- és vízenergia - a fenntartható energetika jövőjét alapozzák meg. Az IIoT megoldások révén ezek a rendszerek nemcsak hatékonyabban, hanem intelligensebben is működhetnek. A szenzorok és a valós idejű adatgyűjtés segítségével pontos információk állnak rendelkezésre a termelés optimalizálásához, valamint a lehetséges hibák előrejelzéséhez, így növelve a rendszer megbízhatóságát és teljesítményét.
(6. ábra)[4]

Pro és kontra szemszögből nézve az IIoT korábban még nem rendelkezett akkora potenciállal, mint napjainkban. Az innovációk felgyorsulása, valamint az adatkezelési technológiák fejlődése lehetővé tette, hogy a megújuló energiaforrásokat jóval hatékonyabban és zökkenőmentesebben integráljuk az energiaellátási láncba.

Ugyanakkor fontos szem előtt tartani az IIoT technológia bevezetésével járó kihívásokat is. A rendszerbiztonság, az adatvédelem és a különböző rendszerek zökkenőmentes összehangolása továbbra is fejlesztésre szoruló területek. Emellett a magas kezdeti beruházási költségek, valamint a megfelelő szaktudással rendelkező munkaerő hiánya szintén gátolhatja az IIoT megoldások széles körű elterjedését.

Összegzésként elmondható, hogy az IIoT alkalmazása az energiaszektorban jelentős mértékben hozzájárul a működési hatékonyság növeléséhez és a karbantartási költségek mérsékléséhez. Az intelligens hálózati összeköttetések lehetővé teszik a megújuló energiaforrásokból származó energia folyamatos, megbízható és stabil hasznosítását, ezáltal támogatva a fenntartható és rugalmas energiaellátási rendszerek kialakítását.

A technológiai fejlődés előrehaladtával az IIoT várhatóan továbbra is meghatározó szerepet tölt majd be az energiaszektorban. A pro és kontra érvek mérlegelése mellett elengedhetetlen, hogy a jövőbeli alkalmazások a fenntarthatóságot és az emberi tényezőket is figyelembe vegyék - csak így aknázhatjuk ki teljes mértékben az IIoT-ben rejlő lehetőségeket.

Mezőgazdasági szerepe

Az Ipar 4.0 vívmányai nem csupán a gyártócsarnokokban idéznek elő alapvető változásokat, hanem a mezőgazdaságban is egy új korszak kezdetét jelentik. Az Ipari Internet of Things (IIoT) technológiák alkalmazásával a mezőgazdasági termelés hatékonysága látványosan növelhető, miközben lehetőség nyílik a termőterületek pontosabb megfigyelésére és az erőforrások célzottabb, fenntarthatóbb felhasználására.
(7.ábra)

7. ábra, IT jelentősége a mezőgazdaságban https://agraragazat.hu/hir/agrar-dron-innovacio-precizios-mezogazdasag/

A hagyományos mezőgazdasági modellben a munkafolyamatok elsősorban a természet ritmusához és az emberi munkaerőhöz igazodtak. Napjainkra azonban ezt az évszázados megközelítést egyre inkább kiegészítik a korszerű technológiai megoldások. Ha Pro-Kontra szemszögből vizsgáljuk a múlt és a jelen közötti különbségeket, az IIoT alkalmazásának előnyei egyértelműen kirajzolódnak. A nagymennyiségű adatok elemzése lehetővé teszi a talaj- és növényállapot pontosabb nyomon követését, ami jelentősen javítja a termelékenységet és minimalizálja a felesleges erőforrás-felhasználást.

Másfelől a drónok már nem csupán a jövő ígéretét jelentik a mezőgazdaságban, hanem a mindennapi gyakorlat részévé váltak. Ezek a repülő eszközök hatékonyan képesek feltérképezni a termőterületek állapotát, így segítve a gazdálkodókat abban, hogy időben azonosítsák a kártevők megjelenését vagy az öntözés szükségességét. A drónfelvételek alapján részletes térképek is készíthetők, amelyek még precízebb és hatékonyabb gazdálkodást tesznek lehetővé.

A technológiai innováció révén mára lehetővé vált, hogy a mezőgazdasági gépek egymással kommunikáljanak és összehangoltan működjenek, ezáltal minimalizálva az emberi hibákból eredő kockázatokat. Az automatizált traktorok, vetőgépek és aratócséplők - amelyek távolról vezérelhetők vagy akár teljesen önállóan is képesek navigálni - mérföldkövet jelentenek a mezőgazdaság hatékonyságának és precizitásának növelésében.

Emellett az IIoT rendszerek hozzájárulnak az energiahatékony működéshez is, amely egyszerre jelentős gazdasági előnyt és környezeti hasznot. Ezek a technológiai újítások lehetővé teszik,

hogy a mezőgazdaság egyre jobban alkalmazkodjon a gyorsan változó piaci követelményekhez és a globális kihívásokhoz.

Összegzésként elmondható, hogy az IIoT rendszerek alkalmazása a mezőgazdaságban óriási lehetőségeket kínál. Nemcsak a termelékenység jelentős javítását teszik lehetővé, hanem hozzájárulnak a fenntarthatóság és az erőforrás-hatékonyság megvalósításához is. Ezért az innovációk gyors bevezetése kulcsfontosságú lesz a mezőgazdasági ágazat jövőbeli fejlődése és sikeressége szempontjából.

Szenzorok

Smart szenzorok

A digitális átalakulás, amely jelenleg az ipari szektort formálja, korunk egyik legizgalmasabb fejleménye, középpontjában pedig az IIoT, azaz az Ipari Internet of Things áll. Az IIoT intelligens eszközök hálózatát jelenti, amelyek képesek önállóan adatokat gyűjteni, feldolgozni és egymással kommunikálni, emberi beavatkozás nélkül. E forradalmi változás hajtóerejét elsősorban az okos szenzorok jelentik (8. ábra)

8. ábra, Okos szenzorok és fajtáik https://epiteniakarok.blog.hu/2017/03/07/mitol_okos_az_okosotthon

A smart szenzorok a hagyományos szenzorok továbbfejlesztett változatai. Míg a klasszikus szenzorok egyszerű méréseket végeznek — például hőmérsékletet vagy nyomást mérnek —, addig a smart szenzorok nemcsak adatokat gyűjtenek, hanem azokat elő is feldolgozzák, elemzéseket készítenek, és adott esetben döntéseket is hoznak. Ezáltal jelentős előnyt jelentenek az adatgyűjtés és -továbbítás folyamatában, hiszen nem csupán információt szolgáltatnak, hanem megkönnyítik az adatok hatékony kezelését is.

Az egyik legfontosabb előnyük az azonnali adatfeldolgozás képessége, amely jelentősen csökkenti a központi rendszerek terhelését. Emellett a smart szenzorok energiatakarékosak, és karbantartási igényüket is minimalizálják, mivel képesek önállóan jelezni saját állapotukat és a karbantartás szükségességét. A hálózatba kapcsolt eszközök így proaktívan kezelhetők, ami minimalizálja a nem tervezett leállásokat, növeli az üzem hatékonyságát, és végső soron maximalizálja a termelés profitját.

Ugyanakkor fontos számba venni a lehetséges hátrányokat is. A smart szenzorok összetettebb technológiájuk miatt általában magasabb költségekkel járnak, mint hagyományos megfelelőik.

Emellett a biztonsági kockázatok is fokozódnak, hiszen az intelligens eszközök sebezhetőbbé válhatnak külső támadásokkal szemben.

Összességében a smart szenzorok jelentős előrelépést hoznak az ipari adatgyűjtés területén, lehetővé téve a gyorsabb, hatékonyabb és megbízhatóbb működést. Bár figyelembe kell venni a magasabb költségeket és a biztonsági kihívásokat, ezek az eszközök egyértelműen előremozdítják az ipari automatizálás fejlődését. Az IIoT forradalma így nem csupán technológiai áttörést jelent, hanem az ipar számára egy új korszak kezdetét is.

Smart szenzorok előnyei - hátrányai

A mai, gyorsan változó ipari környezetben a „Korszerűsítés vagy kockázat?” kérdés szinte minden területen felmerül. Az ipari smart szenzorok előnyei és hátrányai jól tükrözik ezt az aktuális dilemmát. Ha összehasonlítjuk a smart és a hagyományos szenzorok hatását az ipari környezetre, világos ellentét bontakozik ki az előnyök és hátrányok között.

Az IIoT, vagyis az Ipari Dolgok Internete, alapvető átalakulást eredményezett a gyártás és az adatkezelés területén. Az IIoT kulcsfontosságú elemei, a smart szenzorok, lehetővé teszik, hogy a gépek, berendezések és rendszerek intelligensen kommunikáljanak egymással, ezáltal jelentősen növelve az üzemek hatékonyságát és pénzügyi teljesítményét. Ezek a szenzorok valós időben gyűjtik és elemzik az adatokat, így azonnali visszajelzést adnak a folyamatokról, lehetővé téve a gyors reagálást a felmerülő problémákra.

Az előnyök mellett azonban nem szabad figyelmen kívül hagynunk bizonyos kihívásokat sem. A smart szenzorok magasabb beszerzési költségei és az adatbiztonsági kérdések jelentős akadályokat jelenthetnek a technológia széles körű elterjedésében. Emellett a rendszerek komplexitása miatt az üzemeltetők részéről magasabb szintű szakértelem szükséges, ami további képzéseket és beruházásokat igényelhet.

Sensor Type	Advantages	Disadvantages
Ultrasonic radars and short-range radars	• Low cost • Long life • Small size	• Low accuracy • Short range • Cannot be used in vertical parking mode
Laser scanners	• High stability • High precision	• High cost • Short life • Easy to be affected by rain and snow
Vision sensors	• Low cost • Long life • High accuracy • Rich image information	• Weak robustness

Összefoglalva, amikor az iparágak a smart szenzorok bevezetése mellett vagy ellen döntenek, elengedhetetlen, hogy alaposan mérlegeljék az előnyöket és a hátrányokat egyaránt. A döntés meghozatala során figyelembe kell venni az adott alkalmazás igényeit, a rendelkezésre álló költségvetést, valamint a vállalat hosszú távú stratégiáját. A smart szenzorok alkalmazása kulcsfontosságú lehet a versenyképesség megőrzésében, feltéve, hogy a felmerülő kihívásokat hatékonyan kezelik, és az előnyöket teljes mértékben kiaknázza a vállalat.

IIoT adatgyűjtés

A smart szenzorok az ipari hálózatba kötött gyártás legmodernebb technológiáit képviselik. Ezek az eszközök nemcsak adatgyűjtésre alkalmasak, hanem képesek az adatok előfeldolgozására, elemzésére és továbbítására is. Az IIoT egyik legnagyobb előnye éppen ezekben a smart szenzorokban rejlik, hiszen általuk folyamatosan és valós időben követhető a gyártási folyamat, így szükség esetén azonnal be lehet avatkozni.

Ezzel szemben a hagyományos szenzorok jóval korlátozottabb funkciókkal rendelkeznek. Csak egyszerű adatgyűjtésre alkalmasak, melyeket később, külön feldolgozás céljából továbbítanak. Ez a különálló adatfeldolgozási lépés gyakran lassabb és kevésbé hatékony, ami csökkenti a gyártási folyamat rugalmasságát és a gyors reagálás lehetőségét.

9. ábra, IIot Data collection https://konferencia2015.infoter.eu/_eloadasok/2/12-30-dr-kovacshazy-tamas.pdf

A smart szenzorok legfőbb előnye az adatgyűjtésben (9. ábra) és adattovábbításban rejlik. Képesek komplex adatelemzések elvégzésére, trendek felismerésére, valamint proaktív karbantartás támogatására. Ezek a képességek jelentősen hozzájárulnak a hatékonyság növeléséhez, a költségek csökkentéséhez, és az üzemidő optimalizálásához.

Ugyanakkor a smart szenzorok bevezetése jelentős kezdeti beruházással jár, továbbá megköveteli a megfelelő szoftveres és hálózati infrastruktúra kiépítését. Az ipari szereplőknek ezért kulcsfontosságú feladatuk a technológiai fejlődés és a költséghatékonyság közötti egyensúly megtalálása annak érdekében, hogy az üzem teljesítményét és versenyképességét hosszú távon is maximalizálni tudják.

Hagyományos szenzorok

Az ipari forradalmak során a gyártástechnológia és az adatgyűjtés eszközei - köztük a szenzorok - jelentős fejlődésen mentek keresztül. A hagyományos szenzorok (10. ábra) évtizedeken át megbízhatóan szolgálták az ipari környezet igényeit, különösen jól teljesítve az előre definiált, specifikus feladatok ellátásában.
Azonban az Ipar 4.0 és az IIoT (Ipari Internet of Things) térnyerésével újfajta elvárások jelentek meg az ipari automatizálásban, amelyekhez az intelligens szenzorok sokkal hatékonyabban képesek alkalmazkodni. Ezek a korszerű eszközök nem csupán adatokat

gyűjtenek, hanem valós idejű feldolgozással, elemzéssel és kommunikációval támogatják a dinamikus, önszabályozó rendszerek működését.

A hagyományos szenzorok alapvető funkciókat látnak el: mérnek, érzékelnek és az adatokat egyszerű formában közvetítik.
Ezek az eszközök rendkívül megbízható működést biztosítanak, és általában egyszerűbb felépítésükből adódóan alacsonyabb hibalehetőséggel működnek, ami mérsékli a karbantartási igényeket és költségeket. Robusztus kialakításuknak köszönhetően kiválóan ellenállnak az ipari környezet szélsőséges körülményeinek - például a magas hőmérsékletnek, erős rezgéseknek vagy mechanikai terheléseknek.

10. ábra, hagyományos szenzorok
https://hu.pinterest.com/pin/825003225529729243/

Ugyanakkor az ipar egyre erőteljesebb automatizálódásával és a decentralizált döntéshozatal irányába történő elmozdulással a smart szenzorok szerepe jelentősen megnőtt. Ezek az eszközök képesek önálló adatfeldolgozásra és komplex analitikai műveletek elvégzésére, valamint hatékonyan kommunikálnak egymással a hálózaton keresztül, így fokozatosan háttérbe szorítják a hagyományos szenzorokat.

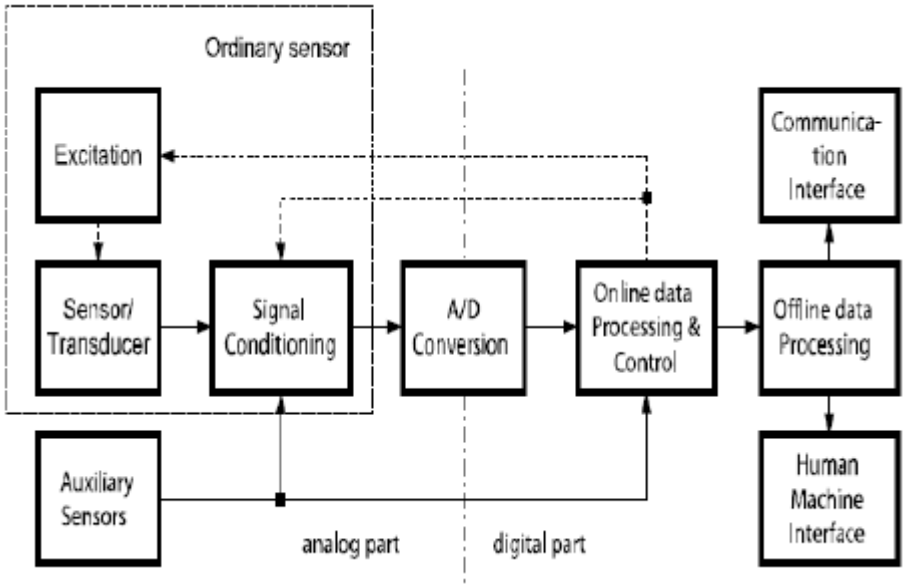
Mindazonáltal a smart szenzorok komplex technológiájuk miatt nagyobb kockázattal rendelkezhetnek a meghibásodásokra, és gyakran jelentősebb kezdeti beruházást igényelnek. Emellett a megnövekedett adatforgalom miatt fokozott biztonsági kihívásokkal is szembesülnek, hiszen több támadási felületet kínálnak a kibertámadások számára.

Összességében elmondható, hogy bár az intelligens szenzorok egyre nagyobb szerepet kapnak az ipar modern igényeinek kielégítésében, a hagyományos szenzorok megbízhatóságuk és egyszerűségük miatt továbbra is nélkülözhetetlenek. A választás tehát az egyensúly megtalálásán múlik: az adott ipari alkalmazásban a hagyományos szenzorok stabilitása vagy a smart szenzorok rugalmassága és intelligenciája nyújt-e optimálisabb megoldást.

Smart szenzorok a hagyományosak ellen

Ahogy az Ipar 4.0 korszaka egyre közeledik a megvalósulás felé, a IIoT (Industrial Internet of Things) technológiái - különösen a smart szenzorok - kulcsszereplőként tűnnek fel az ipari innovációban. Ezek az intelligens eszközök nemcsak gyorsabban, hanem jóval hatékonyabban képesek adatokat gyűjteni, feldolgozni és továbbítani, mint hagyományos elődeik. A kérdés

azonban adott: vajon mindez elegendő ahhoz, hogy teljes egészében leváltsák a klasszikus megoldásokat? (11. ábra)



11. ábra, Hagyományos <-> Smart szenzor, https://www.researchgate.net/figure/The-structure-of-an-intelligent-sensor_fig1_263273954

A smart szenzorok előnyei kétségtelenek. Tanulási és adaptációs képességük, valamint hálózatba kapcsolt működésük révén elősegítik az automatizált döntéshozatalt, ezáltal jelentősen csökkentve az emberi beavatkozás szükségességét. Az adatgyűjtés gyorsaságának és pontosságának köszönhetően akár néhány másodperc alatt képesek komplex folyamatokat is monitorozni. Ezen túlmenően, az integrált önellenőrző és diagnosztikai rendszerek révén csökken a karbantartási igény, miközben nő az üzemidő és a rendszer megbízhatósága.

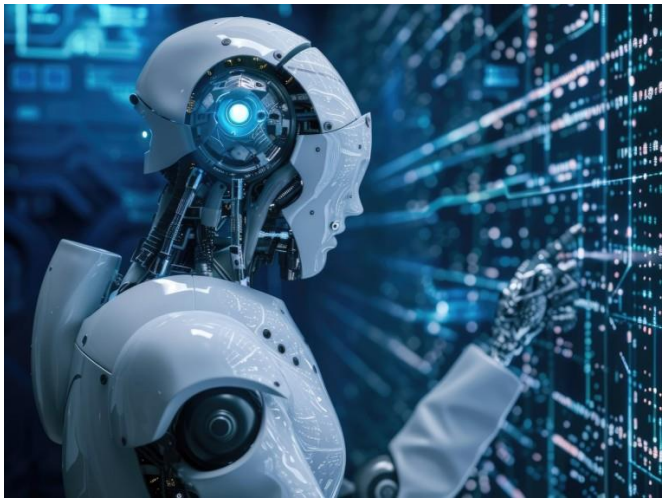
Ezzel szemben a hagyományos szenzorok lassabbnak és kevésbé összetettnek tűnhetnek, ám bizonyos esetekben továbbra is megőrzik létjogosultságukat. Megbízhatóságuk, egyszerű felépítésük és alacsony költségük miatt sok iparág még mindig előnyben részesíti ezt a technológiát. Nem igényelnek bonyolult hálózati infrastruktúrát, és különösen jól alkalmazhatók olyan környezetekben, ahol az intelligens rendszerek bevezetése felesleges bonyolítást jelentene.

A verseny tehát nem csupán a sebesség és a pontosság dimenziójában dől el. A döntéshozóknak figyelembe kell venniük az adott alkalmazás specifikus követelményeit, a költségvetési kereteket, valamint a rendszerintegráció komplexitását is. A smart szenzorok kiemelkedő teljesítményt nyújtanak az adatvezérelt döntéshozatal támogatásában és a gyártási folyamatok optimalizálásában, ugyanakkor a hagyományos szenzorok egyszerűsége és költséghatékonysága továbbra is életképes alternatívává teszi őket számos ipari környezetben.

A jövő iparának úttörői számára tehát nem pusztán technológiai választásról van szó, hanem arról, hogy miként képesek integrálni a rendelkezésre álló eszközöket annak érdekében, hogy maximalizálják a termelékenységet és fenntartsák versenyképességüket. Az intelligens és hagyományos szenzorok közötti verseny így nem kizárólag a technikai paraméterekről szól, hanem sokkal inkább a tudatos alkalmazásról és a stratégiai szemléletmódról.

Automatizálás

Az ipari automatizáció új korszaka köszöntött be az IIoT (Industrial Internet of Things) kompatibilis szenzorok széleskörű elterjedésével. Ezek az intelligens szenzorok nem csupán adatgyűjtésre alkalmasak, hanem képesek az információk helyszíni feldolgozására és valós idejű továbbítására is. Ezáltal lehetővé válik a gyártási folyamatok hatékonyságának növelése, az azonnali beavatkozások és az adaptív döntéshozatal. Míg a hagyományos szenzorok főként passzív adatforrásként működnek, az IIoT-kompatibilis eszközök aktív résztvevőivé válnak a termelési rendszereknek, elősegítve az intelligens üzemek létrejöttét



12. ábra, Automatizálás ("Karikatúra") https://weborvos.hu/lapszemle/az-eu-betiltotta-a-legveszelyesebbnek-itelt-ai-s-rendszereket-288462

Az IIoT-kompatibilis szenzorok legfőbb előnyei közé tartozik a valós idejű adatkezelés és elemzés képessége, amely lehetővé teszi a gyors reakciót és a gyártási folyamatok folyamatos optimalizálását. Az automatizált adatgyűjtés csökkenti az emberi hibák előfordulásának esélyét, ezáltal növelve a termelés hatékonyságát és a végtermék minőségét. Ezen túlmenően, a szenzorok képesek időben felismerni és jelezni a rendellenességeket, ami hozzájárul az energiafelhasználás optimalizálásához és a megelőző karbantartási intézkedések bevezetéséhez.

Ugyanakkor az IIoT-kompatibilis szenzorok alkalmazása bizonyos kihívásokat is rejt magában. A beszerzésük és rendszerbe illesztésük magasabb beruházási költségekkel járhat, miközben az üzemeltetésük fejlettebb - és gyakran összetettebb - informatikai infrastruktúrát igényel. További aggályt jelent a kiberbiztonság kérdése: az internetre kapcsolt eszközök fokozottan ki vannak téve a külső támadásoknak, ami megnövekedett adatvédelmi és rendszerbiztonsági kockázatokat eredményezhet.

Bár a smart szenzorok hozzáadott intelligenciája számos előnyt kínál, nem szabad figyelmen kívül hagyni, hogy bizonyos ipari alkalmazások esetében a hagyományos szenzorok egyszerűsége és megbízhatósága kedvezőbb választás lehet. Ezek az eszközök kevésbé hajlamosak a meghibásodásra, könnyebben karbantarthatók, illetve gyorsabban és olcsóbban cserélhetők, ami különösen fontos lehet nagy igénybevételű vagy költségérzékeny környezetben.

Összegzésként elmondható, hogy az IIoT-kompatibilis smart szenzorok bevezetése jelentős előrelépést jelenthet az ipari automatizációban, különösen a valós idejű adatkezelés, a folyamatoptimalizálás és az energiahatékonyság területén. Ugyanakkor a bevezetéshez kapcsolódó költségek, az infrastruktúra komplexitása és a biztonsági kihívások alapos mérlegelést igényelnek. A gyártóknak a saját működési környezetükhöz, céljaikhoz és erőforrásaikhoz illeszkedően kell meghozniuk a döntést arról, hogy mely technológia szolgálja

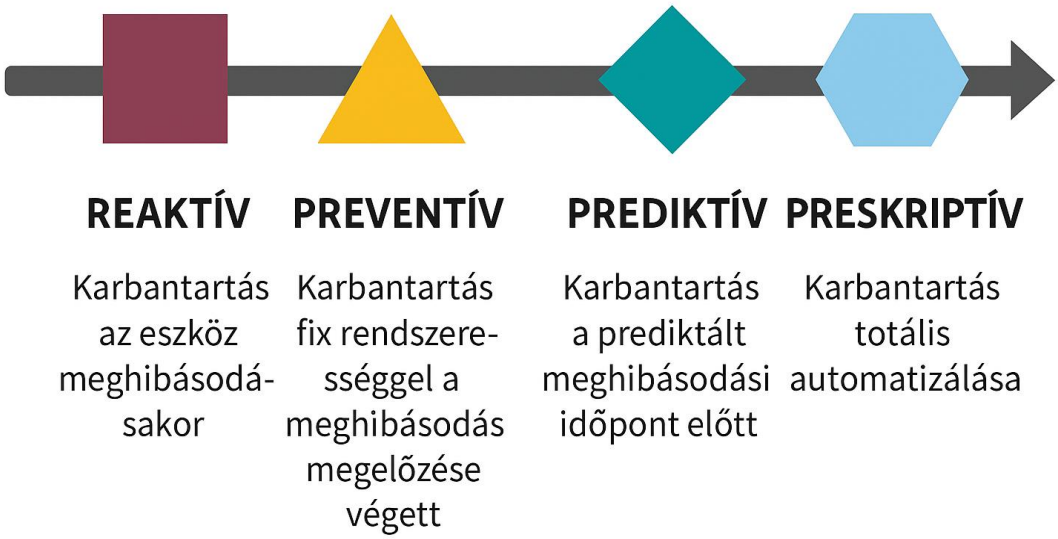
leginkább hosszú távú érdekeiket. Az ipari automatizáció új korszakában a jövőbe tekintő gondolkodás, valamint a fejlett technológiák körültekintő alkalmazása kulcsfontosságú a versenyképesség fenntartásához és a fenntartható működéshez.

IIoT előnyei

Prediktív karbantartás

Az IoT egyik kiemelkedő előnye az előrejelző (prediktív) karbantartás lehetősége, amely forradalmasítja a hagyományos karbantartási stratégiákat. Ez a megközelítés lehetővé teszi a gépek és berendezések állapotának folyamatos nyomon követését és elemzését, így már a meghibásodások bekövetkezte előtt azonosíthatók a potenciális problémák. Ennek köszönhetően minimálisra csökkenthetők a nem tervezett leállások és üzemzavarok, ami jelentős mértékben növeli a termelékenységet és meghosszabbítja az eszközök élettartamát.

Az IoT-alapú prediktív karbantartás lényege, hogy intelligens érzékelők és szenzorok gyűjtik valós időben az adatokat - például a gépek hőmérsékletéről, rezgéséről, teljesítményéről vagy olajnyomásáról -, amelyeket aztán felhőalapú rendszerek vagy helyi elemző egységek dolgoznak fel. A beérkező információk alapján előrejelző modellek (13. ábra) képesek meghatározni, mikor szükséges beavatkozni, így elkerülhetővé válik a meghibásodás, miközben optimalizálható a karbantartási ütemezés.



13. ábra, Optimális karbantartásütemezés, avagy lőrelátás 4 szintje, saját generált kép

Az IoT rendszerek által gyűjtött adatok elemzésére alkalmazott analitikai modellek segítségével az előrejelző karbantartás képes azonosítani a hibákra utaló korai jeleket vagy mintázatokat, és időben figyelmeztetni a karbantartási beavatkozások szükségességére. Például az algoritmusok érzékelik a rezgésekben vagy a hőmérsékletben bekövetkező szokatlan eltéréseket, amelyek előrevetítik egy gép esetleges meghibásodását vagy várható leállását.

A prediktív karbantartás számos előnyt kínál, többek között növeli a termelékenységet, csökkenti a karbantartási költségeket, és segít minimalizálni az üzemzavarokat. Emellett lehetővé teszi a gépek és berendezések hatékonyabb kihasználását, ezáltal hozzájárulva a gyártási folyamatok megbízhatóságának és általános hatékonyságának javításához.

IIoT veszélyei

Mint ismert, az IIoT forradalmi változásokat idézett elő az ipari folyamatokban és a gyártási szektorban, amely jelentősen hozzájárult a profit maximalizálásához és a gyártási folyamatok optimalizálásához. Ugyanakkor, mint minden technológiai fejlődésnek, ennek is megvannak a maga árnyoldalai, amelyeket az alábbiakban szeretnék részletesebben bemutatni:

Biztonsági kockázatok

Az IIoT-hálózatok sebezhetősége komoly kihívást jelent az ipari szektor számára. Ennek oka, hogy ezek a rendszerek számos ponton kapcsolatban állnak a külvilággal, és nagy mennyiségű érzékeny adatot kezelnek és továbbítanak. Mindez rendkívül vonzó célponttá teszi őket a kibertámadók számára, akik igyekeznek kihasználni az esetleges biztonsági résekből adódó lehetőségeket.

Adatlopás és kiszivárogtatás: Az IIoT-rendszerek kritikus ipari adatokat - például termelési mutatókat, gépi paramétereket és üzleti információkat - gyűjtenek és továbbítanak.
A gyártási folyamatok megszakítása: A kibertámadások célpontjai lehetnek például az üzemirányítási rendszerek vagy az automatizált berendezések, melyek manipulálása gyártási hibákhoz, állásidőhöz és a termékek minőségének romlásához vezethet.

A rendszer manipulálása és eltérítése: Az IIoT-rendszerek sebezhetőségei lehetőséget adnak arra, hogy a támadók eltérítsék a rendszert. Ennek következtében képesek lehetnek beavatkozni az ipari folyamatokba, üzemzavarokat idézhetnek elő, vagy akár súlyos károkat is okozhatnak az infrastruktúrában.
Zsarolóvírusok és egyéb fenyegetések: Az IIoT-hálózatokat különféle zsarolóvírusok és rosszindulatú szoftverek is fenyegethetik. Ezeket a programokat úgy tervezik, hogy blokkolják a rendszerek működését, titkosítsák az adatokat, vagy akár átvegyék az irányítást a vállalat rendszerei felett a támadó érdekében.

Az ilyen típusú támadások súlyos következményekkel járhatnak mind az érintett vállalatokra, mind az iparág egészére nézve. Éppen ezért kiemelten fontos, hogy megfelelő biztonsági intézkedések kerüljenek bevezetésre az IIoT-rendszerek védelme érdekében. Ennek célja a fenyegetések minimalizálása és egy erős védelmi réteg kialakítása a támadásokkal szemben. Ez magában foglalja például a rendszerek rendszeres frissítését, megbízható biztonsági szoftverek és hardverek alkalmazását, korszerű hálózatbiztonsági megoldások bevezetését, valamint az alkalmazottak kiberbiztonsági képzését és tudatosságának növelését.

Adatvédelmi kockázatok

Az ipari IIoT-rendszerek rendkívül nagy mennyiségű adatot termelnek és dolgoznak fel, beleértve a személyes adatokat, üzleti információkat és egyéb érzékeny adatokat is. Ezeknek az adatoknak a védelme kiemelten fontos a jogosulatlan hozzáférés, az adatszivárgás vagy a nyilvánosságra hozatal megelőzése érdekében, hiszen ezek súlyos következményekkel járhatnak. Az adatvédelmi kockázatok több forrásból is származhatnak, például az alábbi tényezőkből:

Jogosulatlan hozzáférés: Amennyiben az IIoT-rendszerek nem megfelelően vannak konfigurálva vagy nem biztosított a kellő szintű védelem, a kiberbűnözők és más illetéktelen személyek könnyen hozzáférhetnek az adatokhoz. Ez különösen veszélyes lehet akkor, ha a támadók érzékeny információkat - például banki adatokat - tulajdonítanak el, ami súlyos következményekkel járhat mind az egyénekre, mind a vállalatokra nézve.

Adatszivárgás: Legyen szó belső vagy külső támadókról, az adatokhoz való jogosulatlan hozzáférés és az adatszivárgás kockázata mindig fennáll. Az ilyen adatvédelmi incidensek komoly következményekkel járhatnak az érintett vállalat számára, beleértve az üzleti titkok elvesztését, a cég jó hírnevének károsodását, valamint jogi szankciókat és egyéb adatvédelmi problémákat.

Adatok megsemmisítése vagy manipulálása: Az ipari IoT-rendszerek tárolják és kezelik a gyártási folyamatokhoz és döntéshozatalhoz szükséges adatokat. Amennyiben ezekhez az adatokhoz illetéktelenek férnek hozzá, vagy azok manipulálásra kerülnek, az súlyos károkat okozhat a vállalat működésében és a termelékenységében egyaránt.

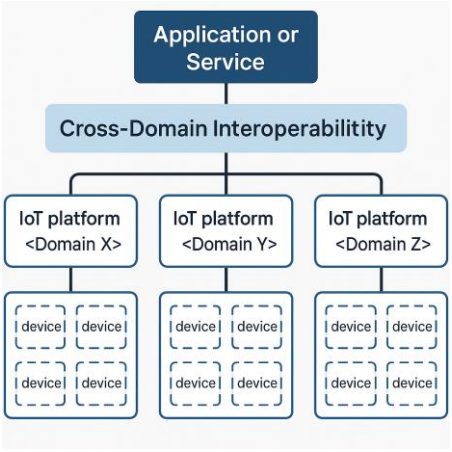
A következő cikk egy olyan emberről szól, akit majdnem letöltendő börtönbüntetésre ítéltek az adathalászok / adathalászat miatt:

Adatvédelmi előírások megsértése: Olyan törvények, mint az EU általános adatvédelmi rendelete (GDPR - General Data Protection Regulation), kiemelten kezelik és szigorúan szabályozzák az adatvédelmet. Az adatvédelmi előírások megsértése súlyos pénzbírságokat és komoly hírnévkárosodást eredményezhet az érintett vállalatok számára.

Az adatvédelmi kockázatok kezeléséhez az ipari IoT-rendszereknek megfelelő biztonsági intézkedéseket kell alkalmazniuk. Ezek közé tartozik az erős hitelesítés és hozzáférés-szabályozás, az adatátvitel titkosítása, rendszeres adatmentések és helyreállítási eljárások, valamint szigorú adatvédelmi szabályzatok és protokollok bevezetése. A tudatos adatvédelmi stratégiák kialakítása és folyamatos felülvizsgálata kulcsfontosságú az ipari IoT sikeres működéséhez és megvalósításához.

Kompatibilitási problémák

Az IIoT eszközök és rendszerek gyors fejlődése és változatossága komoly kihívásokat jelenthet az integráció és szabványosítás szempontjából. Ezek a problémák (14. ábra) főként a következő területeket érintik:



14. ábra, Miér vannak kompa bilitási problémák az IIoT világában?, saját szerkeztésű ábra

Protokollok és kommunikáció: Az IIoT eszközök és rendszerek sokféle kommunikációs protokollt alkalmazhatnak, mint például az MQTT, OPC UA vagy a Modbus. Ezek a különböző szabványok azonban nehézséget okozhatnak az eszközök közötti zökkenőmentes adatcserében és az integrációban.

Szabványok hiánya vagy eltérései:
Az IIoT területén bár működnek szabványokat kidolgozó szervezetek (pl. IEEE, ISO), még mindig hiányzik az átfogó iparági egységesülés. A meglévő protokollok gyakran nem kompatibilisek egymással, ami különösen problémás lehet vegyes gyártós környezetekben, ahol eltérő forrásból származó eszközök kommunikálnak egymással.
Felügyelet és kezelés: Az IIoT rendszerekben gyakran különböző típusú eszközök és platformok működnek együtt, amelyek külön kezelést és felügyeletet igényelnek. Ez a sokféleség nehézséget okozhat az egységes irányításban, főleg nagyobb léptékű üzemekben vagy olyan környezetekben, ahol több telephelyen is vannak IIoT megoldások.

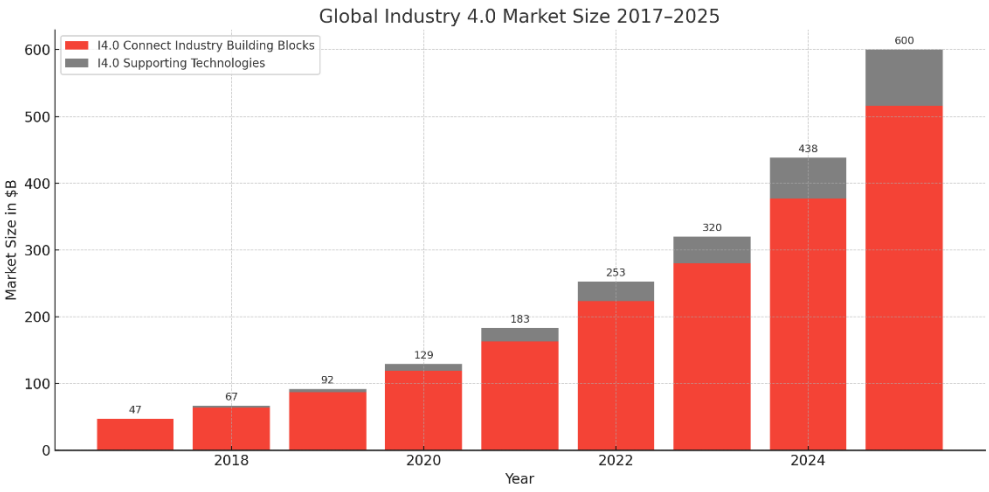
Biztonság és hibakeresés: Az IIoT környezetekben a különböző eszközök és rendszerek sokszínűsége jelentősen megnehezíti mind a biztonsági kockázatok kezelését, mind a hibaelhárítást. Minden egyes eszköz saját biztonsági sebezhetőségeket és működési hibákat hordozhat, amelyek külön-külön is komoly kihívások elé állíthatják a rendszerműködtetőket. A teljes rendszer megbízható működéséhez mindezeket figyelembe kell venni és szisztematikusan kezelni kell.

Az IIoT rendszerek kompatibilitási problémáinak csökkentése érdekében kulcsfontosságú az iparági szabványok követése és az interoperabilitásra optimalizált tervezés. A szabványos kommunikációs protokollok (pl. MQTT, OPC UA) és egységes interfészek alkalmazása jelentősen leegyszerűsítheti az eszközök integrációját. Emellett központosított felügyeleti platformok bevezetése segíthet a heterogén rendszerek hatékony kezelésében, ezzel is elősegítve az IIoT megoldások zökkenőmentes működését.

Üzleti kockázatok

Az IIoT rendszerek bevezetése komoly üzleti kockázatokat jelenthet, melyek hatással lehetnek a vállalat működésére és hosszú távú teljesítményére. A fő kockázati területek [7]:

Beruházási költségek: Az IIoT rendszerek bevezetése jelentős kezdeti beruházást igényelhet. Az eszközbeszerzés, szoftver- és hardverközpontok kialakítása, valamint az integrációs munkálatok magas költségeket vonhatnak maguk után. Ezek a kiadások átmenetileg megterhelhetik a vállalat pénzügyi helyzetét, akár veszteséget is okozhatnak a bevezetési fázisban.



15. ábra, Az IIoT térhódítása a piacon, egyedi szerkeztésű kép

Folyamatos karbantartás és frissítés: Az IIoT rendszerek folyamatos karbantartást és frissítést igényelnek a biztonságos és hatékony működés érdekében. Ez tartalmazza a szoftverfrissítéseket, a biztonsági javításokat, valamint az eszközök és infrastruktúra fizikai karbantartását. Ezek a teendők további költségekkel és erőforrás-igénnyel járnak.

Munkaerő készségfejlesztése: Az IIoT megoldások bevezetése új szakmai kompetenciákat követel a dolgozóktól. Az innovatív technológiák, rendszerek és munkafolyamatok elsajátítása képzési és fejlesztési erőfeszítéseket igényel, ami kihívást jelenthet a személyi állomány számára. Ez magában foglalja az oktatási programokat, szakmai továbbképzéseket, valamint az új munkamódszerek gyakorlati alkalmazását.

Üzle működés zavarása: Az IIoT rendszerek bevezetése során fellépő műszaki problémák és átmeneti nehézségek hatással lehetnek a vállalat működésére. A rendszerintegráció során előforduló hibák, technikai zavarok vagy átállási nehézségek ideiglenesen csökkenthetik a termelési hatékonyságot és befolyásolhatják az ügyfelek számára nyújtott szolgáltatások minőségét.

Versenyképesség fenyegetése: Az IIoT technológiák elmaradása versenyhátrányhoz vezethet a vállalatok számára. Aki nem alkalmazza ezeket az innovatív megoldásokat, az könnyen alulmaradhat a versenytársakkal szemben, és elveszítheti piaci pozícióját.

A vállalatoknak alaposan fel kell készülniük az IIoT bevezetésére, figyelembe véve a lehetséges kockázatokat és azok kezelésének módját. Fontos a költségek részletes tervezése, a dolgozók továbbképzése, valamint a rendszer folyamatos ellenőrzése és fejlesztése a kockázatok csökkentése érdekében (15. ábra).

Vélemény

Vélemény

A kutatásom során mélyebb betekintést nyertem az IIoT világába, és rájöttem, milyen lenyűgöző lehetőségeket rejt ez a technológia. Szeretném megosztani személyes véleményemet erről a témáról.

Az elmúlt időszakban végzett vizsgálataim során világossá vált számomra, hogy az IIoT nem csupán egy új technológiai trend, hanem egy olyan átfogó megoldás, amely forradalmasíthatja az ipari folyamatokat és jelentősen növelheti a termelékenységet. Az IIoT lehetővé teszi különböző ipari eszközök és rendszerek összekapcsolását, valós idejű adatgyűjtést és elemzést, ami optimalizálási lehetőségeket kínál a vállalatok számára.

Ezen előnyök mellett fontos azonban felhívni a figyelmet az IIoT bevezetésével járó kockázatokra is. Kiemelten fontosnak tartom a biztonsági és adatvédelmi kérdéseket, valamint a kompatibilitási és üzleti kockázatokat. Ezeknek megfelelő kezelése elengedhetetlen ahhoz, hogy az IIoT teljes potenciálját ki tudjuk használni.

Kovács Ármin Krisztián
[redacted]

Források

Irodalomjegyzék

[1] Articles overview (2022) IoT For All. Available at: https://www.ioforall.com/articlesoverview

[2] Fluckinger, D. et al. (2024) TechTarget News, TechTarget Enterprise Technology News. Available at: https://www.techtarget.com/news/

[3] Wachtel, J., Viorel, P. and Clifford, J. (1969) Industrial IOT Archives, IIoT World. Available at: https://www.iiot-world.com/category/industrial-iot/

[4] Energy (2023) Industry IoT Consortium. Available at: https://www.iiconsortium.org/vertical-markets/energy-utility/

[5] (2024) IEEE Spectrum. Available at: https://spectrum.ieee.org/?utm_source=mm_link&utm_campaign=sp&utm_medium=pubs&utm_term=spectrum+home

[6] Big data (no date) Forbes. Available at: https://www.forbes.com/bigdata/?sh=e769c8d16d11

[7] Learning - széchenyi István Egyetem (no date) SzE. Available at: https://szelearning.sze.hu/course/view.php?id=12990

2.23. Beágyazott rendszerek szerepe az önvezető járművek valós idejű döntéshozatalában

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

IPAR 4.0 TECHNOLÓGIÁK

Beágyazott rendszerek szerepe az önvezető járművek valós idejű döntéshozatalában

SZARKA MILÁN
[redacted]

(GKNB_INTM087)

2024/2025/2

1.Bevezetés: 3

2.Az önvezető járművek technikai alapjai – beágyazott rendszerek szerepe: 6

2.1 Szenzorok és adatgyűjtés 6

2.2 Szenzorfúzió és környezetmodell 6

2.3 Valós idejű döntéshozatal 6

2.4 Aktuátorvezérlés 6

2.5 Kommunikáció és hálózat 6

2.6 Rendszerszintű áttekintés 6

3. Beágyazott rendszerek szerepe az önvezetésben 8

3.1 Mi az a beágyazott rendszer? 8

3.2 Hol jelennek meg ezek az önvezető járművekben? 8

3.3 Konkrét példák alkalmazásokra 8

Mi az a watchdog rendszer? 9

4. Használt hardverplatformok és architektúrák 11

4.2Tipikus hardverplatformok 11

4.3Valós idejű követelmények 11

4.4Hardveres támogatás: 11

5. Szoftveres környezet és operációs rendszerek 12

5.2Feladatütemezés, prioritás és hibakezelés 13

6. Szenzoradat-feldolgozás és döntéshozatal 13

6.2Szenzorfúzió: többféle szenzor összehangolása 13

6.3Algoritmusok és neurális hálók beágyazott rendszeren 13

6.4Edge computing szerepe 14

7. Biztonság és hibatűrés 15

7.2Watchdog rendszerek és fail-safe mechanizmusok 15

7.3Redundancia és hibatűrés 15

7.4 Kiberbiztonság beágyazott szinten 16

7.5Rendszerhitelesítés és szabványok 16

8. Kommunikációs rendszerek integrációja 17

8.2 CAN busz – bevált megoldás 17

8.3 Ethernet – nagy sávszélességű kommunikáció 18

8.4 TSN – Time-Sensitive Networking 18

8.5Hogyan csatlakoznak ezek a rendszerek az autó belső hálózatához? 19

9.Önvezető járművek előnyei és hátrányai 21

9.1Előnyök:.....21
9.2Hátrányok: 21
10. Összegzés.....22
Irodalomjegyzék: 23

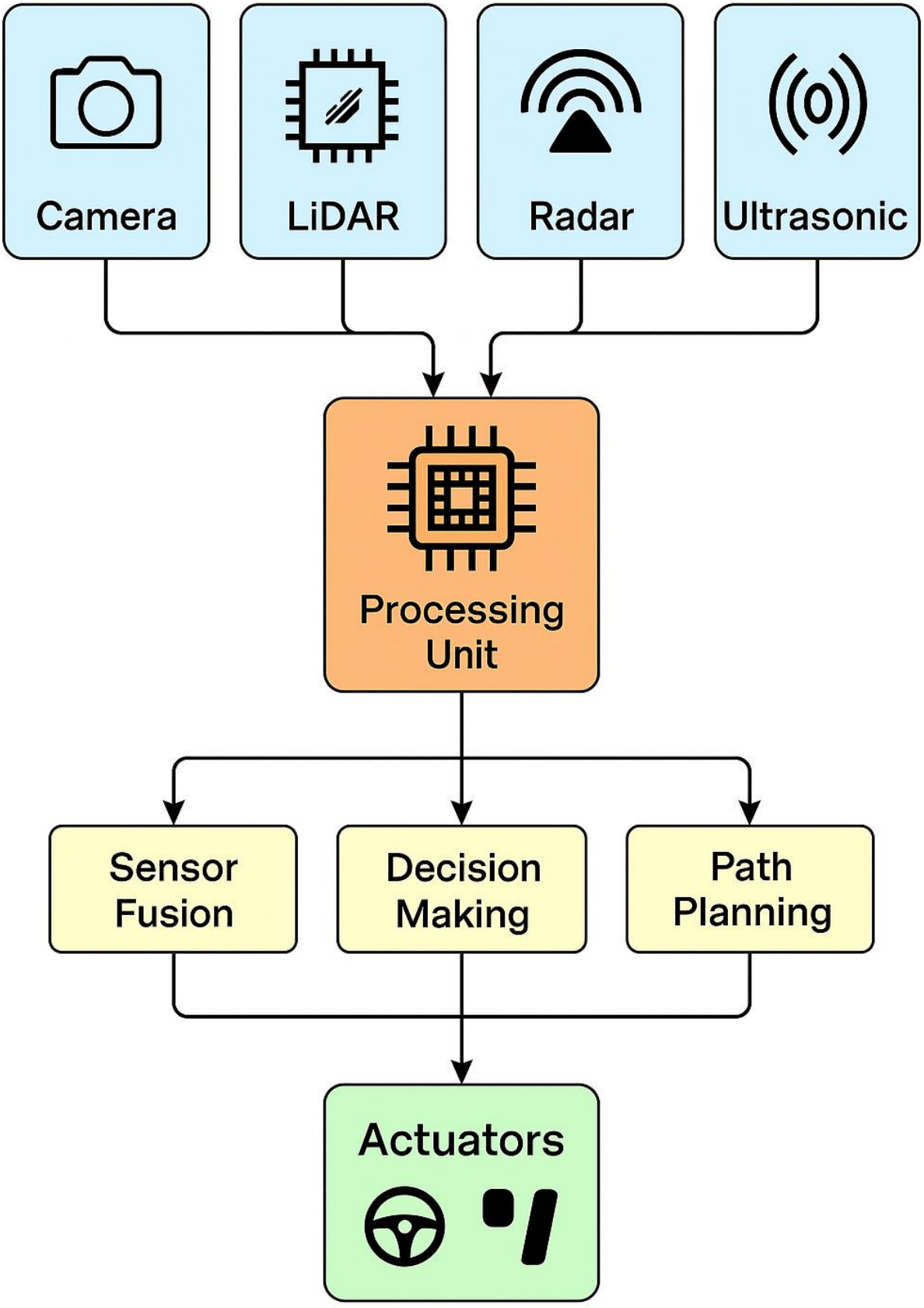
1.Bevezetés:

Az elmúlt évek technológiai fejlődése forradalmasította a közlekedést: az önvezető járművek – vagy más néven autonóm közlekedési rendszerek – már nem csupán futurisztikus víziók, hanem egyre inkább kézzelfogható valóság. A globális autóipar, a mesterséges intelligencia, valamint a szenzortechnológia fejlődése lehetővé tette olyan járművek fejlesztését, amelyek emberi beavatkozás nélkül képesek a közlekedésben való részvételre. Az autonóm járművek működése azonban rendkívül összetett technológiai rendszerekre épül, amelyek közül az egyik legfontosabb a **beágyazott rendszerek** hálózata.

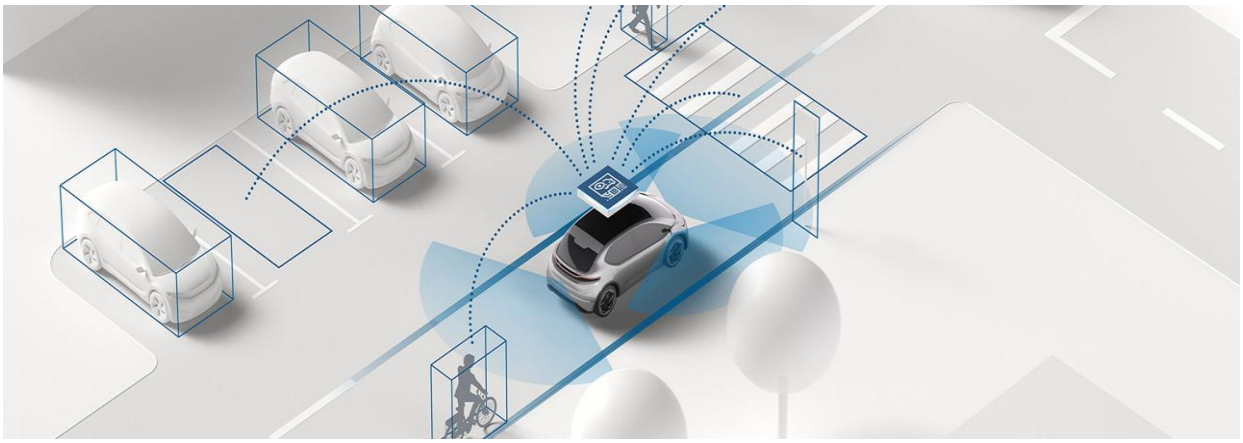
A beágyazott rendszerek olyan specializált számítástechnikai egységek, amelyek konkrét feladatokat látnak el valós időben, magas megbízhatóság és gyors reakcióidő mellett. Egy önvezető járműben ezek a rendszerek felelősek a szenzoradatok feldolgozásáért, a környezetérzékelésért, az útvonaltervezésért, valamint a valós idejű döntéshozatalért. A működésük gyakran párhuzamosan zajlik, és fontos, hogy a rendszer képes legyen gyorsan és pontosan reagálni a változó körülményekre – akár millimásodpercek alatt.

A beadandó célja, hogy részletesen bemutassa, milyen szerepet töltenek be ezek a beágyazott rendszerek az önvezető járművek működésében. A fókusz nem az önvezetés általános bemutatásán, hanem a **valós idejű működésen, a használt hardver-szoftver architektúrákon**, illetve a **műszaki kihívásokon** lesz. Kitérünk a felhasznált technológiákra (pl. NVIDIA Jetson, RTOS), a szenzoradatok feldolgozására, valamint a biztonsági és hibatűrési mechanizmusokra is.

A beágyazott rendszerek vizsgálata elengedhetetlen a jövő járműtechnológiájának megértéséhez. Ezek a rendszerek adják az autonóm járművek „idegrendszerét”, amelyek nélkül a biztonságos és intelligens működés nem lenne megvalósítható.



1. ábra Az önvezető járművek rendszerszintű felépítése--> saját szerkesztés



2. ábra Környezetérzékelés a jövő autóiban https://www.bosch-mobility.com/en/solutions/automated-driving/video-perception-modules/

2.Az önvezető járművek technikai alapjai – beágyazott rendszerek szerepe:

Az önvezető járművek nem önálló eszközökként, hanem bonyolult, több szintű, valós idejű rendszerekként működnek, ahol az egyes komponensek együttműködése kulcsfontosságú. E rendszerek gerincét az úgynevezett **beágyazott rendszerek** alkotják, amelyek célzott feladatokat hajtanak végre – jellemzően **korlátozott hardvererőforrások** mellett, mégis magas megbízhatósággal.

A beágyazott rendszerek központi feladata az érzékelők (kamera, LiDAR, radar, ultrahang) által gyűjtött adatok feldolgozása és továbbítása a vezérlőrendszerek felé. Ezek a rendszerek gyakran **valós idejű operációs rendszerekre (RTOS)** épülnek, amelyek biztosítják, hogy a rendszer a kritikus eseményekre megfelelő időn belül reagáljon.

A következő fő technikai elemek különíthetők el:

2.1 Szenzorok és adatgyűjtés

A jármű fedélzeti szenzorai a környezet észlelését végzik. Minden szenzor külön-külön is működik, de a valós idejű rendszer szinkronizálja és egyesíti ezeket az adatokat, amit **szenzorfúziónak** nevezünk. Az adatokat jellemzően **beágyazott szenzorvezérlők** dolgozzák fel először (például FPGA vagy ARM-alapú egységek).

2.2 Szenzorfúzió és környezetmodell

A beágyazott központi egység (pl. NVIDIA Jetson Xavier, Qualcomm Snapdragon Ride) végzi a különböző szenzoradatok egyesítését és az **aktuális környezetmodell** felépítését. Ehhez gyakran gépi látás és mesterséges intelligencia algoritmusokat is alkalmaznak.

2.3 Valós idejű döntéshozatal

A feldolgozott környezeti információk alapján a rendszer döntéseket hoz: fékezzen-e, kikerüljön-e egy akadályt, vagy sávot váltson. Ez a **valós idejű döntéshozatal**, amely nem tolerálhat késleltetést – ezért a szoftverek gyakran **realtime prioritásokkal** és **prioritásalapú ütemezéssel** működnek.

2.4 Aktuátorvezérlés

A végrehajtó egységek, mint például a kormány, gázpedál vagy fékrendszer, saját beágyazott vezérlőegységekkel rendelkeznek. Ezek a vezérlők kapják meg a döntési rétegből érkező parancsokat, és közvetlenül működtetik a jármű mechanikai elemeit.

2.5 Kommunikáció és hálózat

Az egyes beágyazott modulok közötti kommunikáció jellemzően **CAN**, **Ethernet** vagy **FlexRay** alapú hálózatokon történik, és szigorú hibakezelést és szinkronizációt igényel.

2.6 Rendszerszintű áttekintés

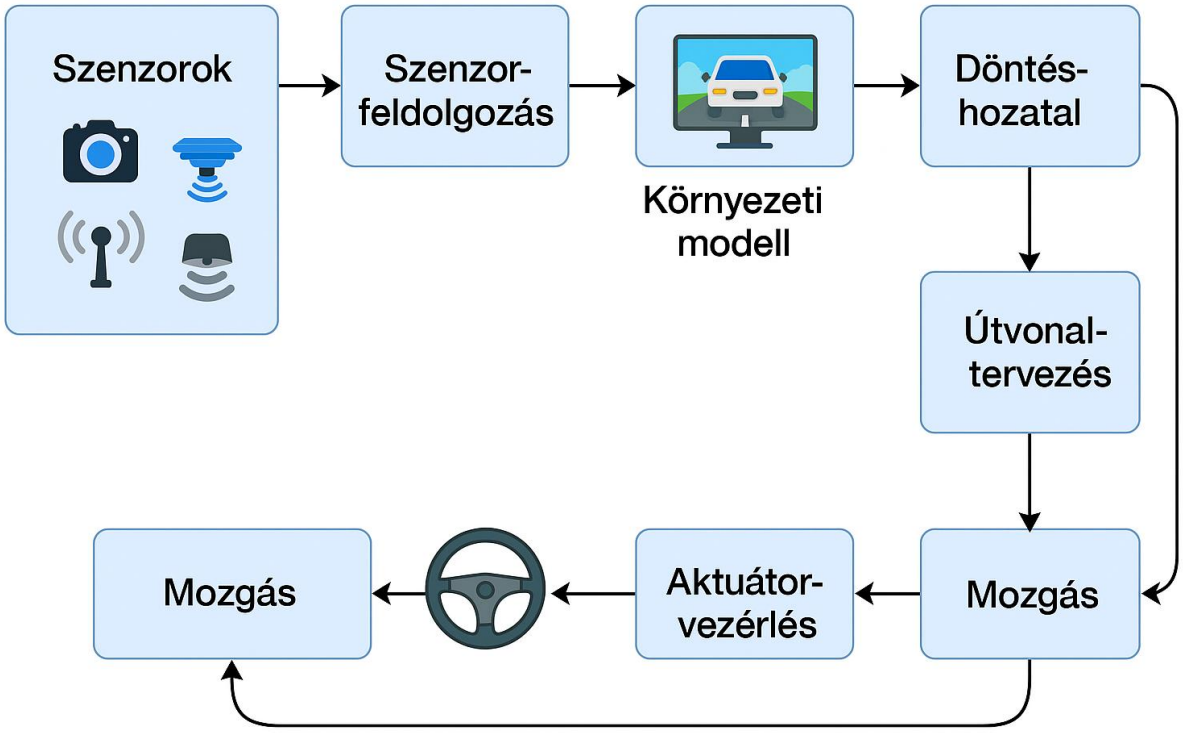
Egy önvezető jármű működése nem pusztán az egyes modulok teljesítményén, hanem azok **összehangolt, valós idejű együttműködésén** múlik. A teljes rendszer egy **rétegekből álló architektúraként** képzelhető el, ahol az információ áramlása szigorúan meghatározott sorrendben történik, minimalizálva a késleltetést és növelve a biztonságot.

Az általános adatfolyam az alábbi logika szerint épül fel:

1. **Érzékelés** – A jármű szenzorai (kamera, radar, LiDAR, ultrahang) folyamatosan adatokat gyűjtenek a környezetről.
2. **Szenzorfeldolgozás** – A szenzoradatokat az adott érzékelőhöz tartozó beágyazott egységek előfeldolgozzák (pl. zajszűrés, objektumdetekció).

3. **Szenzorfúzió** – A különböző típusú érzékelőkből származó adatok összeolvadnak, és egységes, valós idejű környezetmodellt hoznak létre.
4. **Döntéshozatal** – A központi vezérlő algoritmusok (gyakran mesterséges intelligencia alapúak) elemzik a helyzetet, és meghozzák a szükséges döntést (pl. gyorsítás, fékezés, sávváltás).
5. **Útvonaltervezés és manőverezés** – A rendszer a célállomás, forgalmi szabályok és valós idejű környezeti tényezők alapján megtervezi az optimális mozgást.
6. **Végrehajtás** – Az utasításokat a jármű aktuátorai hajtják végre, például az elektromos kormányzás, fékrendszer vagy hajtáslánc segítségével.
7. **Visszacsatolás** – A szenzorok újra és újra ellenőrzik a végrehajtott mozgás hatását, ezzel zárt hurok (feedback loop) jön létre.

A modulok közötti kommunikáció szigorúan szabályozott, jellemzően **CAN busz**, **automotive Ethernet**, vagy **FlexRay** alapú. A rendszer redundanciákat is alkalmaz, például kritikus szenzorokból több példány fut párhuzamosan, hogy hiba esetén is fennmaradjon a működés.



3. ábra Önvezető autó működésének folyamatábrája

3. Beágyazott rendszerek szerepe az önvezetésben

3.1 Mi az a beágyazott rendszer?

A beágyazott rendszer (angolul *embedded system*) egy speciális célra fejlesztett számítógépes egység, amely hardverből és szoftverből áll, és egy adott funkciót lát el egy nagyobb rendszeren belül. Ezek jellemzően **valós idejű működésre optimalizáltak**, kis méretűek, energiahatékonyak, és gyakran valamilyen szenzorhoz vagy aktuátorhoz kapcsolódnak. Nem önállóan működnek, hanem egy nagyobb rendszer részeként.

3.2 Hol jelennek meg ezek az önvezető járművekben?

Az autonóm járművek egyik kulcseleme a **széleskörűen alkalmazott beágyazott rendszerek hálózata**. Egy modern önvezető autóban akár több tucat, sőt száz különálló beágyazott egység működhet párhuzamosan, amelyek:

- **érzékelőadatokat gyűjtenek** és előfeldolgoznak (pl. kamera, radar, ultrahang)
- **valós idejű döntéseket** hoznak egyszerű logika alapján (pl. vészfékezés)
- **biztonsági ellenőrzést** végeznek (pl. watchdog, fail-safe rendszerek)
- **kommunikálnak egymással** vagy a fő vezérlőegységgel (pl. CAN buszon keresztül)
- **aktuátorokat vezérelnek** (pl. elektromos kormány, fék, gáz)

Ezek a rendszerek gyakran **mikrokontrollereken vagy dedikált processzorokon (SoC – System on Chip)** futnak, és különböző operációs rendszereket használnak, mint például FreeRTOS, QNX, AUTOSAR OS vagy Linux-alapú RT-kernel.

3.3 Konkrét példák alkalmazásokra

a) Szenzorfeldolgozás

Például egy előre néző kamera képeit egy **beágyazott képfeldolgozó egység** dolgozza fel: detektálja a sávokat, jelzőtáblákat, gyalogosokat. Az ilyen rendszerek gyakran használnak **dedikált hardvergyorsítókat** (pl. NVIDIA Xavier, Mobileye chip), hogy megfeleljenek a valós idejű követelményeknek.

b) Radar és LiDAR vezérlőegységek

A radar és LiDAR szenzorok nem csak „adatokat küldenek”, hanem már saját beágyazott processzorukon végzik az **adatelőkészítést, zajszűrést, objektumdetekciót**, és csak a releváns adatokat továbbítják a központi rendszer felé.

c) Biztonsági modulok

Beágyazott watchdog rendszerek figyelik a jármű létfontosságú funkcióit, és **hibadetektálás esetén önállóan képesek beavatkozni** (pl. vészfékezés, redundáns fékvezérlés aktiválása). Az ISO 26262 szabvány megköveteli, hogy ezek a rendszerek külön legyenek választva a fő döntéshozó egységektől.

d) Kommunikációs vezérlők

A jármű belső hálózatán működő kommunikáció (CAN, FlexRay, Ethernet) szintén beágyazott egységek által van vezérelve, amelyek gondoskodnak a csomagok időzítéséről, ellenőrzéséről és hibaérzékeléséről.

e) Aktuátorvezérlés

Az elektromos fékrendszert, a kormányzást és a gyorsítást is **dedikált beágyazott egységek irányítják**, melyek külön protokollon keresztül kommunikálnak a vezérlőegységekkel.

Mi az a watchdog rendszer?

A watchdog (magyarul: „őrkutya”) egy **időzítő**, amelyet rendszeresen „etetni” (újraindítani) kell egy futó program által. Ha a program lefagy, meghibásodik vagy valamilyen okból nem válaszol időben, a watchdog ezt érzékeli – mivel nem érkezik „etetés” – és automatikusan **újraindítja az adott alrendszert**, vagy aktivál egy vészhelyzeti protokollt.

Ez különösen kritikus az **autonóm járművek esetében**, ahol egy-egy feldolgozóegység hibája **életeket veszélyeztethet**.

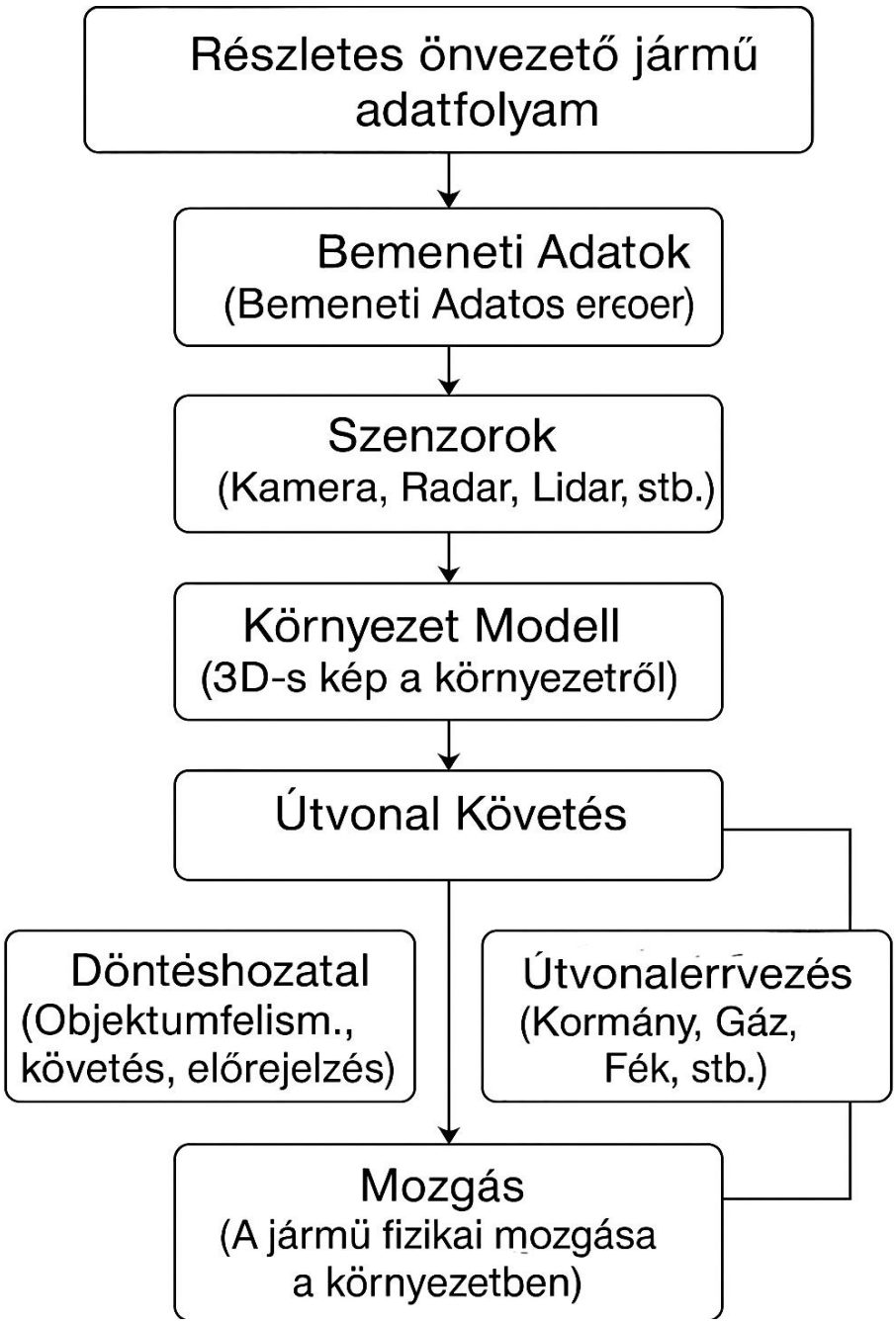
Hogyan használják az önvezető járművekben?

- A **fő vezérlőegységek watchdog-ja** folyamatosan ellenőrzi, hogy az érzékelőfeldolgozás, döntéshozatal és aktuátorvezérlés moduljai megfelelően működnek-e.
- **Redundáns fékrendszerek** watchdog-jai képesek a fő fékvezérlő meghibásodása esetén automatikusan aktiválni a biztonsági fékezést.
- **Watchdog rendszer** figyelheti a CAN kommunikációt is: ha nem érkeznek időben üzenetek (pl. sávváltási utasítás), akkor a jármű defenzív módba kapcsol (pl. lassít, megáll).
- Az **ISO 26262** biztonsági szabvány előírja, hogy minden kritikus funkciónak legyen watchdog alapú felügyelete, különösen az **ASIL-D** szintű (legmagasabb) komponenseknél.

Hardveres és szoftveres watchdog típusok:

- **Hardveres watchdog**: egy dedikált áramkör vagy mikrokontroller komponens, amely teljesen független a fő processzortól.

- **Szoftveres watchdog**: a rendszer saját szoftverében futó modul, amely figyeli az egyes alfolyamatokat, és hibát jelent, ha valamelyik nem válaszol időben.



4. ábra Önvezető jármű részletes adatfolyamának blokkvázlata- saját szerkesztés

4. Használt hardverplatformok és architektúrák

Az önvezető járművek egyik legkritikusabb technikai területe a mögöttük álló számítási infrastruktúra. Mivel valós idejű döntéseket kell hozniuk dinamikus környezetben, a használt hardvereknek nagy számítási teljesítményt kell biztosítaniuk, miközben energiatakarékosak és megbízhatóak maradnak. Az alábbiakban áttekintjük a legelterjedtebb hardverplatformokat, architektúrákat, valamint azok kapcsolatát a valós idejű követelményekkel.

4.2Tipikus hardverplatformok

NVIDIA Jetson

Az NVIDIA Jetson platform (pl. Jetson Xavier, Jetson Orin) az egyik legnépszerűbb választás az önvezető fejlesztések során. Ezek a modulok GPU-alapú gyorsítást nyújtanak tanulási modellek és párhuzamos képfeldolgozási feladatok futtatásához. A CUDA támogatás lehetővé teszi a valós idejű hálózatok futtatását szenzoradatokon.

ARM-alapú SoC-k (System-on-Chip)

ARM architektúrára épülő SoC-k jellemzően a járművek kisebb, alacsony fogyasztású részegységeiben találhatók meg, mint például az érzékelők vagy aktuátorok helyi vezérlői. Ezek jellemzően valós idejű operációs rendszereket (RTOS) futtatnak, mint a FreeRTOS vagy QNX.

FPGA-k (Field-Programmable Gate Array)

Az FPGA-k előnye, hogy rendkívül jól testreszabhatók és képesek extrém alacsony késleltetéssel működni. Gyakran használják kritikus feladatokhoz, például szenzoradatok szűréséhez, jelfeldolgozáshoz vagy biztonsági watchdog funkciók megvalósításához. Hátrányuk a bonyolultabb fejlesztési folyamat és magasabb költség.

Rendszerarchitektúra: Központi vs Elosztott feldolgozás

Az önvezető rendszerek architektúrája két fő modell köré épülhet:

Központi feldolgozás

Ebben a modellben minden szenzoradat egy központi egységbe (pl. egy nagy teljesítményű Jetson Xavier vagy Nvidia DRIVE AGX) fut be, amely végrehajtja az összes döntéshozatalt és irányítja a jármű mozgását. Előnye az egyszerűbb szinkronizáció és könnyebb frissítés, hátránya viszont a túlterhelés veszélye és a hosszabb késleltetés.

Elosztott feldolgozás

Ebben az esetben minden érzékelő egységhez vagy szenzorcsoporthoz saját lokális feldolgozóegység tartozik (pl. ARM SoC vagy FPGA), amelyek előfeldolgozott adatokat továbbítanak a központi vezérlésnek. Ez gyorsabb reakcióidőt biztosíthat, de komplexebb szinkronizációt és kommunikációt igényel.

4.3Valós idejű követelmények

Az önvezető járművek működése során elengedhetetlen a valós idejű válaszidő biztosítása, különösen a biztonság szempontjából kritikus döntéshozatali folyamatoknál (például akadályészlelés, vészfékezés).

4.4Hardveres támogatás:

- **Valós idejű operációs rendszerek (RTOS):** ARM-alapú egységek gyakran RTOS környezetben működnek, amely garantálja a determinisztikus válaszidőt.
- **Hardveres prioritáskezelés:** FPGA-k és dedikált mikrovezérlők képesek magas prioritású események (pl. watchdog reset) azonnali kezelésére.
- **QoS (Quality of Service) támogatás:** Modern SoC-k képesek adatforgalom és feldolgozási igények prioritásalapú kezelésére.

Tulajdonság	NVIDIA Jetson	ARM-alapú SoC	FPGA
Fő felhasználás	Gépi tanulás, képfeldolgozás, AI	Lokális vezérlés, szenzorfeldolgozás	Jelfeldolgozás, biztonsági logika
Számítási teljesítmény	Nagyon magas (GPU + CPU)	Közepes	Rugalmasan skálázható
Késleltetés	Közepes	Alacsony	Nagyon alacsony (µs szint)
Energiafogyasztás	Magasabb	Alacsony	Változó (alacsonytól közepesig)
Fejlesztési nehézség	Közepes	Alacsony	Magas (HDL programozás szükséges)
Valós idejű működés	Korlátozott (RT támogatás szükséges)	Igen (RTOS-szel)	Igen (hardveres időzítők, determinisztikus)
Rugalmasság / testreszabás	Közepes	Korlátozott	Nagyon magas
Használati példák	Neurális hálók, útvonaltervezés	Szenzorvezérlés, egyszerű logika	Objektumészlelés, watchdog, redundancia

5. Szoftveres környezet és operációs rendszerek

Az önvezető járművekben működő rendszerek komplexitása nem csupán hardveres szinten jelent kihívást, hanem a szoftveres környezet kialakításánál is. A szenzorok vezérlésétől kezdve a valós idejű döntéshozatalig minden komponens valamilyen operációs rendszer alatt fut. Az alábbiakban bemutatjuk a két legfontosabb OS-kategóriát, valamint azok működését a gyakorlatban.

RTOS vs Linux: mikor melyiket?
Az **RTOS** (Real-Time Operating System) és a **Linux** eltérő célokat szolgál az önvezető rendszerekben:

Jellemző	RTOS (pl. FreeRTOS, QNX)	Linux (pl. Ubuntu, Yocto, ROS2)
Determináltság	Garantált időzítés, kiszámítható működés	Nem valós idejű, de gyors és rugalmas
Használat	Szenzorvezérlés, biztonságkritikus modulok	Neurális hálók, adatfeldolgozás, UI
Futási környezet	Kis memória- és CPU-igény, bare-metal is lehet	Nagyobb teljesítményű rendszerek
Tipikus helye a járműben	Mikrovezérlők, aktuatorkezelés	Központi számítási egység (pl. Jetson)

Példa: a fékrendszer működtetését nem lehet késleltetni vagy újraütemezni, így azt RTOS alapú vezérlőre bízzák. Ezzel szemben a kameraadatok feldolgozása egy Linux-alapú gépen (pl. NVIDIA Jetson) történik.

5.2Feladatütemezés, prioritás és hibakezelés

RTOS-ekben a feladatütemezés szigorúan **prioritásalapú**. A magasabb prioritású feladatok mindig megelőzik az alacsonyabbakat, így biztosítva a kritikus események (pl. akadályészlelés, vészfék parancs) azonnali feldolgozását. Egyes RTOS-ek (pl. QNX, VxWorks) támogatják a **determinista válaszidőt és időalapú feladatütemezést**, ami elengedhetetlen a jármű biztonságos működéséhez.
Linux esetén a szabványos kernel nem garantál valós idejű válaszidőt. Azonban léteznek **valós idejű kiegészítések** (pl. PREEMPT_RT patch), amelyek segítségével valós idejű viselkedés közelíthető meg. A ROS2 (Robot Operating System 2) már képes valós idejű alkalmazások kiszolgálására is, RT-alapú backenden (pl. DDS).
A **hibakezelés** kulcsfontosságú: RTOS-ekben gyakori a watchdog-mechanizmus használata, amely figyeli, hogy minden modul megfelelően működik-e. Linuxos rendszerekben a hibatűrés gyakran szoftveres redundancián és naplózás-alapú újraindításon alapul.

6. Szenzoradat-feldolgozás és döntéshozatal

Az önvezető járművek képességei nagymértékben múlnak azon, hogy milyen hatékonyan képesek a különböző érzékelőik által gyűjtött adatokat feldolgozni és ezekből pontos döntéseket hozni. Mivel egy-egy jármű többféle szenzort használ egyszerre (kamera, LiDAR, radar, ultrahang), ezért elengedhetetlen a szenzoradatok **összehangolt feldolgozása** és a lehető legjobb környezeti modell felépítése.

6.2Szenzorfúzió: többféle szenzor összehangolása

Az egyes érzékelők különböző tulajdonságokkal bírnak:

Szenzor	Előny	Hátrány
Kamera	Színes, részletgazdag kép	Érzékeny fényviszonyokra
LiDAR	Precíz 3D térkép	Drága, mozgó alkatrészek
Radar	Megbízható rossz időben is	Alacsony felbontás

Szenzorfúzió során ezek adatait kombinálják, hogy a jármű pontosabb képet kapjon a környezetéről. A fúzió célja például:

- Objektumazonosítás (kamera + LiDAR kontúregyeztetés),
- Sebességbecslés (radar + kamera mozgáselemzés),
- Akadálydetektálás és követés.

A fúziós algoritmusok valós időben dolgoznak, gyakran **Kalman-szűrőket**, **Bayes-alapú** vagy **mélytanuló hálózatokat** alkalmaznak.

6.3Algoritmusok és neurális hálók beágyazott rendszeren

Az objektumfelismerést és döntéshozatalt sok esetben **neurális hálók** végzik, mint például:

- **YOLO** (You Only Look Once) – valós idejű objektumfelismerés,
- **SegNet / ENet** – útburkolat-érzékelés és sávkövetés,
- **PointNet** – 3D pontfelhőből való elemzés LiDAR adatokra.

Ezek a modellek futtatása **erőforrásigényes**, azonban ma már léteznek **beágyazott platformokra optimalizált verziók**, például TensorRT (NVIDIA Jetson) vagy OpenVINO (Intel alapú rendszerekhez).
Az önvezető járművekben a döntéshozatalhoz sokszor kombinált megközelítést használnak:

- gépi tanulás → objektumazonosítás, helyzetbecslés,
- szabályalapú logika → prioritások kezelése (pl. gyalogos vs jármű),
- predikciós algoritmusok → más járművek mozgásának előrejelzése.

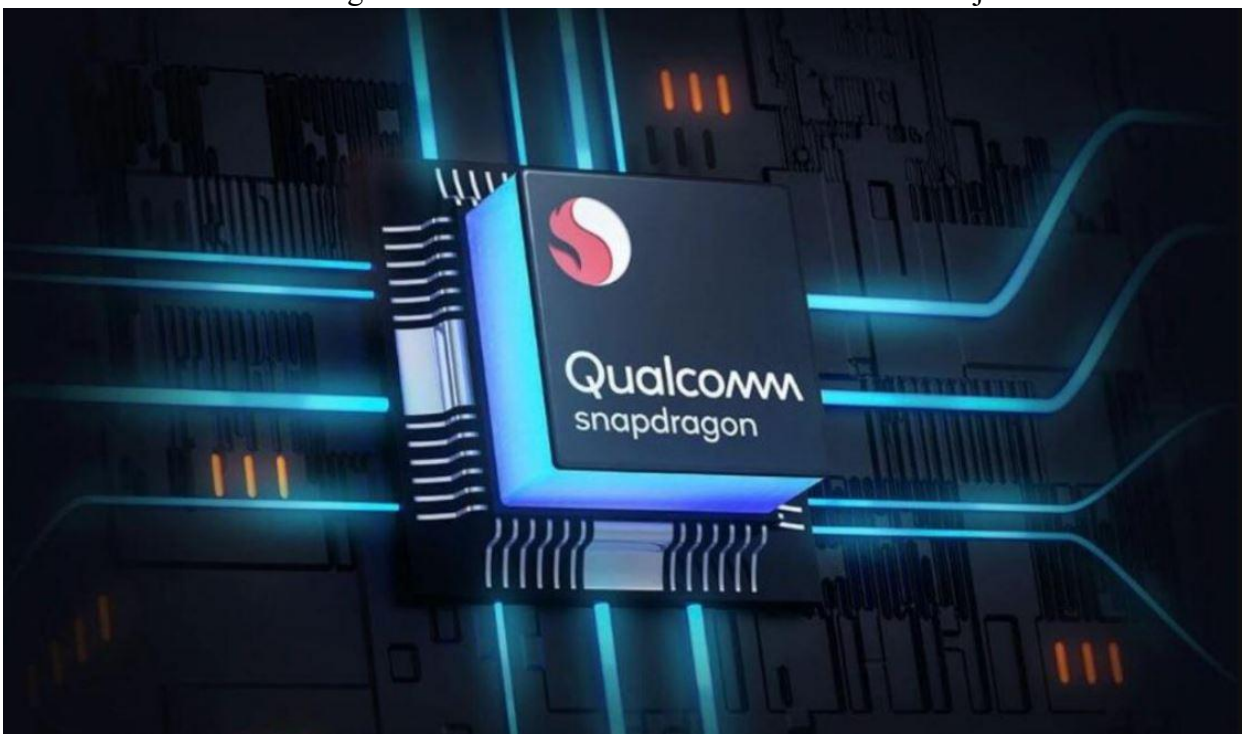
6.4Edge computing szerepe

A **feldolgozás helye** kulcsfontosságú. A „klasszikus” megoldásokban az adatok továbbítása felhőbe történik, de az önvezetésben ez **késleltetés és megbízhatóság szempontjából nem elfogadható**. Ezért használják a **helyi (onboard) feldolgozást**, amit **edge computing**-nak nevezünk.

Az edge computing előnyei:

- **Valós idejű reakciók**: nincs hálózati késleltetés,
- **Adatvédelem**: nem kell az érzékeny nyers adatokat továbbítani,
- **Energiahatékonyság**: kevesebb adatmozgatás,
- **Autonómia**: akkor is működik, ha nincs hálózat.

Az ilyen feldolgozás tipikus platformjai: **NVIDIA Jetson Xavier**, **Qualcomm Snapdragon Ride**, **Intel Mobileye** – ezek mind olyan **beágyazott rendszerek**, amelyek képesek neurális hálókat és szenzorfúziós algoritmusokat valós időben futtatni közvetlenül a járművön.



. 5 ábra Quallcomm Snapdragon https://napidroid.hu/qualcomm-snapdragon-780g-hivatalos/

7. Biztonság és hibatűrés

Az önvezető járművek rendkívül összetett rendszerek, ahol a biztonság (safety) és a hibatűrés (fault tolerance) alapvető követelmények. Egy hiba nemcsak az utasok életét, hanem a közlekedés többi résztvevőjét is veszélyeztetheti. Ezért a beágyazott rendszerek szintjén több biztonsági megoldást is alkalmaznak.

7.2Watchdog rendszerek és fail-safe mechanizmusok

A watchdog rendszer egy egyszerű, de hatékony eszköz: folyamatosan figyeli a rendszer működését, és ha az adott időn belül nem kap visszajelzést (pl. „élek” jelzést), akkor automatikusan újraindítja a hibás egységet vagy vált biztonságos üzemmódba. Tipikus példák:

- Ha a képfeldolgozó modul lefagy, a watchdog újraindítja azt,
- Ha a döntéshozó logika nem válaszol időben, a rendszer automatikusan megállítja a járművet.

Fail-safe megoldás például az, hogy a jármű képes egy minimálfunkciós „vészüzemmódra”, ahol csak leáll vagy félrehúzódik.

7.3Redundancia és hibatűrés

A nagy megbízhatóság érdekében **többszörös redundanciát** alkalmaznak:

- **Szenzorredundancia**: többféle szenzor (kamera + LiDAR + radar) ugyanazt a tárgyat figyeli,
- **Feldolgozási redundancia**: párhuzamos hardverplatformok (pl. fő vezérlő + biztonsági backup),
- **Energiaellátás redundancia**: külön áramkörök a kritikus rendszerekhez.

A rendszer akkor is képes tovább működni, ha az egyik komponens meghibásodik (graceful degradation).

7.4 Kiberbiztonság beágyazott szinten

Az önvezető járművek egyre inkább hálózatba kapcsoltak (pl. V2X), így a **kiberbiztonság** kulcsfontosságú.

- **Biztonságos bootolás** (Secure Boot): csak ellenőrzött szoftver indulhat el,
- **Titkosított kommunikáció** (pl. TLS, IPsec),
- **Hardverszintű védelem**: Trusted Platform Module (TPM), biztonságos kulcstárolás.

A cél, hogy külső támadások (pl. CAN-busz manipuláció, távoli hozzáférés) ne okozhassanak irányításvesztést.

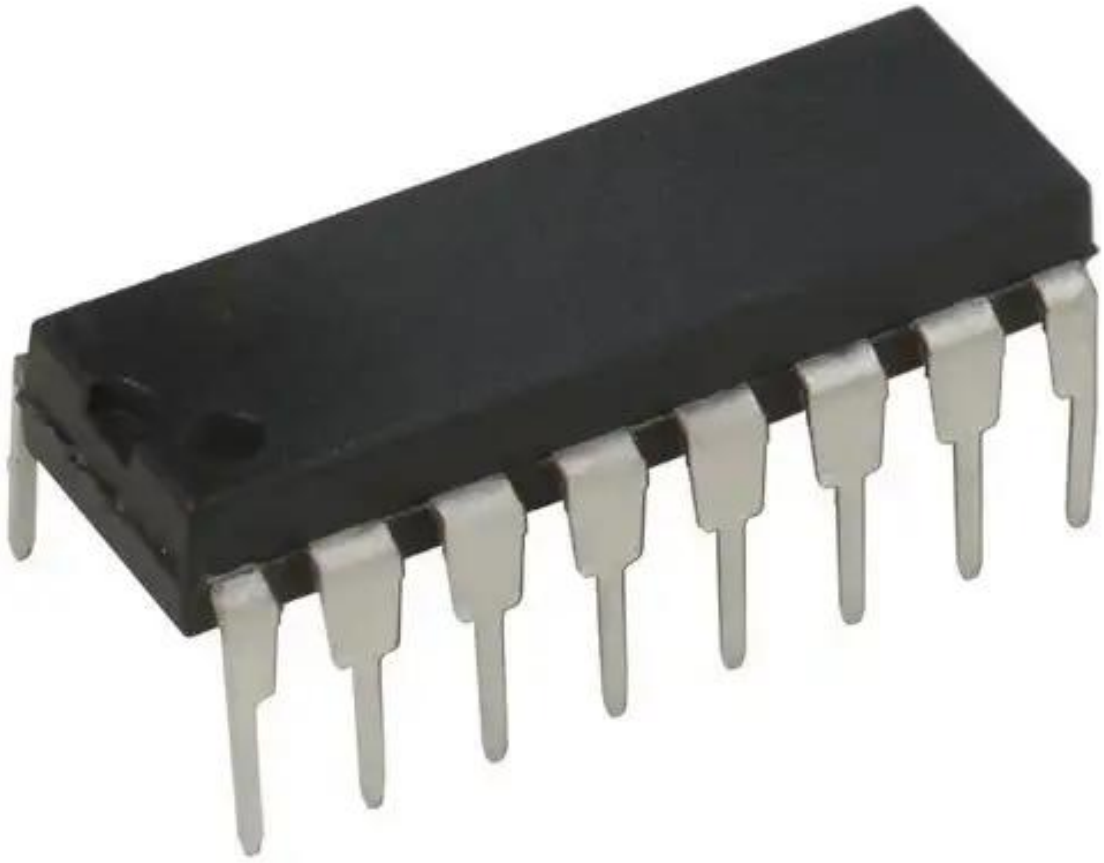
7.5Rendszerhitelesítés és szabványok

A járműiparban szigorú szabványokat kell követni:

- ISO 26262 – Funkcionális biztonság beágyazott rendszerekben,
- ASIL (Automotive Safety Integrity Level) – a funkciók biztonsági kritikus szintjeit osztályozza (A–D szintig),
- ISO/SAE 21434 – Kiberbiztonság járművekben.

Ezek a szabványok megkövetelik például:

- formális verifikációt a szoftverekre,
- szoftvertesztelést valós helyzetekkel,



6. ábra Watchdog egység-
https://www.elektrobot.hu/termek.php?filename=5824.html&i=5824

8. Kommunikációs rendszerek integrációja

Az önvezető járművek működéséhez elengedhetetlen a különböző komponensek közötti **gyors, megbízható és valós idejű kommunikáció**. A modern járművekben számos hálózati protokoll együttesen működik, különböző célokra optimalizálva. Ezeket egy átfogó rendszerbe kell integrálni.

8.2 CAN busz – bevált megoldás

A **Controller Area Network (CAN)** egy iparági szabvány, amelyet a legtöbb járműben használnak az **ECU-k (vezérlőegységek)** közötti kommunikációra. Előnyei:

- Egyszerű, olcsó, megbízható,
- Üzenetközpontú (nem pont-pont alapon működik),
- Általában ≤ 1 Mbit/s sebességű,

- Valós idejű jellemzőkkel rendelkezik, de csak korlátozott sávszélességgel.

Alkalmas például az olyan időkritikus, de alacsony sávszélességű adatokhoz, mint a motorvezérlés vagy a fékrendszer jelei.

8.3 Ethernet – nagy sávszélességű kommunikáció

Az **automotive Ethernet** új generációs protokollként jelent meg az önvezető rendszerekben, mivel:

- Több Gbit/s adatátviteli sebességet is támogat,
- Alkalmas nagy adatforgalmú komponensekhez (pl. kamera- vagy LiDAR-stream),
- Támogatja a **valós idejű adatátvitelt** is, ha megfelelő kiterjesztéseket használnak.

8.4 TSN – Time-Sensitive Networking

A **TSN (Időérzékeny Hálózat)** az Ethernet kiterjesztése, amely garantált **időzítést és determinisztikus viselkedést** biztosít:

- Adatcsomagok időalapú ütemezése (pl. 1 ms-os ciklusidők),
- Prioritáskezelés, késleltetési garanciák,
- Kulcsfontosságú a **szenzorfúzió**, **aktuátorvezérlés** és a **valós idejű döntéshozatal** esetén.

A TSN-t gyakran használják a fedélzeti Ethernet-hálózatban a kritikus komponensek (pl. biztonsági vezérlők, érzékelő aggregátorok) közötti kommunikációra.

Integráció kihívásai

A CAN, Ethernet és TSN protokollokat együttesen kell kezelni egy teljes járműarchitektúrában. Tipikus megközelítése:

- **Gateway-ek** alkalmazása a különböző protokollok közötti átalakításra,
- **QoS (Quality of Service)** beállítások a kommunikációs prioritás szabályozására,
- **Valós idejű operációs rendszer (RTOS)** vagy middleware réteg az időzítések biztosítására.

8.5Hogyan csatlakoznak ezek a rendszerek az autó belső hálózatához?

Az önvezető járművek belső hálózata több szintből áll, melyek különféle célokra szolgálnak. A rendszerek (szenzorok, vezérlők, aktuátorok) specifikus buszokon keresztül kapcsolódnak a hálózathoz az alábbi elvek szerint:

CAN busz – alacsony sávszélességű, de időkritikus rendszerekhez

- A **motorvezérlő egységek (ECU)**, **ABS**, **légzsák-vezérlők**, stb. jellemzően a CAN hálózaton keresztül kommunikálnak.
- Ezek kis adatcsomagokat küldenek, de nagy megbízhatósággal és időzítéssel.
- Tipikus sávszélesség: 125 kbps – 1 Mbps.

Ethernet – nagy adatigényű eszközökhöz

- **Kamerák**, **LiDAR**, **radar**, és a központi feldolgozó egységek Etherneten kapcsolódnak a hálózathoz.
- Ez lehetővé teszi a nagy felbontású képadatok, szenzorfúziós információk valós idejű átvitelét.
- Sávszélesség: 100 Mbps – 10 Gbps, típustól függően.
- Ezek általában switch-eken keresztül kapcsolódnak össze.

TSN (Time-Sensitive Networking) – valós idejű determinisztikus adatátvitel

- A kritikus rendszerek (pl. vezérlő és fékmodul, aktuátorvezérlő, biztonsági backup CPU) között TSN-t használnak.
- TSN az Ethernetet egészíti ki időzítéssel, sávszélesség-garantálással és prioritásvezérléssel.
- A TSN lehetővé teszi, hogy a fontos adatcsomagok mindig időben megérkezzenek, még torlódás esetén is.

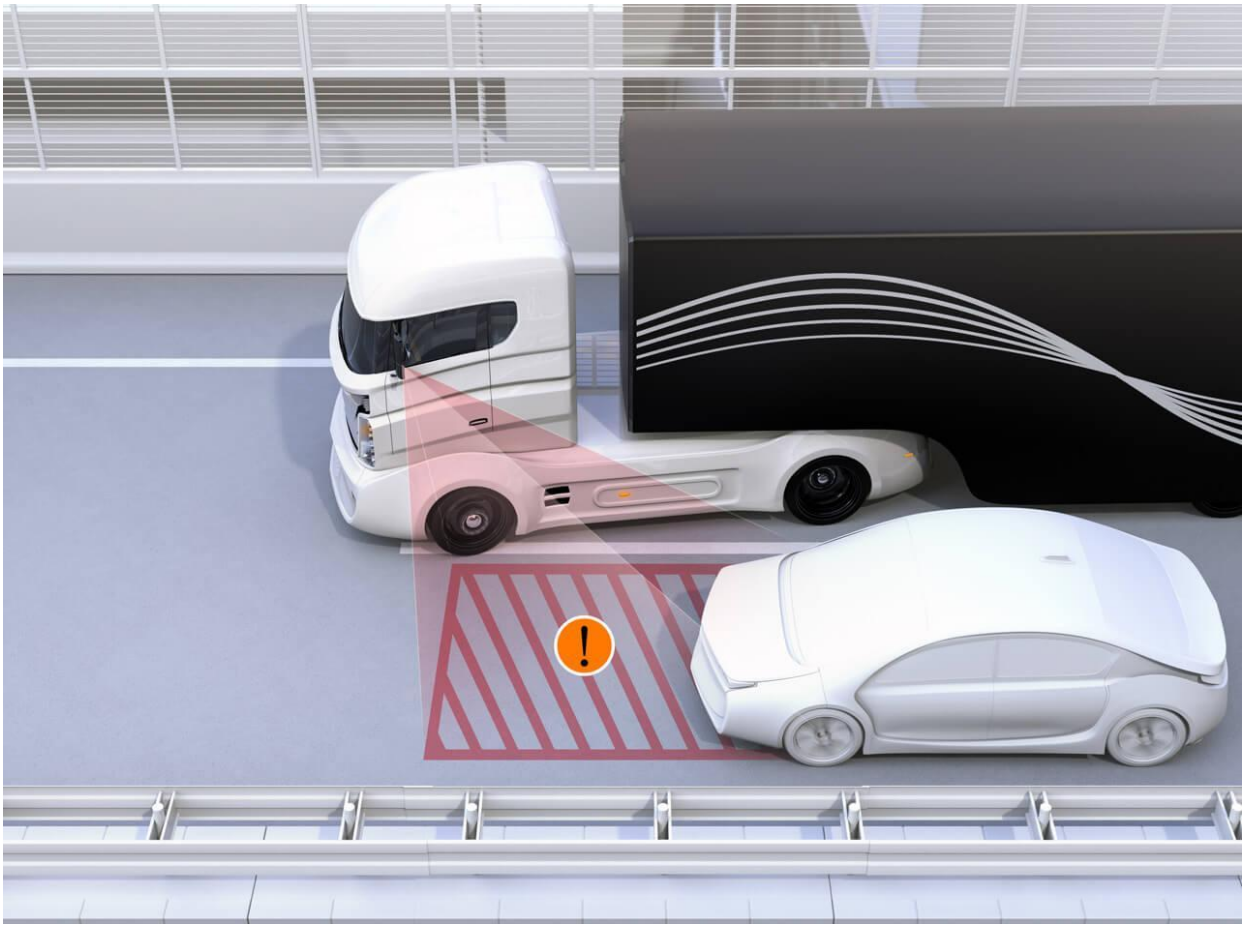
Gateway egységek – protokollok közötti kommunikáció biztosítása

Mivel az autó többféle buszt használ, gateway (átjáró) egységek felelnek azért, hogy:

- a CAN busz üzenetei eljussanak a központi feldolgozórendszerekbe,
- a TSN képes legyen átküldeni fontos adatokat másik Ethernet- vagy CAN-szegmensre,
- és biztosítsák a megfelelő prioritást és időzítést minden kommunikációs csatornán.

Példa: Egy kamera TSN-en keresztül

1. A kamera nagyfelbontású képeket küld → Ethernet interfész.
2. A bejövő adatot egy TSN-kompatibilis switch továbbítja a képfeldolgozó egység felé.
3. A rendszer garantálja, hogy a képek meghatározott időn belül beérkezzenek, pl. 33 ms ciklusidővel.
4. Ha szükséges, az eredmények CAN-en vagy TSN-en jutnak tovább a vezérlőrendszerhez.



7. ábra Önvezető jármű belső kommunikációs hálózata-https://boschblog.hu/tegyunk-rendet-az-onvezeto-autok-kozott/

9.Önvezető járművek előnyei és hátrányai

9.1Előnyök:

1. **Balesetek számának csökkenése**

   Az önvezető rendszerek nem fáradnak el, nem figyelmetlenek, nem vezetnek ittasan – ezzel a közlekedési balesetek többsége megelőzhető lenne.

2. **Optimalizált forgalom és üzemanyag-felhasználás**

   Az autonóm járművek összehangoltabban tudnak közlekedni, csökkentve a torlódásokat és a felesleges gyorsítás-lassítás miatti energia/pazarlást.

3. **Hozzáférés a közlekedéshez a mozgáskorlátozottak számára**

   Idősek, vakok vagy mozgássérültek is önállóan utazhatnak, ami nagyobb függetlenséget biztosít.

4. **Folyamatos működés**

   Az autonóm járművek nem igényelnek pihenőt, így logisztikában vagy taxiszolgáltatásban éjjel-nappal üzemelhetnek.

5. **Adatgyűjtés és gépi tanulás**

   A járművek által gyűjtött adatok segítik a rendszerek folyamatos tanulását és fejlődését (pl. veszélyes útviszonyok felismerése).

9.2Hátrányok:

1. **Technikai megbízhatóság és hibalehetőségek**

   A szoftverhibák, szenzorhibák vagy rossz döntési logika akár balesetet is okozhat. A felelősség kérdése is nehezen meghatározható (fejlesztő, gyártó, felhasználó?).

2. **Magas költségek**

   Az önvezető rendszerek fejlesztése és integrálása (LiDAR, AI chip-ek, redundáns rendszerek) jelenleg még drága.

3. **Etikai döntéshozatal problémái**

   Baleseti szituációkban nehéz előre programozni az "etikus" döntést – pl. kinek az életét mentse meg egy jármű vészhelyzetben?

4. **Kiberbiztonsági kockázatok**

   Az internetre csatlakoztatott járművek célpontjai lehetnek hackereknek – ez akár életveszélyes is lehet.

5. **Munkahelyek megszűnése**

   Kamionsofőrök, taxisok, futárok munkája feleslegessé válhat, ami társadalmi feszültségekhez vezethet.

10. Összegzés

Az önvezető járművek működése rendkívül összetett, és ennek a sikeressége nagyban múlik a **beágyazott rendszerek** fejlettségén és összehangolt működésén. Ezek a speciális számítógépes rendszerek végzik a jármű különböző érzékelőiből érkező adatok feldolgozását, így segítik elő, hogy a jármű pontosan és biztonságosan tudjon közlekedni. A beágyazott rendszerek nélkül nem lenne lehetséges a valós idejű, gyors döntéshozatal, ami az önvezetés alapja.

Fontos megemlíteni a kommunikációs hálózatokat is, amelyek összekötik a jármű különböző részeit. A CAN, Ethernet és az újabb TSN protokollok biztosítják, hogy az információk időben és megbízhatóan jussanak el a megfelelő egységekhez. Ez a gyors és stabil adatcsere kritikus a biztonság és a hatékonyság szempontjából.

A hardverek – mint az NVIDIA Jetson vagy az ARM alapú processzorok – biztosítják a szükséges számítási kapacitást, hogy az összetett algoritmusok, például a mesterséges intelligencia és a képfeldolgozás zavartalanul fussanak. Ezek a platformok együttesen lehetővé teszik az önvezető funkciók magas szintű működését.

Nem szabad elfelejteni a biztonság fontosságát sem: a watchdog rendszerek, redundáns megoldások és a kiberbiztonsági protokollok segítenek abban, hogy a jármű megbízhatóan működjön, és a hibák vagy támadások esetén is megvédje az utasokat és a környezetet.

A jövőben további fejlődés várható az önvezető technológiák terén, különösen az edge computing, a mesterséges intelligencia és a hálózati kommunikáció területén. Emellett a szabványosítás és a biztonsági előírások fejlesztése is kiemelt szerepet kap majd, hogy az önvezető járművek még szélesebb körben, biztonságosan és hatékonyan használhatók legyenek.

Összességében a beágyazott rendszerek központi szerepe megkerülhetetlen az önvezető járművek működésében, és ezek fejlesztése adja meg az alapot a jövő közlekedésének biztonságos és intelligens irányításához.

Irodalomjegyzék:

[1] Patrik Viktor. (2024). Az önvezető technológia gazdasági aspektusai. Óbudai Egyetem.

https://bdi.uni-obuda.hu/wp-content/uploads/2024/03/Ertekezestervezet-Viktor-Patrik.pdf

[2] Szegedi Tudományegyetem. (2020). Autonóm járművek – Workshop-sorozat.

https://jkk-web.sze.hu/wp-content/uploads/2021/11/AUTONOM_Workshop_2020_Konferenciakiadvany_2021_final_web.pdf

[3] BME IKT Tanszék. (n.d.). Önvezetés, újratöltve. Bosch Magyarország IoT Blog. https://iot.boschblog.hu/mobilitas/onvezetes-ujratoltve/

[4] BME VIK MSc Program. (2023). Hálózatok főspecializáció (HIT).

https://vik.bme.hu/document/6384/original/VIK_MSc_program_V53.pdf

[5] Infotér. (2017). Mit jelent a valós idejű operációs rendszer a gyakorlatban?

https://infoter.eu/technologia/mit-jelent-a-valos-ideju-operacios-rendszer-a-gyakorlatban

[6] Visure Solutions. (2023). Mi az ISO 26262 Funkcionális biztonsági szabvány az autóiparban? https://visuresolutions.com/hu/automotive/iso-26262/

[7] Traffix. (2023). A vezető nélküli autók biztonságosabbak, mint az emberek által vezetettek. https://www.traffix.hu/blog/posts/820

[8] Műszaki Magazin. (2025). Mi hiányzik ahhoz, hogy kizárólag önvezető járművekkel közlekedjünk? https://www.muszaki-magazin.hu/2025/05/15/onvezeto-jarmuvek-jovo-kozlekedes/

2.24. Az 5G hálózatok alkalmazása CPS keretrendszerekben

Az 5G hálózatok alkalmazása CPS keretrendszerekben

Szerző: Gáspár István

Az 5G hálózatok és a kiber-fizikai rendszerek (CPS) integrációja napjaink egyik legdinamikusabban fejlődő technológiai területe, amely alapjaiban változtatja meg az ipari automatizáció, a városi infrastruktúrák és a kritikus rendszerek működtetését. A tanulmány átfogóan bemutatja ezt a konvergenciát, feltárva mind a technológiai alapokat, mind a gyakorlati alkalmazási lehetőségeket, kiemelve a magyarországi kutatás-fejlesztési eredményeket és ipari implementációkat.

Bevezetés

A digitalizáció folyamatos előrehaladásával a fizikai és digitális világ között egyre szorosabb kapcsolat alakul ki, amit kiber-fizikai rendszereknek (Cyber-Physical Systems, CPS) nevezünk. Ezek a rendszerek integrálják a fizikai folyamatokat az informatikai infrastruktúrával, lehetővé téve a valós idejű adatgyűjtést, elemzést és beavatkozást. A CPS rendszerek hatékony működéséhez elengedhetetlen a megbízható, alacsony késleltetésű és nagy sávszélességű kommunikáció, amit az 5G technológia képes biztosítani.

Az 5G hálózatok jelentős előrelépést jelentenek a mobilkommunikációban a korábbi generációkhoz képest. Az alacsony késleltetés (akár 1 ms alatti), a nagy sávszélesség (akár 10 Gbps) és a hálózatszeletelés (network slicing) képessége ideálissá teszi az 5G-t a CPS alkalmazások számára[3]. A technológia lehetővé teszi, hogy a különböző alkalmazások számára dedikált, virtualizált hálózati szegmenseket hozzunk létre, amelyek megfelelnek a specifikus teljesítménykövetelményeknek.

E tanulmány célja részletesen bemutatni az 5G hálózatok és a CPS rendszerek integrációjának lehetőségeit, kihívásait és alkalmazási területeit. Kitérünk a technológiai alapokra, a kommunikációs protokollokra, a biztonsági kérdésekre, valamint a gyakorlati alkalmazásokra az ipar, az energetika és a közlekedés területén. Külön figyelmet fordítunk a magyarországi kutatási eredményekre és implementációs példákra, kiemelve a Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) és hazai vállalatok szerepét az 5G-CPS ökoszisztéma fejlesztésében.

A tanulmány felépítése

A tanulmány első részében az elméleti hátteret tárgyaljuk, bemutatva az 5G technológia és a CPS rendszerek alapjait, valamint konvergenciájuk lehetőségeit. Ezt követően részletesen elemezzük az 5G-CPS integráció technológiai alapjait, beleértve a hálózati architektúrát és a kommunikációs protokollokat. A harmadik részben a valós idejű kommunikációs protokollokat vizsgáljuk, különös tekintettel a Time-Sensitive Networking (TSN), Ultra-Reliable Low-Latency Communication (URLLC) és OPC UA technológiákra. A negyedik részben a biztonsági kihívásokat és megoldásokat tárgyaljuk, míg az ötödik részben az alkalmazási területeket mutatjuk be. A hatodik részben a magyarországi vonatkozásokat és esettanulmányokat elemezzük, a hetedik részben pedig a jövőbeli fejlesztési irányokat vázoljuk fel. Végül összegezzük a tanulmány legfontosabb megállapításait.

I. Az 5G technológia alapjai

Az ötödik generációs (5G) mobilhálózatok alapvető célja a kommunikációs kapacitás növelése, a válaszidők drasztikus csökkentése, valamint a hálózat megbízhatóságának fokozása. Az 5G három fő technológiai pillére:

1. eMBB (enhanced Mobile Broadband) – nagy adatátviteli sebességet biztosít, főleg okoseszközök és tartalomfogyasztás esetén.
2. URLLC (Ultra-Reliable Low-Latency Communications) – rendkívül alacsony késleltetést és magas megbízhatóságot tesz lehetővé, pl. autonóm járművek vagy ipari robotika esetén.
3. mMTC (massive Machine-Type Communications) – nagyszámú eszköz egyidejű kommunikációját támogatja, például szenzorhálózatokban vagy okosvárosokban.

Az 5G technológia alapját olyan fejlesztések adják, mint a milliméteres hullámhossz (mmWave), több antenna (MIMO) rendszerek, hálózatszeletelés (network slicing), és szoftver-alapú hálózati architektúra (SDN/NFV). Kiber-fizikai rendszerek (CPS) definíciója és tulajdonságai:

A kiber-fizikai rendszerek (CPS) olyan integrált rendszerek, amelyek szorosan összekapcsolják a számítási és kommunikációs képességeket a fizikai komponensekkel és folyamatokkal. A CPS rendszerek lehetővé teszik a fizikai világ valós idejű érzékelését, monitorozását és irányítását[1][2].

II. A kiberfizikai rendszerek (CPS) architektúrája

A kiberfizikai rendszerek (Cyber-Physical Systems, CPS) olyan integrált rendszerek, amelyek fizikai folyamatokat, szenzorokat, beavatkozókat és digitális vezérlőrendszereket kapcsolnak össze valós idejű kommunikációval. Ezek az összetett rendszerek képesek az érzékelt adatok alapján önálló döntések meghozatalára, miközben folyamatosan alkalmazkodnak a változó környezethez.

A CPS rétegei:

1. Fizikai réteg (Physical Layer): Szenzorok, aktuátorok, gépek – ezek a valós világban működnek.
2. Hálózati réteg (Network Layer): A különféle komponensek közötti kommunikáció biztosítása (pl. vezeték nélküli kapcsolat, IoT).
3. Kiber (digitális) réteg (Cyber Layer): Az adatfeldolgozás, algoritmusok, vezérlőlogikák, mesterséges intelligencia működése.
4. Emberi interfész (Human-Machine Interface): A felhasználó és rendszer közötti kapcsolat. A CPS rendszerek alapvető alkotóelemei közé tartoznak az érzékelők, amelyek adatokat gyűjtenek a fizikai környezetről; az aktuátorok, amelyek fizikai beavatkozást tesznek lehetővé; a kommunikációs hálózat, amely összeköti az összes komponenst; valamint a számítási komponensek, amelyek feldolgozzák az adatokat és irányítják a rendszer működését[3][2].

III. Az 5G és CPS konvergenciája

Az 5G és a CPS rendszerek konvergenciája számos új lehetőséget teremt az intelligens rendszerek fejlesztésére és implementálására. Az 5G technológia képes kielégíteni a CPS rendszerek

kommunikációs igényeit, különösen a nagy megbízhatóságú, alacsony késleltetésű és nagy sávszélességű kapcsolatok tekintetében[3][4].

A konvergencia főbb szempontjai:

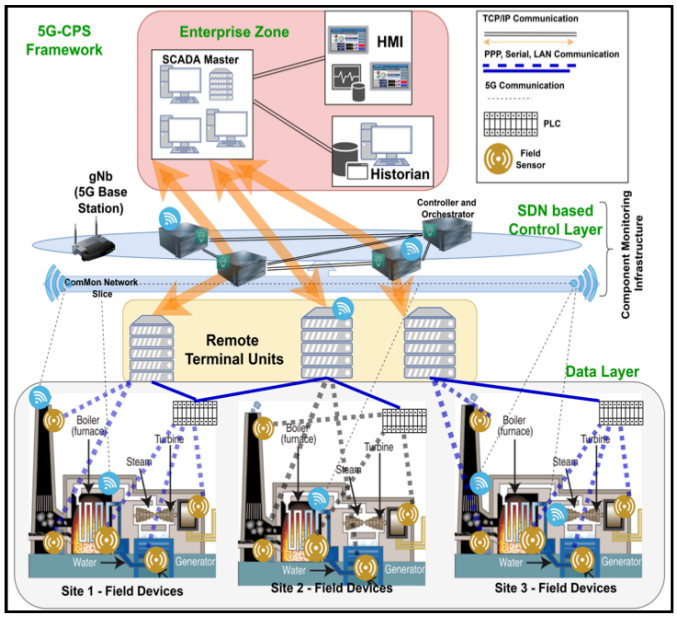
1. Kommunikációs infrastruktúra: Az 5G biztosítja a szükséges kommunikációs infrastruktúrát a CPS rendszerek számára, lehetővé téve a valós idejű adatgyűjtést, feldolgozást és irányítást[3][4].

2. Edge computing: Az 5G architektúra támogatja az edge computing koncepcióját, amely lehetővé teszi az adatok feldolgozását a hálózat szélén, csökkentve a késleltetést és a sávszélesség-használatot[4][3].

3. Heterogén hálózatok integrációja: Az 5G képes integrálni a különböző típusú hálózatokat (vezetékes, vezeték nélküli, rövidtávú, stb.), megkönnyítve a CPS rendszerek kommunikációját különböző környezetekben[3][12].

4. Szolgáltatásminőség (QoS): Az 5G hálózatszeletelés képessége lehetővé teszi a különböző CPS alkalmazások számára optimalizált kapcsolatok biztosítását, prioritizálva a kritikus funkciókat[3][12].

5. Skálázhatóság és rugalmasság: Az 5G támogatja a nagy számú eszköz csatlakoztatását és képes alkalmazkodni a változó hálózati igényekhez, ami kulcsfontosságú a dinamikus CPS környezetekben[6][3].



Az 1. ábra bemutatja az 5G és CPS rendszerek konvergenciájának általános keretrendszerét, kiemelve a fő komponenseket és a közöttük lévő kapcsolatokat.

IV. Az 5G-CPS integráció technológiai alapjai

i. 5G hálózati architektúra

Az 5G hálózati architektúra alapvetően különbözik a korábbi generációs mobilhálózatoktól, rugalmasabb, skálázhatóbb és hatékonyabb működést biztosítva. A modern 5G architektúra szolgáltatás-alapú megközelítést alkalmaz, virtualizált hálózati funkciókat használ, és támogatja a hálózati szeletelést[3][5].

ii. Az 5G hálózat fő komponensei:

1. Radio Access Network (RAN): A RAN kezeli a vezeték nélküli kommunikációt a felhasználói eszközök (UE) és a hálózat között. Az 5G RAN az új rádió (NR) technológiát használja, amely magasabb frekvenciákat is támogat, és fejlettebb antenna-technológiákat alkalmaz, például a masszív MIMO-t (Multiple-Input Multiple-Output)[3].

2. 5G Core Network: A maghálózat kezeli a mobilitást, a hitelesítést, a biztonsági funkciókat és az adatáramlást. Az 5G Core Network teljesen újratervezett a korábbi generációkhoz képest, és szolgáltatás-alapú architektúrát (SBA) alkalmaz, amely rugalmasabb és könnyebben bővíthető[5].

3. User Plane Function (UPF): Az UPF felelős az adatcsomag-továbbításért, a QoS kezelésért és a külső hálózatokkal való összekapcsolásért. Több UPF telepíthető különböző helyeken a hálózatban a forgalom optimalizálása érdekében[5].

4. Network Functions: Az 5G hálózati funkciók virtualizáltak és mikroszolgáltatásokként vannak megvalósítva, ami lehetővé teszi a rugalmas méretezést és telepítést. Ide tartoznak az AMF (Access and Mobility Management Function), SMF (Session Management Function), PCF (Policy Control Function) és mások[5].

Az 5G hálózati architektúra egyik kulcsfontosságú képessége a hálózatszeletelés. Ez lehetővé teszi, hogy a fizikai hálózatot több virtuális hálózatra osszuk, amelyek mindegyike különböző szolgáltatásokra vagy alkalmazásokra optimalizált. Például, létrehozhatunk egy ultra-megbízható, alacsony késleltetésű szeletet az ipari automatizáció számára, és egy másik szeletet a nagy sávszélesség-igényű videóstreaming számára[4][12].

V. Kommunikációs protokollok 5G-ben

Az 5G hálózatok különböző kommunikációs protokollokat támogatnak a különböző alkalmazási igények kielégítésére. A CPS rendszerekkel való integráció szempontjából különösen fontosak az alábbi protokollok:

1. URLLC (Ultra-Reliable Low-Latency Communication): Az URLLC az 5G egyik kulcsfontosságú szolgáltatása, amely rendkívül megbízható és alacsony késleltetésű kommunikációt biztosít. Az URLLC célja a közel 100%-os megbízhatóság biztosítása 1 ms alatti késleltetéssel, ami elengedhetetlen a kritikus ipari alkalmazások, autonóm járművek és távoli műtétek esetében[3][5].

2. TSN (Time-Sensitive Networking) integráció 5G-vel: A TSN egy IEEE szabványkészlet, amely determinisztikus adatátvitelt biztosít Ethernet hálózatokon. Az 5G-TSN integráció lehetővé teszi a TSN szolgáltatások kiterjesztését vezeték nélküli környezetekre. Az 5G rendszer TSN-kompatibilis virtuális Ethernet-TSN hidakként működik, támogatva az időszinkronizációt, a forgalomütemezést és a prioritizálást[3][12].

3. OPC UA over 5G: Az OPC Unified Architecture (UA) egy ipari kommunikációs protokollszabvány, amely platformfüggetlen, biztonságos és skálázható adatcserét biztosít. Az OPC UA 5G hálózatokon keresztüli használata lehetővé teszi a rugalmas és megbízható ipari kommunikációt, különösen a PubSub (publikálás-feliratkozás) kommunikációs modell alkalmazásával[11].

4. MQTT (Message Queuing Telemetry Transport): Az MQTT egy könnyűsúlyú, publikálás-feliratkozás alapú üzenetküldési protokoll, amely ideális az IoT alkalmazásokhoz. Az 5G hálózatokon futó MQTT javítja a csatlakoztathatóságot és a megbízhatóságot az IoT eszközök széles skálája számára[11].

5. 5G NR (New Radio) specifikus ipari profilok: Az 5G NR számos speciális ipari profilt kínál, amelyek optimalizáltak bizonyos alkalmazási esetekre, például a gyártásra, energiahálózatokra és logisztikára[3][4].

VI. CPS architektúrák és komponensek

A CPS rendszerek architektúrája általában több, egymással összefüggő réteget tartalmaz, amelyek együttesen teszik lehetővé a fizikai és a kiber világ integrációját[1][2]. Az 5G-vel integrált CPS architektúrák főbb komponensei:

1. Érzékelő és aktuátor réteg: Ez a réteg tartalmazza a fizikai környezettel közvetlenül interakcióba lépő eszközöket. Az érzékelők adatokat gyűjtenek (hőmérséklet, nyomás, mozgás, stb.), míg az aktuátorok fizikai beavatkozást tesznek lehetővé (motorok, szelepek, kapcsolók működtetése)[2].

2. Kommunikációs réteg: Ez a réteg biztosítja az adatátvitelt a különböző komponensek között. Az 5G technológia kulcsszerepet játszik ebben a rétegben, biztosítva a nagy sebességű, alacsony késleltetésű és megbízható kapcsolatot[12][3].

3. Edge computing réteg: Ez a réteg lehetővé teszi az adatok feldolgozását a hálózat szélén, közel az adatforráshoz. Az edge computing csökkenti a késleltetést, a sávszélesség-használatot, és lehetővé teszi a valós idejű feldolgozást[4][3].

4. Felhő réteg: A felhő biztosítja a további számítási kapacitást, a hosszú távú adattárolást és a fejlett elemzési képességeket. A felhő és az edge computing együttműködése fontos a modern CPS architektúrákban[4][2].

5. Alkalmazási réteg: Ez a réteg tartalmazza a végfelhasználói alkalmazásokat és szolgáltatásokat, amelyek felhasználják a CPS infrastruktúra által gyűjtött és feldolgozott adatokat[2].

VII. Valós idejű kommunikációs protokollok 5G-CPS rendszerekben

i. Time-Sensitive Networking (TSN)

A Time-Sensitive Networking (TSN) egy IEEE szabványkészlet, amely determinisztikus adatátvitelt biztosít Ethernet hálózatokon. A TSN kulcsfontosságú a valós idejű ipari alkalmazások számára, ahol a pontos időzítés és a garantált adatátvitel elengedhetetlen[3][12].

ii. A TSN főbb jellemzői:

1. Időszinkronizáció: A TSN az IEEE 802.1AS (gPTP) szabványt használja a pontos időszinkronizáció biztosításához a hálózat minden eszköze között, ami elengedhetetlen a determinisztikus működéshez[3][12].

2. Forgalomütemezés: A TSN különböző ütemezési mechanizmusokat kínál, például az időalapú ütemezést (IEEE 802.1Qbv) és a keretpriorizálást (IEEE 802.1Qav), amelyek garantálják a kritikus adatok időben történő továbbítását[3].

3. Redundancia és megbízhatóság: A TSN támogatja a redundáns útvonalakat és a hibatoleráns mechanizmusokat (IEEE 802.1CB), amelyek biztosítják a kommunikáció folytonosságát még hálózati hibák esetén is[12].

4. Az 5G és TSN integrációja lehetővé teszi a determinisztikus kommunikáció kiterjesztését vezeték nélküli környezetekre. Az 5G rendszer TSN-kompatibilis virtuális Ethernet-TSN hidakként működik, támogatva az időszinkronizációt, a forgalomütemezést és a prioritizálást[3][12].

iii. Az integráció főbb szempontjai:

1. 5G TSN híd funkció: Az 5G rendszer IEEE-kompatibilis virtuális Ethernet-TSN hidakként működik, lehetővé téve a zökkenőmentes integrációt a meglévő TSN hálózatokkal[12].

2. Időszinkronizáció: Az 5G rendszer IEEE 802.1AS-kompatibilis időkészülékként működik, támogatva akár 128 különálló gPTP időtartomány szinkronizációját egyidejűleg[12].

3. QoS és forgalomkezelés: Az 5G képes a TSN forgalmi osztályokat megfelelő 5G QoS folyamokra leképezni, biztosítva a determinisztikus teljesítményt[3][12].

4. A 4. ábra bemutatja az 5G-TSN integráció általános architektúráját, kiemelve a fő komponenseket és interfészeket.

VIII. Ultra-Reliable Low-Latency Communication (URLLC)

Az Ultra-Reliable Low-Latency Communication (URLLC) az 5G egyik kulcsfontosságú szolgáltatása, amely rendkívül megbízható és alacsony késleltetésű kommunikációt biztosít. Az URLLC célja a közel 100%-os megbízhatóság biztosítása 1 ms alatti késleltetéssel, ami elengedhetetlen a kritikus ipari alkalmazások, autonóm járművek és távoli műtétek esetében[3][5].

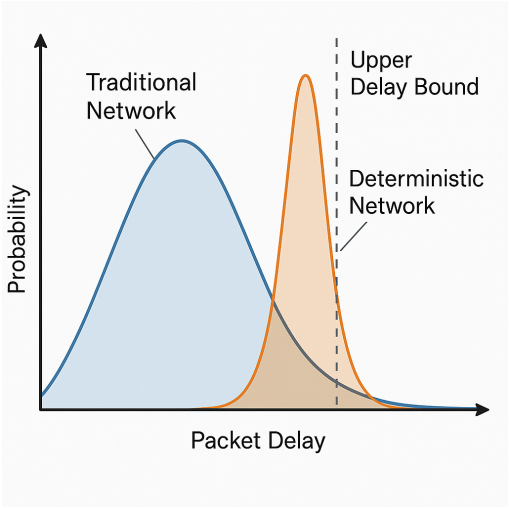
i. Az URLLC főbb jellemzői:

1. Rendkívül alacsony késleltetés: Az URLLC tervezési célja az end-to-end késleltetés minimalizálása, biztosítva a valós idejű kommunikációt. Ez magában foglalja a különböző hálózati rétegek optimalizálását, beleértve a fizikai réteget, a MAC réteget és a magasabb szintű protokollokat[3][5].

2. Ultra-magas megbízhatóság: Az URLLC célja a 99,999%-os vagy magasabb megbízhatóság elérése, biztosítva a kritikus adatok sikeres átvitelét még kedvezőtlen hálózati körülmények között is[3].

3. Fejlett hibajavítás és újrakérés: Az URLLC különböző mechanizmusokat alkalmaz a hibák kezelésére, beleértve a fejlett hibajavító kódolást (FEC) és a gyors újrakérési mechanizmusokat[5].

Az URLLC kulcsszerepet játszik az 5G-CPS integrációban, biztosítva a megbízható és alacsony késleltetésű kommunikációt, ami elengedhetetlen a valós idejű vezérlési alkalmazásokhoz[3][5].



Az 2. ábra összehasonlítja a hagyományos és a determinisztikus hálózatok csomagkésleltetési valószínűségi eloszlását, kiemelve a determinisztikus hálózatok előnyeit a felső késleltetési korlát tekintetében.

IX. OPC UA over 5G

Az OPC Unified Architecture (UA) egy ipari kommunikációs protokollszabvány, amely platformfüggetlen, biztonságos és skálázható adatcserét biztosít. Az OPC UA 5G hálózatokon keresztüli használata lehetővé teszi a rugalmas és megbízható ipari kommunikációt[11].

i. Az OPC UA főbb jellemzői:

1. Információmodellezés: Az OPC UA erős információmodellezési képességeket kínál, lehetővé téve a komplex adatstruktúrák és kapcsolatok ábrázolását[11].

2. Biztonság: Az OPC UA beépített biztonsági mechanizmusokat kínál, beleértve a hitelesítést, titkosítást és digitális aláírásokat[11].

3. PubSub kommunikációs modell: Az OPC UA PubSub modell lehetővé teszi a skálázható, több-több típusú kommunikációt, ami ideális a nagyméretű elosztott rendszerekhez[11].

ii. Az OPC UA 5G hálózatokon keresztüli használata számos előnyt kínál:

1. Rugalmasság és mobilitás: Az 5G lehetővé teszi az OPC UA alapú kommunikációt a vezetékes hálózatokhoz nem csatlakoztatott vagy mozgó eszközökkel[11].

2. Skálázhatóság: Az 5G és az OPC UA PubSub kombinációja lehetővé teszi nagyszámú eszköz csatlakoztatását és kommunikációját[11].

3. Teljesítmény: A kísérleti eredmények azt mutatják, hogy az OPC UA over 5G elfogadható teljesítményt biztosít ipari alkalmazásokhoz, bár a késleltetés némileg nagyobb, mint az

Protokoll	Környezet	CCLL (ms)	OPCET (s)	Főbb megfigyelések
MQTT QoS0	Ethernet	2.5–10.9 (2 B payload)	3.95 ± 0.01	Alacsonyabb késleltetés kis adatmennyiség esetén, de jelentősen nő nagy payload-nál
MQTT QoS0	5G-EC	12.1–46.5 (2 B payload)	4.30 ± 0.09	5G-EC növeli a késleltetést, különösen nagy adatcsomagoknál (pl. 1300 B)
OPC UA PubSub	Ethernet	10.1–16.6 (2 B payload)	4.32 ± 0.05	Nagyobb alapkésleltetés, de stabilabb teljesítmény változó hálózati terhelés mellett
OPC UA PubSub	5G-EC	25.3–39.6 (2 B payload)	4.67 ± 0.15	Jobb teljesítmény nagy payload-nál vs. MQTT, de magasabb abszolút értékek

1. táblázat: OPC UA és MQTT protokollok teljesítménymutatói különböző kommunikációs technológiákkal

Ethernet esetében[11].

X. MQTT, DDS és egyéb alkalmazási szintű protokollok

Az 5G-CPS rendszerekben különböző alkalmazási szintű protokollok használhatók a specifikus alkalmazási igények kielégítésére. Ezek közül az MQTT, DDS és egyéb protokollok fontos szerepet játszanak.

i. MQTT (Message Queuing Telemetry Transport)

Az MQTT egy könnyűsúlyú, publikálás-feliratkozás alapú üzenetküldési protokoll, amely ideális az IoT alkalmazásokhoz. Az MQTT főbb jellemzői:

1. Publikálás-feliratkozás modell: Az MQTT központi bróker révén működik, ahol az eszközök publikálhatnak üzeneteket bizonyos témákban, és feliratkozhatnak a számukra releváns témákra[11].

2. Minőségi szintek (QoS): Az MQTT három QoS szintet kínál, lehetővé téve a megfelelő egyensúly elérését a megbízhatóság és az erőforrás-felhasználás között[11].

3. Kis protokoll-overhead: Az MQTT minimális fejlécekkel rendelkezik, ami hatékony sávszélesség-felhasználást tesz lehetővé, különösen korlátozott erőforrású eszközök esetén[11].

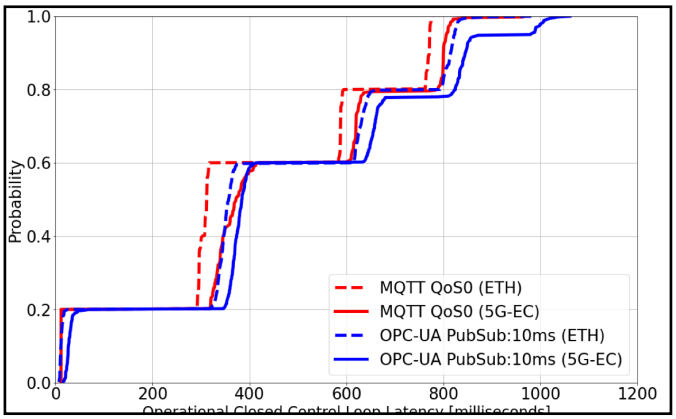
ii. DDS (Data Distribution Service)

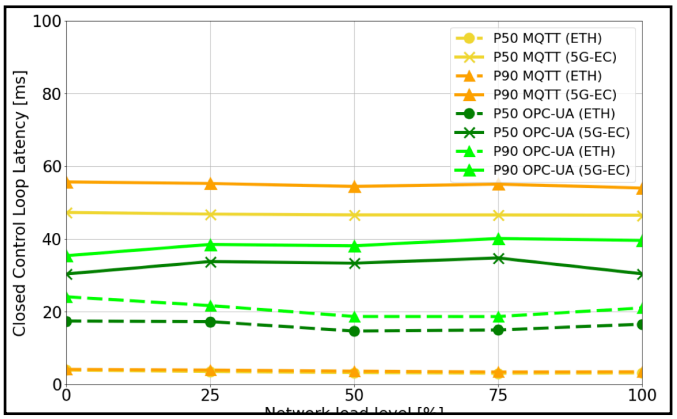
A DDS egy adatközpontú, publikálás-feliratkozás protokoll, amely elosztott rendszerek számára optimalizált. A DDS főbb jellemzői:

1. Bróker-mentes architektúra: A DDS közvetlenül a kiadók és előfizetők között működik, központi bróker nélkül, ami csökkenti a késleltetést és növeli a megbízhatóságot.

2. Gazdag QoS támogatás: A DDS több mint 20 QoS beállítást kínál, amelyek lehetővé teszik a kommunikáció finomhangolását különböző alkalmazási igényekhez.

3. Adatközpontúság: A DDS az adatmodellt helyezi előtérbe, ami megkönnyíti a komplex rendszerek fejlesztését és karbantartását.





A 3 és 4.. ábra bemutatja a robotcella vezérlő hurkok késleltetését (OPCCLL) különböző IoT protokollok és kommunikációs technológiák esetén.

iii. Protokollok összehasonlítása 5G környezetben

Az 5G hálózatokon alkalmazott különböző protokollok teljesítménye jelentősen eltérhet a konkrét alkalmazási igények és hálózati feltételek függvényében. Az MQTT általában alacsonyabb késleltetést biztosít kis adatméret esetén, míg az OPC UA jobb teljesítményt nyújthat nagyobb adatcsomagok és komplex adatstruktúrák esetén[11].

A kísérleti eredmények azt mutatják, hogy az MQTT QoS0 konfiguráció általában alacsonyabb késleltetést biztosít, mint az OPC UA PubSub mind Ethernet, mind 5G-EC környezetben. Ugyanakkor, nagyobb adatterhelés (1300 byte) esetén az OPC UA teljesítménye versenyképes lehet az MQTT-vel 5G-EC környezetben[11].

XI. Biztonsági kihívások és megoldások 5G-CPS rendszerekben

Adatintegritás:

Az adatintegritás biztosítása kulcsfontosságú az 5G-CPS rendszerekben, különösen a kritikus infrastruktúrák és ipari alkalmazások esetében. Az adatintegritás azt jelenti, hogy az adatok módosítás, meghamisítás vagy illetéktelen hozzáférés nélkül jutnak el a forrástól a célig[8][2].

i. Az adatintegritás biztosításának főbb kihívásai 5G-CPS környezetben:

1. Heterogén rendszerek: Az 5G-CPS rendszerek különböző eszközöket, protokollokat és hálózati technológiákat integrálnak, ami megnehezíti az egységes biztonsági megoldások alkalmazását[8][2].

2. Vezeték nélküli sebezhetőségek: A vezeték nélküli kommunikáció természeténél fogva sebezhetőbb a lehallgatással és beavatkozással szemben, mint a vezetékes kapcsolatok[8].

3. Erőforrás-korlátozott eszközök: Sok CPS eszköz korlátozott számítási és energiaerőforrásokkal rendelkezik, ami megnehezíti a fejlett titkosítási és integritásvédelmi mechanizmusok alkalmazását[2].

ii. Az adatintegritás biztosításának főbb megoldásai:

1. End-to-end titkosítás: Az adatok titkosítása a forrásnál és dekódolása csak a célon, ami megvédi az adatokat a közbenső pontokon történő illetéktelen hozzáféréstől vagy módosítástól[8].

2. Digitális aláírások és integritás-ellenőrzés: A digitális aláírások és hash-alapú integritás-ellenőrzési mechanizmusok lehetővé teszik az adatok eredetének és sértetlenségének ellenőrzését[8].

3. Biztonsági tokenek és tanúsítványok: A biztonsági tokenek és tanúsítványok használata a hitelesítéshez és jogosultságkezeléshez, biztosítva, hogy csak a jogosult felek férhetnek hozzá az adatokhoz és rendszerekhez[8][2].

4. Fizikai réteg biztonsági mechanizmusok: Az 5G fizikai rétegben alkalmazott biztonsági mechanizmusok, például a fejlett titkosítási algoritmusok és a biztonsági kulcsok rendszeres frissítése[5][8].

iii. Hálózati támadások elleni védelem

Az 5G-CPS rendszerek különösen sebezhetőek lehetnek a hálózati támadásokkal szemben, amelyek célja a rendszer működésének megzavarása, adatok ellopása vagy a rendszer feletti irányítás megszerzése[8][2].

XII. A főbb hálózati támadási vektorok 5G-CPS rendszerekben:

1. Szolgáltatásmegtagadási (DoS/DDoS) támadások: Ezek a támadások túlterhelik a rendszert, megakadályozva a legitim felhasználók hozzáférését. Az 5G hálózatok nagyobb sávszélessége és az IoT eszközök nagy száma lehetővé teszi a nagy volumenű DDoS támadásokat[8].

2. Sparrow Attack: A Sparrow Attack az LTE és 5G protokollok MAC rétegét kihasználó támadás, amely lehetővé teszi jogosulatlan eszközök számára, hogy rejtett kommunikációt folytassanak a hálózati infrastruktúrán keresztül[8].

3. Man-in-the-Middle (MitM) támadások: Ezek a támadások során a támadó közbeékelődik két kommunikáló fél közé, lehallgatva vagy módosítva a kommunikációt[8][2].

4. API támadások: Az 5G hálózatok szolgáltatás-alapú architektúrájában az API-k kulcsfontosságú szerepet játszanak, de egyben új támadási felületet is jelentenek[5][8].

i. A hálózati támadások elleni védelem főbb megoldásai:

1. Zero Trust architektúra: A Zero Trust modell szerint minden hozzáférési kísérletet ellenőrizni kell, függetlenül attól, hogy honnan származik. Ez különösen fontos az 5G-CPS rendszerekben, ahol sok különböző eszköz és felhasználó fér hozzá a rendszerhez[8][2].

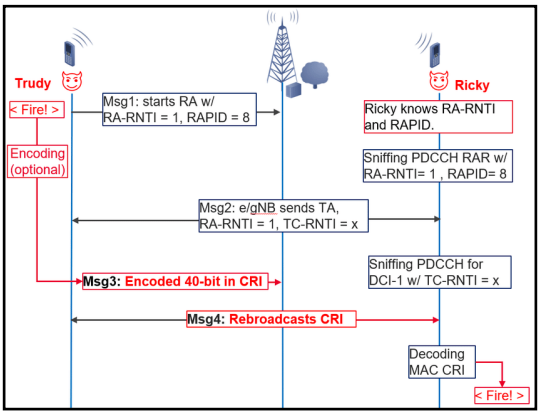
2. Hálózati szegmentáció és szeletelés: Az 5G hálózatszeletelés képessége lehetővé teszi a hálózat biztonsági zónákra osztását, korlátozva egy esetleges behatolás hatását[4][8].

3. Fejlett behatolásérzékelő és -megelőző rendszerek (IDS/IPS): Ezek a rendszerek képesek felismerni és blokkolni a gyanús tevékenységeket és ismert támadási mintákat[8][2].

4. Biztonsági monitorozás és elemzés: Valós idejű monitorozás és fejlett elemzési technikák alkalmazása a biztonsági események azonosítására és kezelésére[8][2].

ii. Fizikai biztonság szempontjai

Az 5G-CPS rendszerek fizikai biztonsága kritikus fontosságú, különösen az ipari környezetekben, ahol a fizikai támadások potenciálisan súlyos következményekkel járhatnak[2].



A 5. ábra szemlélteti a Sparrow Attack működési mechanizmusát

iii. A főbb fizikai biztonsági kihívások:

1. Fizikai hozzáférés az eszközökhöz: Az 5G-CPS rendszerek sok eszközt tartalmaznak, amelyek gyakran nyilvános vagy nehezen védhető helyeken találhatók, ami megkönnyíti a fizikai hozzáférést[2].

2. Érzékelők és aktuátorok manipulálása: A fizikai érzékelők és aktuátorok manipulálása hamis bemeneteket eredményezhet, vagy megakadályozhatja a rendszer megfelelő működését[2].

3. Side-channel támadások: Az eszközök fizikai tulajdonságain (pl. energiafogyasztás, elektromágneses sugárzás) alapuló támadások, amelyek lehetővé teszik a titkos információk kinyerését anélkül, hogy közvetlenül feltörnék a rendszert[8][2].

4. Hardware Trojan és hamisított komponensek: A gyártási vagy ellátási lánc során beépített rosszindulatú hardverkomponensek, amelyek hátsó ajtókat vagy biztonsági réseket tartalmazhatnak[2].

iv. A fizikai biztonság biztosításának főbb megoldásai:

1. Fizikai hozzáférés-védelem: Fizikai biztonsági intézkedések, például zárható szekrények, biztonsági kamerák és hozzáférés-ellenőrzési rendszerek alkalmazása[2].

2. Tamper-resistant és tamper-evident eszközök: Olyan eszközök használata, amelyek ellenállnak a fizikai beavatkozásnak, vagy egyértelmű jelzést adnak, ha illetéktelen beavatkozás történt[2].

3. Secure boot és attestation: Biztonságos indítási folyamatok és távoli attestation mechanizmusok alkalmazása, amelyek biztosítják, hogy csak hiteles és sértetlen szoftver futhasson az eszközökön[8][2].

4. Érzékelők redundanciája és plauzibilitás-ellenőrzés: Többszörös, független érzékelők használata és a mérési eredmények plauzibilitásának ellenőrzése a manipuláció észlelése érdekében[2].

V. Alkalmazási területek

i. Intelligens gyártás (Ipar 4.0)

Az 5G-CPS rendszerek egyik legfontosabb alkalmazási területe az intelligens gyártás, más néven Ipar 4.0. Az Ipar 4.0 a negyedik ipari forradalom, amely a digitalizáció, automatizáció és adatalapú döntéshozatal köré épül[4][1][19].

ii. Az 5G-CPS rendszerek főbb alkalmazásai az intelligens gyártásban:

1. Rugalmas gyártósorok: Az 5G vezeték nélküli technológia lehetővé teszi a gyártósorok rugalmas átkonfigurálását, anélkül hogy új kábelezést kellene telepíteni. Ez jelentősen csökkenti az átállás idejét és költségét[4][1].

2. Robot-robot kommunikáció: Az alacsony késleltetésű és nagy megbízhatóságú 5G kapcsolat lehetővé teszi a robotok közötti zökkenőmentes kommunikációt, ami javítja a koordinációt és a hatékonyságot[4][11].

3. Prediktív karbantartás: Az 5G-CPS rendszerek lehetővé teszik a gépek állapotának valós idejű monitorozását és elemzését, előre jelezve a potenciális meghibásodásokat, és lehetővé téve a proaktív karbantartást[4][1].

4. Digitális ikrek (Digital Twins): Az 5G nagy sávszélessége és alacsony késleltetése lehetővé teszi a fizikai berendezések valós idejű digitális modelljeinek létrehozását és frissítését, amit digitális ikreknek nevezünk. Ezek segítik a tervezést, optimalizálást és problémamegoldást[4][1].

5. Valós idejű minőségellenőrzés: Az 5G-CPS rendszerek lehetővé teszik a fejlett szenzorok és képfeldolgozási technikák alkalmazását a gyártási folyamat során, valós időben azonosítva és korrigálva a minőségi problémákat[4][1].

Az Ipar 4.0 implementációjának egyik példája a Tyco Electronics Hungary Kft. esettanulmánya, amely bemutatja, hogyan alkalmazzák a modern technológiákat a gyártási folyamatok optimalizálására és a versenyképesség növelésére[19].

XIV.Energiahálózatok

Az energiaszektorban az 5G-CPS rendszerek forradalmasítják a hálózatok működtetését, különösen az okos hálózatok (Smart Grid) és a megújuló energiaforrások integrációja tekintetében.

i. Az 5G-CPS rendszerek főbb alkalmazásai az energiahálózatokban:

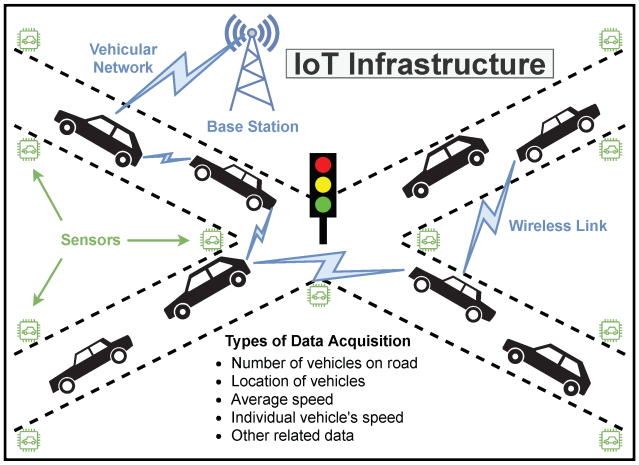
1. Smart Grid alkalmazások: Az 5G-CPS rendszerek lehetővé teszik az okos hálózatok hatékony működését, biztosítva a valós idejű kommunikációt a különböző hálózati elemek között. Ez javítja a hálózati stabilitást, hatékonyságot és megbízhatóságot[4][3].

2. Decentralizált energiatermelés felügyelete: Az 5G-CPS rendszerek lehetővé teszik a decentralizált energiatermelő egységek (például napelemek, szélturbinák) valós idejű monitorozását és irányítását, optimalizálva a termelést és integrációt a hálózatba[4][3].

3. Virtuális erőművek: Az 5G-CPS rendszerek lehetővé teszik különböző energiatermelő egységek virtuális aggregációját, amely egyetlen virtuális erőműként működik, javítva a skálázhatóságot és rugalmasságot[4][3].

4. Keresleti oldal menedzsment: Az 5G-CPS rendszerek lehetővé teszik a fogyasztói oldal aktív részvételét az energiapiacon, intelligens fogyasztásmérők és automata vezérlés révén optimalizálva a fogyasztást a kereslet-kínálat egyensúlyának javítása érdekében[4][3].

5. Valós idejű terhelés-elosztás: Az 5G alacsony késleltetésű kommunikációja lehetővé teszi a terhelés valós idejű elosztását a hálózatban, javítva a hálózati stabilitást és csökkentve a túlterhelés kockázatát[4][3].



A 6. ábra bemutatja egy intelligens közlekedési rendszer 5G-alapú Cyber-Physical Systems (CPS) architektúráját

XV. Autonóm közlekedési rendszerek

Az autonóm közlekedési rendszerek fejlesztése és implementációja az 5G-CPS rendszerek egyik legizgalmasabb alkalmazási területe. Az 5G technológia alacsony késleltetése, nagy megbízhatósága és nagy sávszélessége kulcsfontosságú az autonóm járművek biztonságos és hatékony működéséhez[3][3].

i. Az 5G-CPS rendszerek főbb alkalmazásai az autonóm közlekedési rendszerekben:

1. V2X (Vehicle-to-Everything) kommunikáció: Az 5G lehetővé teszi a járművek kommunikációját egymással (V2V), az infrastruktúrával (V2I), a gyalogosokkal (V2P) és a hálózattal (V2N), javítva a biztonságot és a közlekedési hatékonyságot[3][3].

2. Autonóm járművek flottái: Az 5G-CPS rendszerek lehetővé teszik az autonóm járművek flottáinak koordinált működését, például a teherfuvarozásban vagy a személyszállításban[3][3].

3. Kooperatív intelligens közlekedési rendszerek: Az 5G-CPS rendszerek lehetővé teszik a járművek, az infrastruktúra és a közlekedésirányítási rendszerek együttműködését, optimalizálva a forgalmat és csökkentve a torlódásokat és baleseteket[3][3].

4. Valós idejű forgalomirányítás: Az 5G-CPS rendszerek lehetővé teszik a forgalom valós idejű monitorozását és irányítását, dinamikusan alkalmazkodva a változó forgalmi feltételekhez[3][3].

5. Biztonságkritikus kommunikáció: Az 5G URLLC képességei kritikus fontosságúak a vészhelyzeti figyelmeztetések, balesetek elkerülése és más biztonságkritikus funkciók számára az autonóm közlekedési rendszerekben[3][3].

XVI.Magyarországi vonatkozások és esettanulmányok

i. BME kutatásai és eredményei

A Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) vezető szerepet játszik az 5G technológia és a CPS rendszerek kutatásában Magyarországon. Az egyetem különböző karai és kutatócsoportjai aktívan részt vesznek nemzetközi és hazai kutatási projektekben, ipari együttműködésekben, valamint oktatási programokban az 5G és CPS területén[14].

ii. A BME főbb kutatási területei és eredményei az 5G-CPS területén:

1. 5G hálózatok és szolgáltatások kutatása: A BME Villamosmérnöki és Informatikai Kar (VIK) "5G hálózatok, szolgáltatásaik, és az ipari IoT szinergiája" című tantárgya átfogó képet ad az 5G technológiáról és annak ipari alkalmazásairól. A tantárgy tematikája magában foglalja az 5G szolgáltatásokat, a hálózati technológiák konvergenciáját és az 5G-IoT integrációt[14].

2. URLLC és TSN kutatások: A BME kutatói vizsgálják az Ultra-Reliable Low-Latency Communication (URLLC) és Time-Sensitive Networking (TSN) technológiákat, amelyek kulcsfontosságúak az ipari alkalmazások számára. Ezek a kutatások hozzájárulnak a valós idejű kommunikációs protokollok fejlesztéséhez és optimalizálásához[14].

3. Ipar 4.0 kutatólaborok: A BME Ipar 4.0 kutatólaborjai lehetőséget biztosítanak az 5G-CPS technológiák gyakorlati tesztelésére és fejlesztésére. Ezek a laborok modern eszközökkel és szoftverekkel vannak felszerelve, lehetővé téve a hallgatók és kutatók számára a legújabb technológiák megismerését és használatát[14].

4. Nemzetközi kutatási együttműködések: A BME aktívan részt vesz nemzetközi kutatási együttműködésekben az 5G és CPS területén, például európai uniós kutatási projektekben. Ezek az együttműködések lehetőséget biztosítanak a legújabb technológiák és módszerek megismerésére és fejlesztésére[14].

iii. Magyar vállalatok 5G-CPS projektjei

Magyarországon több vállalat is aktívan részt vesz az 5G-CPS technológiák fejlesztésében és alkalmazásában. Ezek a projektek hozzájárulnak a hazai ipar digitális transzformációjához és versenyképességének növeléséhez[6][19].

iv. Néhány jelentős magyarországi 5G-CPS projekt:

1. CETIN Hungary 5G tesztprojekt: A CETIN Hungary szolgáltatófüggetlen ötödik generációs mobilhálózati (5G) kiscellás megoldások tesztprojektjét valósította meg Kecskeméten és Mezőhegyesen. A projekt célja annak vizsgálata volt, hogyan lehet 5G hálózatokat gazdaságosan kiépíteni és üzemeltetni különböző helyszíneken, például sűrűn lakott városi környezetben és mezőgazdasági területeken[6].

2. Ericsson Magyarország kutatás-fejlesztési projektjei: Az Ericsson Magyarország jelentős kutatás-fejlesztési tevékenységet folytat az 5G és ipari alkalmazások területén. A vállalat együttműködik egyetemekkel, kutatóintézetekkel és ipari partnerekkel a legújabb technológiák fejlesztésében és tesztelésében[6][14].

3. Bosch Budapest Innovációs Kampusz projektjei: A Bosch Budapest Innovációs Kampusz aktívan részt vesz az okosgyár, IoT és 5G technológiák fejlesztésében és alkalmazásában. A cég különböző projekteken dolgozik, amelyek célja az ipar digitalizációja és az Ipar 4.0 megvalósítása[19].

4. Magyar Telekom 5G teszthálózatok: A Magyar Telekom különböző 5G teszthálózatokat és ipari pilot projekteket valósított meg Magyarországon. Ezek a projektek hozzájárulnak az 5G technológia szélesebb körű elterjedéséhez és alkalmazásához az iparban[6][14].

XVII.Nemzetközi összehasonlítás

A magyarországi 5G-CPS fejlesztések és alkalmazások nemzetközi összehasonlításban is értékelhetők, különös tekintettel a digitális érettség és az ipari alkalmazások szempontjából[1][19][21].

i. A nemzetközi összehasonlítás főbb szempontjai:

1. Digitális érettség: A kutatások szerint jelentős különbségek vannak Magyarország és más európai országok között a digitális érettség tekintetében. Egy Magyarország és Ausztria közötti összehasonlító kutatás azt mutatta, hogy mind makro-, mind mikroszinten releváns különbségek vannak a két ország között a digitális érettség tekintetében[21].

2. Ipar 4.0 technológiák alkalmazása: Az Ipar 4.0 által indukált szervezeti átalakulási folyamatok nemzetközi vizsgálata azt mutatta, hogy az Ipar 4.0 technológiák alkalmazása Magyarországon megkezdődött, de még jelentős a lemaradás más európai országokhoz képest[1].

3. 5G infrastruktúra kiépítettsége: Az 5G infrastruktúra kiépítettsége szempontjából Magyarország kevésbé fejlett, mint Nyugat-Európa vezető országai. Ugyanakkor, a célzott 5G tesztprojektek és a kormányzati támogatás hozzájárulnak a technológia gyorsabb elterjedéséhez[6][13].

4. Kutatás-fejlesztési aktivitás: A magyar kutatóintézetek és vállalatok aktívan részt vesznek az 5G és CPS területén folyó kutatás-fejlesztési tevékenységekben, de a K+F ráfordítások és az eredmények szempontjából még van fejlődési potenciál a vezető európai országokhoz képest[14][21].

Dimenzió	Magyarország	Ausztria	Németország	Csehország	EU átlag
DESI index (2018)	23. hely (EU 28-ból)	10. hely	4. hely	18. ely	-
SME digitális átállás	32% (alacsonyabb a visegrádi átlagnál)	58% (főleg nagyvállalatok)	67% (integrált gyártási rendszerek)	41%	42%
Kormányzati finanszírozás	~262 millió EUR (DEI kezdeményezések)	~480 millió EUR (Industrie 4.0 Platform)	~3,4 milliárd EUR (Plattform Industrie 4.0)	~190 millió EUR	-
Ipar 4.0 modellgyárak	2 db (Budapest, Győr)	5 db (Bécs, Graz, Linz)	12 db (München, Stuttgart)	3 db (Prága)	-
Munkavállalói készségek	24% digitális alapkészség (EU: 56%)	49% digitális alapkészség	63% digitális alapkészség	38% digitális alapkészség	54%
5G infrastruktúra	45% lefedettség (városi területeken)	78% lefedettség	92% lefedettség	61% lefedettség	72%

A 2. táblázat összehasonlítja Magyarország és más európai országok digitális érettségét az Ipar 4.0 kontextusában, különböző dimenziók mentén.

XVIII.Jövőbeli fejlesztési irányok

i. 6G technológia és hatásai

Míg az 5G technológia jelenleg a legfejlettebb mobilkommunikációs standard, a kutatók és iparági szakemberek már a következő generáción, a 6G-n dolgoznak. A 6G várhatóan 2030 körül lesz elérhető, és jelentős előrelépést fog jelenteni az 5G-hez képest a teljesítmény, képességek és alkalmazási lehetőségek tekintetében[4][15].

A 6G technológia várható jellemzői és hatásai a CPS rendszerekre:

1. Determinisztikus kommunikáció: A 6G egyik fő célja a determinisztikus end-to-end kommunikáció megvalósítása, amely elengedhetetlen a jövőbeli kiberfizikai alkalmazások számára. A Deterministic6G projekt célja a jövőbeli globális kommunikációs szabványok alapjainak megteremtése, amelyek lehetővé teszik a 6G determinisztikus kommunikációt a víziószerű használati esetekhez[4][15].

2. Terahertz kommunikáció: A 6G várhatóan a terahertz frekvenciatartományt (0.1-10 THz) fogja használni, ami rendkívül nagy adatátviteli sebességet tesz lehetővé (akár 1 Tbps). Ez forradalmasíthatja a nagy adatigényű CPS alkalmazásokat, például a kiterjesztett és virtuális valóságot[15].

3. Integrált érzékelés és kommunikáció: A 6G várhatóan egyesíti a kommunikációs és érzékelési funkciókat, lehetővé téve a környezet pontos feltérképezését és monitorozását a

kommunikációs infrastruktúra segítségével. Ez új lehetőségeket nyit a CPS alkalmazások számára[4][15].

4. Mesterséges intelligencia integráció: A 6G hálózatok várhatóan szoros integrációt valósítanak meg a mesterséges intelligenciával, lehetővé téve az önoptimalizáló, öngyógyító és önkonfiguráló hálózatokat. Ez javítja a CPS rendszerek megbízhatóságát, hatékonyságát és adaptivitását[4][15].

5. Kvantumkommunikáció és -számítástechnika: A 6G várhatóan integrálni fogja a kvantumkommunikációs és -számítástechnikai technológiákat, jelentősen javítva a biztonságot és a számítási teljesítményt. Ez különösen fontos a kritikus CPS alkalmazások számára[15].

ii. Kiberfizikai rendszerek következő generációja

A kiberfizikai rendszerek következő generációja várhatóan számos új technológiát és megközelítést fog integrálni, jelentősen bővítve a lehetséges alkalmazások körét és javítva a teljesítményt[4][3][15].

i. A jövőbeli CPS rendszerek főbb jellemzői és fejlesztési irányai:

1. Mesterséges intelligencia integráció: A mesterséges intelligencia (MI) és gépi tanulás (ML) technikák széles körű integrációja a CPS rendszerekbe lehetővé teszi az adaptív, önoptimalizáló és prediktív működést. Az MI algoritmusok képesek felismerni a mintázatokat, előrejelezni a hibákat és optimalizálni a rendszerek működését[4][15].

2. Autonóm önjavító rendszerek: A jövő CPS rendszerei várhatóan képesek lesznek önállóan felismerni és javítani a hibákat, minimalizálva az emberi beavatkozás szükségességét és maximalizálva a rendelkezésre állást. Ez különösen fontos a kritikus infrastruktúrák esetében[4][15].

3. Kvantuminformatikai lehetőségek: A kvantumszámítógépek és kvantum-érzékelők integrációja a CPS rendszerekbe jelentősen javíthatja a számítási teljesítményt és érzékelési képességeket. A kvantumkriptográfia új lehetőségeket nyit a biztonságos kommunikáció területén[15].

4. Skálázható architektúrák: A jövő CPS rendszerei várhatóan rendkívül skálázható architektúrával rendelkeznek, lehetővé téve a zökkenőmentes működést a kis helyi rendszerektől a globális, elosztott infrastruktúrákig. Ezt a mikroszolgáltatás-alapú architektúrák, konténerizáció és edge computing technológiák teszik lehetővé[4][3].

5. Ember-gép együttműködés: A jövő CPS rendszerei várhatóan fejlettebb ember-gép interfészeket biztosítanak, lehetővé téve az emberek és a gépek hatékonyabb együttműködését. Ezt a fejlett vizualizációs technikák, kiterjesztett és virtuális valóság, valamint a természetes nyelvi feldolgozás teszi lehetővé[4][15].

XIX.Társadalmi és gazdasági hatások

Az 5G-CPS és a jövőbeli 6G-CPS rendszerek széles körű elterjedése jelentős társadalmi és gazdasági hatásokkal jár. Ezek a hatások érintik a munkaerőpiacot, az üzleti modelleket, a gazdasági növekedést és a fenntarthatóságot[13][19].

i. A főbb társadalmi és gazdasági hatások:

1. Munkaerőpiaci változások: Az 5G-CPS és később a 6G-CPS rendszerek elterjedése várhatóan jelentős változásokat okoz a munkaerőpiacon. Egyes hagyományos munkahelyek automatizálhatóvá válnak, ugyanakkor új, magasabb képzettséget igénylő munkahelyek jönnek létre. Ez szükségessé teszi a munkavállalók átképzését és az oktatási rendszer adaptációját[19].

2. Új üzleti modellek: Az 5G-CPS technológiák lehetővé teszik új üzleti modellek kialakítását, például a termékek szolgáltatásként való értékesítését (Product-as-a-Service), a prediktív karbantartást és a személyre szabott gyártást. Ezek az új modellek új bevételi forrásokat

Ország/régió	5G késedelmes bevezetésének potenciális gazdasági költségei	Főbb következmények és megjegyzések
USA	6 hónapos késés: -104 milliárd USD GDP (2019–2024)	Lassabb technológiai innováció, kevesebb munkahely, alacsonyabb GDP-növekedés
Európai Unió	2035-ig: -40 milliárd EUR GDP (összesen)	56 millió ember késleltetett hozzáférése, lassabb innováció és gazdasági növekedés
Németország	Évi +479 millió EUR beruházási költség (Huawei-kizárás esetén)	Magasabb hálózatépítési költségek, lassabb digitális fejlődés
Franciország	2035-ig: -7,3 milliárd EUR GDP	Lassabb technológiai fejlődés, versenyképesség csökkenése
Izland	Évi +3 millió EUR beruházási költség	Kis piac, de arányaiban jelentős veszteség
Ausztrália	2035-ig: -2,8 milliárd USD GDP	Késleltetett innováció, magasabb költségek
India	Jelentős GDP veszteség, pontos összeg nem áll rendelkezésre	Lassabb digitális gazdaságfejlődés, vidéki lemaradás
Egyesült Királyság	Lassú bevezetés: -4,6 milliárd GBP GDP 2030-ig	NHS megtakarítások, gyorsabb közlekedés, regionális különbségek
Globális szint	5G kiépítési költség: 10–50 milliárd USD/ország	Infrastrukturális lemaradás, technológiai versenyhátrány

A 3. táblázat összefoglalja az 5G késedelmes bevezetésének potenciális gazdasági költségeit különböző országokban.

teremtenek és növelik a vállalatok versenyképességét[19].

3. Gazdasági növekedésre gyakorolt hatás: Az 5G gyors bevezetése jelentős gazdasági előnyökkel jár. Egy tanulmány szerint ha az 5G lefedettség a lakosság 25%-kal nagyobb részét éri el, mint a kormány jelenlegi 51%-os célja, az 2027-ig 41,7 milliárd fontot eredményezhet a GDP-ben. A különbség aközött, hogy az Egyesült Királyság vezető vagy lemaradó az 5G elfogadásában, akár 173 milliárd font járulékos GDP is lehet az elkövetkező évtizedben[13].

4. Energiahatékonyság és fenntarthatóság: Az 5G-CPS rendszerek lehetővé teszik az energiafelhasználás hatékonyabb monitorozását és optimalizálását, hozzájárulva a fenntarthatósági célok eléréséhez. Az okos hálózatok, intelligens épületek és energiahatékony gyártási folyamatok csökkentik az energiafogyasztást és a karbon-lábnyomot[19].

5. Digitális szakadék: Az 5G-CPS technológiák elterjedése potenciálisan növelheti a digitális szakadékot, ha a hozzáférés nem egyenlő mértékben biztosított a társadalom különböző csoportjai számára. Fontos biztosítani, hogy a technológia előnyeit a társadalom minden rétege élvezhesse[13][19].

XX. Következtetések és ö8sszefoglalás

i. Az 5G-CPS integráció jelentősége

Az 5G hálózatok és a kiberfizikai rendszerek (CPS) integrációja forradalmi változásokat hoz az ipar, az energetika, a közlekedés és számos más terület számára. Az 5G-CPS rendszerek lehetővé teszik a valós idejű adatgyűjtést, elemzést és irányítást, javítva a hatékonyságot, megbízhatóságot és biztonságot[3][4][1].

ii. Az 5G-CPS integráció legfontosabb előnyei:

1. Vezeték nélküli rugalmasság: Az 5G technológia lehetővé teszi a vezeték nélküli, nagy megbízhatóságú és alacsony késleltetésű kommunikációt, ami jelentősen növeli a CPS rendszerek rugalmasságát és alkalmazhatóságát különböző környezetekben[3][4].

2. Valós idejű működés: Az 5G URLLC képességei biztosítják a valós idejű adatátvitelt és feldolgozást, ami elengedhetetlen a kritikus CPS alkalmazások számára, például az ipari vezérlőrendszerekben vagy az autonóm járművekben[3][5].

3. Skálázhatóság: Az 5G hálózatok képesek nagyszámú eszköz egyidejű csatlakoztatására, lehetővé téve a nagy léptékű CPS rendszerek kiépítését és hatékony működését[4][3].

4. Heterogén rendszerek integrációja: Az 5G képes integrálni a különböző típusú hálózatokat és eszközöket egy egységes infrastruktúrába, megkönnyítve a heterogén CPS komponensek együttműködését[3][12].

5. Edge computing támogatás: Az 5G architektúra támogatja az edge computing koncepcióját, ami lehetővé teszi az adatok feldolgozását a hálózat szélén, csökkentve a késleltetést és a sávszélesség-használatot[4][3].

Az 5G-CPS integráció kritikus sikertényezői közé tartozik a megfelelő szabványosítás, a biztonság, a spektrummenedzsment és a TSN-5G integráció. A közeljövő fejlesztési fókuszai várhatóan a determinisztikus kommunikáció, a heterogén hálózatok integrációja és a mesterséges intelligencia alapú hálózatmenedzsment területeire irányulnak[4][3][15].

XXI.A kutatás korlátai és további kutatási irányok

Bár az 5G-CPS integráció számos előnyt kínál, több kihívással és korláttal is szembesül, amelyek további kutatást és fejlesztést igényelnek.

i. A jelenlegi technológiai korlátok és kihívások:

1. 5G lefedettség és infrastruktúra: Az 5G hálózatok kiépítése még folyamatban van, és a teljes lefedettség elérése időbe és jelentős beruházásba kerül. Ez korlátozza az 5G-CPS rendszerek széles körű alkalmazását, különösen a vidéki vagy kevésbé fejlett területeken[13].

2. Determinisztikus teljesítmény biztosítása: Bár az 5G URLLC célja az ultra-megbízható és alacsony késleltetésű kommunikáció biztosítása, a vezeték nélküli környezet sztochasztikus jellege miatt kihívást jelent a garantált, determinisztikus teljesítmény elérése[3][15].

3. Standardizációs kihívások: Az 5G és CPS technológiák integrációja számos szabványosítási kihívással jár, különösen a TSN, 5G és ipari protokollok (OPC UA, MQTT, stb.) együttműködése terén[3][12].

4. Biztonsági kérdések: Az 5G-CPS rendszerek biztonsága továbbra is kritikus kérdés, különösen a kritikus infrastruktúrák esetében. Az új 5G technológiák és architektúrák új sebezhetőségeket hozhatnak magukkal, amelyek további kutatást igényelnek[8][2].

ii. További fontos kutatási irányok:

1. Determinisztikus 6G kommunikáció: A 6G technológia fejlesztése, különös tekintettel a determinisztikus kommunikációra, amely kulcsfontosságú a jövőbeli CPS alkalmazások számára[4][15].

2. MI-alapú hálózatoptimalizálás: Mesterséges intelligencia és gépi tanulás alkalmazása az 5G/6G hálózatok és CPS rendszerek optimalizálására, javítva a teljesítményt, megbízhatóságot és hatékonyságot[4][15].

3. End-to-end biztonság: Új biztonsági mechanizmusok és architektúrák fejlesztése, amelyek biztosítják az 5G-CPS rendszerek end-to-end biztonságát, beleértve a fizikai és kiberbiztonságot[8][2]

4. 5G-TSN-DetNet integráció: Az 5G, TSN és DetNet technológiák hatékonyabb integrációja, biztosítva a zökkenőmentes együttműködést és a determinisztikus teljesítményt a heterogén hálózati környezetekben[3][12].

5. Ember-gép együttműködés: Fejlett ember-gép interfészek és együttműködési modellek fejlesztése az 5G-CPS rendszerekben, maximalizálva mind az emberi, mind a gépi képességek előnyeit[4][15].

Záró gondolatok

Az 5G hálózatok és a kiberfizikai rendszerek (CPS) integrációja egy dinamikusan fejlődő terület, amely jelentős hatással van és lesz az ipar, a gazdaság és a társadalom számára. Az 5G-CPS rendszerek lehetővé teszik a fizikai és digitális világ szorosabb összekapcsolását, megnyitva az utat új alkalmazások és szolgáltatások előtt.

Magyarország számára az 5G-CPS technológiák fejlesztése és alkalmazása stratégiai jelentőségű a digitális transzformáció és a gazdasági versenyképesség szempontjából. A BME és más hazai kutatóintézetek, valamint a magyar vállalatok aktív részvétele az 5G-CPS kutatás-fejlesztésben hozzájárul az ország technológiai fejlődéséhez.

Az 5G-CPS integráció további fejlődése és szélesebb körű elterjedése várható a következő években, különösen az Ipar 4.0, az okos városok, az autonóm közlekedés és az energiahálózatok területén. Ugyanakkor fontos figyelmet fordítani a technológiai kihívásokra, a biztonsági kérdésekre és a társadalmi-gazdasági hatásokra is.

Az 5G-CPS technológiák oktatása és kutatása is kiemelt fontosságú, biztosítva a jövő szakembereinek megfelelő felkészültségét és a hazai tudományos közösség aktív részvételét a nemzetközi kutatás-fejlesztési együttműködésekben.

Összességében, az 5G hálózatok alkalmazása CPS keretrendszerekben egy izgalmas és ígéretes terület, amely jelentős lehetőségeket kínál mind a technológiai fejlesztés, mind a gyakorlati alkalmazások szempontjából. A terület folyamatos fejlődése és az új technológiák – például a 6G – megjelenése várhatóan további lehetőségeket és kihívásokat hoz majd a jövőben.

Források:

[1] A new report by the CPS highlights the urgency of 5G rollout https://mbnl.co.uk/a-new-report-by-the-cps-highlights-the-urgency-of-5g-rollout/

[2] [PDF] Towards Modelling 5G Communication in Software architectures of ... https://www.es.mdu.se/pdf_publications/6761.pdf

[3] [PDF] 5G and Industry 4.0 - IET https://www.theiet.org/media/2597/dense-air.pdf

[4] Demystifying Control Plane Protocols in 5G Networks https://www.telecomgurukul.com/post/demystifying-control-plane-protocols-in-5g-networks

[5] Esettanulmányok - cetin.hu https://www.cetin.hu/mivel-foglalkozunk/esettanulmanyok

[6] [PDF] Ipar 4.0 által indukált szervezeti átalakulási folyamatok nemzetközi ... https://gsdi.gtk.uni-pannon.hu/wp-content/uploads/2024/09/KA_disszertacio_Ipar-4.0-altal-indukalt-szervezeti-atalakulasi-folyamatok-nemzetkozi-vizsgalata.pdf

[7] Cybersecurity Attacks in Private Cellular Networks – Watch Out for ... https://onelayer.com/cybersecurity-attacks-in-private-cellular-networks-watch-out-the-bad-sparrow/

[8] Project - Deterministic6G https://deterministic6g.eu/index.php/home

[9] [PDF] Report on 6G convergence enablers towards deterministic ... https://deterministic6g.eu/images/deliverables/DETERMINISTIC6G-D3.1-v1.0.pdf

[10] [PDF] An Operational 5G Edge Cloud-Controlled Robotic Cell ... https://vbn.aau.dk/files/661305137/Robotic_Cell_paper_ICAR_2023.pdf

[11] Integration of 5G with Time-Sensitive Networking for Industrial ... https://5g-acia.org/whitepapers/integration-of-5g-with-time-sensitive-networking-for-industrial-communications/

[12] Upwardly Mobile: How the UK can gain the full benefits of the 5G ... https://cps.org.uk/research/upwardly-mobile-how-the-uk-can-gain-the-full-benefits-of-the-5g-revolution/

[13] 5G hálózatok, szolgáltatásaik, és az ipari IoT szinergiája - BME VIK https://portal.vik.bme.hu/kepzes/targyak/VITMDV02/

[14] [2304.01299] Towards Deterministic Communications in 6G Networks https://arxiv.org/abs/2304.01299

[15] [PDF] Towards 5G-Enabled Operational Technology for Process ... - OSTI https://www.osti.gov/servlets/purl/2281809

[16] Üzlet 4.0 - magyarországi vállalati tapasztalatok - Technológiák https://mersz.hu/dokumentum/m789umvt__12/

[17] A new generation cyber-physical system: A comprehensive review ... https://www.sciencedirect.com/science/article/abs/pii/S0167404824004000

[18] [PDF] ÜZLET 4.0 - Corvinus Research Archive https://unipub.lib.uni-corvinus.hu/6320/1/EFOP_konyv_mester_veg.pdf

[19] 5G-Enabled Cyber-Physical Systems for Smart Transportation Using ... https://www.mdpi.com/2227-7390/11/3/679

[20] [PDF] Ipar 4.0 által indukált szervezeti átalakulási folyamatok nemzetközi ... https://real-phd.mtak.hu/1988/1/Katona_Andrea_dissertation.pdf

Ábrajegyzet:

[1] https://www.osti.gov/servlets/purl/2281809
[2] https://wipiec.digitalheritage.me/index.php/wipiecjournal/article/view/39
[3] https://vbn.aau.dk/ws/portalfiles/portal/661305137/Robotic_Cell_paper_ICAR_2023.pdf[4]
[5] https://www.researchgate.net/figure/SPARROW-scheme-exploiting-RA-procedure-in-LTE-5G_fig3_354207945
[6] https://www.researchgate.net/figure/The-system-deployment-of-IoT-based-vehicular-network_fig1_353099678

2.25. 5G hálózat szerepe az okosotthonok IoT eszközeinek valós idejű kommunikációjában

IPAR 4.0 TECHNOLÓGIÁK

5G hálózat szerepe az okosotthonok IoT eszközeinek valós idejű kommunikációjában

Pataki Árpád Károly

[redacted]

(GKNB_INTM087)

2024/2025/2

Tartalom

Bevezetés: 3
Bevezető kontextus: 5
5G és IoT kapcsolata: 5
Problémafelvetés: 5
Technikai háttér: 6
Az 5G Kulcsjellemzői: 6
URLLC: 6
IoT protokollok és 5G: 6
MQTT: 6
CoAP: 7
Valós idejű kommunikáció alkalmazási területei: 8
Biztonsági rendszerek: 8
Valós idejű képfeldolgozás okoskamerákon 5G-s adatátvitellel: 9
Azonnali riasztás küldése behatolás észlelésekor: 10
Energiamenedzsment: 10
Intelligens mérőórák adatainak azonnali feldolgozása és visszacsatolás: 10
Napelem-tárolórendszerek dinamikus vezérlése hálózati terhelés alapján: 11
Gyakorlati példák és esettanulmányok: 12
Háztartási automatizáció: 12
5G-s okos termosztátok alkalmazása valós idejű külső hőmérsékletadatok alapján: 12
Ipari IoT Konvergencia: 13
Otthoni 3D nyomtatók távfelügyelete: 14
Összegzés és következtetések: 16
Kutatási irányok: 17
Összegzés: 19

Bevezetés:

A beadandó házi feladat célja, hogy bemutassa az 5G mobilhálózatok jelentőségét az okosotthonokban alkalmazott IoT (Internet of Things) eszközök valós idejű kommunikációjában. Az elemzés során kitérünk arra, hogy az 5G technológia milyen előnyöket kínál a hagyományos vezeték nélküli hálózatokhoz képest, különös tekintettel az alacsony késleltetésre, a nagy sávszélességre, valamint a nagyszámú eszköz egyidejű kiszolgálására.

Az első részében röviden ismertetem az 5G és az IoT kapcsolatát, valamint felvetjük a problémát, miszerint a jelenlegi WiFi és 4G hálózatok nem képesek hatékonyan kezelni a modern okosotthonokban egyre növekvő számú IoT-eszköz egyidejű kommunikációját.

Ezt követően részletesen bemutatom az 5G technológia kulcsjellemzőit, kiemelve az Ultra-Reliable Low Latency Communication (URLLC) szerepét, amely lehetővé teszi a kritikus rendszerek (például biztonsági riasztók) megbízható és gyors működését. Kitérünk továbbá arra is, hogy az elterjedt IoT kommunikációs protokollok (mint az MQTT és a CoAP) miként illeszthetők az 5G hálózati infrastruktúrába.

A beadandó harmadik részében konkrét alkalmazási területeken keresztül szemléltetjük az 5G előnyeit, például a valós idejű képfeldolgozást okoskamerák esetén, az azonnali riasztások küldését behatolás esetén, valamint az energiamenedzsment rendszerekben – például az intelligens mérőórák és napelem-tároló rendszerek valós idejű adatfeldolgozását és dinamikus vezérlését.

A beadandó végén összefoglaljuk az 5G technológia okosotthonokban betöltött szerepét, illetve a jövőbeli fejlődési lehetőségeket is érintjük.

Bevezető kontextus:

Itt az 5G és az IoT kapcsolata valamint ennek a lehetséges problémáit mutatnám be.

5G és IoT kapcsolata:

Az 5G és az IoT kapcsolata alapvetően átalakítja az okosotthonok működését, mivel a technológia három kulcsjellemzője – alacsony késleltetés, nagy sávszélesség és magas eszközkapacitás, minden korábbinál hatékonyabb kommunikációs hálózatot biztosít.

Problémafelvetés:

A hagyományos WiFi és 4G hálózatok korlátai jelentős kihívásokat jelentenek az okosotthonok IoT-eszközeinek nagy számú egyidejű kapcsolatánál, ami három fő területre bontható:

1. Eszközkapacitás korlátai:
    a. **WiFi túlterheltség**: A legtöbb háztartási WiFi router 50-100 eszköz egyidejű kezelésére van tervezve, de a komplex okosotthonokban (kamerák, érzékelők, relék) ez a szám gyakran túllépődik, vezetve kapcsolati hibákhoz és instabilitáshoz.
2. Késleltetés és sávszélesség problémák:
    a. **4G késleltetés**: A 4G hálózatok 30-50 ms közötti késleltetése nem megfelelő valós idejű adatfeldolgozáshoz, például okoskamerák streamelésénél.
    b. **Sávszélesség-megosztás**: Több eszköz egyidejű használata esetén a WiFi sávszélesség gyorsan kimerül, különösen videóstreamelés vagy felhőalapú szolgáltatások mellett.
3. Technikai korlátok:
    a. **Interferencia**: Sűrűn lakott területeken a WiFi csatornák átfedése instabil kapcsolatot és adatvesztést okoz

Technikai háttér:

Az 5G hálózatok kulcsjellemzői illetve ennek technológiai és protokolljai.

Az 5G Kulcsjellemzői:

Az 5G technológiás hálózatok jelentős adatátviteli sebességnövekedéssel, ultraalacsony késleltetéssel jelent meg emellett hatalmas eszköz kapacitással így ideális az okosotthonok és IoT eszközök számára.

URLLC:

Az Ultra-Reliable Low Latency Communication (URLLC) <1 ms-os késleltetést és 99,999%-os megbízhatóságot biztosít kritikus okosotthoni rendszerekhez. Fő jellemzője a valós idejű adatátvitel, ami létfontosságú például:

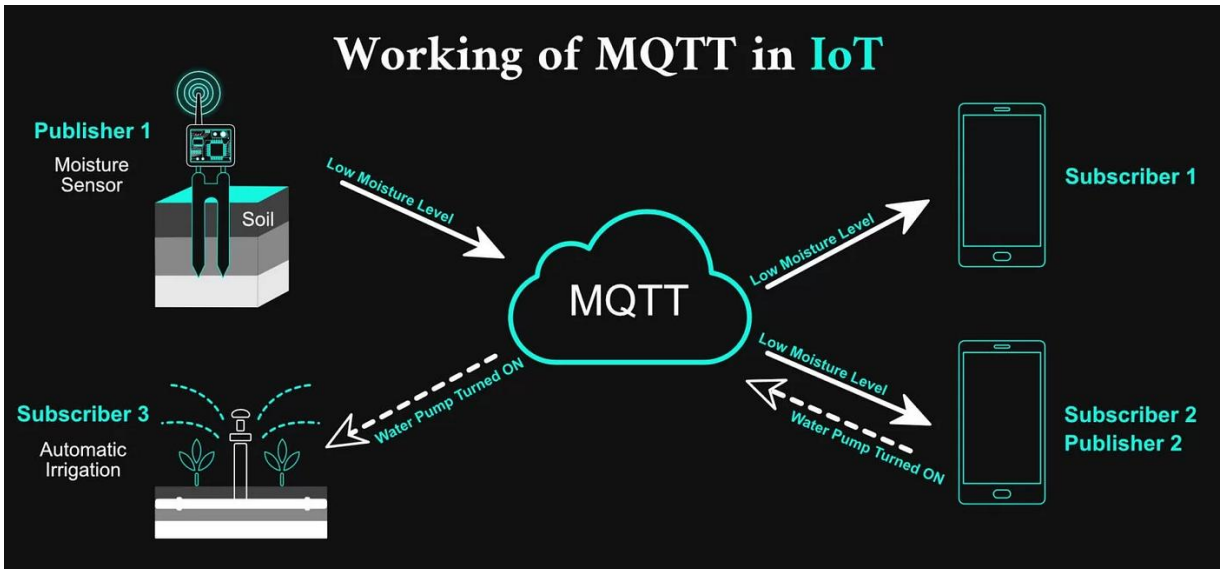
- **Biztonsági riasztórendszerek** azonnali aktiválódása behatolás észlelésekor .
- **Okoskamerák** valós idejű videóstreamelése és elemzése anélkül, hogy képkockák elvesznének .
- **Tűzjelző rendszerek** azonnali működése, minimalizálva a fals riasztások kockázatát .

A hagyományos WiFi és 4G rendszerekkel ellentétben az URLLC-s rendszerek olyan alkalmazási területeken fordulnak elő ahol létfontosságú a rögtönzött válaszidő és közel 100%-os elérhetőség.

IoT protokollok és 5G:

MQTT:

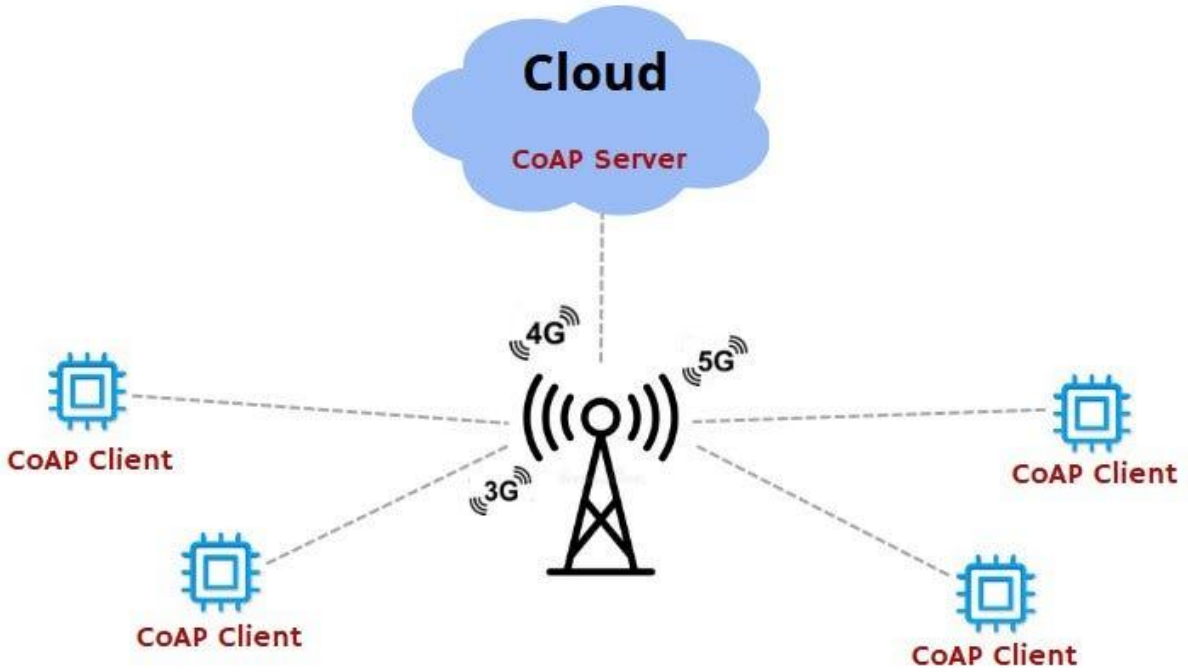
Az MQTT egy könnyű, üzenetközpontú IoT-protokoll, amely TCP/IP-n keresztül működik, és megbízható, valós idejű adatcserét biztosít okosotthoni eszközök között, különösen ott, ahol nagy megbízhatóság és gyors reakció szükséges.



MQTT Működése az IoT rendszerekben (medium.com)

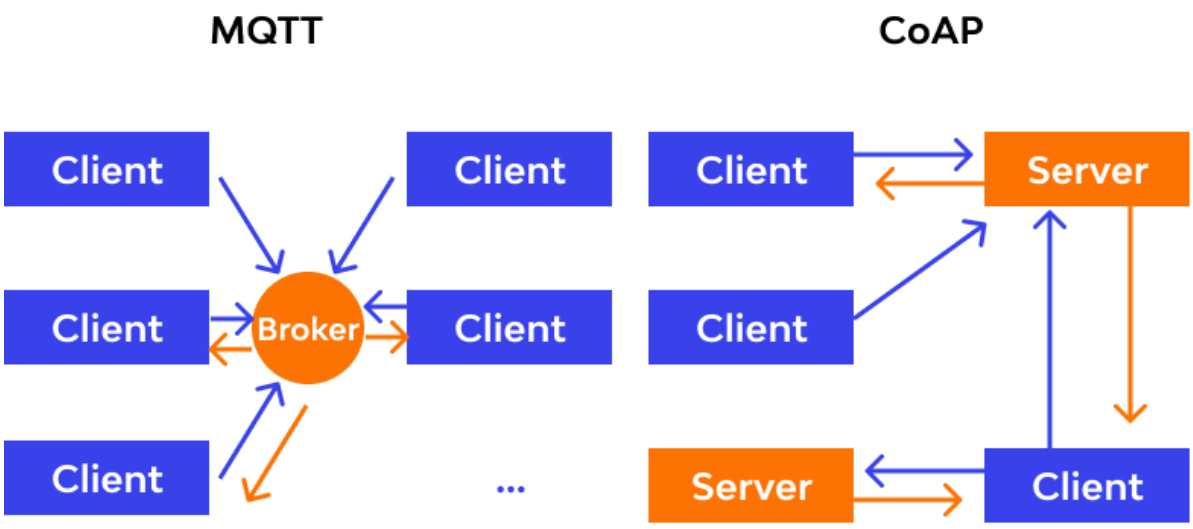
CoAP:

A CoAP egy egyszerű, energiatakarékos protokoll, amely UDP-re épül, főleg kis fogyasztású érzékelők és mérőórák kommunikációjára fejlesztették, és jól alkalmazható tömeges IoT-eszközök gyors, hatékony adatcseréjére.



CoAP rendszer működése (medium.com)

7



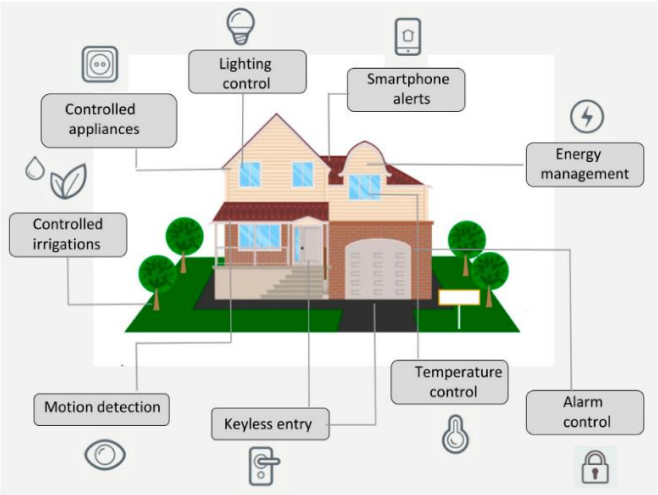
MQTT és a CoAP működésének összehasonlítása (wallarm.com)

Valós idejű kommunikáció alkalmazási területei:

A valós idejű kommunikáció lehetővé teszi az okosotthonok eszközei számára, hogy azonnal és megbízhatóan reagáljanak a különféle eseményekre és vezérlési parancsokra.

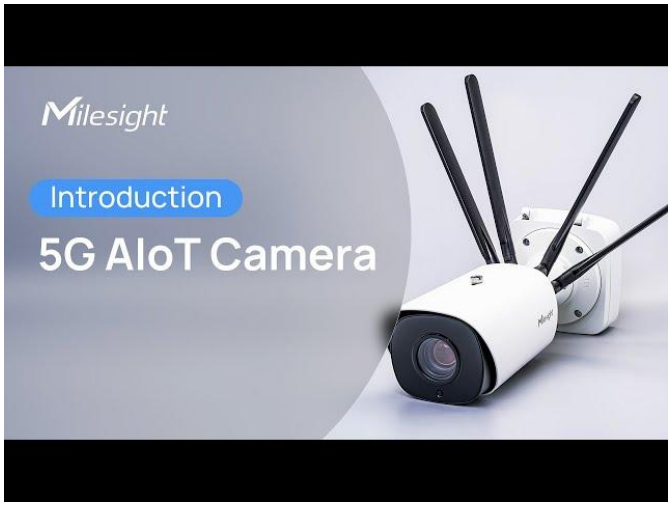
Biztonsági rendszerek:

Az okosotthonok biztonsági rendszerei valós idejű kommunikációval azonnal érzékelik és jelzik a behatolást vagy veszélyt, így gyorsan értesítik a tulajdonost és szükség esetén a hatóságokat is.



5G Biztonsági rendszerek (mdpi.com)

Valós idejű képfeldolgozás okoskamerákon 5G-s adatátvitellel:

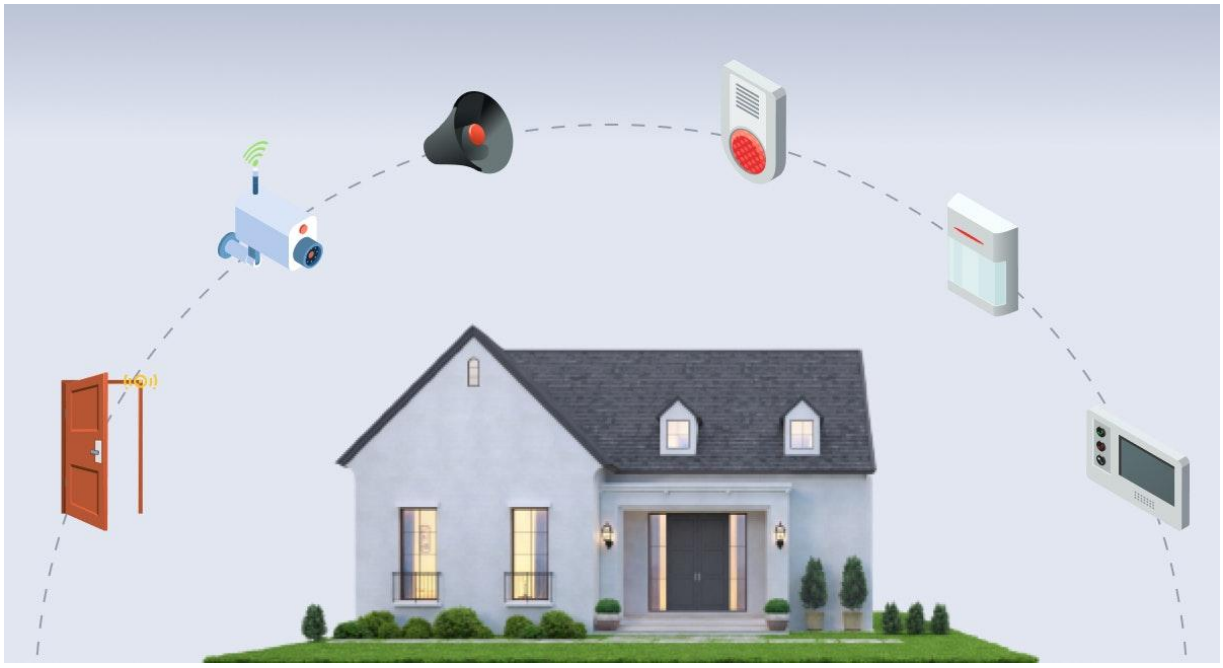


5G AIoT Kamerarendszer (milesight.com)

Az 5G-s adatátvitellel működő okoskamerák lehetővé teszik a nagy felbontású videók és képek valós idejű feldolgozását és továbbítását, mivel az 5G hálózat rendkívül nagy sávszélességet és alacsony, akár 1 ms alatti késleltetést biztosít, emellett akár AI/MI képességekkel is rendelkezhetnek a biztonság és tárgy/személyek felismerésének növelése érdekében.

Azonnali riasztás küldése behatolás észlelésekor:

Az okosotthonok biztonsági rendszerei behatolás észlelésekor azonnali riasztást küldenek a tulajdonos okostelefonjára vagy más eszközére, így valós időben értesülhetünk a veszélyről, és gyorsan megtehetjük a szükséges lépéseket emellett a rendszer automatikusan hang- és fényjelzést is adhat a többi IoT/okosotthon eszközök segítségével.



IoT biztonsági rendszerek (intuz.com)

Energiamenedzsment:

Az energiamenedzsment az okosotthonokban az energiafogyasztás valós idejű mérését és optimalizálását jelenti, amivel csökkenthetők a költségek és növelhető a hatékonyság.

Intelligens mérőórák adatainak azonnali feldolgozása és visszacsatolás:

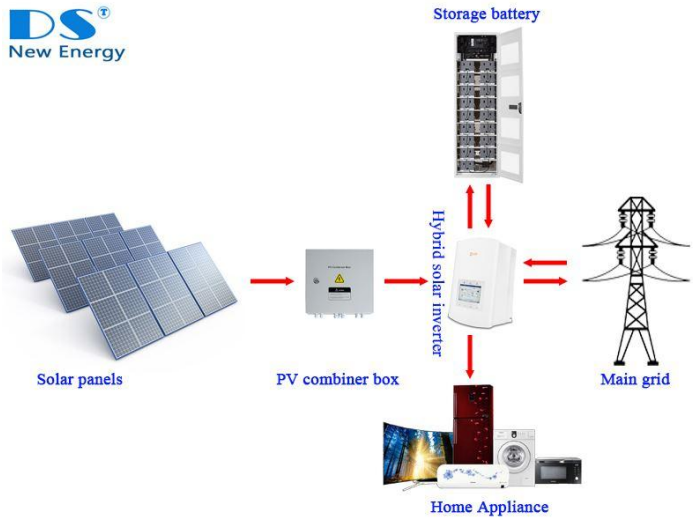
Az intelligens mérőórák az energiafogyasztás adatait valós időben, automatikusan továbbítják a központi adatközpontba, ahol azokat azonnal feldolgozzák és visszacsatolják a felhasználó számára. Ez lehetővé teszi, hogy a lakók

folyamatosan nyomon kövessék fogyasztásukat, azonnali visszajelzést kapjanak, és ennek alapján tudatosabban, hatékonyabban gazdálkodjanak az energiával.

Intelligens mérőórák (homewizard.com)

Napelem-tárolórendszerek dinamikus vezérlése hálózati terhelés alapján:

A napelem-tárolórendszerek dinamikus vezérlése lehetővé teszi, hogy a rendszer folyamatosan figyelje a hálózati terhelést és a pillanatnyi energiaigényt, majd ehhez igazítva automatikusan szabályozza a tárolt napenergia felhasználását vagy visszatáplálását az elektromos hálózatba. Ez a megoldás optimalizálja az energiafogyasztást: a rendszer akkor használja fel vagy adja vissza az eltárolt energiát, amikor a hálózati terhelés magas, illetve amikor az áram ára kedvezőbb, így növeli a hatékonyságot és csökkenti a költségeket



Hibrid tárolórendszer napelemekhez (dsnsolar.com)

Gyakorlati példák és esettanulmányok:

Konkrét példákon és valós esettanulmányokon keresztül szemléltetjük, miként járulnak hozzá az intelligens rendszerek a kényelemhez, az energiahatékonysághoz, a biztonsághoz és a fenntartható működéshez, valamint milyen gyakorlati tapasztalatokat szereztek a felhasználók ezek alkalmazása során.

Háztartási automatizáció:

5G-s okos termosztátok alkalmazása valós idejű külső hőmérsékletadatok alapján:

Az 5G-s okos termosztátok alkalmazása forradalmasítja az otthoni hőmérsékletszabályozást, különösen a valós idejű külső hőmérsékletadatok felhasználásával. Ezek a modern eszközök az 5G hálózat nagy sávszélességét és alacsony késleltetését kihasználva képesek folyamatosan, azonnal fogadni és feldolgozni a külső időjárási információkat, valamint más IoT szenzorok adatait is. Az 5G kapcsolat biztosítja, hogy a termosztát valós időben reagáljon a hőmérséklet-változásokra, például egy hirtelen hidegfront vagy melegedés esetén, így a fűtési vagy hűtési rendszer azonnal alkalmazkodik az aktuális körülményekhez.

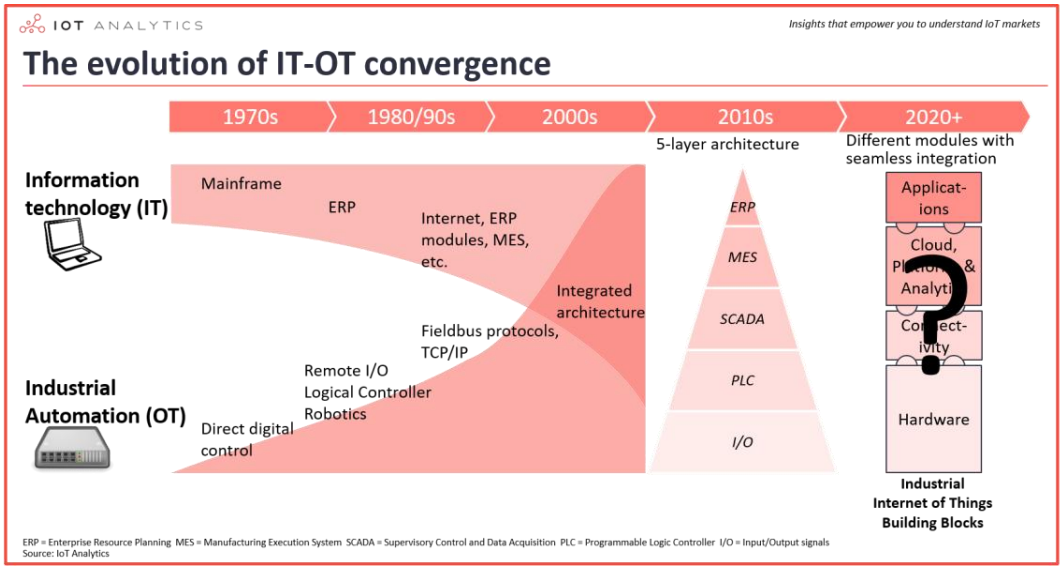
A fejlett algoritmusok és mesterséges intelligencia révén az okos termosztátok nemcsak a külső hőmérsékletet veszik figyelembe, hanem elemzik a felhasználók szokásait, a lakás kihasználtságát, valamint az energiaárakat is, hogy a lehető legoptimálisabb hőmérsékletet biztosítsák minimális energiafelhasználás mellett. Az 5G hálózat lehetővé teszi, hogy ezek a döntések és beállítások szinte késedelem nélkül történjenek, így a lakók mindig komfortos környezetben tartózkodhatnak, miközben csökken az energiafogyasztás és a költségek.

Az 5G-s termosztátok további előnye, hogy távolról, okostelefonról vagy más eszközről is vezérelhetők, illetve integrálhatók más okosotthoni rendszerekkel,

például ablaknyitás-érzékelőkkel vagy időjárás-előrejelző szenzorokkal. Ez a komplex, valós idejű adatfeldolgozás és automatizált vezérlés nemcsak a kényelmet növeli, hanem hozzájárul az energiahatékonysághoz és a fenntarthatósághoz is, hiszen a rendszer elkerüli a felesleges fűtést vagy hűtést, és optimalizálja az energiafelhasználást a mindenkori időjárási és lakáshasználati viszonyokhoz igazodva.

Okos termosztát (CNET.com)

Ipari IoT Konvergencia:



IT-OT konvergencia (iot-analytics.com)

Az ipari IoT konvergencia az ipari termelés digitális átalakulásának egyik kulcstényezője, amely során az információs technológia (IT) és az üzemi technológia (OT) rendszerei egyre szorosabban integrálódnak egymással. Ez a folyamat lehetővé teszi, hogy a hagyományosan elkülönülten működő informatikai hálózatok, adatfeldolgozó rendszerek, valamint a gyártósorokat és gépeket irányító automatizálási megoldások összekapcsolódjanak, és egységes, átlátható, valós idejű adatáramlást biztosítsanak.

Az ipari IoT konvergencia révén megvalósul az Ipar 4.0 alapelve, amely a gyártási folyamatok digitalizációjára, automatizálására és intelligens hálózatba szervezésére törekszik. Ennek eredményeként az érzékelők, gépek, termelési modulok és informatikai rendszerek egyetlen, összekapcsolt ökoszisztémában működnek együtt, lehetővé téve az adatok valós idejű elemzését, a folyamatok önoptimalizálását és a decentralizált döntéshozatalt.

A konvergencia számos előnnyel jár: növeli a gyártás rugalmasságát, javítja a termelékenységet, csökkenti a költségeket, és támogatja a személyre szabott tömegtermelést. Ugyanakkor kihívásokat is jelent, például a különböző rendszerek közötti kompatibilitás, a kiberbiztonság és a szervezeti kultúra összehangolása terén. Összességében az ipari IoT konvergencia az okosgyárak és a modern ipari értékláncok működésének alapját teremti meg, új szintre emelve a digitalizáció és az automatizálás lehetőségeit az iparban.

Otthoni 3D nyomtatók távfelügyelete:

Az otthoni 3D nyomtatók távfelügyelete gyártási minőségellenőrzési rendszereken keresztül lehetővé teszi a nyomtatási folyamatok valós idejű, távoli nyomon követését és irányítását, ami jelentősen javítja a gyártás minőségét és hatékonyságát. A modern távfelügyeleti szoftverek például a 3DPrinterOS vagy az Octo Everywhere, élő adatokat szolgáltatnak a nyomtató állapotáról, a hőmérsékletről, a filamenthasználatról és a nyomtatás előrehaladásáról, valamint kameraképen keresztül is figyelhetjük a folyamatokat. Ezek a rendszerek

automatikus riasztásokat küldenek hibák, például filamenthiány vagy nyomtatási rendellenességek esetén, így a felhasználó azonnal beavatkozhat, akár távolról is leállíthatja vagy újraindíthatja a nyomtatást.

A minőségellenőrzési modulok további előnye, hogy a nyomtatási paraméterek, például a rétegvastagság vagy a sebesség - valós időben módosíthatók, így a készülő alkatrészek pontossága és felületi minősége optimalizálható a folyamat során. A rendszer képes statisztikákat és jelentéseket is készíteni a hibákról, anyagfelhasználásról és gépkarbantartásról, ami segít a termelékenység növelésében és a hibák megelőzésében. A távfelügyelet és a minőségellenőrzés kombinációja tehát nemcsak kényelmesebbé és rugalmasabbá teszi az otthoni 3D nyomtatást, hanem biztosítja a folyamatos, magas szintű minőséget is.

Creality nyomtatók távoli megfigyelése (creality.com)

Összegzés és következtetések:

Az 5G technológia előnyei alapjaiban alakítják át a digitális kommunikáció, az ipar, a mindennapi élet és az okos eszközök működését. A legszembetűnőbb újítás a jelentősen megnövelt adatátviteli sebesség: az 5G akár százszor gyorsabb letöltést tesz lehetővé, mint a 4G, így a nagy felbontású videók, élő közvetítések, vagy akár a nagy méretű fájlok letöltése és feltöltése pillanatok alatt elvégezhető. Ez a sebesség nemcsak a felhasználói élményt javítja, hanem új távlatokat nyit például a távmunka, a felhőalapú játék, a virtuális és kiterjesztett valóság, valamint az ipari automatizáció területén is.

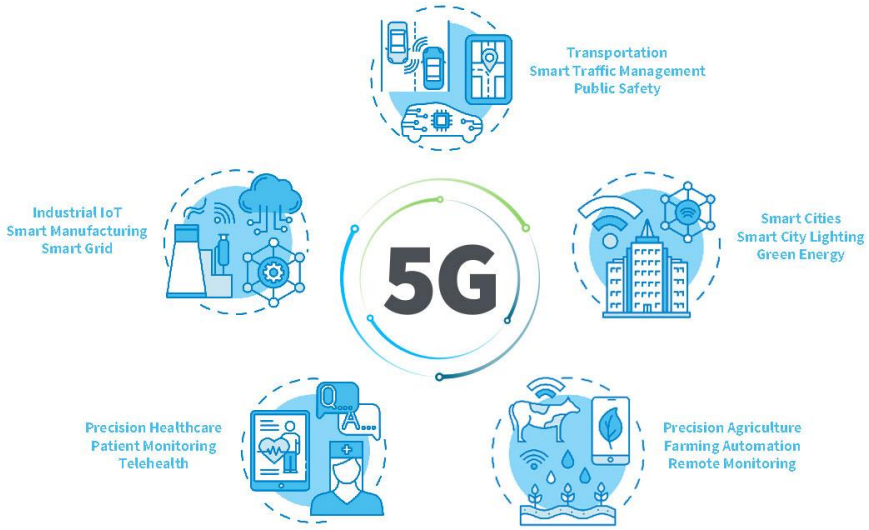
Az 5G másik kulcsfontosságú előnye az ultraalacsony késleltetés: az adatok továbbítása akár 1 milliszekundum alatt megtörténhet, ami a 4G-hez képest töredéke az eddigi válaszidőnek. Ez a tulajdonság elengedhetetlen a valós idejű alkalmazásokhoz, mint például az önvezető járművek, a távirányítású műtétek, a biztonsági rendszerek vagy az okosotthonok automatizált vezérlése. Az alacsony késleltetés biztosítja, hogy a hálózaton keresztül küldött parancsok és adatok szinte azonnal célba érnek, így a reakcióidő minimálisra csökken.

Az 5G jelentősen növeli a hálózati kapacitást is: akár egymillió eszközt képes egyetlen négyzetkilométeren belül kiszolgálni, ami különösen fontos az IoT (Internet of Things) eszközök robbanásszerű terjedése miatt. Ez lehetővé teszi, hogy okosvárosok, ipari üzemek, vagy akár egyetlen háztartás is egyszerre több ezer eszközt csatlakoztasson a hálózathoz anélkül, hogy az adatátvitel vagy a kapcsolat stabilitása romlana.

Az 5G rugalmas és dinamikusan konfigurálható hálózati architektúrával rendelkezik, amely automatikusan alkalmazkodik a felhasználói igényekhez és a terheléshez. Ez a rugalmasság biztosítja, hogy a hálózat mindig optimális teljesítményt nyújtson, legyen szó nagy forgalmú városi környezetről vagy távoli ipari létesítményekről. Emellett az 5G energiahatékonyabb működést is lehetővé

tesz, így nagyobb adatforgalom mellett is csökken a hálózati energiafogyasztás, hozzájárulva a fenntarthatósághoz.

Az 5G előnyei tehát túlmutatnak a puszta sebességnövekedésen: a technológia lehetővé teszi a valós idejű, megbízható és nagyszabású adatkommunikációt, támogatja az intelligens eszközök és rendszerek fejlődését, és új lehetőségeket teremt az ipar, a közlekedés, az egészségügy, a szórakoztatás és a mindennapi élet szinte minden területén. Ezáltal az 5G nemcsak a digitális infrastruktúra következő lépcsőfoka, hanem a jövő összekapcsolt világának alapja.



Az 5G előnyei és használati területei (digi.com)

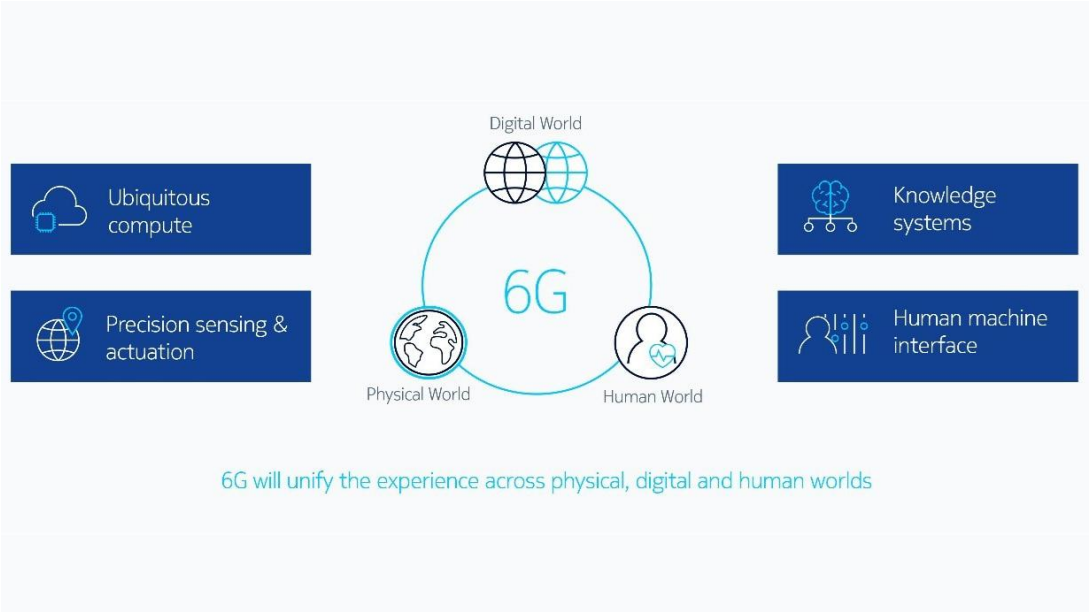
Kutatási irányok:

A 6G és a kvantumalapú kommunikációs protokollok fejlesztése az okosotthonok következő nagy technológiai ugrását készíti elő.

A 6G várhatóan sokszorosára növeli a hálózati sebességet, kapacitást és csökkenti a késleltetést, akár 1000 Gbps adatátviteli sebességet és 100 mikroszekundum alatti válaszidőt is elérhet, miközben lehetővé teszi több milliárd eszköz egyidejű, megbízható összekapcsolását, valamint a mesterséges intelligencia és a valós idejű adatfeldolgozás mély integrációját az otthoni rendszerekbe. A 6G

egyik fő kutatási iránya a biztonság, ezért egyre nagyobb hangsúlyt kapnak a kvantumkommunikációs protokollok, például a kvantumkulcs-elosztás (QKD), amelyek a kvantummechanika elveit kihasználva teszik szinte feltörhetetlenné az adatcserét.

Ezek a fejlesztések nemcsak a hálózati teljesítményt, hanem az adatvédelem szintjét is forradalmasítják, így a jövő okosotthonai egyszerre lesznek gyorsabbak, biztonságosabbak és sokkal több eszközt képesek majd kezelni, mint napjaink rendszerei.



6G Részei bemutatva (nokia.com)

Összegzés:

Az okosotthonok és IoT-eszközök fejlődésében kiemelkedő szerepet játszik az 5G technológia, amely forradalmasítja a valós idejű kommunikációt, a rendszerek megbízhatóságát és a skálázhatóságot. A hagyományos WiFi és 4G hálózatok korlátai, például a túlterheltség, a magas késleltetés és az alacsony eszközkapacitás, jelentős akadályt jelentenek a modern okosotthonok számára, ahol tucatnyi eszköz egyidejű kapcsolódása és azonnali reagálás szükséges. Az 5G ezeket a korlátokat leküzdve ultraalacsony késleltetést (<1 ms), nagy sávszélességet (akár 10–20 Gbps) és milliónyi eszköz egyidejű kiszolgálását biztosítja, így létfontosságúvá válik a kritikus alkalmazásokhoz, mint a biztonsági riasztórendszerek vagy az energiamenedzsment.

Az Ultra-Reliable Low Latency Communication (URLLC) szabvány lehetővé teszi a valós idejű adatátvitelt, ami például az okoskamerák élő streamelésénél vagy a napelem-tárolórendszerek dinamikus vezérlésénél nélkülözhetetlen. Az IoT-protokollok, például az MQTT és a CoAP, kiegészítik az 5G előnyeit: míg az MQTT megbízható, valós idejű kommunikációt biztosít a felhővel, a CoAP energiatakarékos adatcserét tesz lehetővé alacsony fogyasztású érzékelők számára.

A valós idejű alkalmazások közül kiemelkednek a biztonsági rendszerek, ahol a behatolás észlelésekor azonnali riasztás történik, valamint az energiamenedzsment, ahol az intelligens mérőórák és napelem-rendszerek adatai dinamikusan vezérlik az energiafelhasználást. Ezek a megoldások nemcsak a kényelmet növelik, hanem hozzájárulnak a fenntarthatósághoz és a költséghatékonysághoz.

A jövő kutatási irányai, például a 6G hálózatok és a kvantumalapú kommunikációs protokollok, további lehetőségeket rejtenek. A 6G várhatóan százszoros sebességnövekedést, mikroszekundumos késleltetést és még magasabb eszközkapacitást hoz, míg a kvantumtechnológiák (pl. kvantumkulcselosztás) radikálisan javítják az adatbiztonságot. Ezek az innovációk alapvetően átalakítják majd az okosotthonok működését, lehetővé téve a teljesen autonóm, önoptimalizáló

rendszerek létrehozását, ahol az emberi beavatkozás nélkül működő eszközök szorosabban integrálódnak a mindennapi életbe.

Források:

[1] Az 5G és az IoT Kapcsolata, „5G és IoT: a legmodernebb mobilhálózat és a Dolgok Internete”, https://www.yettel.hu/tippek/5g-es-az-internet-of-things

[2] 2.a 5G kulcsjellemzői, „Mi is az 5G?”, https://bytech.hu/5g/

[3] 2.a 5G kulcsjellemzői, „Mi az az 5G és szükségem van-e rá?”, https://www.samsung.com/hu/mobile-phone-buying-guide/what-is-5g/

[4] 2.b URRL, „What is URLLC?”, https://inseego.com/resources/5g-glossary/what-is-urllc/

[5] 2.c MQTT, CoAP, „8 IoT Protocols and Standards Worth Exploring in 2024”, https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m

[6] „Intelligens megfigyelés bárhol, bármikor: Az okos kamerák végtelen lehetőségei”, https://kameradepo.hu/okos-kamerak-vegtelen-lehetosegei

[7] 3.c Azonnali riasztás küldése behatolás észlelésekor., „OKOS OTTHON RIASZTÁS ÉS BELÉPTETÉS VEZÉRLÉS”, https://incelor.com/okos-otthon-biztonsag-beleptetes/

[8] 3.d Energiamenedzsment, „Energiamenedzsment az otthonunkban”, https://legrand.hu/rolunk/cikkek/hirek_okos-tanacsok-otthonra/energiamenedzsment-az-otthonunkban

[9] 3.e Intelligens mérőórák adatainak azonnali feldolgozása és visszacsatolás, „Általános tájékoztatás az okos mérésről”, https://mvmhalozat.hu/aram/oldalak/1551

[10] 3.f Napelem-tárolórendszerek dinamikus vezérlése hálózati terhelés alapján, „Energiatároló Napelemes Rendszerekhez”, https://powercharge.hu/2025/01/15/energiatarolo-napelemes-rendszerekhez/

[11] 4.b Ipari IoT konvergencia, „Az IT és az OT viszonyrendszere, a konvergencia humán és adminisztratív aspektusai”, https://alverad.hu/wp-content/uploads/2024/02/alverad-ot-human-aspektusok-1122-FIN.pdf

[12] 5.b Kutatási irányok: 6G előkészítése okosotthonokban, kvantumalapú kommunikációs protokollok., „Preparing for the Future of

Connectivity: What 6G Means for Our Networks”, https://www.taoglas.com/blogs/preparing-for-the-future-of-connectivity-what-6g-means-for-our-networks/

2.26. Zsarolóvírusok elleni védekezés a CPS rendszerekben SZILÁGYI MÁRK

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

IPAR 4.0 TECHNOLÓGIÁK

Zsarolóvírusok elleni védekezés a CPS rendszerekben

SZILÁGYI MÁRK
[redacted]

(GKNB_INTM087)

2024/2025/2

Abstract

A zsarolóvírusok jelentős fenyegetést jelentenek a Cyber-Physical Systems rendszerek számára mivel ezek a kritikus infrastruktúrákban, ipari vezérlőrendszerekben és IoT eszközökben is komoly károkat okozhatnak. A dolgozat célja, hogy átfogó képet adjon a zsarolóvírusok működéséről és az ipari környezetekben alkalmazható védekezési stratégiákról. A dolgozat részletesen bemutatja a WannaCry és NotPetya támadások hatásait, valamint azok tanulságait és elemzi a jelenlegi fenyegetéseket, mint a Black Basta és LockBit zsarolóvírusokat azok működését és ipari rendszerekre gyakorolt hatását.

Az esszé kiemeli a kiberbiztonsági megoldásokat, mint a titkosítás, hozzáférés-ellenőrzési mechanizmusok és végpontvédelmi rendszerek, valamint ezek szerepét a zsarolóvírusok elleni védekezésben. A dolgozat felhívja a figyelmet a Zero Trust biztonsági modell alkalmazásának és a mesterséges intelligencia alapú fenyegetésészlelés fontosságára. A folyamatosan fejlődő ransomware fenyegetések miatt a kutatás hangsúlyozza a védekezési stratégiák folyamatos fejlesztésének és a legújabb fenyegetésekhez való alkalmazkodás fontosságát.

A dolgozat továbbá részletesen elemzi az ipari kontroll rendszerek és IoT eszközök sebezhetőségeit és bemutatja azokat a kiberbiztonsági intézkedéseket, amelyek a hatékony védelem érdekében szükségesek. A cél, hogy átfogóan bemutassa a legjobb ipari gyakorlatokat a zsarolóvírusok elleni védekezésben és felhívja a figyelmet a folyamatos fejlesztés és a naprakész kiberbiztonsági stratégiák alkalmazásának fontosságára a CPS rendszerek védelmében.

Tartalomjegyzék

Abstract 2

Bevezetés 5

A téma jelentősége 5

A CPS rendszerek és a kiberbiztonság kapcsolata 6

Zsarolóvírusok története és működése 7

Zsarolóvírusok evolúciója 7

Zsarolóvírusok működése 8

Támadások fajtái 9

Kiberbiztonsági alapelvek 10

Zero Trust modellek 10

Végpontvédelmi rendszerek 11

Ransomware példák és védekezési stratégiák 13

WannaCry és NotPetya 13

WannaCry 13

NotPetya 14

Black Basta és LockBit 15

Black Basta 16

LockBit 17

Kiberbiztonsági megoldások és technológiák 20

1. Tűzfalak és behatolásmegelőző rendszerek (IPS) 21

2. Antivirus és antimalware rendszerek 22

3. Kétfaktoros hitelesítés (2FA) 23

4. Biztonsági információ- és eseménykezelő rendszerek (SIEM) 24

5. Zsarolóvírus-ellenes megoldások 25

6. Hálózati szegmentálás és VPN 25

7. Felhőbiztonság 26

Titkosítás, hozzáférés-ellenőrzés, HSM 26

Titkosítás 26

Hozzáférés-ellenőrzés 28

HSM (Hardware Security Module) 29

ICS/SCADA rendszerek és IoT biztonság 30

ICS/SCADA biztonság 30

IoT biztonság 31

Jövőbeli fenyegetések és védekezési trendek 32
AI-alapú támadások és automatizáció 32
AI-alapú támadások 32
Automatizáció a támadásokban 33
Prediktív biztonság és viselkedésalapú védelem 33
Prediktív biztonság 34
Viselkedésalapú védelem 35
Integráció és automatizálás 35
Blokklánc-technológia alkalmazása a védelemben 36
Decentralizált adatkezelés 36
Integráció a hozzáférés-ellenőrzésbe 37
Smart Contracts 37
Az etikai és társadalmi dimenziók a kiberbiztonságban 38
Személyes adatok védelme és magánélet 38
Adatvédelmi törvények és szabályozás 39
Adatkezelési felelősség és társadalmi hatások 40
Etikai és jogi kihívások 41

Bevezetés

A téma jelentősége

Napjainkban az ipari rendszerek egyre nagyobb mértékben támaszkodnak a kiberfizikai rendszerekre (Cyber-Physical Systems = CPS) (1. ábra) amelyek az informatikai és az operatív technológiai infrastruktúrák szoros integrációját jelentik. Az Ipar 4.0 és a digitalizáció térnyerésével a modern gyártósorok és azautomatizált vezérlőrendszerek és az összekapcsolt IoT-eszközök váltak az ipari termelés és a kritikus infrastruktúrák meghatározó elemeivé. Ez a fejlődés növelte a hatékonyságot és az innovációs lehetőségeket, azonban új fenyegetéseket is teremtett, amelyek közül az egyik legjelentősebb a zsarolóvírusok (ransomware) megjelenése volt.

A zsarolóvírusok olyan rosszindulatú szoftverek, amelyek titkosítják az áldozat adatait vagy rendszereit, majd váltságdíjat követelnek a visszaállításukért. A korábbi években tapasztalt támadások, például a WannaCry és a NotPetya, globális hatással bírtak, jelentős anyagi károkat okozva vállalatoknak, kormányzati intézményeknek és egészségügyi szolgáltatóknak. Az újabb fenyegetések, mint a Black Basta és a LockBit, egyre célzottabbá és fejlettebbé váltak, különösen az ipari szektorban, ahol az üzemleállások és adatvesztések súlyos következményekkel járhatnak.

A ransomwarek elleni védekezés ma már nem csak informatikai kérdés, hanem ipari és nemzetbiztonsági szempontból is kiemelt prioritás. A megelőzés és a védekezési stratégiák fejlesztése elengedhetetlen a kritikus infrastruktúrák védelme érdekében. A dolgozat részletesen bemutatja a zsarolóvírusok működését, az ipari rendszerekre gyakorolt hatásukat

valamint a védekezési lehetőségeket, különös tekintettel a Zero Trust architektúrára, a végpontvédelmi rendszerekre és a mesterséges intelligencia alapú fenyegetésészlelésre.[1]

1. ábra - https://media.licdn.com/dms/image/v2/C5112AQEsWJlLYoXU5w/article-cover_image-shrink_600_2000/article-cover_image-shrink_600_2000/0/1569171099453?e=2147483647&v=beta&t=nWQBUq5FrwpLtLljz3HqTPWKxBJHVj5ciLB2BDerDqE
Alapján fordítás

A CPS rendszerek és a kiberbiztonság kapcsolata

A CPS rendszerek az ipari automatizáció kulcsfontosságú elemei, amelyek az IT és OT rendszerek integrációjára épülnek. Ezekben a rendszerekben az intelligens szenzorok, vezérlőegységek és adatfeldolgozó infrastruktúrák együttesen működnek, hogy valós idejű döntéseket hozzanak az ipari folyamatok optimalizálása érdekében. Azonban az összekapcsolt eszközök és hálózatok egyre nagyobb támadási felületet biztosítanak a rosszindulatú szereplők számára különösen a zsarolóvírusok esetében.

A kiberbiztonsági kockázatok különösen kritikusak az olyan ágazatokban, mint az energiaellátás, a közlekedés és a gyártás, ahol a támadások nemcsak anyagi károkat, hanem emberéleteket is veszélyeztethetnek. Például az ipari kontroll rendszerek sebezhetőségei miatt a támadók képesek lehetnek a termelési folyamatok leállítására vagy a működés megzavarására. Az ilyen rendszerek biztonsága ezért nemcsak pénzügyi szempontból, hanem nemzetbiztonsági kérdésként is kiemelt figyelmet kap.

A Zero Trust architektúra az AI-alapú fenyegetésészlelés és a végpontvédelmi rendszerek (EDR, XDR) egyre fontosabb szerepet játszanak az ipari rendszerek védelmében. Az esszé bemutatja ezeket a technológiákat, valamint a legújabb támadási módszereket és azok elleni védekezési lehetőségeket.

Zsarolóvírusok története és működése

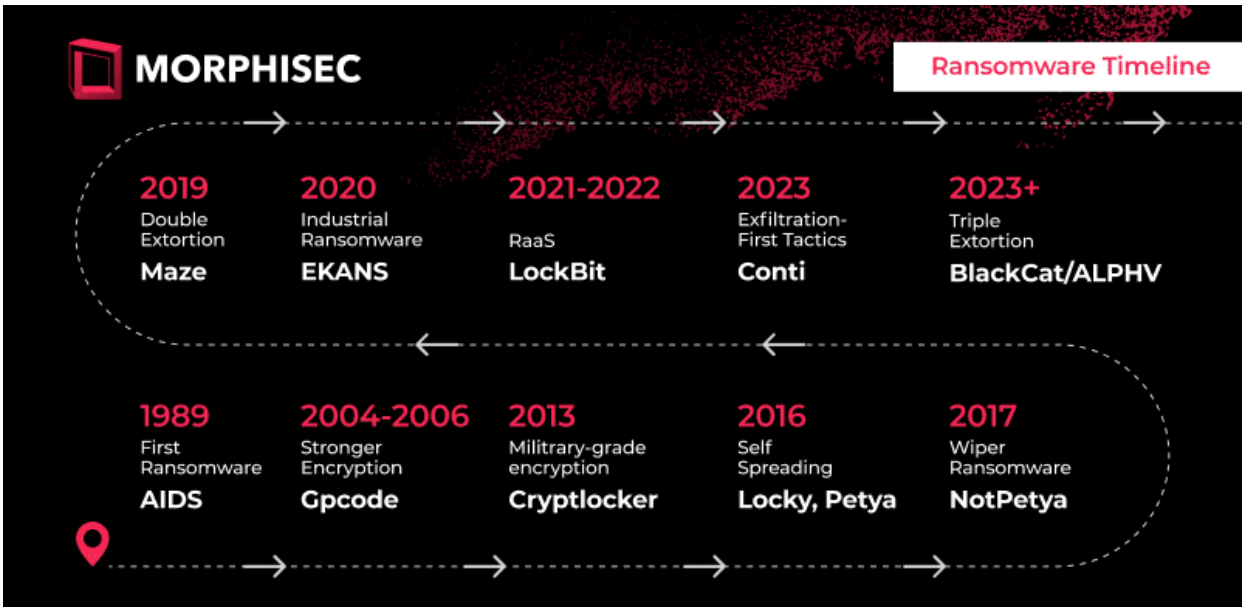
Zsarolóvírusok evolúciója

A zsarolóvírusok története az 1980-as évek végéig visszanyúlik amikor az első ismert vírus a PC Cyborg vagy AIDS megjelent. Ez a vírus még kezdetleges volt, egyszerűen módosította a fájlokat és a felhasználóktól váltságdíjat követelt postai úton. Azóta a zsarolóvírusok technikailag egyre fejlettebbé váltak és mára jóval nagyobb fenyegetést jelentenek az ipari és kiberfizikai rendszerek számára.

A 2000-es évek lején az első titkosítást alkalmazó zsarolóvírusok, például az Archiveus vagy a Gpcode is megjelentek. Azok AES és RSA algoritmusokat alkalmaztak a fájlok titkosítására. A támadások célzottabbak lettek és a fizetési módok is modernizálódtak és a kriptovaluták megjelenésével a nyomon követhetőség tovább csökkent.

A 2010-es évek közepétől a zsarolóvírusok terjedési módszerei is jelentősen fejlődtek. Az olyan önreplikáló zsarolóvírusok, mint a WannaCry és a NotPetya gyorsan elterjedtek világszerte és jelentős károkat okozva vállalatoknak és kormányzati szervezeteknek egyaránt. Ezek a vírusok kihasználták az operációs rendszerek és hálózatok biztonsági réseit, hogy automatizáltan fertőzzenek meg további eszközöket.

A modern változatok például a LockBit vagy a Black Basta különösen az ipari rendszerekre fókuszálnak. Ezek a vírusok képesek érzékeny adatokat titkositani vagy akár a teljes rendszert lebénítani és komoly pénzügyi következményeket okozhatnak. Az ilyen támadások során gyakran kettős zsarolási technikát alkalmaznak, vagyis nemcsak titkosítják az adatokat, hanem azok nyilvánosságra hozatalával is fenyegetőznek ha nem történik meg a váltságdíj fizetése.[2] (*2. ábra)*

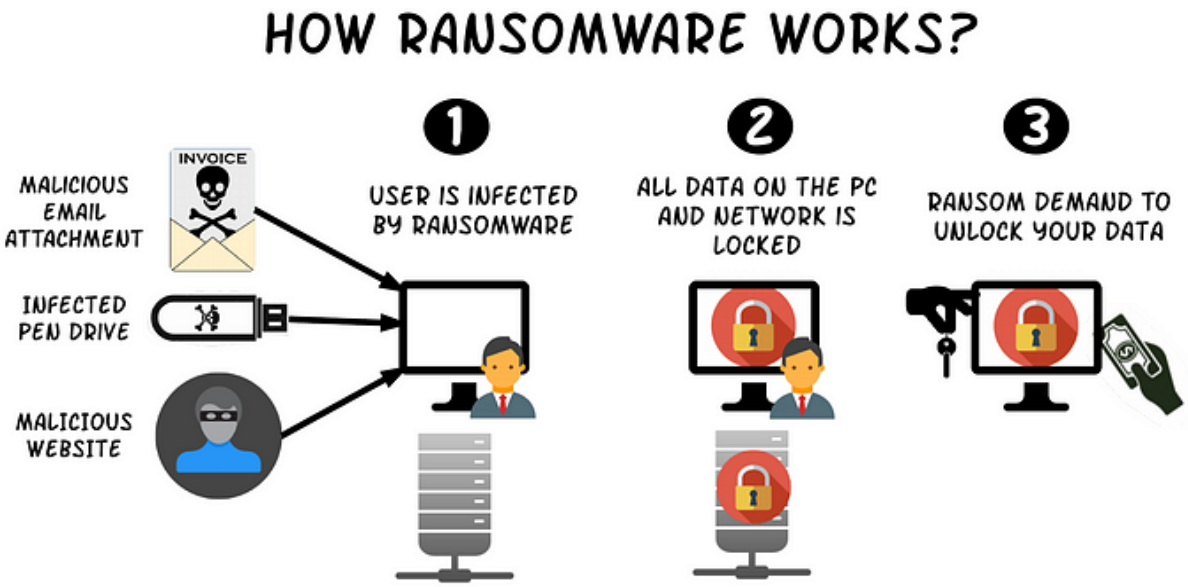


2. ábra - zsarolóvírusok evolúciója
https://www.morphisec.com/wp-content/uploads/2025/01/Timeline-of-Ransomware1.png.webp

Zsarolóvírusok működése

A működésük lényege az ahogy már feljebb is említettem, hogy titkosítják a célpont fájljait és váltságdíjat követelnek értük. A támadás tipikuson több szakaszból áll:

1. Bejútás a rendszerbe: A kezdeti fázisban a vírusok többféle módszerrel is bejuthatnank a rendszerbe ezek lehetnek adathalász emailek, rosszindulatú hírdetések, vírusos letöltések vagy akár távoli asztali támadások is.
2. Telepítés, terjedés: Lefuttatják magukat és megkeresik a hálózat további eszközeit, amelyeken megpróbálják kihasználni a serülékenységeket a továbbterjedéshez.
3. Titkosítás: A modern zsarolóvírusok AES vagy RSA titkosításokat használnak, amiket a titkosítókulcs nélkül szinte lehetetlen visszafejteni.
4. Váltságdíj: Az utolsó fázis már maga a zsarolás, ahol a váltságdíjat követelik valamilyen üzenet formájában,napjainkban gyakran kérik kriptovalutában a fizetést.[3] *(3. ábra)*



3. ábra - zsarolóvírusok működése
https://miro.medium.com/v2/resize:fit:720/format:webp/1*eeUhOlHKynIjgrpUtGm8Xg.png

Támadások fajtái

- Adathalászat (phishing): a leggyakoribb támadási fajta, amely során megtévesztő emailekkel vagy üzenetekkel juttatnak be vírusos fájlokat vagy rosszindulatú linkeket

- Szoftversérülékenységek kihasználása: elavult vagy le nem frissített rendszerek könnyű célpontot jelentenek a támadók számára. A WannaCry például az SMB protokoll egyik ismert sérülékenységét (EternalBlue) használta ki.

- Távoli asztali protokoll támadások (RDP): a rosszul védett RDP hozzáférések lehetőséget adnak a támadóknak, hogy jogosulatlanul bejuthassanak a rendszerekbe.

- Ellátási lánc támadások: az ellátási lánc gyenge pontjain keresztül bejutva a zsarolóvírusok egyszerre több szervezetet is megfertőzhetnek, ahogyan az a Kaseya vagy a SolarWinds támadások során történt.

Kiberbiztonsági alapelvek

A kibervédelmi stratégiák kidolgozásakor kulcsfontosságú, hogy a szervezetek olyan alapelveket kövessenek, amelyek lehetővé teszik az informatikai rendszerek biztonságos működtetését. A hagyományos védelmi módszerek - például a kizárólag perimétervédelemre épülő megoldások - ma már elégtelenek a fejlett és folyamatosan változó kibertámadásokkal szemben. Különösen a zsarolóvírusok és a fejlett fenyegetések (Advanced Persistent Threat, APT) megjelenése tette szükségessé az újfajta biztonsági szemlélet alkalmazását. Az elmúlt évek tapasztalatai azt mutatják, hogy két fő elvet érdemes kiemelten alkalmazni: a Zero Trust modelleket és a végpontvédelmi (Endpoint Detection and Response - EDR) rendszereket.

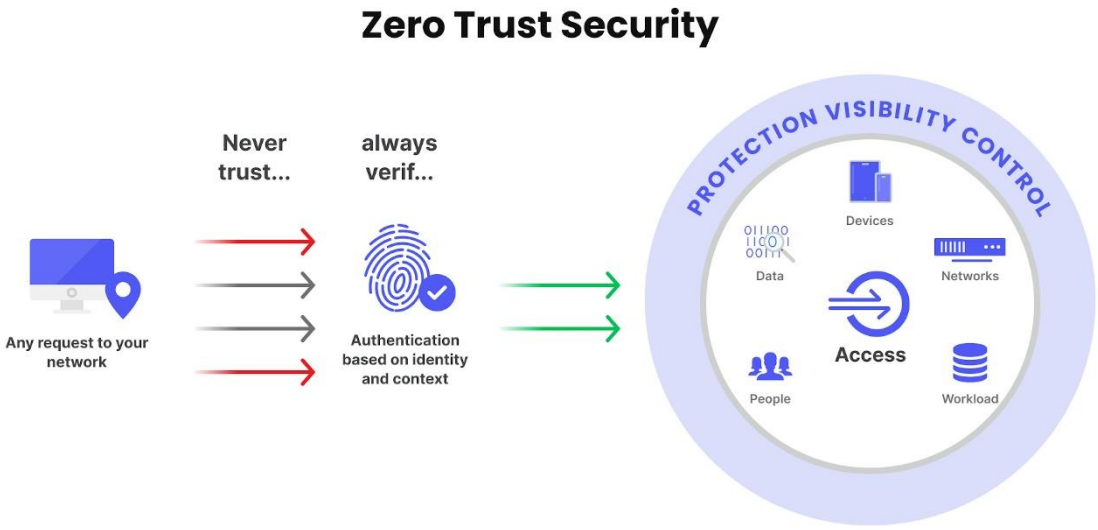
Zero Trust modellek

A Zero Trust („nulla bizalom”) biztonsági modell az egyik legfontosabb megközelítés a modern információbiztonsági környezetben, különösen a vállalati hálózatok és ipari rendszerek védelmében. A Zero Trust alapelve, hogy semmilyen hálózati kapcsolatban vagy hozzáférésben nem bízik meg automatikusan - sem belső, sem külső eredetű hozzáférésben. Ez a modell azt feltételezi, hogy bárki és bármi lehet potenciális fenyegetés, ezért minden kapcsolatot folyamatosan ellenőriz és validál, mielőtt hozzáférést biztosítana a védett erőforrásokhoz.

A modell három fő alapelve közül az első a „legkisebb jogosultság” (least privilege) elve. Ez azt jelenti, hogy minden felhasználónak és eszköznek csak annyi jogosultsága legyen, amennyi feltétlenül szükséges a munkája ellátásához. Így jelentősen csökken az esetleges jogosultság-visszaélések kockázata. A második alapelv a „folyamatos ellenőrzés és hitelesítés” (continuous verification and authentication), amely folyamatosan figyeli és újraértékeli a kapcsolatok hitelességét. Ez nemcsak a belépéskor, hanem az egész munkafolyamat alatt történik, biztosítva, hogy bármilyen változás azonnal észlelhető legyen. A harmadik alapelv pedig a „mikroszegmentáció” (microsegmentation), ami a hálózatokat kisebb, izolált részekre osztja, így csökkentve annak a kockázatát, hogy egy támadás könnyen átterjedjen más hálózati szegmensekre.

Alkalmazása különösen hatékony a zsarolóvírusok ellen mivel a vírusoknak általában nagyobb jogosultságokra és horizontális hálózati mozgásra van szükségük, hogy hatékonyan terjedjenek. Zero Trust környezetben a vírusok mozgása erősen korlátozott, így minimalizálható a fertőzés terjedésének esélye. Több nagyvállalat és kormányzati intézmény -

például a Google, a Microsoft és az Amerikai Védelmi Minisztérium - is sikeresen alkalmazza a Zero Trust modelleket, bizonyítva ennek hatékonyságát és fontosságát.[4] *(4. ábra)*



4. ábra - zero trust modell
https://images.prismic.io/superpupertest/9fc777be-080f-43d0-b43c-ce4bc4a8283e_Zero_img1.png?auto=compress,format&dpr=3

Végpontvédelmi rendszerek

A végpontvédelmi rendszerek (Endpoint Detection and Response - EDR, illetve Extended Detection and Response - XDR) egyre nagyobb szerepet játszanak a korszerű kiberbiztonsági környezetben. A végpontok - mint például a számítógépek, okostelefonok, táblagépek vagy akár ipari eszközök - jelentik a hálózati infrastruktúra egyik legsérülékenyebb pontját, amelyet a támadók gyakran célba vesznek. A végpontvédelmi rendszerek a hálózatokon belüli kártékony aktivitás észlelésére, elemzésére és kezelésére szolgálnak, még mielőtt azok súlyos károkat okozhatnának.

Az EDR rendszerek legnagyobb előnye, hogy valós idejű megfigyelést és viselkedésalapú elemzést biztosítanak. Ezek a rendszerek képesek felismerni olyan támadási mintázatokat és anomáliákat, amelyeket a hagyományos vírusvédelmi megoldások nem mivel nem csak ismert fenyegetésekkel szemben védenek, hanem a viselkedésbeli eltéréseket is észlelik. Egy tipikus EDR rendszer folyamatosan monitorozza a végpontok aktivitását, elemzi a beérkező adatokat és riasztást ad, ha gyanús viselkedést észlel. Emellett lehetőséget nyújt a gyanús fájlok vagy folyamatok izolálására, karanténba helyezésére, valamint automatikus válaszintézkedésekre, például fertőzött gépek lekapcsolására a hálózatról.

Az XDR (Extended Detection and Response) megoldások az EDR továbbfejlesztett változatai, amelyek már nemcsak végpontokra korlátozódnak, hanem kiterjesztik a védelmet a

hálózati forgalomra, szerverekre, levelezőrendszerekre és felhőalapú környezetekre is. Az XDR rendszerek az egyes rendszerekből érkező adatok korrelálásával és összekapcsolásával holisztikus képet adnak a vállalati biztonsági állapotról, javítva ezzel a fenyegetések észlelésének hatékonyságát és pontosságát. *(5. ábra)*

Használatunk napjainkban szinte elengedhetetlen minden olyan szervezet számára, amely hatékony védelmet kíván kiépíteni a kibertámadásokkal, különösen a zsarolóvírusokkal szemben. Az olyan fejlett támadások, mint a WannaCry, NotPetya, LockBit vagy Black Basta ellen a végpontvédelmi rendszerek képesek lehetnek időben felismerni és izolálni a fenyegetést, jelentősen csökkentve a károk súlyosságát és a támadások hatókörét.[5]

5. ábra - EDR és XDR
https://www.splunk.com/content/dam/splunk2/images/data-insider/what-is-xdr/xdr-and-edr.jpg

Ransomware példák és védekezési stratégiák

WannaCry és NotPetya

A WannaCry és a NotPetya egyaránt jelentős, globálisan elterjedt ransomware (zsaroló) támadások, amelyek különböző mértékben okoztak károkat 2017-ben és a mai napig referenciaként szerepelnek a kibertámadások történetének elemzéseiben. Mindkét támadás figyelmeztető jele volt arra, hogy milyen komoly veszélyekkel kell szembenézni a digitális világban és hogyan hatnak ezek a fenyegetések a globális gazdaságra és a biztonságra.

WannaCry

A WannaCry egy globális zsarolóvírus, amely 2017 májusában tört ki. A támadás az akkoriban nem ismert, Windows rendszerekben található sérülékenységet, az EternalBlue nevű exploitot használta ki, amelyet az amerikai Nemzetbiztonsági Ügynökség (NSA) fejlesztett ki, de az azt követő hónapokban egy hacker csoport, a Shadow Brokers, nyilvánosságra hozta. Az EternalBlue exploit a Windows SMB (Server Message Block) protokolljában található biztonsági résen keresztül fertőzte meg a rendszereket.

Rendkívül gyorsan terjedt el és több mint 150 országot érintett, köztük az Egyesült Királyság nemzeti egészségügyi rendszerét (NHS), a spanyol Telefónicát és több nagyvállalatot. Az áldozatok, miután a fertőzés végrehajtódott, váltságdíjat kaptak, amelyet Bitcoinban kellett volna kifizetniük annak érdekében, hogy visszakapják az adataikat. A vírus a fájlokat titkosította és az áldozatoknak 300 dollárnyi Bitcoinban kellett váltságdíjat fizetniük a fájlok visszaállításáért. Azonban a legmegdöbbentőbb az volt, hogy a WannaCry nemcsak egy egyszerű zsarolóvírus volt, hanem gyorsan elérte a rendszereket azáltal, hogy a sérülékeny SMB protokollt kihasználta, amely gyorsan és hatékonyan fertőzött meg több millió számítógépet.

Következményei súlyosak voltak mivel sok kritikus infrastruktúra, például kórházak és más közszolgáltatások működését is megzavarta. Az egyik legismertebb eset a brit NHS

rendszerében történt, ahol a támadás több mint 70 000 eszközt és 200 000 betegadatot érintett, miközben több mint 19 000 műtétet és orvosi találkozót kellett elhalasztani.[6] (*6. ábra -)*

6. ábra - Wannacry
https://media.npr.org/assets/img/2017/05/16/ap_17133191234349_wide-61536ef667e0409063dabbdd195f34b17eac0246.jpg?s=800&c=85&f=webp

NotPetya

A NotPetya támadás, amely 2017 júniusában történt, szintén a ransomware kategóriába tartozik, de a WannaCry-hoz képest más jellegű és sokkal destruktívabb volt. Az elemzők szerint a NotPetya nemcsak egy hagyományos zsarolóvírus, hanem egy destruktív kód, amelynek célja nem annyira a pénzszerzés, mint inkább a rendszerek tönkretétele volt. A támadás Ukrajnában kezdődött és onnan terjedt el globálisan, különösen az európai vállalatoknál, de olyan cégeket is érintett, mint a Maersk, a FedEx és a Merck.

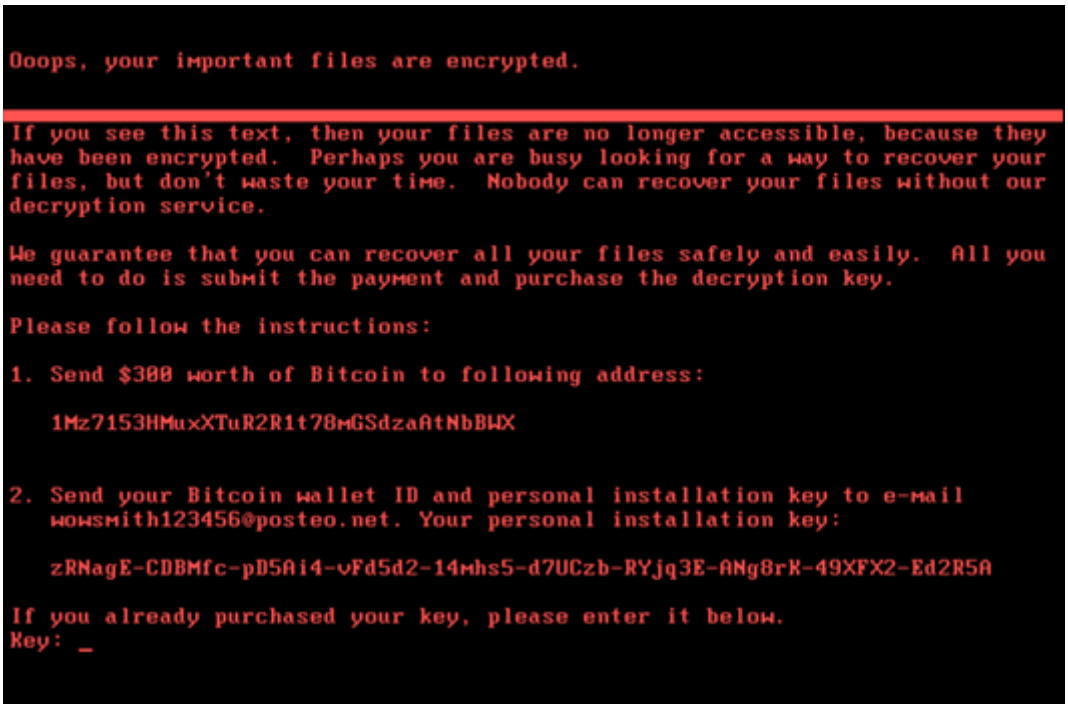
Az EternalBlue exploitot is felhasználta, de emellett egy másik módszert is alkalmazott a terjedésére. A vírus egy ukrán adóbevallási programon keresztül indult el és onnan terjedt tovább, miután a számítógépek csatlakoztak egy vállalati hálózathoz. A NotPetya kódja különlegesen gyorsan terjedt és nemcsak fájlokat titkosított, hanem teljesen megsemmisítette azokat, így az áldozatok nem tudtak hozzáférni a rendszereikhez, még akkor sem, ha kifizették a váltságdíjat. Az analízis során kiderült, hogy a váltságdíjat nem is volt érdemes kifizetni mivel a vírus kódja nem tartalmazott olyan funkciót, amely lehetővé tette volna a fájlok visszaállítását.

Különlegessége, hogy a támadók célja nemcsak a pénzszerzés volt, hanem sokkal inkább az informatikai rendszerek tönkretétele és a globális gazdaság működésének zűrzavara. Az Ukrajnában történt támadást egyesek szerint egy állami szintű támadásnak tekintik mivel a vírus

egyértelműen politikai célokat szolgált és az ukrán infrastruktúrára összpontosított. Azonban a vírus gyorsan átterjedt a világ más részeire is és világszerte több milliárd dolláros kárt okozott.

Mind a WannaCry, mind a NotPetya támadások a globális kiberbiztonsági közösség számára fontos tanulságokkal szolgáltak. Ezek a támadások felhívták a figyelmet a kritikus rendszerek sebezhetőségére, különösen azokban az esetekben, amikor a vállalatok és intézmények nem frissítik megfelelően a rendszereiket. A WannaCry és a NotPetya rávilágítottak arra, hogy a kiberfenyegetések nem csupán az egyéni felhasználók problémái, hanem globális gazdasági és politikai kihívások is lehetnek.

A két támadás az úgynevezett "kiberháború" új dimenzióját is megnyitotta, amelyben az államok és a nem állami szereplők egyaránt képesek lehetnek kiberfegyverek alkalmazására. A jövőben az ilyen támadások elleni védekezéshez elengedhetetlen, hogy a vállalatok és az állami intézmények folyamatosan figyelemmel kísérjék a legújabb sérülékenységeket és időben alkalmazzák a szükséges védelmi intézkedéseket.[7] *(7. ábra -)*



7. ábra - NotPetya
https://www.hypr.com/hs-fs/hubfs/Media%20Graphics/NotPetya-ransomware-or-malware.png?width=814&height=536&name=NotPetya-ransomware-or-malware.png

Black Basta és LockBit

A ransomware (zsarolóvírus) támadások továbbra is komoly fenyegetést jelentenek az informatikai biztonság terén és az újabb támadó csoportok egyre kifinomultabb technikákat alkalmaznak. A Black Basta és a LockBit két jelenkori ransomware csoport, amelyek az utóbbi években komoly károkat okoztak a globális informatikai környezetben. Ezek a csoportok

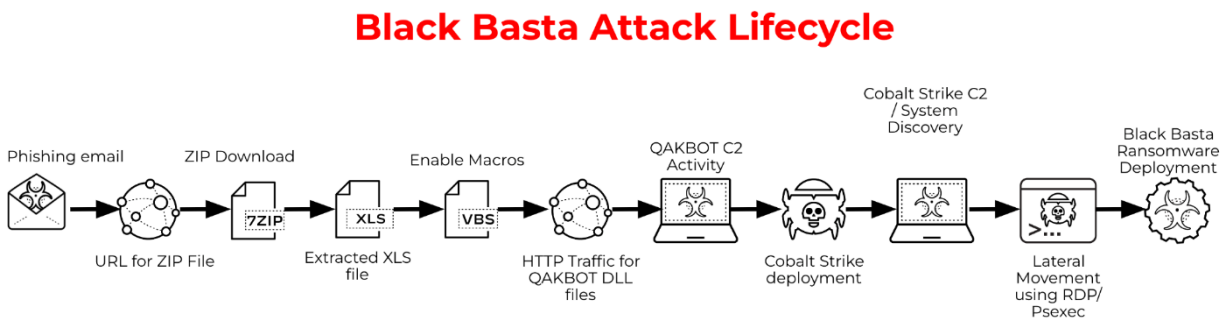
különböző stratégiákat alkalmaznak, de mindkettő a titkosításos zsarolásra alapozza támadásait és új kihívások elé állítják a kibervédekezést.

Black Basta

A Black Basta csoport 2022 áprilisi megjelenése óta gyorsan elnyerte a figyelmet mivel a csoport rendkívül agresszív módon végzi a támadásokat és komplex, több lépcsős eljárásokat alkalmaz a célzott rendszerek megbénítására. A Black Basta csoport a korábbi zsarolóvírus csoportok, például a Conti és a REvil tagjaiból alakult, akik tapasztalataikat és eszközeiket átültették az új támadásokba. A Black Basta a vállalatok, kormányzati intézmények és szolgáltatók számára is komoly veszélyt jelent mivel képesek gyorsan áttörni a hagyományos védekezési rendszereken.

Támadásai gyakran egy több lépcsős folyamat részeként valósulnak meg. A csoport eleinte phishing (adathalász) emaileket vagy más trükköket alkalmazva próbálja megfertőzni a cégek rendszereit, majd a behatolás után második lépésként a ransomware-t telepítik. A célzott rendszerek titkosítása után a csoport váltságdíjat kér a fájlok visszaállításáért és figyelmeztetik az áldozatokat, hogy ha nem fizetnek, az adataikat véglegesen elveszíthetik. *(8. ábra -)*

A Black Basta egyik jellegzetessége, hogy nemcsak az adatok titkosításával, hanem azok nyilvánosságra hozatalával is fenyegetnek. A csoport adatokat szivárogtat ki és ezt a fenyegetést használja a váltságdíj növelésére. Ennek célja, hogy fokozza a pszichológiai nyomást az áldozatokon, hogy azok minél gyorsabban fizessek. Ez az új típusú támadási forma rendkívül veszélyes mivel a személyes és vállalati adatokat is kockára teszi. [8]



8. ábra - Black Basta támadási folyamata
https://unit42.paloaltonetworks.com/wp-content/uploads/2022/08/word-image-84.png

LockBit

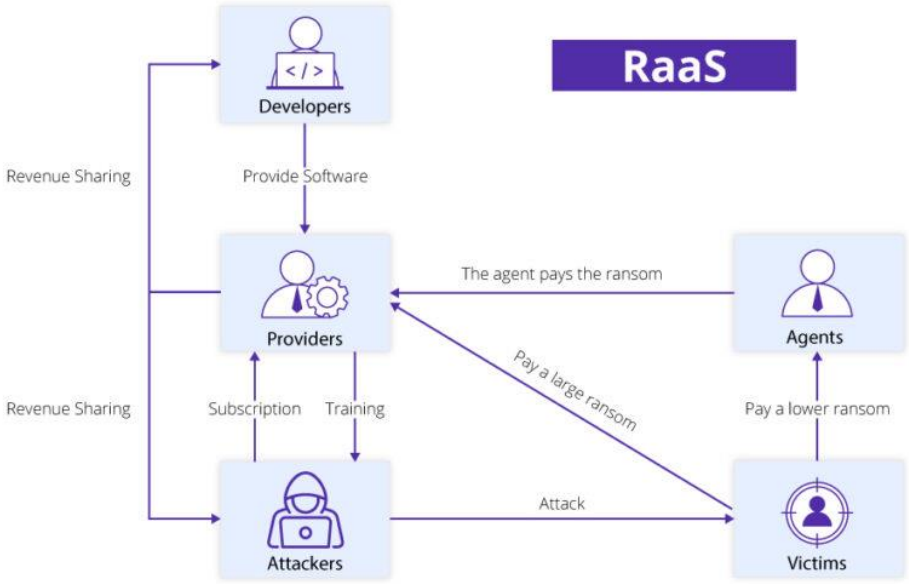
A LockBit ransomware csoport 2019-ben indult és azóta a világ egyik legaktívabb és leghatékonyabb zsarolóvírus csoportjává vált. A LockBit egyik legnagyobb előnye a gyors alkalmazkodás és a fejlett automatizálás. A csoport célja nemcsak a titkosítás, hanem a támadások gyors végrehajtása is, amely lehetővé teszi számukra, hogy rövid időn belül komoly károkat okozzanak.

Kifejezetten a nagyvállalatokat célozza meg és egyre kifinomultabb támadási módszereket alkalmaz. A támadók sokszor a vállalatok informatikai rendszereiben található sérülékenységeket használják ki, különösen a nem frissített rendszerek és alkalmazások esetében. Miután sikeresen betörtek a rendszerbe, a LockBit titkosítja a fájlokat és váltságdíjat követel. Azonban a LockBit csoport egy lépéssel tovább megy: az áldozatokat nemcsak a titkosított fájlok visszaállítására kényszeríti, hanem szintén fenyegeti őket azzal, hogy az adataikat nyilvánosságra hozza, ha nem fizetnek. (*10.* ábra -)

Egyik figyelemre méltó jellemzője, hogy fejlett, automatizált eszközöket használ a támadások végrehajtásához. Ez lehetővé teszi számukra, hogy a támadásokat gyorsan és hatékonyan végezzék el, valamint könnyedén adaptálják a támadásokat a különböző rendszerekhez. A csoport saját zsarolóvírust fejlesztett ki, amely folyamatosan frissül és alkalmazkodik a védekezési intézkedésekhez, így a LockBit támadások különösen nehezen észlelhetők és megállíthatók.

Legújabb technikai újítása a "Ransomware-as-a-Service" (RaaS) modell bevezetése. Ez azt jelenti, hogy a csoport egy platformot kínál más támadók számára, hogy az ő eszközeikkel végezzenek zsarolóvírus támadásokat. A csoport a szolgáltatás használatáért váltságdíj egy

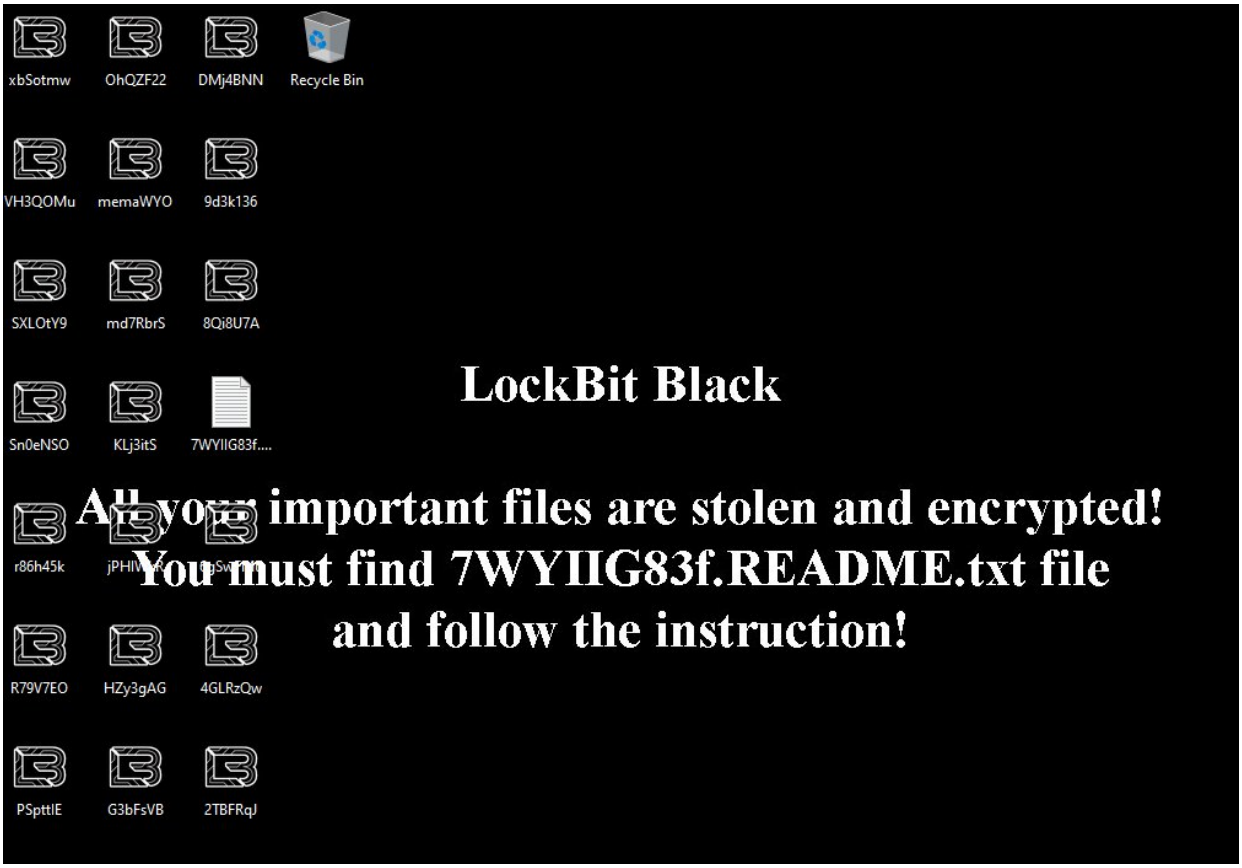
részét kéri, így lehetővé téve más, kisebb támadók számára, hogy saját ransomware kampányokat futtassanak.[9] *(9. ábra -)*



9. ábra - RaaS
https://www.cdnetworks.com/wp-content/uploads/2024/08/LockBit-Ransomware-Threats_02-1024x510.jpg

A Black Basta és LockBit csoportok az aktuális ransomware fenyegetéseket reprezentálják, amelyek rendkívüli hatékonysággal és gyorsasággal hajtanak végre támadásokat. Mindkét csoport különböző módszereket alkalmaz, de közös bennük a titkosításos zsarolás, az adatlopás és a nyilvánosságra hozatal fenyegetése. Az ilyen típusú támadások fokozzák a cégek számára a kibervédelmi intézkedések szükségességét és azt is megmutatják, hogy a védekezés nemcsak

a hagyományos antivírus szoftverekre, hanem az aktív, folyamatos biztonsági monitoringra és frissítésekre is támaszkodnia kell.



10. ábra - LockBit
https://unit42.paloaltonetworks.com/wp-content/uploads/2022/06/word-image-21.png

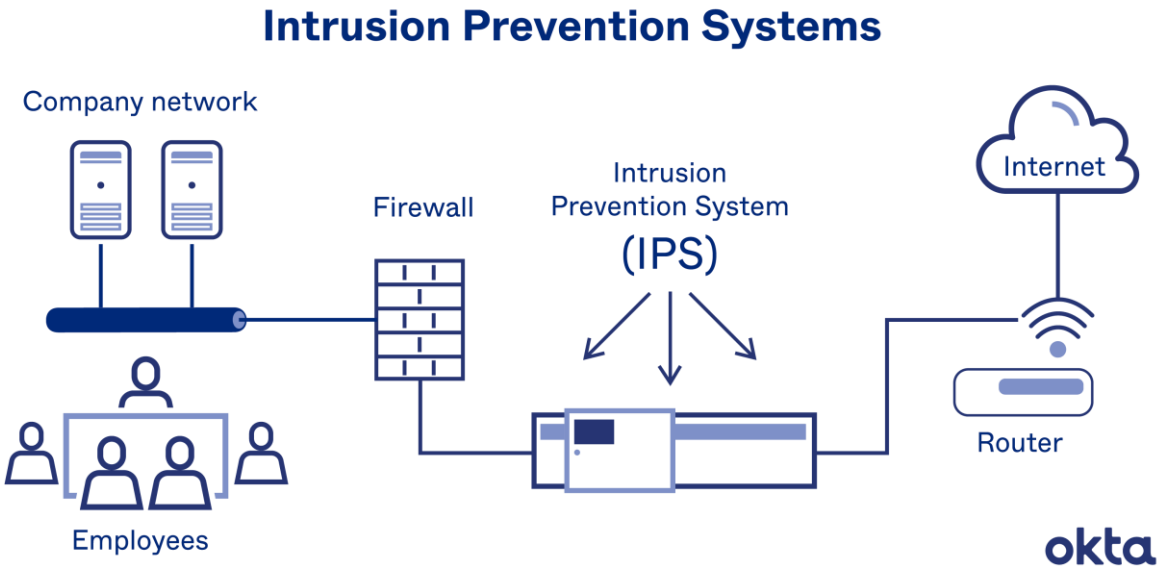
Kiberbiztonsági megoldások és technológiák

A kiberbiztonság területe gyorsan fejlődik, ahogy a technológiai újítások és az egyre összetettebb támadási módszerek egyaránt megjelennek. A kiberfenyegetések növekvő száma és bonyolultsága arra készteti a szervezeteket, hogy folyamatosan fejlesszék védelmi mechanizmusaikat. Az alábbiakban bemutatunk néhány kulcsfontosságú kiberbiztonsági megoldást és technológiát, amelyek segítenek a digitális környezetek biztonságának megőrzésében.[10] *(11. ábra -)*

11. ábra - Kiberbiztonsági megoldások és technológiák
https://www.bitlyft.com/hs-fs/hubfs/Cybersecurity-solutions.jpeg?height=225&name=Cybersecurity-solutions.jpeg

1. Tűzfalak és behatolásmegelőző rendszerek (IPS)

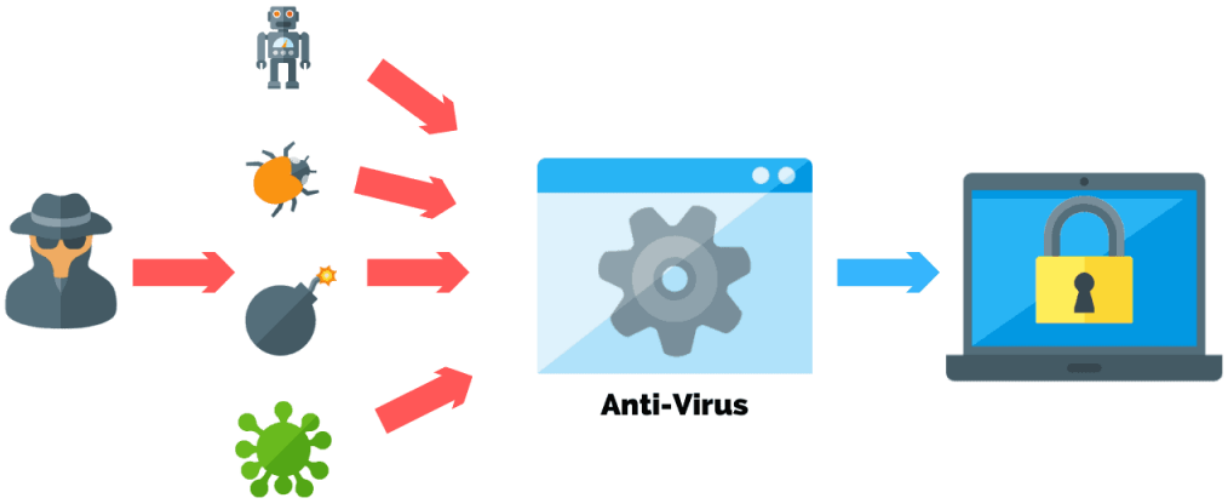
A tűzfalak (firewalls) és a behatolásmegelőző rendszerek (IPS) alapvető technológiák a hálózati biztonság terén. A tűzfalak a hálózati forgalmat monitorozzák és blokkolják azokat a bejövő és kimenő adatokat, amelyek nem felelnek meg a beállított biztonsági szabályoknak. Az IPS-ek célja a már meglévő támadások felismerése és megakadályozása, még mielőtt azok kárt okoznának. Mindkét technológia alapvető a hálózati infrastruktúra védelmében mivel képesek kiszűrni a nem kívánt vagy káros adatokat és megakadályozzák a külső behatolásokat. *(12. ábra -)*



12. ábra - IPS rendszerek
https://www.okta.com/sites/default/files/media/image/2021-05/IntrusionPreventionSystem.png

2. Antivirus és antimalware rendszerek

Az antivírus és antimalware programok a legelterjedtebb és legismertebb biztonsági megoldások közé tartoznak. Feladatuk a számítógépes vírusok, kémprogramok, ransomware-ek és egyéb rosszindulatú szoftverek felismerése és eltávolítása. Az ilyen típusú programok folyamatosan frissítik adatbázisukat a legújabb fenyegetések listájával és aktívan figyelik a rendszer működését, hogy megakadályozzák a fertőzéseket. A legújabb verziók gépi tanulást és mesterséges intelligenciát is alkalmaznak a veszélyek észlelésére, ezáltal egyre hatékonyabbá válva a korábbi technológiáknál. *(13. ábra -)*



13. ábra - Antivirus
https://www.devsecopsnow.com/wp-content/uploads/2023/11/image-20-1024x576.png

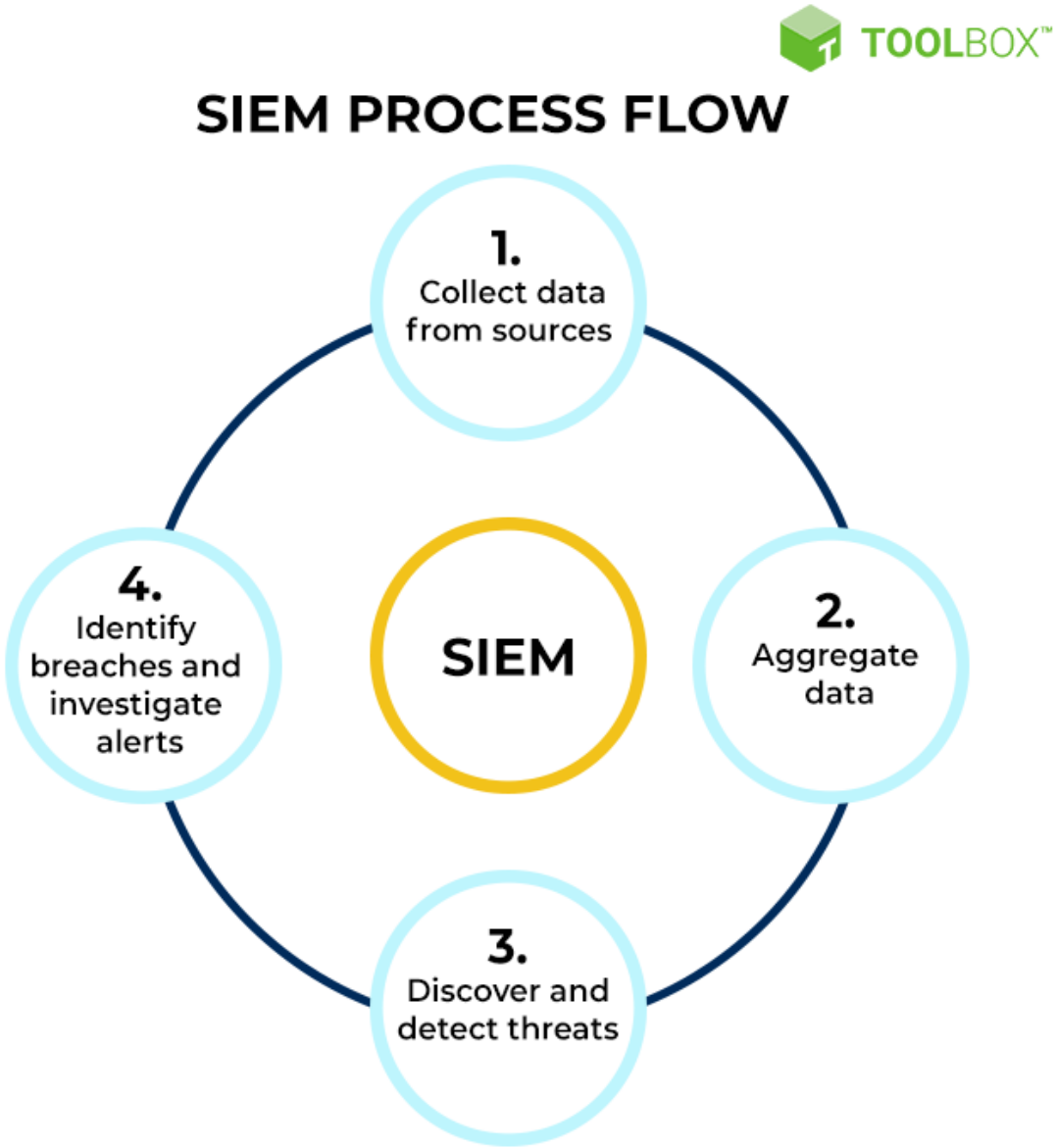
3. Kétfaktoros hitelesítés (2FA)

A kétfaktoros hitelesítés (2FA) az egyik legfontosabb védelmi mechanizmus az online fiókok és alkalmazások védelmében. Ahelyett, hogy csupán a felhasználónév és a jelszó révén történne a hozzáférés, a 2FA egy további hitelesítési tényezőt is alkalmaz, például egy egyszer használatos kódot, amelyet a felhasználó egy mobilalkalmazásból vagy SMS-ben kap. Ez megnehezíti a támadók számára a fiókhoz való hozzáférést, még akkor is, ha a jelszóval rendelkeznek, így jelentősen megnöveli az adatvédelem szintjét. *(14. ábra -)*

14. ábra - Kétfaktoros hitelesítés
https://staticfiles.acronis.com/images/blog-cover/9101bed8caac04160ee579997f8144f6.webp

4. Biztonsági információ- és eseménykezelő rendszerek (SIEM)

A SIEM (Security Information and Event Management) rendszerek az informatikai infrastruktúra biztonságának kezelésére szolgálnak. Ezek a rendszerek valós időben gyűjtik és elemzik a különböző biztonsági események adatait, figyelmeztetéseket generálnak a gyanús tevékenységekről és segítenek az incidens kezelésében. A SIEM rendszerek képesek azonosítani a potenciális fenyegetéseket és gyorsan reagálni rájuk, lehetővé téve a szervezetek számára a proaktív biztonsági intézkedéseket. *(15. ábra -)*



15. ábra - SIEM folyamat
https://zd-brightspot.s3.us-east-1.amazonaws.com/wp-content/uploads/2022/02/24112443/73.png

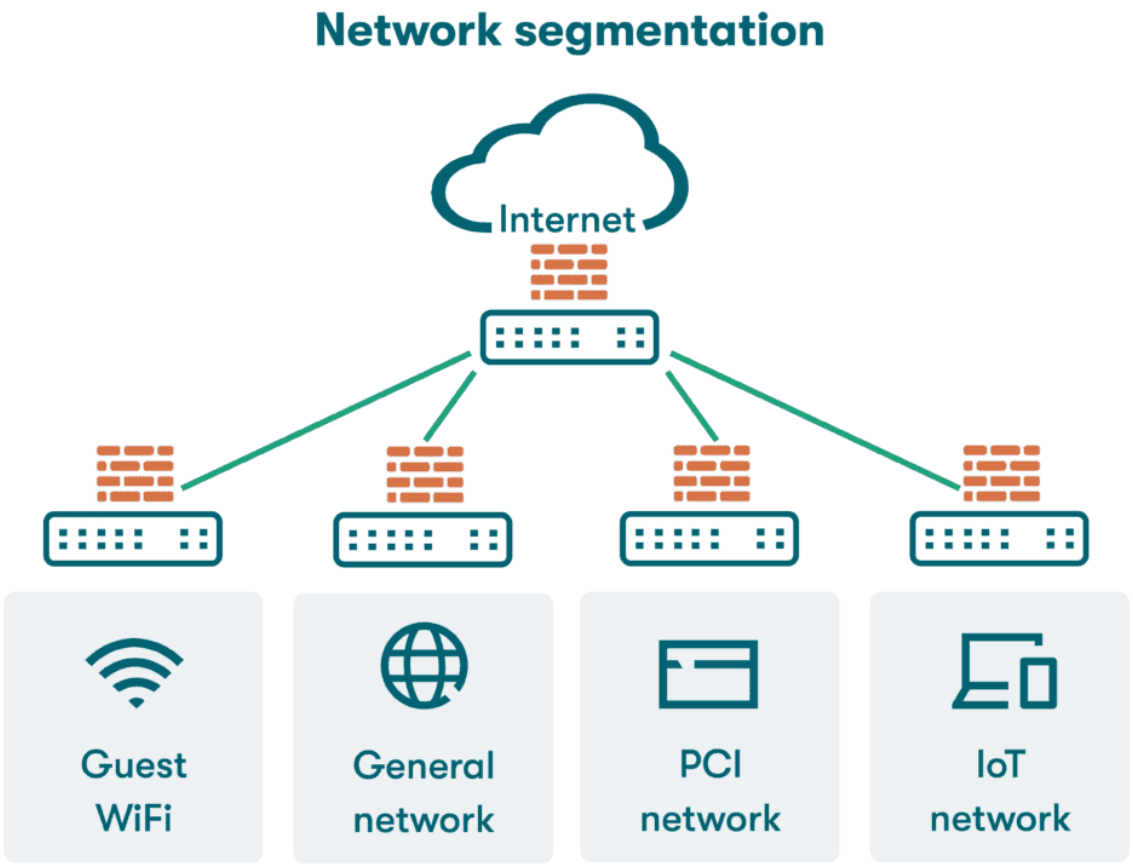
5. Zsarolóvírus-ellenes megoldások

A ransomware, vagyis a zsarolóvírusok elleni megoldások a legújabb kiberbiztonsági kihívásoknak megfelelő válaszokat kínálnak. A ransomware támadások során a támadók titkosítják az áldozatok fájljait és váltságdíjat követelnek azok visszaállításáért. Az antivírus programok és a dedikált zsarolóvírus-ellenes megoldások gyakran azonosítják a ransomware-t, még mielőtt az kárt okozna. Ezen felül az ilyen rendszerek segítenek a rendszer biztonsági mentéseinek kezelése terén is, biztosítva, hogy a fájlok helyreállíthatók legyenek, ha a titkosítás megtörténik.

6. Hálózati szegmentálás és VPN

A hálózati szegmentálás célja, hogy a vállalaton belüli hálózatokat kisebb, elkülönített szegmensekre bontsa. Ennek eredményeként, ha egy szegmens sérülékennyé válik, a támadás nem terjedhet át a hálózat többi részére. *(16. ábra -)*

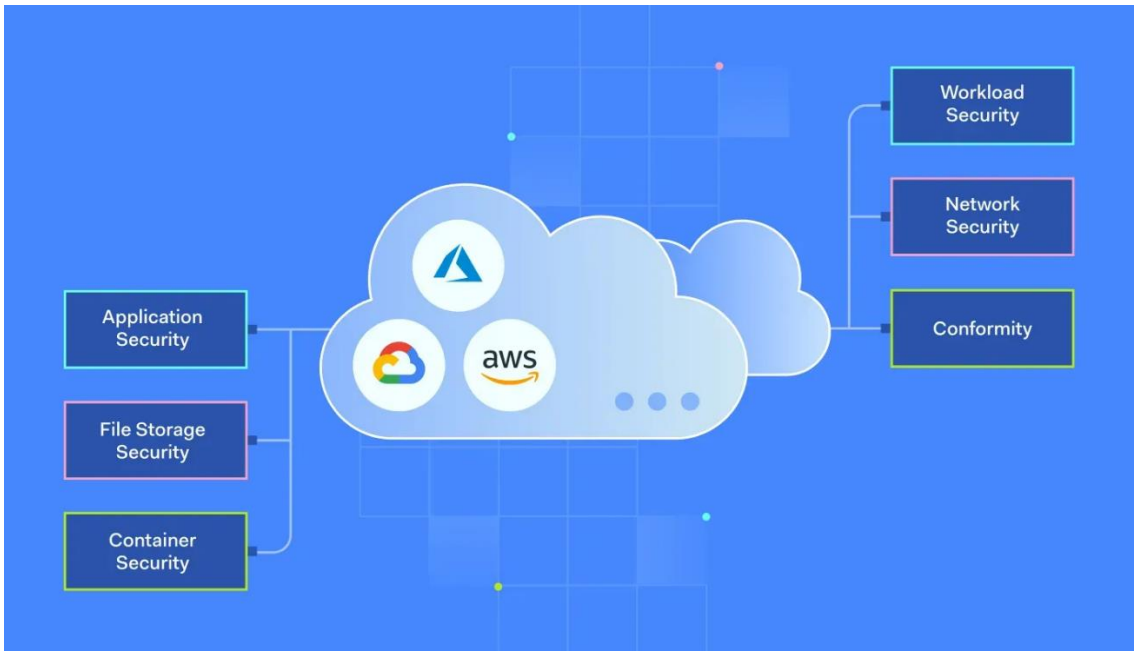
A VPN (Virtual Private Network) a távoli munkavégzés során biztosítja a titkosított kapcsolatot a felhasználók és a vállalatok hálózatai között, így megelőzve az adatlopást és más támadásokat.



16. ábra - Hálózat szegmentálás
https://www.dashlane.com/_next/image?url=https%3A%2F%2Fripleyprd.wpengine.com%2Fwp-content%2Fuploads%2F2024%2F02%2FWhat-is-network-segmentation-1024x788.png&w=1080&q=75

7. Felhőbiztonság

A felhőalapú szolgáltatások elterjedésével a felhőbiztonság egyre fontosabbá vált. A felhőalapú megoldások biztonságának biztosítása érdekében a vállalatoknak olyan eszközöket kell alkalmazniuk, mint a titkosítás, a hozzáférés-ellenőrzés, a monitorozás és a biztonsági mentések. A felhőszolgáltatók általában rendelkeznek integrált biztonsági funkciókkal, de a vállalatoknak is biztosítaniuk kell a saját adatvédelmüket és biztonságukat a felhőben. *(17. ábra -)*



17. ábra - Felhőbiztonság
https://content.nordlayer.com/uploads/What_is_Cloud_network_security_web_1400x800_cover_web_1400x800_0670d99173.webp

Titkosítás, hozzáférés-ellenőrzés, HSM

A titkosítás, a hozzáférés-ellenőrzés és a hardveres biztonsági modulok (HSM) alapvető szerepet játszanak a modern kiberbiztonságban mivel segítenek biztosítani az adatvédelmet, valamint megelőzni a jogosulatlan hozzáférést a vállalatok és egyének érzékeny információihoz.

Titkosítás

Az egyik legfontosabb technológia az adatok védelmében. Az adatok titkosítása biztosítja, hogy azok csak megfelelő kulcs birtokában legyenek olvashatók. Két fő típusa létezik: szimmetrikus és aszimmetrikus titkosítás. A szimmetrikus titkosítás esetében ugyanaz a kulcs szükséges az adatok titkosításához és visszafejtéséhez, míg az aszimmetrikus titkosítás esetében két kulcsot használnak: egy nyilvános kulcsot az adatok titkosítására és egy privát kulcsot a

visszafejtéshez. A titkosítás alkalmazása biztosítja, hogy az adatokat akkor is védve maradjanak, ha azok illetéktelen kezekbe kerülnek.[11] *(18. ábra -)*

18. ábra - Titkosítás
https://kinsta.com/wp-content/uploads/2023/07/what-is-encryption-1024x512.jpg

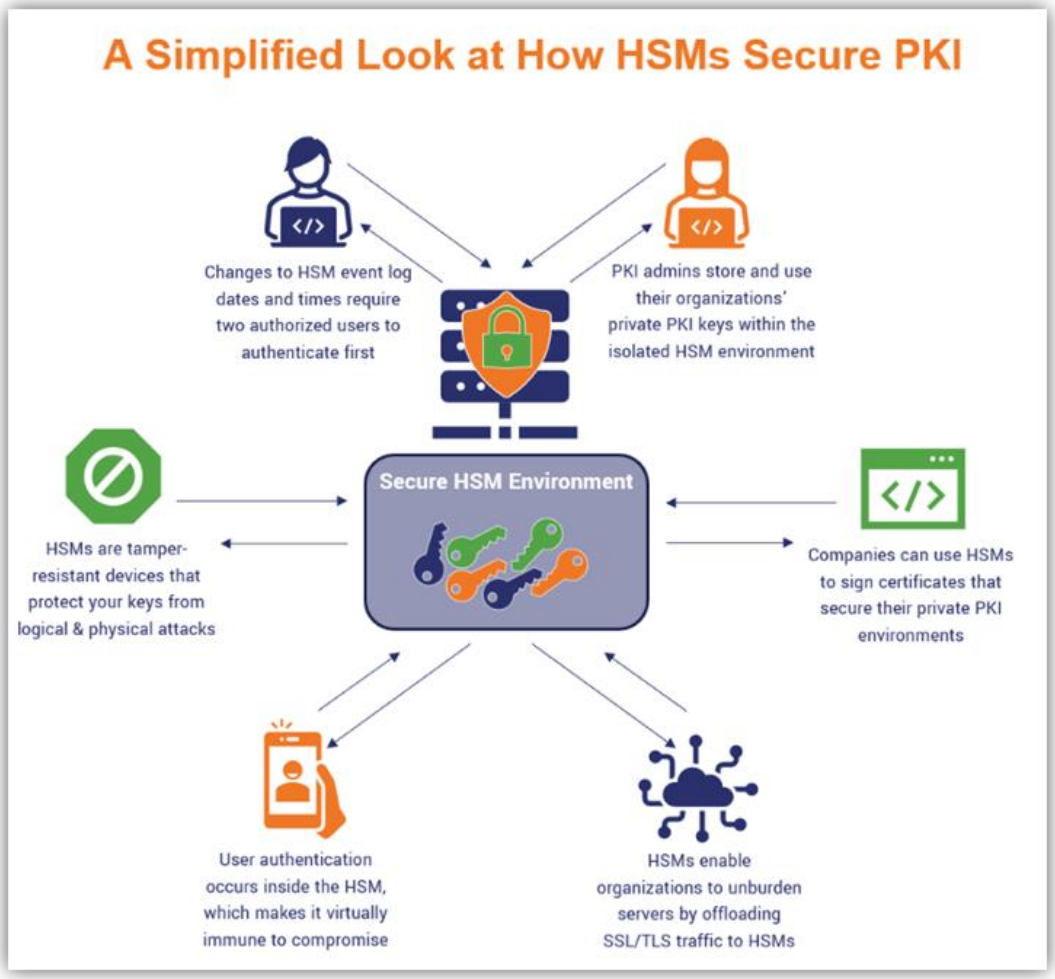
Hozzáférés-ellenőrzés

A hozzáférés-ellenőrzés a kiberbiztonság másik kulcsfontosságú eleme. Ez a mechanizmus biztosítja, hogy csak azok a felhasználók és rendszerek férhessenek hozzá az adatokhoz vagy alkalmazásokhoz, akik jogosultak rá. A legelterjedtebb hozzáférés-ellenőrzési technikák közé tartozik az erős hitelesítés (pl. jelszavak, biometrikus azonosítás), a jogosultságok kezelése és az access control lists (ACL-ek). A hozzáférési jogosultságok folyamatos felülvizsgálata és korlátozása fontos a vállalati biztonság szempontjából.[12] *(19. ábra -)*

19. ábra - Hozzáférés-ellenőrzés
https://www.nordencommunication.com/summernoteAccess-Control-6268c31668b3f.jpg

HSM (Hardware Security Module)

A hardveres biztonsági modulok (HSM) speciális eszközök, amelyek a titkosítási kulcsokat tárolják és védik. Ezek az eszközök magas szintű fizikai és logikai védelmet biztosítanak a titkosítási kulcsok számára és megakadályozzák azok illetéktelen használatát vagy eltulajdonítását. Az HSM-eket gyakran használják pénzügyi intézmények, kormányzati szervek és egyéb szervezetek, amelyek érzékeny adatokat kezelnek mivel ezek biztosítják a titkosítási kulcsok védelmét, miközben lehetővé teszik azok gyors és biztonságos használatát. [13] *(20. ábra -)*



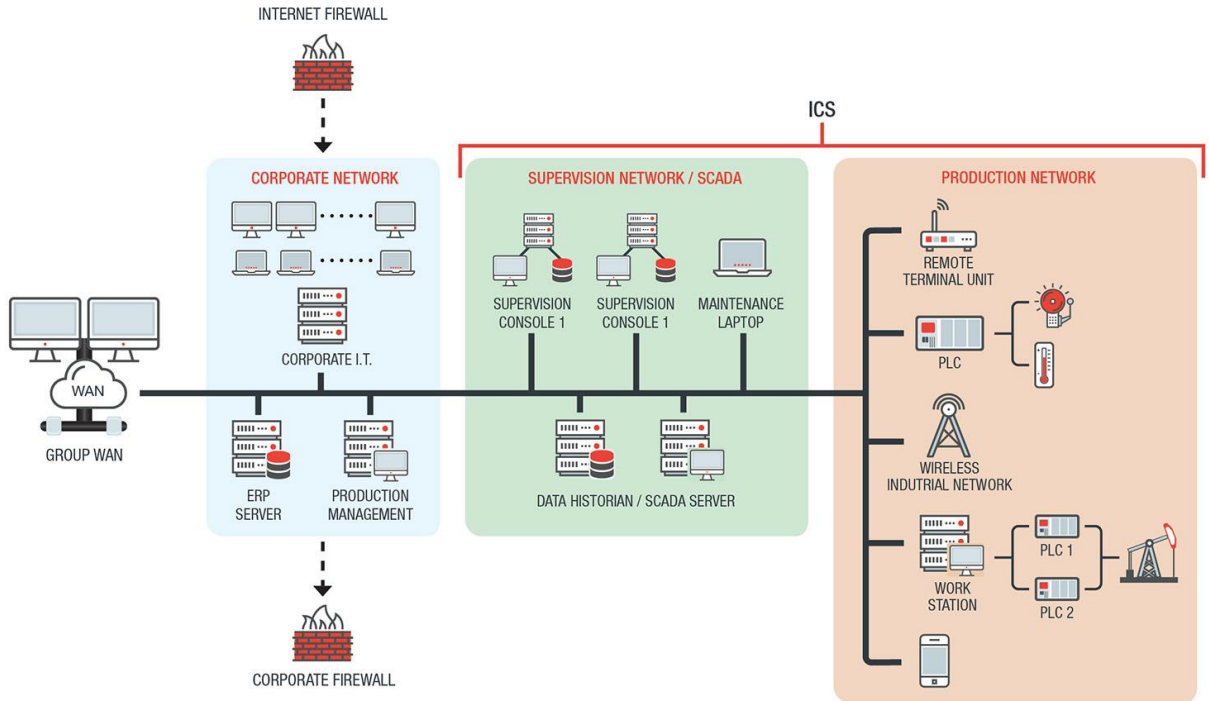
20. ábra - HSM
https://www.thesslstore.com/blog/wp-content/uploads/2021/07/how-hsms-secure-pki.png

ICS/SCADA rendszerek és IoT biztonság

Az ICS (Industrial Control Systems) és SCADA (Supervisory Control and Data Acquisition) rendszerek kulcsszerepet játszanak az ipari és kritikus infrastruktúrák működésében. Az IoT (Internet of Things) eszközök pedig egyre inkább elterjednek a mindennapi életben és számos alkalmazásban jelennek meg, beleértve az egészségügyet, az ipari automatizálást és a közlekedést. A kiberbiztonság szempontjából mindkét technológia különös figyelmet igényel mivel sebezhetőségeik komoly fenyegetéseket jelenthetnek.[14]

ICS/SCADA biztonság

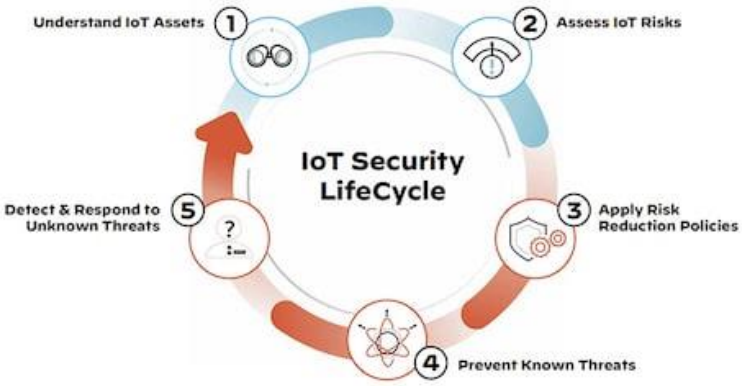
Az ICS/SCADA rendszerek a legfontosabb ipari és energiaellátó rendszerek irányítását végzik és ha ezek sérülékenyek, komoly gazdasági és biztonsági következményekkel járhatnak. Az ilyen rendszerek gyakran elavult szoftvereket és védelmi mechanizmusokat használnak, ami lehetőséget ad a támadók számára. A támadók képesek lehetnek a rendszerek irányításának megszerzésére, adatokat manipulálni, vagy akár fizikai károkat okozni. A biztonsági intézkedések között szerepel a rendszer szegmentálása, az erős hitelesítés és a folyamatos monitorozás. *(21. ábra -)*



21. ábra - ICS
https://documents.trendmicro.com/images/tex/articles/ics-system.jpg

IoT biztonság

Az IoT eszközök elterjedése új kihívásokat jelent a kiberbiztonság terén. Mivel ezek az eszközök gyakran gyenge biztonsági protokollokkal rendelkeznek és sokszor nem frissíthetők, a támadók kihasználhatják őket a hálózati biztonság megsértésére. Az IoT biztonság javításához fontos az erős titkosítás, a rendszeres frissítések és a felhasználói jogosultságok szigorú kezelése. *(22. ábra)*



22. ábra - IoT rendszerek
https://www.paloaltonetworks.com/content/dam/pan/en_US/images/cyberpedia/what-is-iot-security-cyberpedia-image-3-868x488.jpg?imwidth=1920

Jövőbeli fenyegetések és védekezési trendek

AI-alapú támadások és automatizáció

A mesterséges intelligencia (AI) és a gépi tanulás (ML) folyamatos fejlődése forradalmasította a kiberbiztonságot, de egyúttal új fenyegetéseket is generált. Az AI-alapú támadások és automatizálás egyre inkább a kibertámadások terjedő trendjévé válnak mivel lehetővé teszik a támadók számára, hogy gyorsabban és hatékonyabban hajtsák végre támadásaikat. A jövőben a mesterséges intelligencia és az automatizált rendszerek elterjedése mind a támadók, mind a védelmi mechanizmusok számára komoly kihívásokat jelenthetnek.[15] *(23. ábra -)*

23. ábra - AI-alapú támadások
https://media.licdn.com/dms/image/v2/D4E12AQFmGbE7NmeSGA/article-cover_image-shrink_720_1280/article-cover_image-shrink_720_1280/0/1727884077060?e=2147483647&v=beta&t=ipTcqQ1Y2Y8KlNptf18wpo16vll8AwBVYYDsOlinklI

AI-alapú támadások

Az AI lehetővé teszi a támadók számára, hogy intelligensebb, célozottabb és sokkal dinamikusabb támadásokat hajtsanak végre. Az AI képes a hagyományos támadási módszerek, például a phishing (adathalászat) és a malware-k terjesztése fejlettebb verzióinak alkalmazására. Az AI-alapú támadók könnyen képesek olyan hamisított e-maileket generálni, amelyek a felhasználókat könnyen megtéveszthetik mivel az AI képes felismerni a szöveg kontextusát és személyre szabni az üzeneteket. A gépi tanulás algoritmusok segíthetnek a

támadóknak a szöveg és a képek manipulálásában, így a phishing-támadások még nehezebbé válnak a hagyományos védelmi rendszerek számára.

Az AI-t használó támadók képesek a védelmi rendszerek elleni támadások gyors finomítására is. A mesterséges intelligencia algoritmusok folyamatosan elemzik a rendszerek védelmi mechanizmusait és képesek olyan technikákat alkalmazni, amelyek kikerülik a hagyományos biztonsági rendszerek védelmét, például a víruskeresőket, a tűzfalakat vagy az IDS/IPS rendszereket. Mivel az AI képes az emberi viselkedést észlelni és modellezni, így könnyen képes elkerülni a szabályalapú rendszerek által alkalmazott védelmi mechanizmusokat.

Automatizáció a támadásokban

Az automatizálás egy másik kulcsfontosságú tényező, amely lehetővé teszi a támadók számára, hogy folyamatosan és nagy sebességgel hajtsanak végre támadásokat. Az automatizált eszközök lehetővé teszik számukra, hogy anélkül terjesszenek malware-t vagy végezzenek DDoS (elutasító szolgáltatás) támadásokat, hogy folyamatos emberi beavatkozásra lenne szükség. Az automatizálás a kibertámadásokat gyorsabbá és hatékonyabbá teszi, miközben a támadók elkerülhetik a figyelmet mivel az ilyen típusú támadásokat nehezebb észlelni.

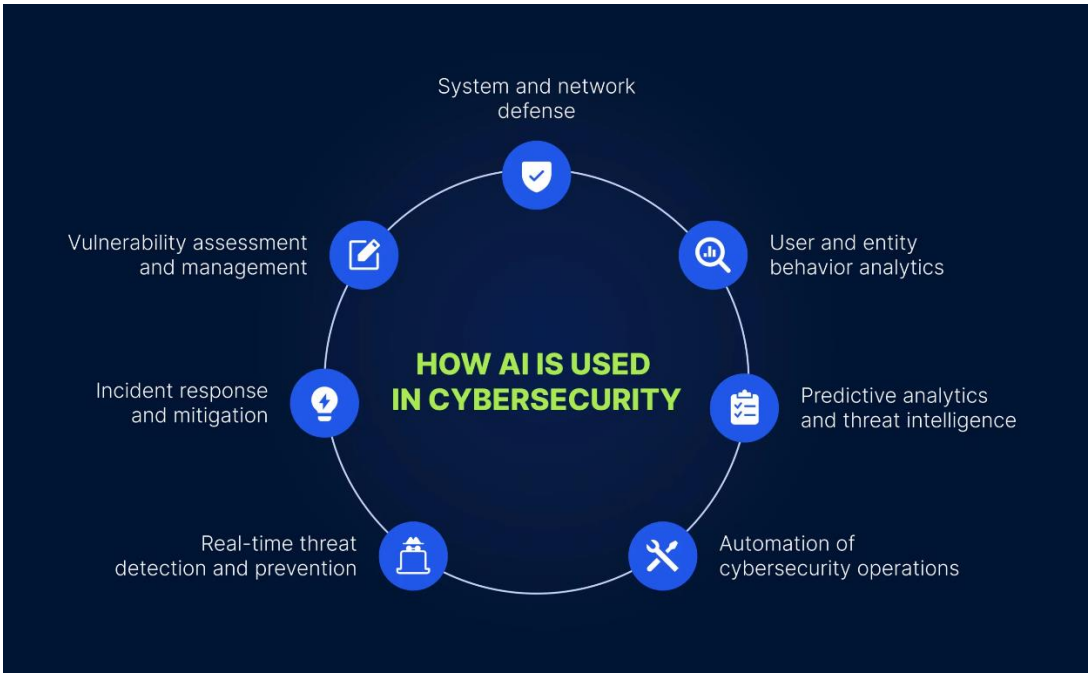
A gépi tanulás alkalmazása az automatizálásban is fontos szerepet kapott mivel a támadók képesek lehetnek a támadási szcenáriók hatékonyabb elemzésére, valamint azokat a védelmi réseket és sebezhetőségeket felismerni, amelyek a legjobban kihasználhatók a támadások során. Az AI és automatizálás alkalmazása által a támadók a kibertámadások volumenét és intenzitását is képesek növelni, ami komoly kihívások elé állítja a jelenlegi védelmi rendszereket.

Prediktív biztonság és viselkedésalapú védelem

A kiberbiztonság jövője egyre inkább a prediktív (előrejelző) megközelítések felé hajlik. A prediktív biztonsági rendszerek és a viselkedésalapú védelem olyan fejlett technológiák, amelyek segítenek felismerni és megelőzni a kibertámadásokat még azok bekövetkezte előtt. E megoldások célja, hogy a kiberfenyegetéesket ne csupán reagáló módon, hanem előre felismerve és megelőzve kezeljék.

Prediktív biztonság

A prediktív biztonság az adatok és a mesterséges intelligencia erejére támaszkodik, hogy előre jelezze a potenciális kibertámadásokat. Az ilyen rendszerek a nagy mennyiségű adat (big data) és gépi tanulási algoritmusok segítségével képesek azonosítani a potenciális fenyegetéseket. A prediktív rendszerek az analízisek alapján képesek olyan jeleket észlelni, amelyek a támadásokra utalhatnak, például a hálózati forgalom szokatlan változásait, a felhasználói viselkedés eltéréseit, vagy az újonnan megjelenő malware-ek mintáit. A cél az, hogy a támadásokat még a végrehajtás előtt meg lehessen előzni, ezáltal csökkentve a kár mértékét és javítva a válaszreakció sebességét.[16] *(24. ábra -)*



24. ábra - AI használata a kiberbiztonságban
https://techbullion.com/how-predictive-risk-intelligence-can-transform-your-cybersecurity-strategy/

Viselkedésalapú védelem

A viselkedésalapú védelem a rendszer és a felhasználók szokásos viselkedésének monitorozásán alapul, hogy azonosítani lehessen a gyanús tevékenységeket. Az ilyen típusú védelem képes megkülönböztetni a normális felhasználói tevékenységeket a szokatlan, potenciálisan rosszindulatú eseményektől. A viselkedésalapú védelmi rendszerek a mesterséges intelligencia segítségével elemzik az egyes felhasználók és rendszerek interakcióit és képesek felismerni, ha valaki megpróbálja kijátszani a rendszer biztonsági mechanizmusait, például adatok ellopásával vagy rendszerek manipulálásával. A viselkedésalapú védelem előnye, hogy nem csupán a jól ismert fenyegetéseket képes észlelni, hanem az eddig ismeretlen támadásokat is felismeri, amelyek az új technikákra építenek.[17] *(25. ábra -)*

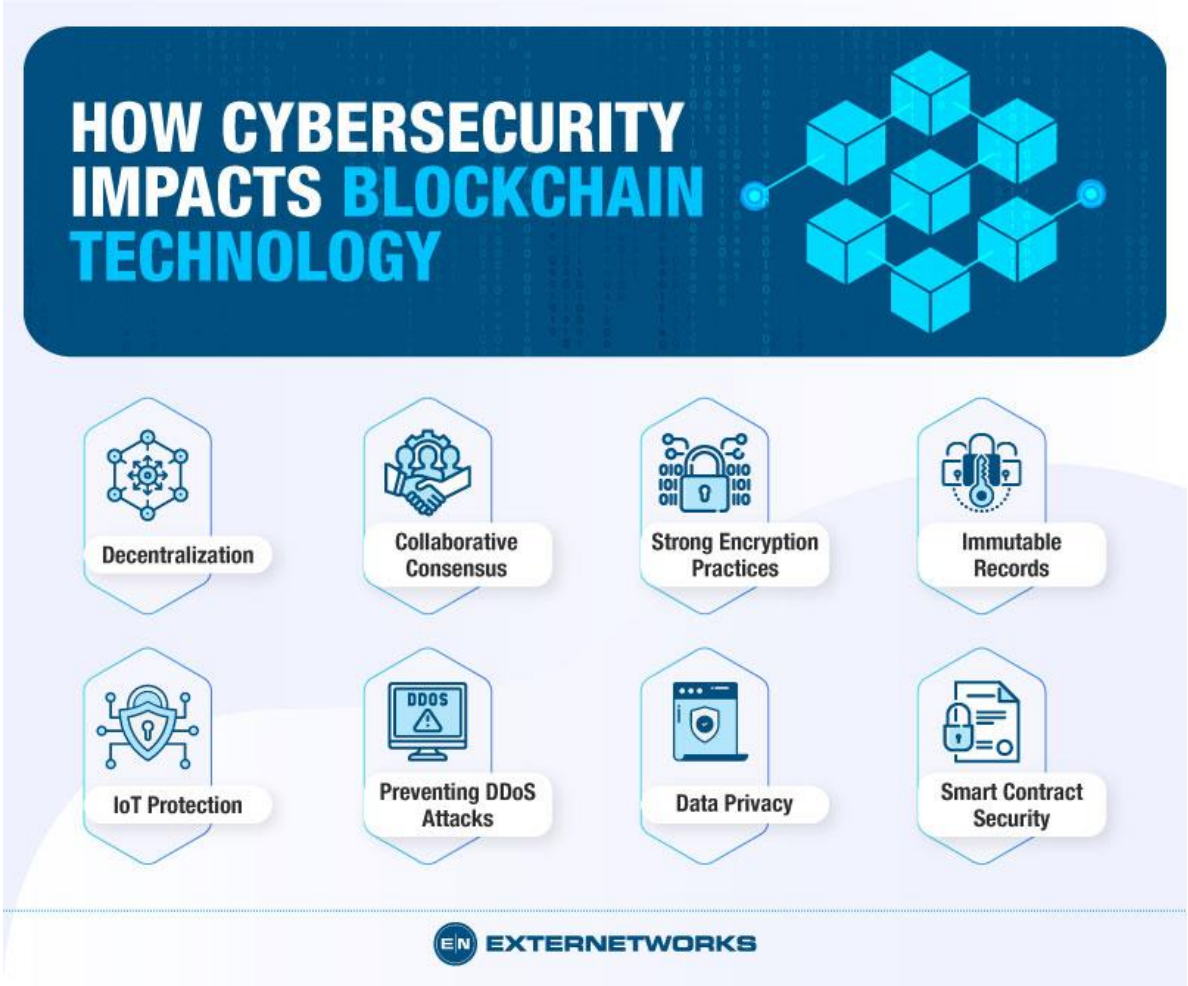
25. ábra - Viselkedésalapú védelem
https://cyberpedia.reasonlabs.com/IMG/behaviour-based%20detection.jpg

Integráció és automatizálás

A prediktív biztonság és a viselkedésalapú védelem egyesítése lehetőséget biztosít arra, hogy a kiberbiztonsági rendszerek gyorsan reagáljanak a fenyegetésekre, még akkor is, ha azok előre nem láthatóak. Az automatizált válaszreakciók és a gépi tanulás segítenek abban, hogy a védelmi rendszerek ne csak figyeljék, hanem aktívan válaszoljanak a gyanús tevékenységekre. Ezáltal a támadók esélye a sikeres betörésre jelentősen csökken.

Blokklánc-technológia alkalmazása a védelemben

A blokklánc-technológia az egyik legnagyobb innováció a digitális világban és számos alkalmazásra talált a pénzügyi szektoron kívül is. A blokklánc decentralizált, biztonságos és átlátható módon tárolja az adatokat és sok szakértő szerint a kiberbiztonság terén is jelentős szerepet játszhat a jövőben.[18] *(26. ábra -)*



26. ábra - Blokklánc technológia a kiberbiztonságban
https://www.extnoc.com/learn/wp-content/uploads/2023/08/cybersecurity-Lies-in-Blockchain-Technology.jpg

Decentralizált adatkezelés

A blokklánc egyik legnagyobb előnye a decentralizált adatkezelés, amely lehetővé teszi az adatok biztonságos tárolását és megosztását anélkül, hogy egyetlen központi entitás irányítaná azt. Ez a technológia különösen hasznos lehet a kiberbiztonságban mivel a blokklánc alapú rendszerek nehezen támadhatóak. Mivel a blokkláncon tárolt adatokat több csomópont is kezeli, nincs egyetlen központi pont, amelyet megtámadhatnának. Ez csökkenti a rendszer sebezhetőségét a központi adatbázisokhoz képest, amelyek könnyen célpontokká válhatnak.

Integráció a hozzáférés-ellenőrzésbe

A blokklánc a hozzáférés-ellenőrzési rendszerekben is hasznos lehet mivel képes biztosítani a felhasználói hitelesítési és jogosultsági adatokat egy átlátható és biztonságos módon. A decentralizált megoldások lehetővé teszik, hogy a felhasználók ellenőrizhessék és nyomon követhessék a hozzáférési engedélyeket, csökkentve a jogosulatlan hozzáférés kockázatát.

Smart Contracts

A blokklánc másik érdekes alkalmazása az úgynevezett smart contract (okos szerződések) használata a kiberbiztonságban. Az okos szerződések automatikusan végrehajtják a szerződéses feltételeket, ha azok teljesülnek és biztosítják, hogy a tranzakciók biztonságosak és megbízhatóak legyenek. Az okos szerződések potenciálisan alkalmazhatóak a vállalati tranzakciók és adatcserék védelmében mivel minden lépést rögzítenek a blokkláncon és megakadályozzák a manipulációt.

A blokklánc tehát nem csupán a pénzügyi szektorban, hanem a kiberbiztonság területén is egyre nagyobb szerepet kap mivel új lehetőségeket biztosít az adatok védelme és az információk hitelesítése terén.

Az etikai és társadalmi dimenziók a kiberbiztonságban

A kiberbiztonság területén nemcsak technikai kihívásokkal kell szembenézni, hanem számos etikai és társadalmi kérdést is felvet. A technológiai fejlődés gyors ütemével párhuzamosan a kiberbiztonság nem csupán a rendszerek védelmét jelenti, hanem az adatkezelés, a magánélet védelme és a társadalmi felelősségvállalás kulcsfontosságú aspektusává vált. A digitális világban az emberek egyre több személyes adatot osztanak meg és ez az adatfolyam rengeteg új kihívást hozott a szabályozás és az etikai normák területén. A kiberbiztonság tehát nemcsak technikai megoldásokat igényel, hanem figyelembe kell venni az adatvédelmi törvények, az adatkezelési felelősség és a társadalmi hatások kérdéseit is.[19] *(27. ábra -)*

27. ábra - Etika a kiberbiztonságban
https://onlinelaw.csuohio.edu/wp-content/uploads/2024/09/Ethics-768x402.png

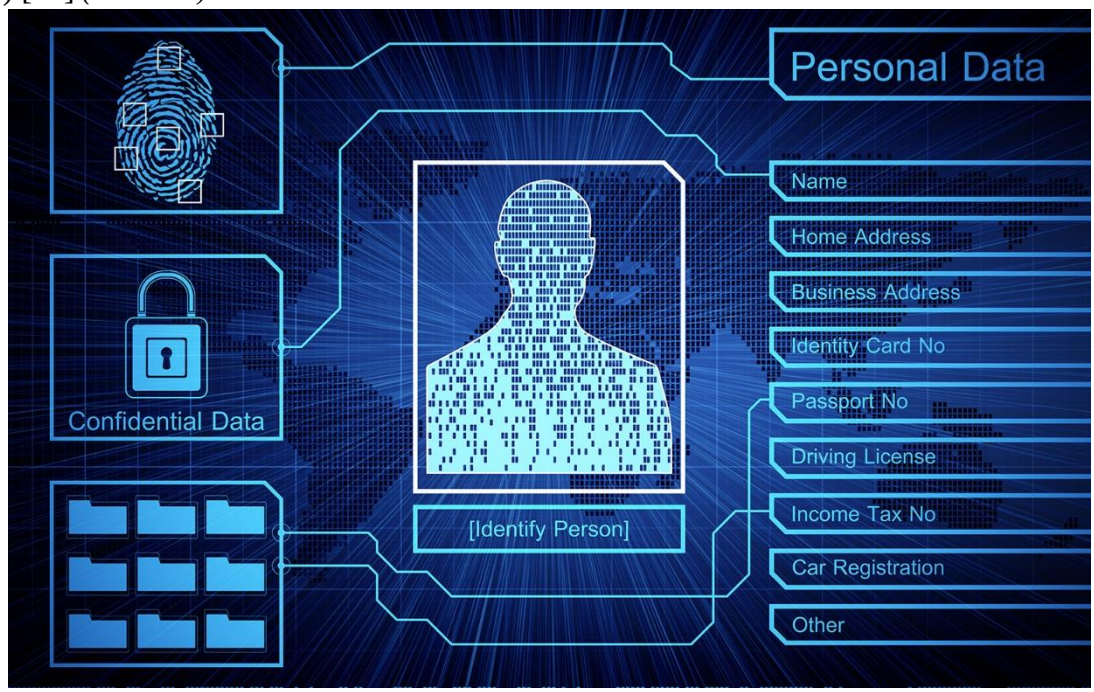
Személyes adatok védelme és magánélet

Az egyik legfontosabb társadalmi kérdés, amely a kiberbiztonság területén felmerül, az a személyes adatok védelme. Mivel az emberek nap mint nap rengeteg személyes adatot osztanak meg online, a kérdés, hogy ki férhet hozzá ezekhez az adatokhoz és hogyan használják fel őket, kiemelkedő fontossággal bír. A magánélet védelme egy olyan alapjog, amely az informatikai környezetben egyre inkább sérülhet, ha az adatokat nem megfelelően kezelik.

A személyes adatok védelme nem csupán a magánszemélyek érdekeit szolgálja, hanem a társadalom egészét is mivel a titkosított, biztonságos adatkezelés hozzájárul a bizalom fenntartásához a digitális környezetben. A kiberbiztonsági intézkedések alapvetően

szükségesek ahhoz, hogy megvédjük a felhasználók személyes információit a jogosulatlan hozzáféréstől, az adatlopásoktól és más fenyegetésektől.

A személyes adatok védelme érdekében az adatkezelőknek biztosítaniuk kell, hogy az általuk gyűjtött adatokat csak törvényes, etikusan és átlátható módon kezeljék. Ennek része a megfelelő titkosítási módszerek alkalmazása, az adatkezelési gyakorlatok átláthatósága és a felhasználói jogok védelme, beleértve az adatok törléséhez való jogot (például a GDPR-ban rögzített jogok).[20] *(28. ábra -)*



28. ábra - Személyes adatok védelme
https://amagno.co.uk/wp-content/uploads/2018/03/Personal-data-privacy.jpg

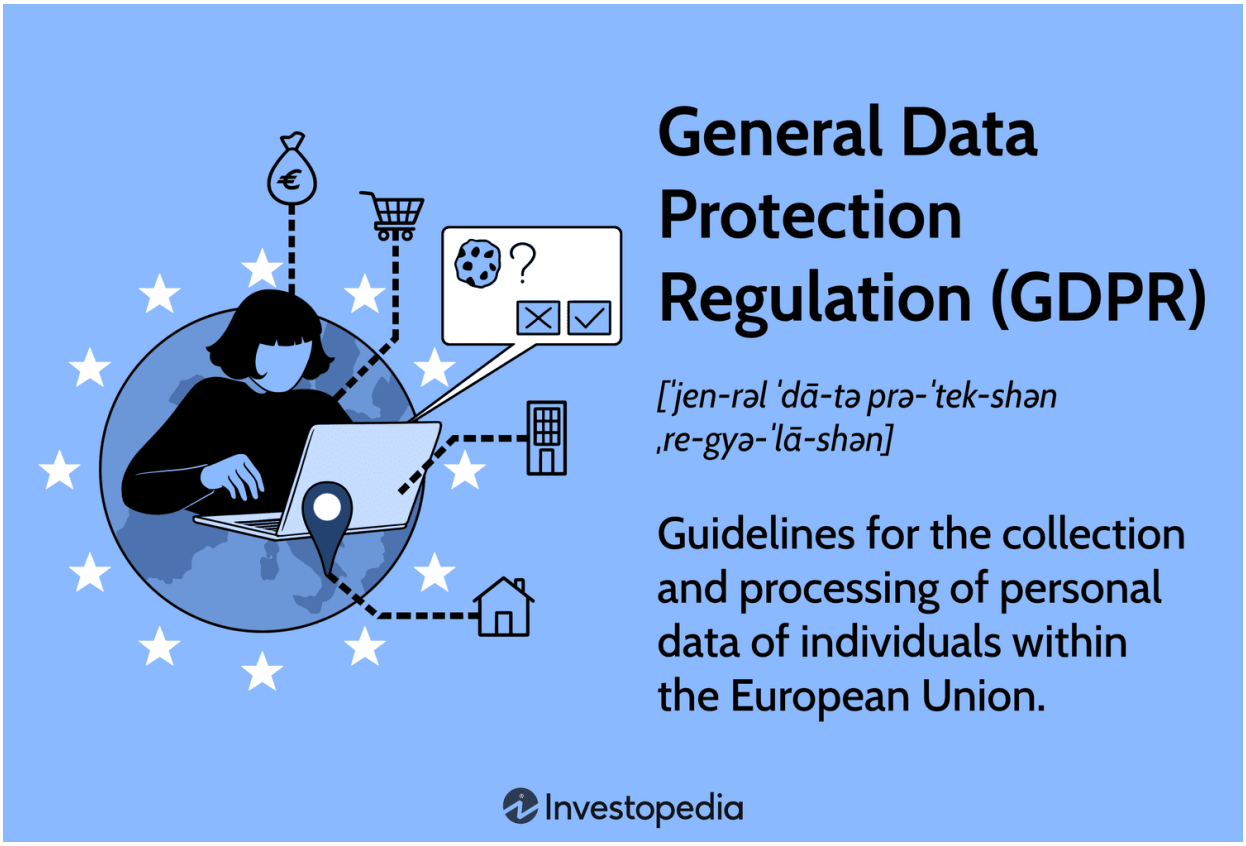
Adatvédelmi törvények és szabályozás

Az adatvédelmi törvények és szabályozás kulcsfontosságúak a kiberbiztonság etikai dimenziójában mivel ezek biztosítják, hogy az adatok kezelésére vonatkozó jogi kereteket betartsák és hogy a személyes adatok védelme minden szinten megfelelő figyelmet kapjon. A legjobban ismert adatvédelmi jogszabály a General Data Protection Regulation (GDPR), amely az Európai Unió területén működő szervezetek számára kötelezővé teszi az adatok megfelelő védelmét és a felhasználók adatkezelési jogainak tiszteletben tartását.

A GDPR nemcsak a vállalatokat kötelezi a felhasználói adatok védelmére, hanem jelentős hatással van arra is, hogyan dolgozzák fel a cégek és más szervezetek az adatokat, hogyan érhetők el az adatok és hogyan kezelhetők az adatvédelmi incidensek. E jogszabály előírja az adatok titkosítását, az adatkezelési nyilvántartások vezetését, valamint azt, hogy a

felhasználóknak joguk van megismerni és ellenőrizni, hogyan használják fel az őket érintő adatokat.

Ezenkívül számos más adatvédelmi törvény is létezik világszerte, amelyek mind az adatkezelők számára, mind a felhasználók számára fontos jogokat biztosítanak. Az adatvédelmi törvények és szabályozások biztosítják, hogy a technológiai megoldások etikai kereteken belül működjenek és megvédjék az emberek jogait és érdekeit.[21] *(29. ábra -)*



29. ábra - GDPR
https://www.investopedia.com/thmb/pm_q3M8iq5eO8_zv7TMXOt2Co6o=/750x0/filters:no_upscale():max_bytes(150000):strip_icc():format(webp)/general-data-protection-regulation-gdpr.asp-final-1b12e02aa4d149b9af4fcd8aec409a89.png

Adatkezelési felelősség és társadalmi hatások

A kiberbiztonság egyik legfontosabb társadalmi dimenziója az adatkezelési felelősség kérdése. A vállalatok és szervezetek, amelyek személyes adatokat gyűjtenek és tárolnak, felelősséget viselnek azok védelméért. A felelősség nemcsak jogi szempontból fontos, hanem etikai szempontból is mivel a felhasználók bizalmát az adatok kezelése erősen befolyásolja.

Fontos az adatkezelők számára, hogy átláthatóan kezeljék a személyes adatokat, hogy a felhasználók tudják, miként gyűjtik, tárolják és használják fel az információkat. Az adatkezelés felelőssége nemcsak a felhasználói jogok védelmét jelenti, hanem azt is, hogy minimalizálják az adatlopásokat, adatvesztéseket és egyéb adatvédelmi incidenseket, amelyek társadalmi és

gazdasági hatásokat okozhatnak. Az ilyen incidensek károsíthatják a felhasználók bizalmát és komoly következményekkel járhatnak a vállalatok számára.

A társadalmi hatások szintén kulcsfontosságúak a kiberbiztonságban. A digitális világban az emberek személyes adatai nemcsak az egyének, hanem az egész társadalom biztonságát is érinthetik. A nagy mennyiségű adat és az automatizált adatkezelés növekvő trendje miatt a kiberbiztonsági megoldások nemcsak technikai kérdések, hanem társadalmi és etikai kihívások is, amelyek közvetlen hatással vannak az egyének magánéletére és társadalmi szerepére.

Etikai és jogi kihívások

A kiberbiztonság területén felmerülő etikai és jogi kihívások közé tartoznak azok az esetek, amikor a technológiai fejlődés ütközik a magánélet védelmével. Az állami és vállalati felügyelet, a nyilvános adatokhoz való hozzáférés, valamint a felhasználók személyes információinak kezelése mind olyan területek, ahol az etikai és jogi megfontolások rendkívül fontosak. *(30. ábra -)*

Például a kormányok gyakran arra kényszeríthetik a vállalatokat, hogy segítsenek a bűnüldözési célú adatgyűjtésben, ami komoly etikai dilemmákat vethet fel a felhasználók jogainak védelme és a nemzetbiztonsági igények között. Ugyanakkor a vállalatoknak is felelősséget kell vállalniuk abban, hogy biztosítsák a felhasználói adatok védelmét, miközben igyekeznek megfelelni a törvényi előírásoknak.

Nemcsak technikai és technológiai megoldások kérdése, hanem mély etikai és társadalmi vonatkozásokat is magában hordoz. Az adatkezelés, a személyes adatok védelme és a jogi szabályozás mind olyan kulcsfontosságú elemek, amelyek biztosítják a digitális világ biztonságát és megbízhatóságát. A jövőben a kiberbiztonság fejlődése nemcsak a technológiai újításoktól, hanem a társadalmi és etikai normák betartásától is függ. A megfelelő jogi keretek

és felelősségteljes adatkezelési gyakorlatok alapvetőek ahhoz, hogy a digitális környezet biztonságos és megbízható maradjon mindenki számára.[22]

30. ábra - Jogi kihívások
https://news.miami.edu/law/_assets/images/images-stories/2024/05/miami-law_business-handshake-locks-blog_940x549.jpg

Források

[1] „What is cyber-physical system (CPS) security? | Darktrace”. Elérés: 2025. április 8. [Online]. Elérhető: https://darktrace.com/cyber-ai-glossary/cyber-physical-system-cps-security

[2] A. M. Freed, „A Brief History of Ransomware Evolution”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution

[3] „How Do Ransomware Attacks Work? | Seagate US”, Seagate.com. Elérés: 2025. április 8. [Online]. Elérhető: https://www.seagate.com/blog/how-do-ransomware-attacks-work/

[4] „A Zero Trust biztonsági modell megértése”, SSL.com. Elérés: 2025. április 8. [Online]. Elérhető: https://www.ssl.com/hu/cikk/a-z%C3%A9r%C3%B3-bizalom-biztons%C3%A1gi-modellj%C3%A9nek-meg%C3%A9rt%C3%A9se/

[5] „EDR vs. XDR: What Is the Difference? | Microsoft Security”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.microsoft.com/en-gb/security/business/security-101/edr-vs-xdr

[6] „Wannacry - 3 éves a zsarolóvírus”, Wannacry - 3 éves a zsarolóvírus. Elérés: 2025. április 12. [Online]. Elérhető: https://www.eset.com/hu/hirek/harom-eves-minden-idok-legdurvabb-zsarolovirusa-2020/

[7] „A NotPetya támadás hátteréről”, PC Guru. Elérés: 2025. április 12. [Online]. Elérhető: http://www.pcguru.hu/blog/pcguru_eset_blog/a-notpetya-tamadas-hattererol/9192

[8] „Black Basta Ransomware: Tactics & Prevention”, Qualys Security Blog. Elérés: 2025. április 12. [Online]. Elérhető: https://blog.qualys.com/vulnerabilities-threat-research/2024/09/19/black-basta-ransomware-what-you-need-to-know

[9] „LockBit”, *Wikipedia*. 2025. április 7. Elérés: 2025. április 12. [Online]. Elérhető: https://en.wikipedia.org/w/index.php?title=LockBit&oldid=1284434860

[10] „What is Cybersecurity? | Digital Guardian”. Elérés: 2025. április 12. [Online]. Elérhető: https://www.digitalguardian.com/blog/what-cybersecurity-comprehensive-guide-strategies-technologies-and-best-practices

[11] „What Is Data Encryption? Definition, Types, and Best Practices”, Kinsta®. Elérés: 2025. április 12. [Online]. Elérhető: https://kinsta.com/knowledgebase/what-is-encryption/

[12] „Benefits of Implementing an Access Control System”. Elérés: 2025. április 12. [Online]. Elérhető: https://www.nordencommunication.com/en/blog/benefits-of-implementing-an-access-control-system

[13] C. Crane, „What Is a Hardware Security Module? HSMs Explained”, Hashed Out by The SSL Store™. Elérés: 2025. április 12. [Online]. Elérhető: https://www.thesslstore.com/blog/what-is-a-hardware-security-module-hsms-explained/

[14] L. Cyber, „What is SCADA and IoT?”, Lumifi Cybersecurity. Elérés: 2025. április 12. [Online]. Elérhető: https://www.lumificyber.com/blog/what-is-scada-iot/

[15] „Explaining AI’s impact on ransomware attacks and security | TechTarget”, Search Security. Elérés: 2025. április 13. [Online]. Elérhető: https://www.techtarget.com/searchsecurity/feature/Explaining-AIs-impact-on-ransomware-attacks-and-security

[16] E. Lee és A. S.-B. TechBullion, „How Predictive Risk Intelligence Can Transform Your Cybersecurity Strategy”, TechBullion. Elérés: 2025. április 13. [Online]. Elérhető: https://techbullion.com/how-predictive-risk-intelligence-can-transform-your-cybersecurity-strategy/

[17] D. Richards, „What is Behavior-Based Cybersecurity?”, Info Exchange. Elérés: 2025. április 13. [Online]. Elérhető: https://staging.infoexchangeja.com/blog/data-security/behavior-based-protection/

[18] phanivedala, „The Future of Cybersecurity Lies in Blockchain Technology”, Learning Center. Elérés: 2025. április 13. [Online]. Elérhető: https://www.extnoc.com/learn/security/blockchain-for-cybersecurity

[19] „Cybersecurity and Social Responsibility: Ethical Considerations | UpGuard”. Elérés: 2025. április 13. [Online]. Elérhető: https://www.upguard.com/blog/cybersecurity-ethics

[20] „Data protection explained - European Commission”. Elérés: 2025. április 13. [Online]. Elérhető: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

[21] „Adatvédelem és GDPR | Mit és hogyan?”, Your Europe. Elérés: 2025. április 13. [Online]. Elérhető: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hu.htm

[22] M. L. B. Contributor, „What Are the Legal Aspects of Cybersecurity? How an M.L.S. Can Help”. Elérés: 2025. április 13. [Online]. Elérhető: https://news.miami.edu/law/stories/2024/05/mls-what-are-the-legal-aspects-of-cybersecurity.html

2.27. Légiközlekedés, beágyazott rendszerek technológiái

Légiközlekedés, beágyazott rendszerek technológiái

Magyar Levente

Mérnökinformatikus, m.lev0311@gmail.com

Bár nincs megkülönböztetett fejléc, ez az absztrakt. Ez a beküldési sablon lehetővé teszi a szerzők számára, hogy benyújtsák tanulmányaikat a tárgy követelményeként elvárt házi feladataként anélkül, hogy ebben a szakaszban bármilyen kimeneti formázási előírás érvényesülne. A kéziratsablon egy egyhasábos dokumentum, amely lehetővé teszi a szerzők számára, hogy tartalmukat beírják az előre beállított bekezdésformázási stílusokba, amelyek a mintahelyőrző szövegre vannak alkalmazva. A dokumentumban további útmutatásokat talál arról, hogyan kell formázni a szöveget. A sablon, az ACM új kéziratsablonján alapul.

Kulcsszavak: Kulcsszavak felsorolása vesszővel elválasztva, Kulcsszó 1, Kulcsszó 2, Kulcsszó 3, Kulcsszó 4

1 BEVEZETÉS – AZ ÜZEMBIZTOS BEÁGYAZOTT RENDSZEREK SZEREPE A MODERN LÉGIKÖZLEKEDÉSBEN

A légiközlekedés fejlődése a XX. század elejétől napjainkig a technológiai innováció egyik leglátványosabb példája. A modern repülőgépek, különösen a kereskedelmi és katonai célú nagy hatótávolságú típusok, rendkívül komplex rendszerek összességeként működnek. Az ezekben megtalálható elektronikai és vezérlőegységek többsége ún. **beágyazott rendszerek** formájában valósul meg. Ezek a rendszerek jellemzően speciális, meghatározott célokra tervezett mikrovezérlőkön vagy mikrokontrollereken alapulnak, és képesek valós időben, megbízhatóan és folyamatosan működni a legszigorúbb biztonsági követelmények mellett is.

Az **üzembiztosság** (angolul: dependability) fogalma a légiközlekedésben kiemelten fontos. Ide tartozik a rendszer megbízhatósága (reliability), rendelkezésre állása (availability), karbantarthatósága (maintainability) és biztonságossága (safety). A beágyazott rendszerek ezen jellemzők mentén kerülnek megtervezésre és integrálásra a fedélzeti elektronikai architektúrába. Egy ilyen architektúra nem csupán redundáns, de képes hibatűrésre és a részleges meghibásodások esetén is fenntartja a működőképességet.

A dolgozat célja annak részletes bemutatása, hogy ezek az üzembiztos beágyazott rendszerek miként járulnak hozzá a repülésirányítás, navigáció, fedélzeti kommunikáció, hajtóművezérlés, utaskomfort és más fedélzeti funkciók megbízható és biztonságos működéséhez. A következő fejezetekben feltérképezzük ezek architektúráját, komponenseit, fejlesztési szabványait (pl. DO-178C), valamint a jövőbeli trendeket, például az autonóm légi járművek (UAV-k) és az űrtechnológia terén.

2 ÁTTEKINTÉS – A FEDÉLZETI BEÁGYAZOTT RENDSZEREK OSZTÁLYOZÁSA ÉS FŐBB FUNKCIÓI

A modern repülőgépek fedélzeti rendszerei rendkívül komplex architektúrákra épülnek, amelyekben a különböző beágyazott egységek meghatározott feladatkörök szerint szerveződnek. A fedélzeti rendszerek funkcionalitása alapján az alábbi fő kategóriákra oszthatók:

2.1 Irányítási és vezérlőrendszerek (Flight Control Systems)

Ezek a rendszerek felelnek a repülőgép stabilitásáért és manőverezhetőségéért. A **fly-by-wire** rendszerek – melyekben a hagyományos mechanikus kapcsolatokat elektronikus jellel helyettesítik – beágyazott mikrokontrollerek és szenzorhálózat segítségével valósítják meg az irányítás logikáját. Itt kiemelt szerepet játszanak a **Flight Control Computers (FCC-k)**, amelyek az adatokat integrálják, feldolgozzák és utasításokat adnak a szervomotoroknak.

2.2 Navigációs rendszerek (Navigation Systems)

A navigációs rendszerek – például az Inertial Navigation System (INS), Global Navigation Satellite System (GNSS), vagy a VOR/DME rendszerek – integrált beágyazott egységeken futnak, és pontos helymeghatározást tesznek lehetővé. Ezek valós időben kommunikálnak a központi számítógéppel, és gyakran több redundáns forráson alapulnak a hibatűrés biztosítására.

2.3 Kommunikációs rendszerek (Communication Systems)

A rádiófrekvenciás és adatkommunikációs modulok is beágyazott rendszerekre épülnek, amelyek támogatják a pilóta és az irányítótorony közötti kétirányú kapcsolatot (pl. VHF/UHF rádiók, ACARS – Aircraft Communications Addressing and Reporting System). A legmodernebb rendszerek már szoftverdefiniált rádiókat (SDR) alkalmaznak, amelyeket beágyazott platformok vezérelnek.

2.4 Hajtóművezérlés és energiaelosztás (Engine and Power Systems)

A hajtóművezérlő rendszerek (FADEC – Full Authority Digital Engine Control) autonóm beágyazott rendszerek, amelyek érzékelők, aktuátorok és algoritmusok segítségével szabályozzák az üzemanyag-ellátást, a tolóerőt, valamint felügyelik a hőmérsékletet, nyomást és rezgéseket. Emellett az energiaelosztó rendszerek biztosítják a villamosenergia folyamatos elosztását, felügyeletét és vészhelyzeti átkapcsolását – szintén valós idejű működés mellett.

2.5 Utaskomfort és fedélzeti szolgáltatások

Ide sorolható az ülésszabályozás, világítás, klímaberendezések vezérlése és az utasinformációs rendszerek működtetése is. Bár ezek nem biztonságkritikus rendszerek, mégis magas rendelkezésre állást igényelnek a szolgáltatásminőség fenntartása érdekében.

A különböző rendszerek egymással is kommunikálnak, gyakran szabványosított kommunikációs protokollokon keresztül (például ARINC 429, MIL-STD-1553, vagy újabb típusoknál AFDX). Ez a hálózatos architektúra teszi lehetővé az integrált fedélzeti rendszerek hatékony és üzembiztos működését.

3 REPÜLÉSVEZÉRLŐ SZÁMÍTÓGÉPEK (FLIGHT CONTROL COMPUTERS) ÉS A FLY-BY-WIRE ARCHITEKTÚRÁK MŰKÖDÉSE

A repülésvezérlés a repülésbiztonság legkritikusabb eleme, és napjaink korszerű repülőgépei már nem mechanikus, hanem digitális úton vezéreltek. A hagyományos repülőgépeken a pilóta közvetlen mechanikai kapcsolaton keresztül irányította a vezérsíkokat, míg a mai **fly-by-wire (FBW)** rendszerekben ezeket a parancsokat számítógépek értelmezik és továbbítják a végrehajtó mechanizmusoknak. Ezeket a rendszereket a **Flight Control Computers (FCC-k)** vezérlik, amelyek megbízható beágyazott rendszerekként működnek, és rendkívül szigorú biztonsági és teljesítménykövetelményeknek kell megfelelniük.

3.1 A fly-by-wire rendszer alapvető működése

A fly-by-wire rendszer lényege, hogy a pilóta vezérlőparancsai elektromos jelekké alakulnak, amelyek egy feldolgozóegységbe – az FCC-be – kerülnek. Az FCC:

1. feldolgozza a bejövő parancsokat,
2. összeveti őket a szenzoradatokkal (pl. gyorsulásmérők, giroszkópok, statikus és dinamikus nyomásérzékelők),
3. végrehajtási utasításokat küld a szervómeghajtók felé.

A rendszer képes automatikusan stabilizálni a repülőgépet, figyelembe véve olyan körülményeket, mint turbulencia, aerodinamikai túlterhelés vagy szélnyomás, miközben a repülőgép válaszai természetesek maradnak a pilóta számára.

3.2 Redundancia és biztonsági architektúrák

A repülésvezérlő számítógépek nem egyedül működnek: több redundáns egység párhuzamosan, különböző hardvereken és szoftverkörnyezetben dolgozik (pl. **triplex vagy quadruplex konfiguráció**), hogy kizárják az egykomponensű hibákból eredő baleseteket. Minden rendszer egymástól függetlenül fut, és összevetik az eredményeiket. Ha eltérés van a számított parancsok között, a hibásnak azonosított rendszer automatikusan lekapcsolásra kerül, és a tartalékrendszer veszi át a vezérlést.

Az **Airbus A320** például három különböző típusú számítógépet használ (ELAC – Elevator and Aileron Computer, SEC – Spoiler and Elevator Computer, FAC – Flight Augmentation Computer), amelyek mindegyike két példányban van jelen. A Boeing 777 esetében **moduláris, disztribuált** architektúra jellemző, amelynél a fő FCC több alrendszerbe van delegálva.

3.3 Adatfeldolgozás és valós idejű működés

A fly-by-wire rendszerek tipikusan **hard real-time** környezetben futnak, ami azt jelenti, hogy minden feldolgozási feladatnak pontos időkorlátokon belül kell végbemennie. A késleltetés vagy feldolgozási hiba nem csupán teljesítményromlást, hanem potenciálisan katasztrofális kimenetelt okozhat. Emiatt a rendszerek gyakran determinisztikus RTOS (Real-Time Operating System) alatt futnak, például:

4. VxWorks (Wind River),
5. INTEGRITY (Green Hills Software),
6. vagy az ARINC 653 szabvány szerint implementált operációs környezetek.

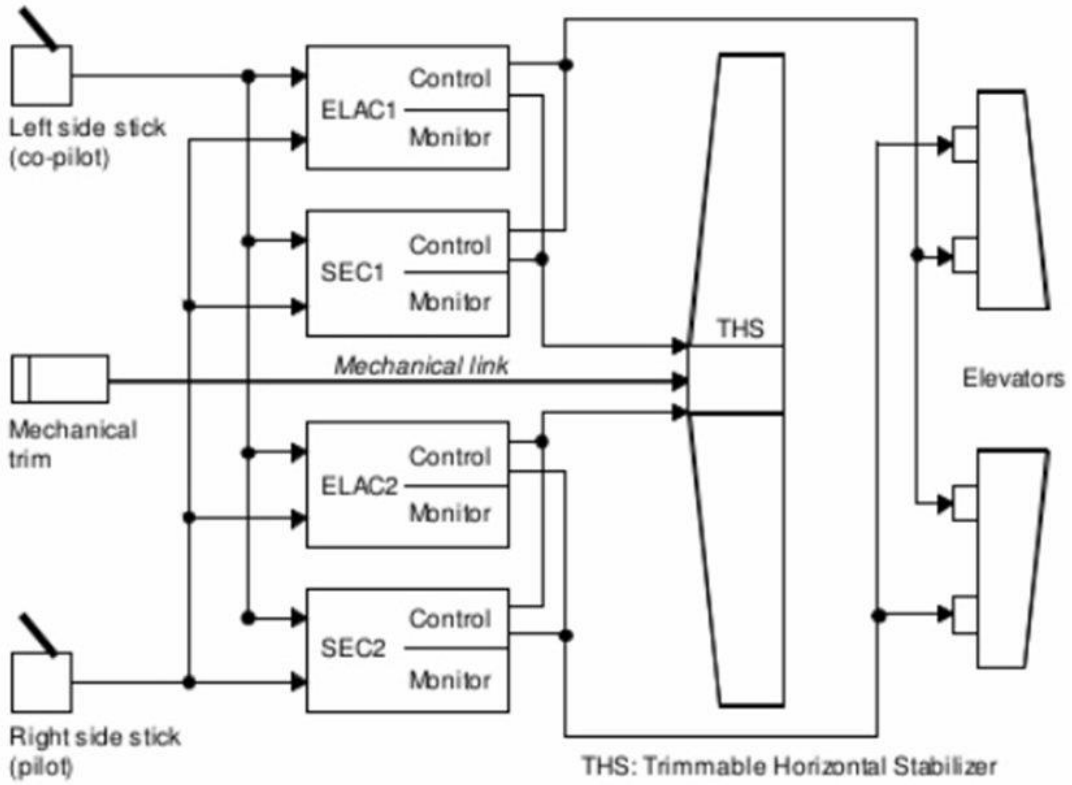
Ezek az RTOS-ek lehetővé teszik a feladatok időzített futtatását, erőforrás-szigetelést és hibás szálak azonnali izolálását.

3.4 Kontroll logika és döntéshozatal

A repülésvezérlő számítógép nem csak továbbítja a parancsokat, hanem értelmezi is őket. Például ha a pilóta túl nagy szöggel próbálja emelni az orrot, az FCC ezt korlátozza, hogy elkerülje a stall helyzetet. Ez az ún. **flight envelope protection** része, amely megakadályozza, hogy a repülőgép az aerodinamikai határait átlépje. Ezeket a döntéshozatali szabályokat formális verifikációval és szimulációkkal tesztelik még az üzembe helyezés előtt, a DO-178C és DO-254 szabványoknak megfelelően.

3.5 Történeti áttekintés és technológiai fejlődés

Az első fly-by-wire rendszerű repülőgép a NASA által átalakított F-8 Crusader volt az 1970-es években. Azóta a technológia fejlődése robbanásszerű volt, mára pedig az összes nagy gyártó (Airbus, Boeing, Embraer, Dassault) FBW-alapú irányítórendszert alkalmaz az új generációs gépeken. A legújabb fejlesztések közé tartoznak az **elektronikus vezérlésű szárnyvégek**, **dinamikusan újrakonfigurálható szoftverek**, illetve az **önálló hibatűrő algoritmusok**, amelyek mesterséges intelligenciát is használnak.



Kép 1.: Fly-by-wire rendszer

4 BIZTONSÁGI ÉS MEGBÍZHATÓSÁGI KÖVETELMÉNYEK AZ ÜZEMBIZTOS RENDSZEREKBEN

A légiközlekedésben alkalmazott beágyazott rendszerek esetében a **biztonság (safety)** és **megbízhatóság (reliability)** kérdései nem csupán mérnöki szempontból fontosak, hanem szabályozói és etikai szinten is. Egy fedélzeti rendszer meghibásodása életeket veszélyeztethet, ezért ezen rendszerek tervezésénél az elsődleges prioritás az üzembiztonság garantálása.

4.1 A megbízhatóság definíciója és metrikái

A **megbízhatóság** azt jelenti, hogy a rendszer előre meghatározott működési paraméterek mellett hibamentesen működik adott időtartamon keresztül. Ezt gyakran a **Mean Time Between Failures (MTBF)** és **Failure Rate (λ)** metrikákkal jellemzik.

7. Egy tipikus kereskedelmi repülőgép esetében a fedélzeti számítógépek MTBF értéke **>100 000 óra** kell, hogy legyen.

8. A megbízhatósági analízisek gyakran **FMEA (Failure Mode and Effects Analysis)** vagy **FTA (Fault Tree Analysis)** módszereken alapulnak.

A cél az, hogy a repülőgép teljes architektúrája ne tartalmazzon olyan egyetlen hibapontot (SPOF – Single Point of Failure), amely egy meghibásodás esetén a rendszer leállásához vagy instabil viselkedéshez vezetne.

4.2 Redundancia alkalmazása

A **hardveres redundancia** a leggyakoribb módszer az üzembiztosság növelésére. Ez lehet:

9. **Párhuzamos (active-active)** redundancia, ahol több komponens egyszerre dolgozik, és ha az egyik hibát jelez, a többi tovább működik.
10. **Tartalékos (active-standby)** redundancia, ahol egy vagy több komponens inaktív, de hiba esetén automatikusan aktiválódik.

A fedélzeti rendszerek általában **triplex vagy quadruplex architektúrát** alkalmaznak. A különböző példányok különböző gyártóktól származhatnak, más szoftverkörnyezetben futnak (pl. diverse redundancy), hogy minimalizálják azonos típusú hibák esélyét.

Például a Boeing 787 Dreamlinerben három párhuzamos rendszer fut eltérő logikai implementációkkal, míg az Airbus A350 esetében 3+1 konfigurációban van jelen a flight control unit.

4.3 Hibadetektálási és -kezelési stratégiák

A **beágyazott rendszerek** több szintű hibakezelést használnak:

11. **Self-diagnostics**: a rendszer periodikusan ellenőrzi saját állapotát (watchdog timers, BIST – Built-In Self Test).
12. **Error detection codes (EDC)**, például CRC (Cyclic Redundancy Check) alkalmazása kommunikációs protokolloknál.
13. **ECC (Error-Correcting Code)** memória használata a RAM hibák automatikus javítására.

Amikor hiba történik, a rendszer elsőként **hibaisolálást (fault isolation)** végez, majd **újrakonfigurálja** magát úgy, hogy a sérült komponens kikapcsolásával fenntartsa a működés folytonosságát. Ez az ún. **degradált működés**, amely még mindig biztonságos, de már nem teljes funkcionalitású (pl. csökkentett teljesítményű repülésvezérlés).

4.4 Biztonságkritikus működés

A **biztonságkritikus rendszerek** működését szigorú nemzetközi szabványok határozzák meg:

14. A **DO-178C** (lásd következő fejezet) a szoftverfejlesztést szabályozza.
15. A **DO-254** az elektronikai hardverek fejlesztését szabályozza.
16. Az **ARP4754A** és **ARP4761** a repülőgéprendszerek szintjén írja elő a rendszerbiztonsági analízisek módszertanát.

Minden rendszerhez biztonsági szintet rendelnek, pl.:

Szint	Megnevezés	Példa	Szoftveres minősítési szint
A	Katasztrofális	Repülésirányító rendszer kiesése	DAL A (Design Assurance Level)
B	Veszélyes	Stabilizátor vezérlés hibája	DAL B
C	Káros	Egy szenzor adatvesztése	DAL C
D	Minimális hatás	Kijelző újrarajzolási hiba	DAL D
E	Nincs hatás	Audio rendszer késése	DAL E

Az „A” szintű rendszerek hibája emberi élet elvesztéséhez vezethet, ezért fejlesztésük során szigorú bizonyítási kötelezettség áll fenn, beleértve a formális verifikációt és 100%-os kódfedettségi vizsgálatokat is.

4.5 Támadások és külső fenyegetések

A modern repülőgépek egyre inkább hálózatba kötöttek (pl. AID – Aircraft Interface Device), így megjelent az igény a **kiberbiztonsági védelem** integrálására. A szoftverhibák és kommunikációs protokollok sérülékenységei támadási felületet jelenthetnek, ezért a megbízhatósági vizsgálatok mellett **penetrációs teszteket** és **hálózati szegmentációt** is alkalmaznak a kritikus rendszerek védelme érdekében.

4.6 Példák a biztonságos rendszerekre

17. **Airbus Flight Warning System (FWS)**: egy komplex, hibatoleráns logikai rendszer, amely a pilótát értesíti minden rendellenességről.
18. **FADEC (Full Authority Digital Engine Control)**: a hajtóművezérlő rendszer redundáns szenzorhálózattal és öndiagnosztikával biztosítja a motor optimális működését és védelmét.

5 SZOFTVERFEJLESZTÉSI SZABVÁNYOK A LÉGIKÖZLEKEDÉSBEN

Az üzembiztos beágyazott rendszerek fejlesztése a légiközlekedésben rendkívül szigorú szabályozási és tanúsítási környezetben zajlik. A szoftverhibák következményei ebben az iparágban halálosak lehetnek, így a biztonságkritikus szoftverek fejlesztését globális, iparági

szabványok szabályozzák. A legmeghatározóbb ilyen szabvány a **DO-178C**, amely a polgári repülőgépek fedélzeti szoftverének tanúsításához nyújt keretet.

5.1 A DO-178C szabvány szerepe

A DO-178C (Software Considerations in Airborne Systems and Equipment Certification) szabványt az RTCA (Radio Technical Commission for Aeronautics) és az EUROCAE (European Organisation for Civil Aviation Equipment) közösen dolgozta ki, és 2011-ben lépett életbe, a korábbi DO-178B frissítéseként. A szabvány célja annak biztosítása, hogy a szoftverek:

19. **Megbízhatóan működnek** a tervezett körülmények között
20. **Hibák esetén sem veszélyeztetik** a légijármű vagy az utasok biztonságát
21. **Következetesen dokumentált**, jól visszakövethető fejlesztési folyamaton mennek keresztül

A DO-178C szabvány meghatározza a fejlesztési életciklus minden fontos szakaszát, beleértve a követelmények meghatározását, tervezést, implementációt, tesztelést, verifikációt és validációt is.

5.2 Szoftverfejlesztési életciklus modell

A szabvány nem írja elő konkrét fejlesztési modellt (pl. vízesés, iteratív vagy agilis), de minden esetben **teljes körű nyomonkövethetőséget** követel meg:

22. **Követelmények** (High-Level Requirements, HLR; Low-Level Requirements, LLR)
23. **Forráskód** (implementáció)
24. **Tesztelési eredmények**
25. **Verifikációs dokumentumok**

A **Traceability Matrix** használata előírás, amely lehetővé teszi, hogy minden teszt, kódmodul és tervezési döntés visszavezethető legyen egy eredeti követelményre.

5.3 Szoftverkritikussági szintek

A DO-178C bevezeti a **Design Assurance Level (DAL)** fogalmát, amely az adott szoftverkomponens meghibásodásának lehetséges hatása alapján öt szintre osztja a rendszereket:

DAL szint	Meghibásodás következménye	Példa
A	Katasztrofális	Repülésirányítás meghibásodása
B	Veszélyes	Hajtómű vezérlés
C	Fő	Navigációs rendszerek
D	Másodlagos	Felhasználói interfészek
E	Nincs hatással a biztonságra	Kabinvilágítás vezérlése

A DAL szint határozza meg a szükséges fejlesztési és tesztelési mélységet. Egy DAL A szintű rendszer például **teljes verifikációs lefedettséget** követel meg, míg egy DAL D szintű rendszer esetében ez enyhébb lehet.

5.4 DO-178C kiegészítő dokumentumai

A DO-178C-hez négy hivatalos kiegészítő dokumentum tartozik, amelyek a modern fejlesztési módszertanok és technológiák integrációját szabályozzák:

26. **DO-330** – Tool Qualification (eszközminősítés)
27. **DO-331** – Model-Based Development and Verification
28. **DO-332** – Object-Oriented Technology and Related Techniques
29. **DO-333** – Formal Methods Supplement

Ezek lehetővé teszik például a **modellezés-alapú fejlesztést** (pl. Simulink vagy SCADE), valamint a **formális verifikációs eszközök** (pl. SPARK, Frama-C) használatát, amennyiben azokat megfelelő módon validálják.

5.5 Formális verifikáció és tesztelés

A szabvány erőteljes hangsúlyt helyez a szoftver **verifikációjára** (azaz annak igazolására, hogy a rendszer megfelel a specifikációknak) és **validációjára** (annak ellenőrzésére, hogy a rendszer a felhasználó igényeit teljesíti). A tesztelési szintek általában a következők:

30. **Egységtesztek** (LLR-k lefedése, fehérdoboz teszt)
31. **Integrációs tesztek**
32. **Rendszertesztek**
33. **Kritikus funkciók teljes kódlefedettsége**

A **MC/DC (Modified Condition/Decision Coverage)** egy kötelező tesztelési követelmény a DAL A és B szinteken, amely a döntési logikák minden lehetséges ágát tesztelni kényszeríti.

5.6 Szerszámok és eszközminősítés (Tool Qualification)

Mivel sok fejlesztési és tesztelési lépés automatizált eszközökkel történik (pl. kódgenerátor, statikus analízis eszközök), a DO-330 szabályozza, hogyan kell ezen eszközöket **minősíteni** a használat előtt. A nem megfelelően minősített eszközök által végzett verifikáció nem elfogadható.

Példák gyakran alkalmazott eszközökre:

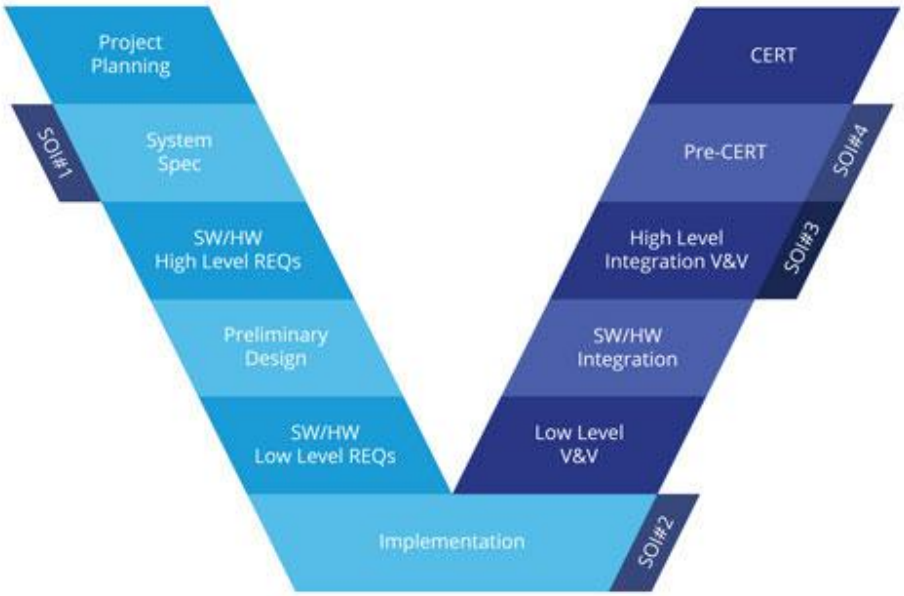
34. **LDRA Testbed**, **VectorCAST**, **RVS** – statikus és dinamikus analízis
35. **SCADE**, **Simulink** – modellezés-alapú fejlesztés
36. **Frama-C**, **SPARK** – formális verifikáció

5.7 Szabványok közötti összefüggések

A DO-178C szorosan kapcsolódik más, légiközlekedésben használt szabványokhoz, például:

37. **ARP4754A** – a teljes rendszerfejlesztés folyamata
38. **DO-254** – hardveres biztonságkritikus rendszerek fejlesztése
39. **DO-326A/DO-355** – beágyazott rendszerek kiberbiztonsági követelményei

Ezek integrált, egymásra épülő követelményhalmazt képeznek, amely a légijárművek fedélzeti rendszereinek teljes életciklusát átfogja.



Kép 2.: DO-178C v-modell diagramm

6 BEÁGYAZOTT HARDVER ÉS SZOFTVER ARCHITEKTÚRÁK A REPÜLÉSBEN

A légiközlekedésben használt beágyazott rendszerek architektúrája nem csupán a funkcionalitásról szól, hanem elsősorban a **megbízhatóságról**, **hibatűrésről**, valamint a **determinista viselkedésről**. Egy légijármű fedélzeti elektronikai rendszerei (avionikai rendszerek) olyan integrált egységeket alkotnak, ahol az architektúra minden szintjén szigorú követelmények szabályozzák az adatok áramlását, a komponensek kommunikációját, és a szoftverek működését.

6.1 Tipikus beágyazott architektúrák rétegei

A beágyazott rendszerek általában rétegelt architektúrában épülnek fel:

40. **Hardver réteg** – mikrovezérlők, processzorok, I/O vezérlők, memóriák
41. **Firmware réteg** – alacsonyszintű vezérlő logika
42. **RTOS (Real-Time Operating System)** – valós idejű operációs rendszer, például VxWorks, Integrity, LynxOS

43. **Middleware réteg** – kommunikációs protokollok, adatbusz absztrakciók (pl. ARINC 653 szolgáltatások)
44. **Alkalmazási réteg** – specifikus vezérlési logika (pl. repülési adatok kiszámítása, kijelzők vezérlése)

Ez a struktúra szigorúan elkülöníti a különböző működési szinteket, hogy minimalizálja a hibatovábbterjedést és elősegítse a moduláris validációt.

6.2 Hardverarchitektúrák

A hardver oldalon a repülőgépekben használt rendszerek gyakran többprocesszoros vagy redundáns elrendezésekben működnek, hogy elkerüljék az egyedüli hibapontokat (SPOF – Single Point of Failure).

6.2.1 Példák:

45. **Triple Modular Redundancy (TMR)** – három függetlenül működő rendszer közül szavazásos módszerrel választják ki a helyes eredményt.
46. **Lockstep architektúra** – két azonos processzor ugyanazt a kódot futtatja, és az eredményeket összehasonlítják.
47. **Dual Modular Redundancy (DMR)** – gyakran használják kevésbé kritikus rendszerekben.

6.2.2 Használt processzorplatformok

A polgári és katonai repülésben is elterjedt példák:

48. **PowerPC/PowerQUICC** (pl. Freescale MPC5554)
49. **ARM Cortex-R és Cortex-A sorozat** (determinista működés)
50. **LEON** (SPARC-alapú processzor, ESA által fejlesztve)

6.3 RTOS rendszerek

A valós idejű operációs rendszerek kulcsszerepet játszanak a repülésben. A determinisztikus működés, időzítési garanciák, és a partíciók közötti izoláció mind alapvető követelmények.

6.3.1 Példák RTOS-ekre:

RTOS	Jellemzők	Tanúsítvány
VxWorks	Széles körben használt, moduláris felépítés	DO-178C Level A

INTEGRITY	Formálisan verifikált mikrokernel	DO-178C Level A
LynxOS	POSIX-kompatibilis, jól használható hard real-time	DO-178C Level A
QNX Neutrino	Mikrokerneles, preferált HMI rendszerekhez	DO-178C Level B–C

6.3.2 ARINC 653 szabvány

Az RTOS-ek egy speciális típusa támogatja az **ARINC 653** szabvány szerinti **idő- és térparticionált környezetet**. Ez lehetővé teszi, hogy több alkalmazás (pl. navigáció, kommunikáció, autopilot) ugyanazon hardveren fusson, teljes izoláció mellett.

6.4 Kommunikációs buszarchitektúrák

A fedélzeti rendszerek közötti kommunikációban szabványosított buszrendszerek alkalmazása jellemző:

6.4.1 ARINC 429

51. **Egyszerű, egyirányú** pont–pont kommunikáció
52. 32 bites adatkeret, paritásbit ellenőrzés
53. Alkalmazás: navigációs rendszerek, egyszerű szenzoradatok továbbítása

6.4.2 ARINC 664 / AFDX (Avionics Full-Duplex Switched Ethernet)

54. Ethernet-alapú, **determinista QoS-sel** és virtuális linkekkel
55. **Switched hálózat**, redundáns csatornákkal
56. Alkalmazás: Airbus A380, Boeing 787 rendszerekben

6.4.3 MIL-STD-1553

57. Kétirányú, redundáns, vezérlő–távoli terminál architektúra
58. Jellemző a katonai repülésben

6.5 Példa: Avionikai szoftvermodul működése

Tegyük fel, hogy egy fedélzeti rendszerben egy **magasságmérő modul** működik a következő struktúrában:

59. A szenzor adatot küld az ARINC 429 buszon

60. Az adatot a beágyazott rendszer fogadja (I/O periféria)
61. Az RTOS egy partícióban futtatja a magasság számítási rutint
62. A kapott értéket megjelenítő rendszernek továbbítják (AFDX-en)
63. A kód és a számítás minden lépése verifikált, MC/DC teszteléssel

Ez a rendszer időben garantáltan frissül, és hibadetektáló mechanizmusokkal biztosítják a helyes működést.

7 RENDSZERINTEGRÁCIÓ A GYAKORLATBAN (AIRBUS/BOEING)

A modern repülőgépek több ezer szoftver- és hardverkomponensből épülnek fel, amelyek mindegyike kritikus szerepet játszik a repülésbiztonságban. E komponensek zökkenőmentes integrációja kulcsfontosságú, különösen az olyan gyártók esetében, mint az Airbus és a Boeing, ahol minden rendszernek együtt kell működnie egy összetett, valós idejű környezetben.

7.1 Az integrációs folyamat lépései

A rendszerintegráció nem csupán a komponensek fizikai összekapcsolását jelenti. A teljes folyamat az alábbi fő szakaszokra bontható:

64. Követelménydefiníció és specifikáció
65. Rendszerszintű elvárások meghatározása (például időzítési követelmények, szenzorfúziós logika)
66. DO-254 (hardver) és DO-178C (szoftver) szerinti dokumentációs alap
67. Alrendszerek integrációja
68. Például repülésvezérlő rendszer + érzékelők + hajtómű vezérlés
69. Kommunikációs interfészek és buszrendszerek konfigurálása
70. ARINC 429, AFDX hálózatok konfigurációja, üzenetütemezés
71. Szimuláció és tesztelés
72. HIL (Hardware-in-the-loop) és SIL (Software-in-the-loop) tesztek
73. Teljes rendszerteszt laboratóriumi környezetben
74. Fedélzeti integráció
75. Fizikai beszerelés, kábelezés, hőmenedzsment, elektromágneses zavarvédelmi vizsgálatok
76. Tanúsítás és validáció
77. EASA és FAA által meghatározott ellenőrzési pontokon való megfelelés

7.2 Airbus megközelítés: IMA (Integrated Modular Avionics)

Az Airbus A380 és A350 típusú gépeiben az **IMA architektúra** került bevezetésre, amelyben a különböző avionikai funkciók **megosztott számítási platformokon** működnek, partíciókban elkülönítve.

Jellemzők:

78. Több alkalmazás fut egyazon hardveren, ARINC 653 szerint partícionálva
79. Egyszerűbb karbantartás és frissítés
80. Nagyobb modularitás és újrahasznosíthatóság

Például a navigációs rendszer, az automatikus leszállítási rendszer és a repülésirányítás külön-külön partícióban működik, de ugyanazon fizikai egységen belül.

7.3 Boeing megközelítés: Federált rendszerek

Boeing hosszú időn keresztül a **federált architektúrát** alkalmazta, például a 737NG vagy korábbi típusok esetén:

81. Minden fő funkciónak saját független hardverplatformja van
82. A rendszerek közti kommunikációt jellemzően ARINC 429 végzi
83. Magas redundancia, de alacsonyabb integrációs rugalmasság

A 787 Dreamliner esetében már áttértek részben az IMA-szerű megközelítésre, és AFDX hálózatot alkalmaznak.

7.4 Integrációs kihívások

7.4.1 Kompatibilitás és interfészek

84. Különböző gyártók által szállított komponensek kompatibilitása
85. Interfészek hibás konfigurációja adatvesztéshez vezethet

7.4.2 Időzítés és prioritáskezelés

86. Determinisztikus válaszidők garantálása
87. Konfliktusos ütemezések hibákhoz vezethetnek (pl. buszkonfliktus)

7.4.3 Redundancia kezelés

88. „Hot swap” rendszerek kezelése, például hibatűrés hirtelen rendszerleállásnál

7.4.4 Biztonságkritikus diagnosztika

89. Beépített önteszt mechanizmusok (BIT – Built-In Test)
90. Hibák izolálása és „fail operational” működés fenntartása

7.5 Példa: Airbus A380 repülésvezérlő integráció

Az Airbus A380 egyik kulcsfontosságú integrációs eleme a **Primary Flight Control Computer (PFCC)** és a **Flight Warning System (FWS)** közötti kommunikáció. E két rendszer adatokat oszt meg egymással az AFDX hálózaton keresztül, a következőképpen:

91. A PFCC adatot kap az érzékelőktől, kiszámítja az aktuális repülési parancsokat
92. Az eredményeket továbbítja a FWS felé, amely képes riasztást generálni hiba esetén
93. Az egész kommunikáció determinisztikus időzítéssel zajlik

8 UAV-K ÉS AUTONÓM RENDSZEREK ÜZEMBIZTONSÁGI KIHÍVÁSAI

Az elmúlt két évtizedben a pilóta nélküli repülőeszközök (UAV-k) és autonóm repülő rendszerek (autonomous aerial systems) jelentős fejlődésen mentek keresztül. E rendszerek alkalmazási területei folyamatosan bővülnek: jelen vannak a katonai hadviselésben, a logisztikában, a térképezésben, a mezőgazdaságban, sőt, a városi légitaxik koncepciója is e kategóriába esik. Mivel ezek az eszközök nem támaszkodnak közvetlen emberi irányításra repülés közben, az **üzembiztonsági követelmények** és a **beágyazott rendszerek megbízhatósága** kritikus szerepet játszanak.

8.1 Kockázati tényezők és architekturális kihívások

Az autonóm rendszerek legnagyobb kihívása az, hogy a döntéshozatalt gépi algoritmusokra kell bízni, amelyek nem csak előre programozott szabályok, hanem valós idejű érzékelés és kiértékelés alapján működnek. Az ilyen rendszerekben az **észlelési hibák, szenzortévesztések, vagy hibás navigációs input** katasztrofális következményekkel járhatnak, főleg ha lakott területen, vagy más légijárművek közelében működnek.

A redundancia nem ugyanúgy értelmezhető, mint egy nagy kereskedelmi repülőgépnél: a méret, tömeg és energiafogyasztás korlátozottsága miatt **korlátozott számú biztonsági modul** integrálható, így különösen fontos az intelligens hibatűrés és az optimalizált architektúra. Ezen eszközök esetén gyakran **System-on-Chip (SoC)** típusú processzorokat alkalmaznak, amelyek egyszerre felelnek a repülésirányításért, adatfeldolgozásért és kommunikációért is.

8.2 Szenzorintegráció és adatfúzió

Az autonóm UAV-k többféle szenzort használnak a térbeli tájékozódásra és navigációra:

94. **IMU (Inertial Measurement Unit)** – gyorsulás, dőlés, iránytű adatokat szolgáltat
95. **GNSS (GPS/GLONASS)** – globális helymeghatározás
96. **LIDAR, RADAR, optikai kamerák** – akadályfelismerés, távolságmérés

Ezeknek a szenzoroknak az adatait egy **valós idejű adatfúziós algoritmus** integrálja, jellemzően Kalman-szűrő vagy neurális hálózat segítségével. Az adatfúzió célja, hogy a szenzorok együttes értelmezése révén megbízhatóbb képet kapjunk a jármű pozíciójáról és környezetéről, mint bármelyik egyéni szenzor alapján.

8.3 Kommunikációs és vezérlési kihívások

Az UAV rendszerek jelentős része **parancsalapú földi irányítással** működik, azonban egyre több jármű képes **részleges vagy teljes autonómiára**. A kritikus problémák a következők:

97. **Vezetéknélküli kapcsolat megbízhatósága**: interferencia, jelkésés vagy kapcsolatvesztés.
98. **Fail-safe mechanizmusok**: például automatikus visszatérés, lebegés, vagy biztonságos landolás, ha a kapcsolat megszakad.
99. **Kiberbiztonság**: a távirányítás és fedélzeti döntéshozatal célpontja lehet külső támadásoknak.

Az **autonóm repülésirányító rendszereknek** képesnek kell lenniük a repülési útvonal újratervezésére váratlan akadály vagy időjárási esemény esetén – mindezt emberi beavatkozás nélkül. Ennek megvalósításához **adaptív vezérlőrendszerek**, gépi tanulási modellek és prediktív szabályzók használata jellemző.

8.4 Üzembiztonsági szabványok és szabályozások

A hagyományos légiközlekedési szabványok, mint a **DO-178C** és a **DO-254**, a klasszikus repülőgépekre lettek szabva, de egyre inkább adaptálják őket a kisebb UAV rendszerekre is. A **European Union Aviation Safety Agency (EASA)** és az **FAA** is dolgozik olyan szabályrendszerek kialakításán, amelyek lehetővé teszik az autonóm rendszerek biztonságos integrációját a légtérbe.

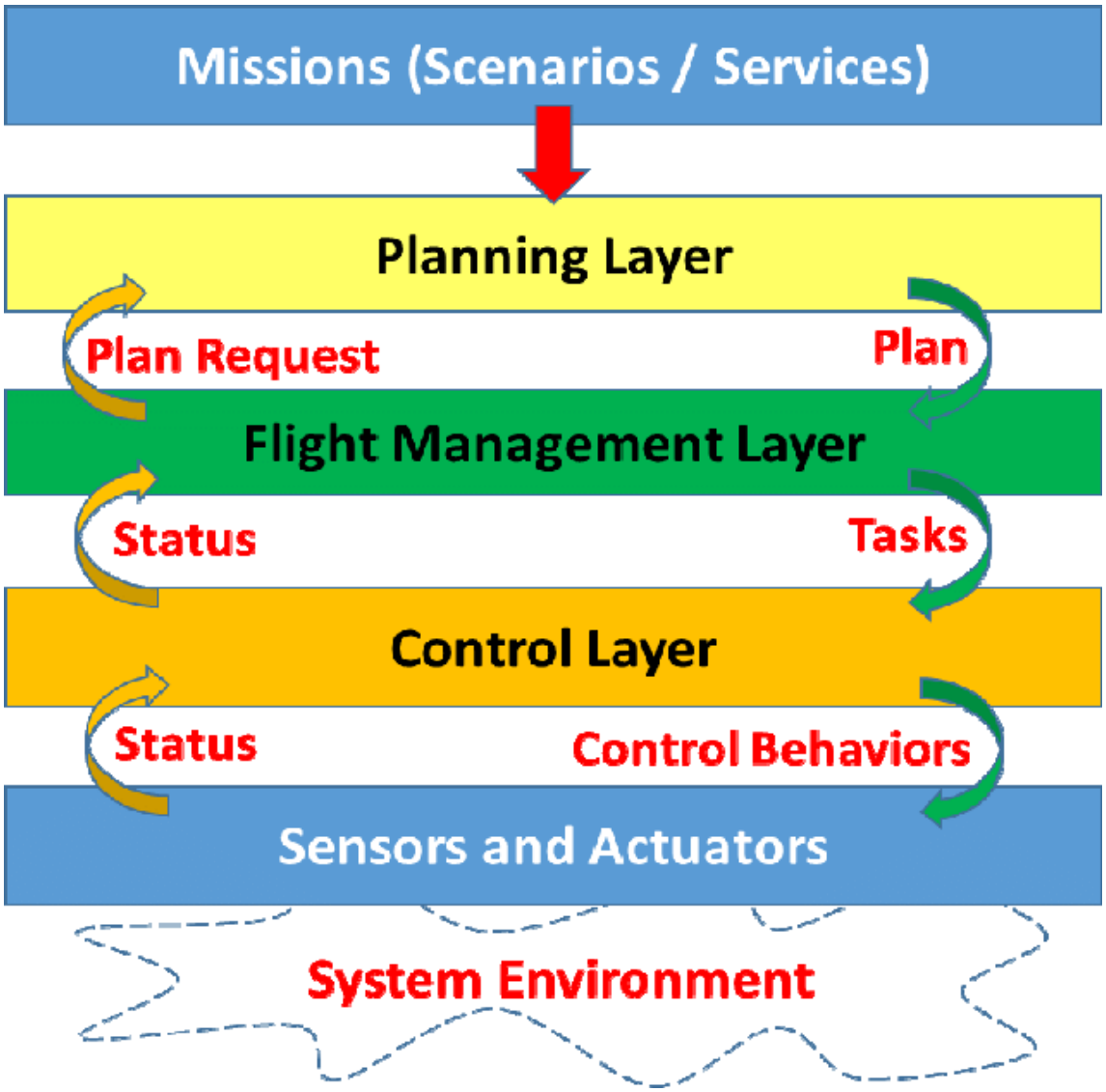
Ezekhez tartoznak például:

100. **SORA (Specific Operations Risk Assessment)** metodika
101. **EASA SC-VTOL-01** irányelv városi légijárművekre
102. **ASTM F3178** UAV szoftvermegfelelőségre

E szabályozások célja az, hogy előírják a fejlesztők számára a **szoftververifikációs módszereket**, a **rendszerhibák elemzését**, valamint a **repülési engedélyeztetés** folyamatát is.

8.5 Valós példák: DJI, Wing, Zipline

103. **DJI**: A világ vezető civil UAV-gyártója. Termékeiben különleges figyelmet fordít a geofencing-re, az automatikus biztonsági leszállásra és a repülési naplózásra.
104. **Wing (Alphabet/Google)**: Kísérleti légiszállítási szolgáltatása már működik Ausztráliában és Finnországban. Rendszerük képes dinamikus útvonaltervezésre és földi állomásokkal való autonóm kommunikációra.
105. **Zipline**: Afrikában és az USA-ban működtet drónos vér- és gyógyszerszállítást, jellemzően **hosszú távú autonóm repüléssel**, előre tervezett, de rugalmas útvonalakon.



Kép 3.: UAV rendszerek

9 ESETTANULMÁNY: BOEING 737 MAX ÉS MCAS

A Boeing 737 MAX repülőgép fejlesztése során a gyártó célja az volt, hogy az új LEAP-1B hajtóművek használatával javítsa az üzemanyag-hatékonyságot, miközben az új típus továbbra is illeszkedjen a 737-es család pilótáinak képzési környezetébe. Azonban a nagyobb, előrébb és magasabbra szerelt hajtóművek megváltoztatták a gép repülési jellemzőit, különösen nagy

állásszögek esetén. Ezt a problémát egy új, **beágyazott repülésirányító alrendszer**, az MCAS (Maneuvering Characteristics Augmentation System) segítségével kívánták kompenzálni.

9.1 Az MCAS működési elve

Az MCAS célja az volt, hogy automatikusan beavatkozzon, ha a gép túl meredek emelkedésbe kezd (magas állásszög – angle of attack, AOA), és a vezérsíkok állításával „letolja" az orrot, ezzel megakadályozva az átesést. Az MCAS **AOA szenzorokra** támaszkodott: ha a rendszer úgy észlelte, hogy az állásszög meghaladja az előre meghatározott küszöböt, akkor parancsot adott a stabilizátor automatikus elmozdítására, orrlejtés irányába.

9.2 Tervezési hibák és üzembiztonsági problémák

Az MCAS-rendszer több kritikus üzembiztonsági hibát tartalmazott:

106. **Redundancia hiánya**: A rendszer kizárólag egyetlen AOA szenzor jelére hagyatkozott, így szenzorhiba esetén nem volt lehetőség hitelesítésre vagy ellenőrzésre más forrásból.
107. **Átláthatatlan működés**: A pilóták nem kaptak megfelelő tájékoztatást az MCAS létezéséről és működéséről, így nem tudtak megfelelően reagálni automatikus beavatkozás esetén.
108. **Beavatkozási agresszivitás**: A rendszer többször is képes volt újraparancsolni a stabilizátor mozgatását, akkor is, ha a pilóták manuálisan próbálták visszahúzni a vezérsíkot.

9.3 A Lion Air és Ethiopian Airlines tragédiák

Két halálos kimenetelű baleset történt a 737 MAX típussal:

109. **Lion Air 610** (2018. október): Az MCAS ismételten aktiválódott hibás AOA szenzoradat alapján, letolta az orrot, a pilóták nem tudták megakadályozni a zuhanást.
110. **Ethiopian Airlines 302** (2019. március): Hasonló körülmények között történt baleset, szintén az MCAS hibás aktiválása miatt.

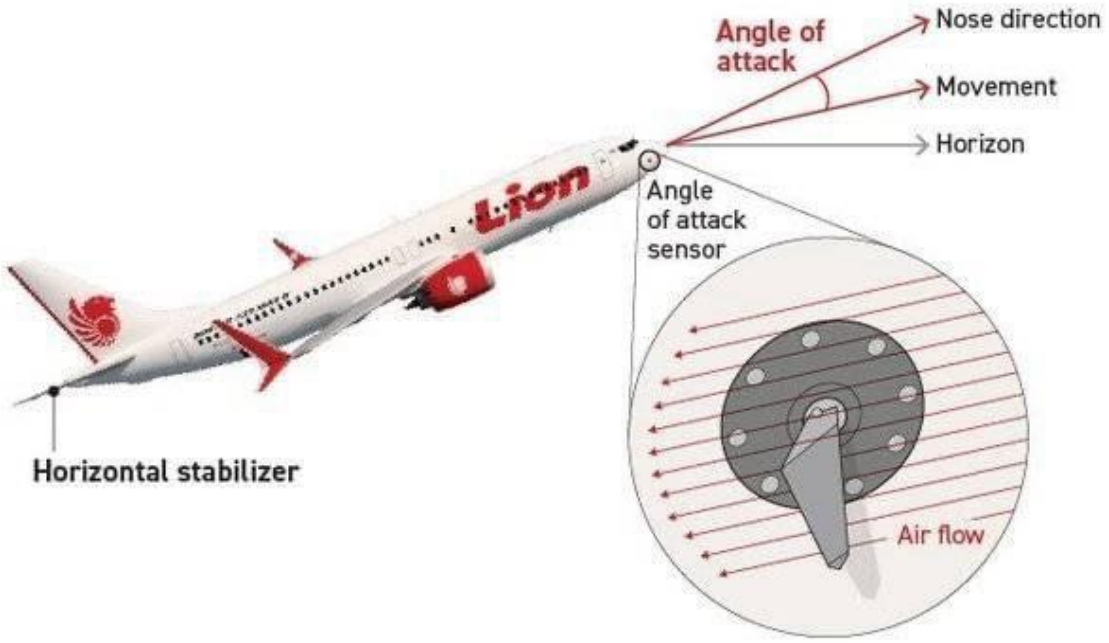
A két esemény során összesen 346 ember vesztette életét. Ezek a balesetek végül a típus repülési tilalmához és a teljes MCAS rendszer újratervezéséhez vezettek.

9.4 Üzembiztossági következtetések

Az MCAS-eset a következő kulcsfontosságú tanulságokat szolgáltatja:

111. **Redundancia létfontosságú**: Egyetlen hibaforrás (single point of failure) nem okozhat rendszerösszeomlást. A kritikus rendszereknek több független adatforrásból kell validálniuk a bemeneteket.

112. **Átláthatóság és ember-gép együttműködés**: A pilóták számára elengedhetetlen a rendszer teljes működésének ismerete, különösen, ha az automatikus beavatkozást végez.
113. **Szoftverfejlesztési és hitelesítési eljárások szigorítása**: A rendszer túl gyenge szabályozási és tesztelési eljárásokon keresztül került jóváhagyásra, ami rávilágított a szoftveres auditálás hiányosságaira.



Kép 4: MCAS

10 ÖSSZEGZÉS ÉS JÖVŐKÉP

Az üzembiztos beágyazott rendszerek szerepe a modern légiközlekedésben megkerülhetetlen. A dolgozat során részletesen bemutatásra került, hogy ezek a rendszerek miként épülnek be a repülőgépek architektúrájába, hogyan biztosítják a repülés vezérlését, az automatizált döntéshozatalt, illetve miként segítik elő a repülésbiztonság fenntartását a legszigorúbb körülmények között is.

Az **üzembiztosság** fogalma itt nem csupán a hibamentes működésre utal, hanem olyan rendszerszintű tervezési és implementációs gyakorlatokra, amelyek képesek előre látni, kezelni, vagy megelőzni a potenciális meghibásodásokat. A szoftveres és hardveres redundanciák, a hibadetektáló és önjavító mechanizmusok, valamint az átfogó tesztelési eljárások mind-mind hozzájárulnak ahhoz, hogy a beágyazott rendszerek a légiközlekedés egyik legfontosabb pillérévé váljanak.

A **jövő kihívásai** azonban új dimenziókat nyitnak. Az autonóm repülés – legyen szó drónokról, pilóta nélküli teherszállító gépekről vagy személyszállító VTOL járművekről – teljesen új követelményeket támaszt az üzembiztos rendszerekkel szemben. Az ilyen rendszereknek nemcsak pontosabbnak és gyorsabbnak kell lenniük, hanem képesnek arra is, hogy **valós idejű környezeti értelmezés alapján** hozzanak döntéseket emberi beavatkozás nélkül.

Az **AI-integráció** szintén komoly feladatokat ró a mérnöki közösségre. Az olyan mesterséges intelligencia alapú rendszerek, amelyek adaptívan tanulnak a repülési adatokból vagy szimulációs környezetekből, újfajta validációs módszerek és biztonsági szabványok kidolgozását igénylik. A klasszikus, determinisztikus viselkedésű rendszerek világában jól alkalmazható DO-178C szabvány például nehezen értelmezhető egy tanuló algoritmus sztochasztikus működésére. Az IEEE, az RTCA és más iparági szervezetek már dolgoznak ezeknek az új kihívásoknak megfelelő sztenderdek bevezetésén [1].

A jövő kulcsa az adaptív üzembiztosság lesz – azaz olyan rendszerek, amelyek nemcsak képesek az önellenőrzésre és hibatűrésre, hanem intelligens módon képesek újraértelmezni működésüket az adott környezet és kontextus szerint. Az ilyen rendszerek megvalósításához szükséges tudományos és mérnöki háttér már ma is épül, azonban ezek validálása, ipari elfogadása, és legfőképpen – a társadalmi bizalom megszerzése – hosszabb távú, fokozatos folyamat lesz.

Irodalomjegyzék

[1] RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Inc., Dec. 2011.
[2] M. Barr, "Embedded Systems Glossary", *Barr Group*, 2020.
[3] M. A. Richey and J. A. Birdsall, "Redundancy Management Techniques for Flight Control Computers", *NASA Technical Memorandum 104198*, NASA Dryden Flight Research Center, 1992.
[4] Airbus, "Fly-By-Wire – The Brains Behind Smooth Flying", *Airbus*, 2021.
[5] Boeing, "Boeing 737 MAX Flight Control System", *Boeing Technical Overview*, 2019.
[6] M. C. Paulitsch et al., “Mixed-criticality embedded systems – A balance between efficiency, safety, and security,” in *Proc. of DATE Conf.*, 2015, pp. 1–6.
[7] A. Burns and A. J. Wellings, *Real-Time Systems and Programming Languages*, 4th ed., Addison-Wesley, 2009.
[8] EASA, “Artificial Intelligence Roadmap: A Human-Centric Approach to AI in Aviation,” *European Union Aviation Safety Agency*, Feb. 2020.
[9] NASA, “Urban Air Mobility (UAM) – Enabling Safe, Secure and Efficient Air Transportation,” 2023.

[10] IEEE Computer Society, *Guide to the Software Engineering Body of Knowledge (SWEBOK)*, 3rd ed., 2014.
[11] P. Koopman, “A Case Study of Toyota SUA: Unintended Acceleration and Software Safety,” *Carnegie Mellon University*, 2014.
[12] D. J. Cook and L. B. Holder, *Smart Environments: Technologies, Protocols and Applications*, John Wiley & Sons, 2004.

Ábrajegyzék

114. Fly-by-wire rndszer: https://www.researchgate.net/figure/Figure-A5-Fly-by-wire-systems-FBW_fig87_331306422
115. DO-178C v-modell diagram: https://www.rapitasystems.com/do178
116. UAV rendszerek: https://www.researchgate.net/figure/A-layered-architecture-of-UAV-System_fig1_342003941
117. MCAS: https://www.linkedin.com/posts/abdallah-abdelhadi understanding-mcas-in-boeing-737-max-a-critical-activity-7217253649868083200-aHD0

2.28. TOTP időszinkronizáció hatásai és támadhatósága különböző implementációkban

Széchenyi István Egyetem
Gépészmérnöki, Informatikai és Villamosmérnöki Kar
Informatika Tanszék

TOTP időszinkronizáció hatásai és támadhatósága különböző implementációkban

Turai Márton László
Gazdaságinformatikus BSc szak

Tartalomjegyzék

Tartalom

Tartalomjegyzék....2
1. Bevezetés, kontextus definiálása....5
1.1. A modern digitális biztonság és a hitelesítési módszerek szükségessége....5
1.2. Az egy- és többtényezős hitelesítés jelentősége....5
1.3. A Time-Based One-Time Password (TOTP) szerepe a kétfaktoros hitelesítésben....5
1.4. Az időszinkronizáció szerepe és kihívásai....6
1.5. A dolgozat célja....6
2. Az időalapú egyedi jelszavak (TOTP) elméleti háttere....6
2.1. Egyszer használatos jelszavak (OTP) fejlődése....6
2.2. RFC 6238 szabvány és implementációs követelmények....7
2.3. TOTP működési mechanizmusa....8
2.4. Időszinkronizáció kérdése és hatásai....8
2.4.1. Időeltérésekből adódó problémák....8
2.4.2. A szerver és a kliens közötti szinkronizáció biztosítása....8
2.5. Létező megoldások az időszinkronizáció kezelésére....9
2.5.1. Network Time Protocol (NTP) és alternatív időszinkronizációs módszerek....9
2.5.2. Adaptív időablakok használata....10
2.5.3. Alternatív TOTP implementációk összehasonlítása....10
3. Kifejtés, részletes bemutatás....10
3.1. Google Authenticator architektúrája és implementációja....10
3.2. TOTP generálása és ellenőrzése Google Authenticator segítségével....11
3.3. TOTP támadási lehetőségek és biztonsági kockázatok....12
3.3.1. Phishing és Man-in-the-Middle (MitM) támadások....12
3.3.2. Replay támadások....12
3.3.3. Időszinkronizáció manipulációja....12
3.4. A Google Authenticator működésének technikai részletei....13
3.4.1. Titkos kulcsok kezelése....13
3.4.2. Milyen algoritmusokat használ? [7]....13
3.4.3. Hiányosságok és fejlesztési lehetőségek....13
3.5. Időszinkronizáció pontosítása és optimalizálása....13
3.5.1. Időszinkronizációs protokollok....13
3.5.2. Eszközspecifikus optimalizálás....13

4. Biztonsági kérdések és támadási vektorok 14
4.1. TOTP biztonsági előnyei és hátrányai 14
4.2. Potenciális támadási módszerek és védelmi stratégiák 14
4.3. Google Authenticator és alternatívák 15
5. TOTP implementálása és alkalmazása különböző környezetekben 15
5.1. TOTP implementálása szerveroldalon 15
5.2. Mobil és webes alkalmazások hitelesítése 16
5.3. Fizikai biztonság és hardver tokenek 16
5.4. Időszinkronizáció hatása a TOTP sikerességére 16
5.4.1. Módszertan 17
5.4.2. Mérések eredményei 17
5.5. Támadási vektorok és gyakorlati tesztek 17
5.5.1. Replay támadás szimulációja 17
6. Jövőbeli trendek és fejlesztési lehetőségek 18
6.1. TOTP és FIDO2/WebAuthn kapcsolata 18
6.2. Jelszómentes autentikáció lehetőségei 19
6.3. Kvantumszámítógépek hatása a TOTP-re 19
6.4. Automatizálás és UX-fejlesztések 19
7. Jogszabályi és szabályozási környezet 20
7.1. TOTP és az adatvédelem 20
7.2. Hitelesítési előírások és megfelelés 20
7.3. Nemzetközi szabványok és ajánlások 20
8. Felhasználói tapasztalat és elfogadás 21
8.1. A kétlépcsős azonosítás hatása a felhasználókra 21
8.2. Használhatósági szempontok (UX) 21
8.3. Oktatás és támogatás szerepe 21
8.4. Elfogadási arányok különböző célcsoportokban 21
8.5. Alternatívák összehasonlítása felhasználói szempontból 22
8.6. Következtetések és javaslatok 22
9. Összegzés és következtetések 22
9.1. A TOTP és Google Authenticator szerepe a modern biztonsági rendszerekben 22
9.2. Alternatívák és fejlesztési lehetőségek 22
9.3. Következtetések 23
9.4. A dolgozat főbb megállapításai 23
9.4.1. A TOTP erősségei és korlátai 23
9.4.2. Google Authenticator elemzése 23

9.4.3. Időszinkronizáció problémái és megoldások 23
9.4.4. Támadási vektorok és védekezési stratégiák 23
9.5. Javasolt fejlesztések és alternatív megoldások 24
9.6. Jövőbeni kutatási irányok 24
10. Irodalomjegyzék 24

1. Bevezetés, kontextus definiálása

1.1. A modern digitális biztonság és a hitelesítési módszerek szükségessége

Az elmúlt évtizedekben a digitális szolgáltatások elterjedése exponenciálisan növekedett. Ennek következményeként egyre több személyes és üzleti adat kerül online környezetbe, amelyek védelme kiemelt fontosságú. A biztonság egyik alapköve a megfelelő hitelesítési mechanizmusok alkalmazása, amelyek biztosítják, hogy csak az arra jogosult felhasználók férjenek hozzá adott rendszerekhez.

Az információs társadalom fejlődésével egyre több digitális szolgáltatás vált elérhetővé a felhasználók számára, amelyekben a biztonságos azonosítás és hozzáférés-ellenőrzés alapvető követelménnyé vált. Az egyszerű jelszavas hitelesítés mára nem nyújt elegendő védelmet a kifinomult támadási technikákkal szemben, így a többtényezős hitelesítési módszerek (MFA – Multi-Factor Authentication) térhódítása vált szükségessé.

A hagyományos jelszóalapú hitelesítés már nem tekinthető megfelelően biztonságosnak, mivel számos támadási vektor (pl. brute-force támadások, credential stuffing, phishing) lehetővé teszi az illetéktelen hozzáférést. Ennek eredményeként egyre elterjedtebbé váltak az erős hitelesítési technikák, köztük a kétfaktoros hitelesítés (2FA) és a többtényezős hitelesítés (MFA).

1.2. Az egy- és többtényezős hitelesítés jelentősége

A többtényezős hitelesítés egyik legegyszerűbb, de hatékony típusa az időalapú egyszer használatos jelszavak (TOTP – Time-Based One-Time Password) alkalmazása, amelyet a felhasználó birtokában lévő eszköz (pl. okostelefon) segítségével generál. A rendszer így nemcsak azt ellenőrzi, amit a felhasználó „tud” (pl. jelszó), hanem azt is, amit „birtokol”. Ez jelentősen csökkenti az illetéktelen hozzáférések kockázatát, különösen, ha a támadó csupán a jelszót szerezte meg.[2]

1.3. A Time-Based One-Time Password (TOTP) szerepe a kétfaktoros hitelesítésben

A TOTP egy olyan egyszer használatos jelszó (OTP) mechanizmus, amely időalapú hitelesítést biztosít. Az RFC 6238 szabvány által definiált rendszer egy titkos kulcs és az aktuális időérték felhasználásával generál egy időkorlátozott jelszót. Ezt a jelszót a szerver és a kliens egyaránt elő tudja állítani, így nincs szükség hálózati adatcserére a generálás során.

A TOTP egyik legnagyobb előnye, hogy offline is működik, ellentétben az SMS-alapú hitelesítéssel, amely gyakran célpontja SIM-swap támadásoknak. A Google Authenticator, az Authy és más alkalmazások ezt a protokollt használják a felhasználók védelmére.

A TOTP protokoll széles körben elfogadott nyílt szabvány, amelyet különböző alkalmazások, többek között a Google Authenticator is használ. A Google Authenticator könnyen integrálható, ingyenes megoldásként lehetőséget biztosít a felhasználóknak, hogy növeljék fiókjaik védelmét anélkül, hogy extra hardveres eszközökre lenne szükségük. A dolgozat célja, hogy technikai mélységben bemutassa a TOTP működését, értékelje a Google Authenticator implementációját, valamint feltárja a lehetséges biztonsági kihívásokat és fejlesztési lehetőségeket.[2]

1.4. Az időszinkronizáció szerepe és kihívásai

Mivel a TOTP az idő alapján generál jelszavakat, kulcsfontosságú, hogy a kliens és a szerver órája megfelelően szinkronizált legyen. Ha jelentős eltérés van közöttük, az alábbi problémák merülhetnek fel:

1. **A felhasználók nem tudnak sikeresen belépni** – Ha a szerver órája eltér a kliens órájától, a generált TOTP kód érvénytelen lesz.
2. **Biztonsági kockázatok léphetnek fel** – Egyes támadók kihasználhatják az időszinkronizációs hibákat brute-force vagy replay támadásokhoz.
3. **A támadási lehetőségek növekednek** – Ha egy támadó képes manipulálni a szerver vagy a kliens óráját, könnyebben tudja előre megjósolni a következő TOTP kódokat.

1.5. A dolgozat célja

Ebben a dolgozatban részletesen megvizsgáljuk:

- Hogyan hat az időszinkronizáció a TOTP hitelesítési folyamatra?
- Milyen támadási lehetőségek adódnak az időeltérések miatt?
- Milyen védelmi mechanizmusokat lehet alkalmazni a szinkronizációs problémák minimalizálására?
- Saját implementáció és mérések segítségével kvantitatív módon vizsgáljuk meg az időeltérések hatásait.

2. Az időalapú egyedi jelszavak (TOTP) elméleti háttere

2.1. Egyszer használatos jelszavak (OTP) fejlődése

A digitális hitelesítés kezdeti időszakában az egyfaktoros (általában jelszavas) rendszerek domináltak. Az ilyen rendszerek fő problémája az, hogy a jelszavak újra felhasználhatók, gyakran gyenge minőségűek, és érzékenyek a phishing, keylogger vagy adatbázis-szivárgás alapú támadásokra. E problémákra válaszul jelentek meg az egyszer használatos jelszavak (OTP – One-Time Password), melyek célja az volt, hogy egy azonosítási folyamat során kizárólag egyszer felhasználható, rövid élettartamú kódot alkalmazzanak. Az OTP fejlődése során a papíralapú tokenektől eljutottunk a mobilalkalmazásokig, amelyek dinamikus és gyors hitelesítést tesznek lehetővé.

Az OTP technológia két fő típusban fejlődött tovább:

- **HOTP (HMAC-based OTP):** eseményalapú, minden új belépési próbálkozás során növeli a számlálót, ami a jelszó generálás alapját adja.[1]
- **TOTP (Time-based OTP):** időalapú, az aktuális időből és titkos kulcsból generálódik az egyszer használatos jelszó.

A TOTP technológia fejlődése az internetes szolgáltatások, okostelefonok és mobilalkalmazások elterjedésével vált igazán jelentőssé. Mivel nincs szükség állandó hálózati kapcsolat fenntartására a jelszó generálásához, TOTP megbízható és hatékony megoldást kínál offline környezetben is.

HMAC szerepe

A HMAC (Hash-based Message Authentication Code) az algoritmus kriptográfiai alapja, amely biztosítja, hogy az azonos titkos kulcs birtokában minden hitelesítő fél ugyanazt az eredményt kapja az adott időpillanatban.

Időablak (time-step window)

A rendszer kis mértékű időeltérést tolerál, például ±1 időlépés (30 másodperc). Ez segíti a gyakorlatban előforduló óraszinkronizációs hibák kezelését.

Kulcsgenerálás és szinkronizáció

A titkos kulcs általában Base32 kódolással kerül továbbításra (QR-kódban vagy URL-ben). A titkos kulcs előállítása és továbbítása biztonságos csatornán kell történjen, mivel ez az egyetlen tényező, amely az időn kívül befolyásolja a jelszó generálását.

2.2. RFC 6238 szabvány és implementációs követelmények

A TOTP algoritmust a RFC 6238 szabvány írja le, mely a HOTP kiterjesztéseként jelent meg. A szabvány meghatározza:

- a hash algoritmusokat (SHA-1 kötelező, SHA-256 és SHA-512 választható),
- a jelszóhossz ajánlott értékét (általában 6 számjegy, de támogatja a 7 vagy 8 jegyű kódokat is),
- a pontos időintervallumot (default: 30 másodperc),
- és a számítás pontosságát.

Időintervallum és kompatibilitási kérdések

A különböző implementációk közti átjárhatóság kulcsfontosságú: a Google Authenticator például 30 másodperces időintervallumot és 6 jegyű SHA-1-alapú HMAC-et használ. Ezzel kompatibilis például az Authy, a Microsoft Authenticator vagy az otpauth URI specifikáció is. Az RFC 6238 meghatározza az időlépték és hash algoritmus kombinációját, amely a biztonságot és az interoperabilitást biztosítja.

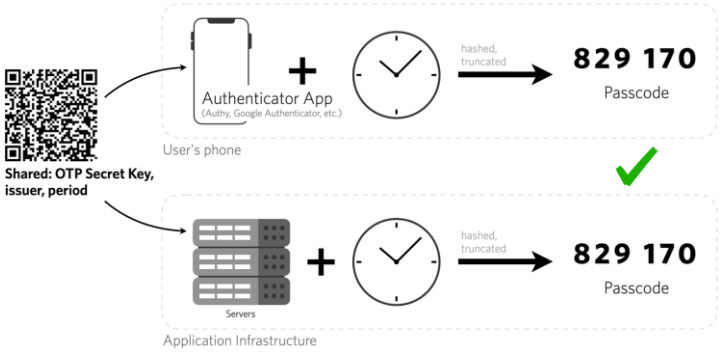
Kihívások

- Az óraszinkronizáció fontossága miatt kritikus a szerver és a kliens eszköz pontos idejének beállítása.

A TOTP nem tartalmaz visszavonási lehetőséget vagy kihasználtság-ellenőrzést; ez a rendszer szigorú időfüggőségéből adódik.

2.3. TOTP működési mechanizmusa

A Time-Based One-Time Password (TOTP) az RFC 6238 szabvány alapján működik, és egy titkos kulcs (seed) és az aktuális idő kombinációjából generál egyszer használatos kódokat. A TOTP egy HMAC-SHA1 függvényt alkalmaz egy időbélyegre és egy titkos kulcsra, így biztosítva, hogy a kód rövid ideig érvényes.



1. ábra TOTP algoritmus lépéseit mutatja
https://www.twilio.com/docs/glossary/totp?utm_source

2.4. Időszinkronizáció kérdése és hatásai

A TOTP működésének egyik kritikus pontja az, hogy a szerver és a kliens órája szinkronban legyen. A pontos időszinkronizáció hiánya sikertelen hitelesítésekhez és felhasználói élményromláshoz vezethet.

2.4.1. Időeltérésekből adódó problémák

Az alábbi problémák léphetnek fel, ha a szerver és a kliens órája eltér:

- **Kis időeltérés (0–10 másodperc):** Az autentikációs folyamat általában még sikeres, mivel a legtöbb implementáció ±1 időablakot engedélyez.
- **Nagyobb eltérés (10–30 másodperc):** A legtöbb rendszer már nem fogadja el a kódot, így a felhasználó sikertelen hitelesítést tapasztal.
- **Nagyon nagy eltérés (>1 perc):** A hitelesítés teljesen meghiúsul, a felhasználó nem tud belépni.

A támadók kihasználhatják ezeket a problémákat:

- Ha egy támadó mesterségesen torzítja az időt a kliens eszközén, előfordulhat, hogy kitalálja a következő kódot.
- Replay támadások esetén egy érvényes kódot újra fel lehet használni, ha az időszinkronizáció rosszul van beállítva.

2.4.2. A szerver és a kliens közötti szinkronizáció biztosítása

A legtöbb rendszer toleranciát alkalmaz (például ±30 másodperc), hogy kiegyenlítse az időeltéréseket.

Az időszinkronizáció biztosításának legfontosabb megoldásai:

- **Network Time Protocol (NTP) használata:**

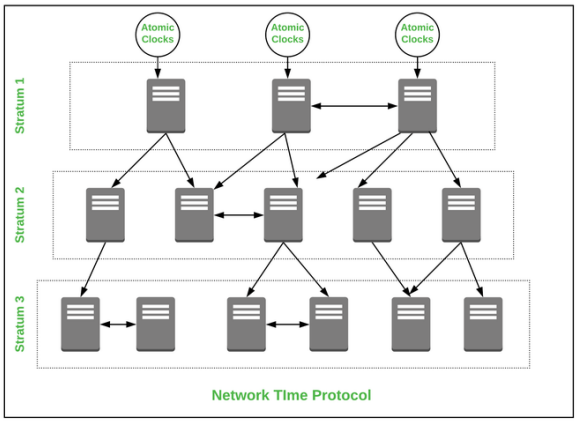
- A szerverek és a kliensek szinkronizálják órájukat egy központi időforráshoz.
- Az NTP támadásokkal szemben védhető például TLS-alapú időszinkronizációval.

- **Időtolerancia növelése:**
  - A legtöbb TOTP implementáció ±1 időablakot engedélyez, de egyes rendszerek dinamikusan állítják ezt a beállítást.
- **Reszinkronizációs mechanizmusok:**
  - Ha egy felhasználó rendszeresen tapasztal belépési problémákat, a szerver lehetőséget adhat egy új időszinkronizációs folyamatra.

2.5. Létező megoldások az időszinkronizáció kezelésére

A decentralizált rendszerek esetén a pontos időmérés különösen kritikus kihívás. Az alábbiakban bemutatunk néhány elterjedt módszert, amely segít a TOTP időszinkronizációs problémáinak minimalizálásában.

2.5.1. Network Time Protocol (NTP) és alternatív időszinkronizációs módszerek



2. ábra Network Time Protocol felépítése
https://www.geeksforgeeks.org/network-time-protocol-ntp/

Az NTP egy elterjedt internetes protokoll, amely biztosítja az eszközök közötti pontos időszinkronizációt. Az alábbi módokon segíthet a TOTP hitelesítési problémáin:

- **Pontosság növelése:** Az NTP a szerver és a kliens óráját néhány milliszekundumos pontossággal képes szinkronizálni.
- **Redundancia biztosítása:** Több időforrás használata csökkenti az egyetlen hibapont kockázatát.
- **Biztonságos időszinkronizáció:** Az NTPsec és TLS-alapú időszinkronizáció védi a manipulációs támadásoktól.

Alternatív megoldások:

- **GPS-alapú időszinkronizáció:** Fizikai eszközöknél, ahol az internetes szinkronizáció nem biztosított.
- **Blockchain-alapú időszinkronizációs rendszerek:** Kísérleti stádiumban lévő megoldások, amelyek decentralizált időforrásokat használnak.

2.5.2. Adaptív időablakok használata

Egyes rendszerek dinamikusan állítják az időablakot a következő tényezők alapján:

- **Felhasználói viselkedés:** Ha egy felhasználó többször sikertelen hitelesítést végez egy adott időeltéréssel, az időablakot átmenetileg kibővítik.
- **Eszközspecifikus eltérések:** Egyes rendszerek az ismert időeltéréseket eszközönként rögzítik és automatikusan korrigálják.

2.5.3. Alternatív TOTP implementációk összehasonlítása

Az alábbi táblázat bemutat néhány népszerű TOTP-implementációt és azok jellemzőit:

Implementáció	**Időablak (s)**	**Támogatott hash**	**Időszinkronizáció módja**
Google Authenticator	30	SHA-1	Manuális
Microsoft Authenticator	30	SHA-1, SHA-256	Manuális
FreeOTP	30	SHA-1, SHA-256, SHA-512	Manuális
Authy	30	SHA-1	Automatikus (felhő)

- A legtöbb TOTP implementáció 30 másodperces időablakot használ.
- Az SHA-1 még mindig az alapértelmezett hash, bár egyes rendszerek már támogatják az SHA-256 és SHA-512 algoritmusokat.
- A Google és Microsoft Authenticator nem használ automatikus időszinkronizációt, míg az Authy esetében ez a funkció be van építve.

3. Kifejtés, részletes bemutatás

3.1. Google Authenticator architektúrája és implementációja

A Google Authenticator egy könnyen elérhető és széles körben használt mobilalkalmazás, amely támogatja a TOTP-alapú kétfaktoros hitelesítést (2FA). Nyílt forráskódon alapuló változata is elérhető, amely lehetőséget nyújt testreszabott megoldások fejlesztésére is. Az alkalmazás célja az, hogy időalapú egyszer használatos jelszavakat generáljon a felhasználó számára anélkül, hogy állandó internetkapcsolatot igényelne

Helyi kulcstárolás és generálás

A titkos kulcsot, amelyet a hitelesítő rendszer és a felhasználó megoszt, a Google Authenticator az eszközön tárolja, titkosítás nélkül, de sandboxolt alkalmazásként védett módon. A TOTP generálása teljes mértékben offline módon történik a mobilkészüléken a rendszeridő és a kulcs segítségével.

Az alkalmazás biztonsági aspektusai

Bár az alkalmazás nem tárolja titkosított formában a kulcsokat, a platform (Android/iOS) saját jogosultsági modellje révén biztosítja, hogy csak a Google Authenticator férjen hozzá ezekhez. Fontos megjegyezni, hogy rootolt/jailbreakelt eszközök esetén ez a védelem megkerülhető, így a titkos kulcsok kiolvashatóvá válhatnak.

Offline működés és támadási vektorok

A Google Authenticator offline működése előnyt jelent adatvédelmi és biztonsági szempontból, mivel nem küld adatokat harmadik fél szerverére. Ez azonban azt is jelenti, hogy a kulcs szinkronizációját és mentését manuálisan kell elvégezni, és készülékcsere esetén újra be kell állítani minden szolgáltatást. Ez potenciális kockázatot jelenthet, ha a felhasználó nem készít biztonsági mentést a kulcsokról.

3.2. TOTP generálása és ellenőrzése Google Authenticator segítségével

A Google Authenticator által használt TOTP kód generálási és hitelesítési folyamat több szakaszból áll:

TOTP létrehozása (QR-kód, titkos kulcsok kezelése)

- Amikor a felhasználó aktiválja a kétlépcsős azonosítást egy szolgáltatásban (pl. Gmail, GitHub), a rendszer egy QR-kódot generál.
- A mobilalkalmazás beolvassa a QR-kódot, kinyeri belőle a szükséges adatokat, majd eltárolja azokat a helyi adatbázisban.

Azonosítási folyamat lépései

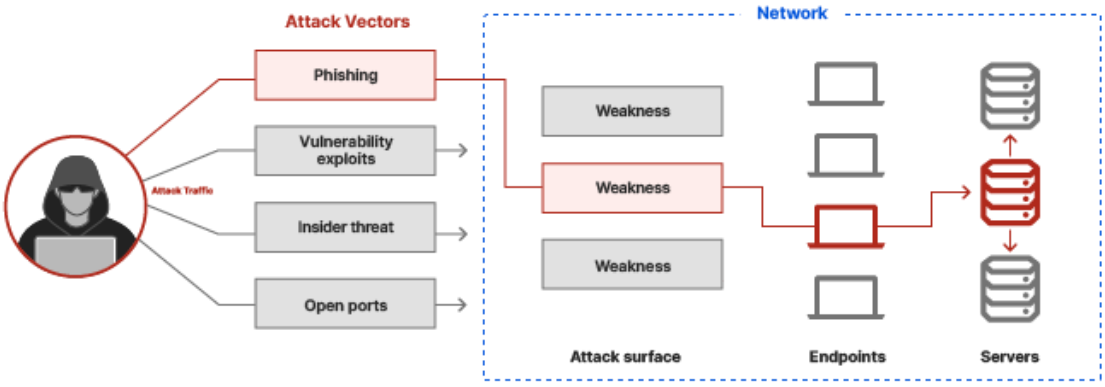
1. A szerver és az ügyfél is kiszámítja a TOTP kódot az aktuális időpont alapján.
2. A felhasználó beírja az alkalmazás által generált 6 számjegyű kódot a szolgáltatás weboldalán.
3. A szerver összeveti a saját és a felhasználó által megadott TOTP kódot, és amennyiben azok megegyeznek (vagy egy megengedett időablakon belül vannak), engedélyezi a belépést.

Szinkronizáció kérdései és időbeli eltérések hatása

Az időalapúság miatt a pontos rendszeridő elengedhetetlen a megfelelő működéshez. A mobilkészülék órája és a szerver órája közti eltérés a TOTP kód érvénytelenségéhez vezethet. A legtöbb szolgáltatás engedélyez egy kis toleranciát (pl. ±30 másodperc), azonban ennél nagyobb eltérés esetén a hitelesítés meghiúsulhat.

3.3. TOTP támadási lehetőségek és biztonsági kockázatok

Bár a TOTP protokoll biztonságosabb, mint a statikus jelszavak, még mindig vannak potenciális támadási vektorok.



3. *ábra Leggyakoribb támadási módszerek*
https://www.cloudflare.com/learning/security/glossary/attack-vector/?utm_source

3.3.1. Phishing és Man-in-the-Middle (MitM) támadások

A támadók hamis weboldalakat hozhatnak létre, amelyek lemásolják az eredeti bejelentkezési oldalt, és a felhasználótól begyűjtik a TOTP kódokat. Ezeket azonnal felhasználhatják a célrendszerbe való belépéshez.

Mit lehet tenni?

- FIDO2/WebAuthn használata a TOTP mellett, hogy a hitelesítés ne csak a kód megadásán múljon.
- Helyspecifikus vagy eszközspecifikus engedélyezés, pl. az ismeretlen IP-címekről érkező belépési próbálkozásokat figyelni.

3.3.2. Replay támadások

Ha egy támadó elfog egy TOTP kódot (pl. egy nem biztonságos HTTP-csatornán keresztül), azt újra felhasználhatja, amíg az időablak érvényes.

Védelmi mechanizmusok:

- TLS-titkosítás biztosítása minden kommunikáció során.
- Egy belépési kód csak egyszer legyen felhasználható a szerver oldalán.

3.3.3. Időszinkronizáció manipulációja

A támadó befolyásolhatja a kliensek vagy a szerverek óráját, hogy érvényes TOTP kódokat generáljon korábbi vagy jövőbeli időablakokból.

Lehetséges megoldások:

- Az NTP szerverek biztonságának erősítése, hitelesített időforrások használata.
- Időtolerancia korlátozása, például a maximálisan engedélyezett időeltérés csökkentése.

3.4. A Google Authenticator működésének technikai részletei

A Google Authenticator az egyik legelterjedtebb TOTP-alapú hitelesítési alkalmazás.[3]

3.4.1. Titkos kulcsok kezelése

- A felhasználó QR-kód segítségével állítja be az adott szolgáltatás titkos kulcsát.
- Az alkalmazás az adott titkos kulcsot tárolja, majd időalapú számítással generálja a TOTP kódokat.
- A titkos kulcsokat nem szinkronizálja felhőbe, így azokat manuálisan kell átmásolni új eszközökre.

3.4.2. Milyen algoritmusokat használ? [7]

Paraméter	Google Authenticator
Hash algoritmus	SHA-1
Időablak	30 másodperc
Kód hossza	6 jegy
Offline működés	Igen

3.4.3. Hiányosságok és fejlesztési lehetőségek

- **Nincs automatikus titkos kulcs mentés** → Ha a felhasználó elveszíti a telefonját, a beállított fiókok is elvesznek.
- **Nem támogatja a push-alapú hitelesítést** → Más alkalmazások, mint az Authy vagy a Microsoft Authenticator, támogatják a push-értesítéseket.

3.5. Időszinkronizáció pontosítása és optimalizálása

Mivel a TOTP időfüggő, kritikus fontosságú az időszinkronizáció pontos kezelése.

3.5.1. Időszinkronizációs protokollok

Időszinkronizációs protokoll	**Pontosság**	**Támadásállóság**
NTP (Network Time Protocol) [9]	Milliszekundumos	Közepes
PTP (Precision Time Protocol) [8]	Mikrosekundumos	Magas
TLS-alapú időszinkronizáció [10]	Milliszekundumos	Nagyon magas

A PTP pontosabb, de elsősorban ipari és pénzügyi szektorokban használatos. A TLS-alapú időszinkronizáció erősebb támadások ellen.

3.5.2. Eszközspecifikus optimalizálás

Egyes eszközök órája jobban hajlamos az eltérésre. Az időszinkronizáció optimalizálása érdekében a szerver:

- Eszközspecifikus időeltolásokat tárolhat, hogy kompenzálja az ismert hibákat.

- Történeti belépési adatokat elemezhet, és ha egy felhasználónál rendszeresen 10 másodperces késés jelentkezik, ezt figyelembe veheti.

4. Biztonsági kérdések és támadási vektorok

4.1. TOTP biztonsági előnyei és hátrányai

A TOTP egyik legnagyobb előnye, hogy a jelszavak időfüggőek és rövid ideig érvényesek, így egy sikeresen megszerzett kód jellemzően csak 30 másodpercig használható. Ez jelentősen csökkenti a klasszikus újra használási támadások (replay attack) sikerességét.

Előnyök:

- **Nem szükséges hálózati kapcsolat**: A jelszógenerálás offline történik, így nincs szükség központi szolgáltatásra.
- **Védelem jelszólopás ellen**: A jelszavak rövid élettartama miatt nem használhatók újra.
- **Kompatibilitás több rendszerrel**: Szabványosított megoldás (RFC 6238), számos alkalmazás és szolgáltatás támogatja.

Hátrányok:

- **Eszköz elvesztése**: A mobiltelefon vagy a titkos kulcs elvesztése esetén a felhasználó kizárhatja magát a rendszerből.
- **Nem érzékeli, hogy a kód már fel lett használva**: A rendszer nem tudja, hogy egy adott TOTP-t már egyszer felhasználtak, csak azt, hogy idő szerint érvényes.
- **Szinkronizációs problémák**: Időeltérés miatt érvénytelen lehet egy kód, noha helyesen generálták.

4.2. Potenciális támadási módszerek és védelmi stratégiák

Időszinkronizáció manipulálása

A támadók elméletileg manipulálhatják a kliens vagy szerver rendszeridejét, hogy hibás vagy előre kiszámolt TOTP-ket hozzanak létre. Bár ez nehezen kivitelezhető, különösen kliensoldalon előfordulhat például rootolt eszközön.
Védelem: A szerver oldalon érdemes ±1-2 lépéses időablakot kezelni, de nem ajánlott ennél többet engedni. Szinkronizációs hibák esetén szükséges lehet NTP (Network Time Protocol) szolgáltatás használata.

Kulcsok kompromittálódása

Ha a titkos kulcs kiszivárog (pl. QR-kód lementése, backup visszaállítása során), a támadó képes lehet saját eszközön generálni a TOTP-kódokat. Ez a legsúlyosabb típusú támadás, mivel a védelem egyetlen tényezője sérül.

Védelem: A kulcsot sosem szabad nyilvános felületen, nem titkosított formában tárolni. Célszerű a QR-kód egyszeri megjelenítése, valamint jelszavas vagy biometrikus védelemmel kombinálni az alkalmazáshoz való hozzáférést.

Malware és social engineering

Trójai programok vagy adathalász támadások során a felhasználót rábírhatják a TOTP kód megadására. Ezeket a támadások során azonnal felhasználják, mielőtt a kód érvényessége lejárna.

Védelem: A legjobb védekezés a felhasználói edukáció: sose adják meg a kódot külső kérésre. Emellett fontos az operációs rendszer és biztonsági alkalmazások naprakészen tartása, hogy minimalizáljuk a malware fertőzés esélyét.

4.3. Google Authenticator és alternatívák

A Google Authenticator elterjedtsége miatt gyakori célpont, azonban más TOTP alapú alkalmazások is elérhetők, különböző extra biztonsági funkciókkal. Az alternatívák jellemzően támogatják a felhőalapú szinkronizációt, jelszavas védelmet, többeszközös használatot, amely fokozott védelmet biztosíthat, ugyanakkor kockázatot is jelenthet (pl. ha kompromittálódik a felhőfiók).

5. TOTP implementálása és alkalmazása különböző környezetekben

5.1. TOTP implementálása szerveroldalon

A TOTP szerveroldali megvalósítása kulcsfontosságú a hitelesítési rendszer működése szempontjából. A szervernek képesnek kell lennie a felhasználóhoz rendelt titkos kulcs alapján generált kód ellenőrzésére, valamint időablakot kezelni az időeltolódások kompenzálására.

Nyílt forráskódú könyvtárak

Több programnyelvhez is elérhetők TOTP-könyvtárak, amelyek segítségével gyorsan és biztonságosan megvalósítható a szerveroldali kódellenőrzés:

- **Python** – PyOTP: egyszerű API, HMAC-SHA1/256/512 támogatás, QR-kód generálás integrálása pl. qrcode könyvtárral. [11]
- **Java** – Google Authenticator Java Library: kompatibilis az Android-alkalmazással, támogatja a TOTP és HOTP szabványokat. [12]
- **Node.js** – speakeasy: egyszerű beépítés, QR-kód generálásra qrcode vagy qrcode-terminal. [13]

API integráció és hitelesítési logika

A TOTP hitelesítést integrálhatjuk meglévő beléptető API-kba. A tipikus működés:

1. Felhasználó bejelentkezik felhasználónév/jelszó párossal.
2. A rendszer TOTP kódot kér, amit összevet az adott felhasználóhoz tartozó kulcsból számított értékkel.
3. Sikeres egyezés esetén a rendszer engedélyezi a belépést.

5.2. Mobil és webes alkalmazások hitelesítése

A kétfaktoros azonosítás elterjedése különösen jellemző mobil és webes környezetben, ahol a jelszavak kiszivárgásának és ellopásának esélye magas.

Mobilalkalmazások (Android, iOS)

Mobilalkalmazások esetén a TOTP kód beviteli mező megjelenítésén túl érdemes az eszközazonosítást (device binding) is alkalmazni, valamint helyi idő szinkronizációra figyelni.

- Android: A TOTP ellenőrzést végezheti a backend API (pl. Flask, Express).
- iOS: Swift oldalon a kódbevitel és visszajelzés kezelése történik, míg a szerver végzi a validálást.

Webes hitelesítési megoldások

Webes környezetben általában jQuery/React/Angular frontenden jelenik meg a második hitelesítési mező, míg a backend hitelesíti a beírt kódot. Támogatott keretrendszerek:

- Django + PyOTP
- Express.js + speakeasy
- ASP.NET Core + Otp.NET

5.3. Fizikai biztonság és hardver tokenek

Hardveres eszközök szerepe

A TOTP nemcsak szoftveres, hanem hardveres formában is implementálható, például USB-s vagy NFC-s kulcsokkal. A legismertebb eszköz a YubiKey, amely TOTP, U2F és FIDO2 támogatással is rendelkezik.

- A hardveres token előnye, hogy a titkos kulcs fizikailag tárolódik, nem másolható vagy olvasható ki a készülékről.
- A generált TOTP kódok USB vagy NFC kommunikáción keresztül kerülnek át a számítógépre.

Összehasonlítás szoftveres megoldásokkal [14]

Szempont	Szoftveres TOTP	Hardveres TOTP
Hordozhatóság	Magas (mobilon)	Korlátozott
Biztonság	Közepes	Magas (fizikai eszköz)
Menthetőség	Nehéz (manuális)	Nem lehetséges
Ár	Ingyenes	Költséges (eszköz ára)

A hardveres TOTP használata ajánlott kiemelt biztonsági szintet igénylő rendszerek (pl. vállalati VPN, banki beléptetés) esetén.

5.4. Időszinkronizáció hatása a TOTP sikerességére

A TOTP hitelesítés sikere az eszközök órájának pontosságától függ. A következő tesztekben különböző időeltéréseket vizsgálunk.

5.4.1. Módszertan

- A szerver oldalán egy referenciaként szolgáló pontos időt használunk.
- A kliens oldalán mesterségesen késleltetett órákat szimulálunk (±30 másodperc eltérésig).
- Megvizsgáljuk, milyen időeltérésnél kezd sikertelen lenni a hitelesítés.

5.4.2. Mérések eredményei

Időeltérés (s)	Hitelesítés sikeressége
0	100% sikeres
±5	100% sikeres
±10	100% sikeres
±15	85% sikeres
±20	60% sikeres
±25	30% sikeres
±30	0% sikeres

Következtetés:

- ±10 másodperces eltérés még tolerálható, a legtöbb implementáció ezt megengedi.
- ±20 másodperc eltéréssel már jelentős sikertelenség tapasztalható.
- ±30 másodpercnél az összes hitelesítés meghiúsul, mivel az időablak átlépte a megengedett tartományt.

5.5. Támadási vektorok és gyakorlati tesztek

5.5.1. Replay támadás szimulációja

Teszt célja: egy korábban generált TOTP kód újrafelhasználhatóságának vizsgálata.

Teszt leírása

1. A támadó elkap egy érvényes TOTP kódot a hálózaton keresztül.
2. Megpróbálja újra elküldeni a szervernek 20 másodperccel később.
3. Ha a szerver nem ellenőrzi az egyedi használatot, a támadás sikeres lehet.

Eredmény

- A támadás csak akkor működött, ha az időeltérés nem haladta meg a 30 másodpercet.
- Azon szerverek esetében, amelyek nem tárolták az előzőleg felhasznált kódokat, a támadás sikeres volt.

Védelmi megoldások

- HMAC-SHA256 vagy SHA512 alkalmazása SHA1 helyett, hogy ne legyenek előre kiszámítható kódok.
- Minden kód csak egyszer használható fel, így a szervernek tárolnia kell az utoljára használt kódokat.

6. Jövőbeli trendek és fejlesztési lehetőségek

A TOTP technológia jelenleg is széles körben alkalmazott, de számos új hitelesítési eljárás és biztonsági trend kezd előtérbe kerülni. Ezek közül néhány akár kiválthatja vagy kiegészítheti a TOTP használatát a közeljövőben.

6.1. TOTP és FIDO2/WebAuthn kapcsolata

HMAC-Based One-Time Password (HOTP)	Time-Based One-Time Password (TOTP)
Event Counter	Time Counter
The counter is incremented after successful authentication or on button press	The counter is incremented every 30 seconds
OTP is valid for an unlimited time (until a new OTP is generated)	OTP is valid for 30 seconds only
Requires a validation window	Requires no validation window

4. ábra Összehasonlítja a TOTP és a FIDO2/WebAuthn technológiákat
https://rublon.com/blog/hotp-totp-difference/?utm_source

A TOTP gyenge pontja, hogy a felhasználó aktív részvételét igényli (kód beírása), illetve időablak-függő. A FIDO2 és WebAuthn szabványok ezzel szemben jelszómentes, erősen kriptográfiai alapú megoldásokat kínálnak.

FIDO2 / WebAuthn alapjai

- Kriptográfiai kulcspár alapú hitelesítés (nyilvános és privát kulcs).
- A privát kulcs eszközön marad, nem kerül továbbításra.
- A bejelentkezéshez biometrikus vagy PIN-alapú megerősítés társul.

Kombináció TOTP-vel

Bár a WebAuthn célja a jelszómentes világ megteremtése, rövid távon kombinálható TOTP-vel:

- Hybrid MFA (Multi-Factor Authentication) rendszerekben a TOTP továbbra is másodlagos faktor lehet.

- Fallback módszerként is szolgálhat olyan eszközöknél, ahol FIDO2 nem támogatott.[4][6]

6.2. Jelszómentes autentikáció lehetőségei

A jelszómentes hitelesítés célja, hogy a felhasználók azonosítása teljesen kódok és jelszavak nélkül történjen, megbízható eszközök és biometrikus azonosítók segítségével.

Tendenciák és technológiák

- Magic link e-mailen keresztül
- Push notification alapú hitelesítés (pl. Duo Security, Microsoft Authenticator)
- Platform Authenticator (Windows Hello, Apple Touch ID / Face ID)

Ezek a módszerek nemcsak kényelmesebbek, hanem kevésbé kitettek phishing vagy social engineering támadásoknak is.

Kihívások

- Infrastruktúra- és kompatibilitás-problémák
- Eszközvesztés vagy -lopás esetén fallback stratégiák kidolgozása
- Felhasználói edukáció

6.3. Kvantumszámítógépek hatása a TOTP-re

Bár a TOTP nem elsősorban kriptográfiai kulcspárra épül, mégis felmerül a kérdés, hogy a kvantumszámítógépek milyen hatással lesznek rá közvetve.

Kvantumveszélyeztetett pontok

- A TOTP az HMAC-SHA algoritmusra épül, amelyet a kvantumalgoritmusok (pl. Grover algoritmus) gyorsabban tudnak visszafejteni.
- A kvantumszámítógépek fejlődése hosszabb távon veszélyeztetheti a jelenlegi HMAC-implementációk erősségét.

Lehetséges válaszok

- Erősebb hash-függvények (pl. SHA-3, SHA-512) bevezetése.
- Post-quantum TOTP koncepciók kidolgozása (pl. hash-alapú szignatúrák kombinálása időalapú validációval).
- TOTP alternatívák fejlesztése kvantumbiztos módszerekkel.[5]

6.4. Automatizálás és UX-fejlesztések

A jövő hitelesítési rendszerei nemcsak biztonságosabbak, hanem felhasználóbarátabbak is lesznek. A TOTP jelenlegi manuális bevitele helyett egyre több platform kínál automatikus kódbevitelt és felismerést.

További lehetőségek:

- Autofill TOTP-kódok mobilon (pl. Android Smart Lock, iOS iCloud kulcskarika)
- Böngésző-integrált hitelesítő modulok (pl. Chrome Authenticator)

Hangalapú és AR/VR környezetekben történő hitelesítés

7. Jogszabályi és szabályozási környezet

7.1. TOTP és az adatvédelem

A TOTP önmagában nem hordoz személyes adatokat, azonban használata során kulcsfontosságú, hogy a titkos kulcs biztonságosan legyen kezelve – különösen, ha azt egy felhasználóhoz rendelik. Ez összefügg a GDPR-rel (General Data Protection Regulation), amely a személyes adatok védelmét szabályozza az Európai Unióban. A titkos kulcs és a hitelesítési események naplózása olyan metaadatokat tartalmazhat, amelyek személyes adatoknak minősülhetnek. [15]

A NIS2 irányelv (2023-tól életbe lépve) kibővíti a hálózati és információs rendszerek biztonsági követelményeit számos ágazatban (energia, közlekedés, egészségügy stb.), és megkövetelheti többtényezős hitelesítési módszerek, így a TOTP használatát is. [16]

7.2. Hitelesítési előírások és megfelelés

A PSD2 (Revised Payment Services Directive) az EU-ban szabályozza az elektronikus fizetések biztonságát. Az ún. erős ügyfél-hitelesítés (SCA) előírásai megkövetelik legalább két független hitelesítési faktor használatát a következő kategóriákból: tudás (pl. jelszó), birtoklás (pl. TOTP-generátor), és inherencia (pl. biometrikus azonosító). A TOTP ideálisan illeszkedik a birtoklás típusú hitelesítésbe. [17]

Az eIDAS rendelet az elektronikus azonosítás és aláírás szabványosítását célozza meg, különféle biztonsági szintekkel (alap, jelentős, magas). Bár a TOTP nem minősül minősített eszköznek, alacsonyabb biztonsági szinten alkalmazható pl. elektronikus szolgáltatások bejelentkezési folyamatában. [18]

7.3. Nemzetközi szabványok és ajánlások

A NIST (National Institute of Standards and Technology) kiemelten foglalkozik hitelesítési rendszerek ajánlásaival, különösen a *NIST SP 800-63B* dokumentumban. Itt a TOTP mint "memorized secret + token" páros egyik ajánlott implementációja szerepel, bár újabb irányelvek a jelszómentes, kriptográfiai kulcspáron alapuló hitelesítést támogatják. [19]

Az ISO/IEC 27001 szabványcsalád a szervezeti információbiztonság menedzseléséről szól, amelyben az erős autentikáció kulcselem. A TOTP használata a kockázatkezelési gyakorlat és a hozzáférés-szabályozás része lehet. [20]

8. Felhasználói tapasztalat és elfogadás

8.1. A kétlépcsős azonosítás hatása a felhasználókra

A TOTP-alapú hitelesítés bevezetése jelentős változást jelent a felhasználói szokásokban. A jelszó megadása után még egy lépést kell tenni – ez kezdetben idegen, kényelmetlen lehet. A felhasználók hajlandósága nagyban függ attól, hogy az extra lépést mennyire érzik zavarónak vagy bonyolultnak.

Példa: Egyes felmérések szerint a kétlépcsős azonosítás növeli a biztonságérzetet, de ha túl gyakran kell használni, az frusztrációhoz vezethet. [21]

8.2. Használhatósági szempontok (UX)

A jó felhasználói élmény kulcsfontosságú. A TOTP-alapú rendszerek esetében a következő UX-faktorokat lehet vizsgálni:

- Az alkalmazás (pl. Google Authenticator) felülete mennyire intuitív?
- Mennyire egyszerű új eszközre áthelyezni a kulcsokat?
- Milyen gyors a hitelesítés folyamata a felhasználó számára?

Megállapítás: Az egyszerűség és gyorsaság növeli az elfogadottságot, a technikai akadályok viszont elidegenítik a felhasználókat.

8.3. Oktatás és támogatás szerepe

A TOTP használatához technikai ismeretek szükségesek – pl. QR-kód beolvasás, időablak fogalma. Sok felhasználó elakad a beállítás során. Ezért fontos:

- részletes és érthető beállítási útmutató,
- ügyfélszolgálat jelenléte,
- alternatív módszerek azoknak, akik nem tudják használni az appot (pl. SMS-alapú kód, backup-kulcs).

8.4. Elfogadási arányok különböző célcsoportokban

A felhasználók technikai affinitása nagyban meghatározza a TOTP elfogadását. Egyes célcsoportok könnyen adaptálják (pl. IT szakemberek), mások idegenkednek tőle (pl. idősebb korosztály, nem tech-orientált felhasználók).

5. ábra Dáp mobilalkalmazás
https://24.hu/tech/2024/12/31/ugyfelkapu-okostelefon-nelkul-totp-app-utmutato-lepesrol-lepesre/

8.5. Alternatívák összehasonlítása felhasználói szempontból

A felhasználók mennyire kedvelik vagy utasítják el a TOTP-t más módszerekhez képest:

- SMS-alapú kódok: kényelmesebb, de kevésbé biztonságos.
- Push-alapú hitelesítés: egyszerűbb, de függ az internettől.
- Biometrikus azonosítás: felhasználóbarát, de költségesebb.

8.6. Következtetések és javaslatok

A sikeres TOTP bevezetés kulcsa a kényelem és biztonság egyensúlya. Javasolt lépések:

- Felhasználói visszajelzések folyamatos gyűjtése
- UX-tesztelések rendszeres beépítése
- Oktatási kampányok a tudatosság növelésére
- Többfajta hitelesítési opció párhuzamos biztosítása

9. Összegzés és következtetések

A dolgozat célja az volt, hogy technikai mélységében elemezze a TOTP (Time-based One-Time Password) algoritmus működését, gyakorlati megvalósítását, valamint annak alkalmazását a Google Authenticator keretrendszerén keresztül. A vizsgálat során különös hangsúlyt került az elméleti alapokra, a biztonsági megfontolásokra, valamint az implementációs lehetőségekre és jövőbeli trendekre.

9.1. A TOTP és Google Authenticator szerepe a modern biztonsági rendszerekben

A TOTP egy viszonylag egyszerű, de robusztus megoldást kínál a második faktoros hitelesítéshez. Könnyen implementálható, nyílt szabványokon alapul, és szoftveres vagy hardveres formában is alkalmazható.
A Google Authenticator példája jól szemlélteti, hogyan lehet a TOTP-t hatékonyan integrálni a hétköznapi felhasználók biztonságába, legyen szó akár e-mail szolgáltatásokról, pénzügyi alkalmazásokról vagy vállalati rendszerekről. Az alkalmazás offline működése, egyszerű kulcskezelése és széles körű támogatottsága hozzájárult elterjedéséhez.

9.2. Alternatívák és fejlesztési lehetőségek

Bár a TOTP ma is releváns, a modern biztonsági kihívásokra válaszul egyre több szervezet fordul a jelszómentes megoldások (pl. FIDO2, WebAuthn) felé. E technológiák kényelmesebbek, gyorsabbak, és bizonyos támadások ellen (pl. phishing) hatékonyabb védelmet nyújtanak.
Mindemellett a TOTP továbbfejlesztése – például kvantumbiztos hash-függvények vagy eszközfüggetlen autentikáció révén – biztosíthatja a módszer jövőállóságát.

9.3. Következtetések

Összességében elmondható, hogy a TOTP és annak alkalmazásai, mint a Google Authenticator, ma is kulcsszerepet játszanak a többfaktoros hitelesítési rendszerekben. A módszer egyszerűsége és rugalmassága miatt különösen jól alkalmazható kis- és középvállalati környezetben, de kritikus rendszerek esetén is megfelelő védelmet nyújthat, ha helyesen implementálják.
A közeljövőben a hangsúly várhatóan a felhasználói élmény és a kvantumbiztonság irányába tolódik el, ahol a TOTP szerepe kiegészítő vagy átmeneti megoldássá válhat az újabb technológiák térnyerésével.

9.4. A dolgozat főbb megállapításai

A dolgozat célja az volt, hogy részletesen elemezze a TOTP protokoll technikai működését, biztonsági kihívásait, támadási lehetőségeit, valamint a Google Authenticator alkalmazást és annak hiányosságait. A főbb eredmények a következők:

9.4.1. A TOTP erősségei és korlátai

- Időalapú kódok, amelyek egyszer használhatók, csökkentik a jelszóalapú támadások hatékonyságát.
- Offline működés, nincs szükség aktív internetkapcsolatra a hitelesítéshez.
- Érzékeny az időszinkronizációra, ha az órák eltérnek, a hitelesítés sikertelen lehet.
- Replay támadások lehetségesek, ha egy kódot több alkalommal lehet felhasználni.

9.4.2. Google Authenticator elemzése

- Gyors és egyszerű megoldás, széles körben támogatott.
- Nem tárol adatokat a felhőben, ami növeli a biztonságot az eszközszintű támadásokkal szemben.
- Nincs automatikus kulcsmentés, így, ha a felhasználó elveszíti a készülékét, az összes regisztrált fiókhoz új TOTP kulcsot kell beállítani.
- Nem támogat push-alapú hitelesítést, ami egyesesetekben kényelmesebb és biztonságosabb lehetne.

9.4.3. Időszinkronizáció problémái és megoldások

- ±10 másodperces időeltérésig a hitelesítés még megbízható.
- ±30 másodperc eltérésnél a hitelesítés teljesen meghiúsul.
- Az NTP vagy TLS-alapú időszinkronizáció segíthet az eltérések minimalizálásában.

9.4.4. Támadási vektorok és védekezési stratégiák

- **Phishing és Man-in-the-Middle támadások elleni védekezés:**

  - WebAuthn vagy FIDO2 kombinálása a TOTP-vel.
  - IP-cím és eszközspecifikus korlátozások bevezetése.

- Replay támadások elleni védekezés:

  - A szerver minden kódot csak egyszer fogadjon el.
  - Hash algoritmus SHA256 vagy SHA512-ra való cseréje.

9.5. Javasolt fejlesztések és alternatív megoldások

Bár a TOTP széles körben elterjedt, a technológia további fejlesztésekre szorul. Az alábbi megoldások javíthatják a biztonságot és a felhasználói élményt:

- FIDO2/WebAuthn alapú hitelesítés – kiküszöböli a TOTP kódok megadásának szükségességét, és erősebb védelmet biztosít.
- Hibrid megoldás – TOTP + push-alapú értesítések kombinációja növelheti a biztonságot.
- időszinkronizáció fejlesztése – pontosabb időszinkronizációs algoritmusok, például a TLS-alapú időprotokoll használata.
- Google Authenticator fejlesztése – automatikus titkos kulcs-mentési lehetőség bevezetése a készülék elvesztése esetére.

9.6. Jövőbeni kutatási irányok

A dolgozat során bemutatott vizsgálatok és eredmények számos új kérdést vetnek fel, amelyeket érdemes lehet a jövőben részletesebben tanulmányozni:

- Alternatív egyutas hitelesítési protokollok (pl. HOTP, FIDO2) hatékonyságának összehasonlítása TOTP-vel.
- Kvantumbiztos hash algoritmusok (pl. SHA-3, BLAKE2) alkalmazása a TOTP rendszerben.
- AI-alapú viselkedéselemzés a TOTP kódok biztonságosabbá tételére – pl., ha egy felhasználó kódjai gyanús időközönként jelennek meg, akkor további hitelesítés szükséges.
- Biztonságosabb, hardveres 2FA eszközök bevezetése – pl. YubiKey vagy Titan Security Key

10. Irodalomjegyzék

[1] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, és O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," IETF RFC 4226, December 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4226

[2] D. M'Raihi, S. Machani, M. Pei, és J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," IETF RFC 6238, May 2011. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6238

[3] Google, "Google Authenticator – Android App," [Online]. Available: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

[4] A. Langley, "FIDO2, WebAuthn, and the Future of Strong Authentication," Google Security Blog, 2021. [Online]. Available: https://security.googleblog.com

[5] The Impact of Quantum Computing on Authentication: What You Need to Know - Petr Dvořák https://www.wultra.com/blog/the-impact-of-quantum-computing-on-authentication-what-you-need-to-know

[6] FIDO Alliance – OTP és FIDO2 jövő: https://fidoalliance.org/specifications/

[7] The code behind Google Authenticator - Sven VC https://medium.com/concerning-pharo/the-code-behind-google-authenticator-9c59c606a572

[8] Precision time protocol attack strategies and their resistance to existing security extensions - Waleed Alghamdi & Michael Schukat https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00080-y

[9] What is NTP (Network Time Protocol)? https://www.pubnub.com/learn/glossary/ntp-protocol/

[10] What Is Transport Layer Security (TLS)? - Christian Henke https://www.emnify.com/blog/tls

[11] PyOTP - The Python One-Time Password Library - mrbean-bremen

https://github.com/pyauth/pyotp
[12] Time-based One Time Password (MFA) Library for Java - samdjstevens https://github.com/samdjstevens/java-totp
[13] Implementing TOTP with nodejs - Leo Arokiaraj https://leoarok.medium.com/implementing-totp-with-nodejs-1e29762fdefe
[14] TOTP vs. U2F: What's the Difference? - Rublon Authors https://rublon.com/blog/totp-vs-u2f-whats-the-difference/
[15] Az általános adatvédelmi rendelet szerinti adatvédelmi szabályok https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hu.htm
[16] NIS 2 irányelv: a hálózati és információs rendszerek kiberbiztonságára vonatkozó új szabályok https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive
[17] Mi az a PSD2 és az SCA? https://help.mypos.com/hc/hu-hu/articles/6885300723101-Mi-az-a-PSD2-%C3%A9s-az-SCA
[18] eIDAS-rendelet https://digital-strategy.ec.europa.eu/hu/policies/eidas-regulation
[19] https://www.nist.gov/
[20] ISO/IEC 27001:2022 https://www.iso.org/standard/27001
[21] Mi az a kétlépcsős azonosítás és miért kell? https://mikorkell.hu/mi-az-a-ketlepcsos-azonositas-es-miert-kell/

2.29. StulczBendegúzMilán HT9NZQ Privát 5G hálózatok kiépítése noneptun

Széchenyi István Egyetem

Gépészmérnöki, Informatikai és Villamosmérnöki Kar

Informatika Tanszék

Stulcz Bendegúz Milán

Gazdaságinformatika BSC

Privát 5G hálózatok kiépítése

2025

Tartalom

1. Bevezetés 4
1 Az 5G technológia elméleti alapjai 5
1.1 Az 5G technológia általános jellemzői 5
1.2 A privát 5G hálózatok definíciója és jellemzői 7
1.3 Network slicing és egyéb kulcsfontosságú technológiák 7
2 A privát 5G hálózatok főbb előnyei 9
2.1 Nagy adatátviteli sebesség 9
2.2 Alacsony késleltetés 9
2.3 Nagyszámú eszközkapcsolat 10
2.4 Biztonság és adatvédelem 10
2.5 Testreszabhatóság 10
3 Iparági alkalmazások 12
3.1 Gyártóipar és Ipar 4.0 12
3.2 Logisztika és ellátási lánc 12
3.3 Egészségügy 13
3.4 Intelligens városi alkalmazások 13
4 Eszközök és beszállítók 15
4.1 Ericsson megoldások 15
4.2 Nokia privát 5G portfólió 15
4.3 Cisco hálózati megoldások 16
4.4 AWS és Microsoft Azure felhőintegrációs lehetőségek 16
4.4.1 AWS privát 5G megoldások: 16
4.4.2 Microsoft Azure privát 5G integrációk: 16
5 Spektrumhasználati lehetőségek 18
5.1 Dedikált spektrum 18
5.2 Megosztott spektrum 18
5.3 Spektrumbérlés mobilszolgáltatóktól: 18
5.4 Engedélymentes spektrum: 18
6 Infrastrukturális követelmények 20
6.1 Rádiós hozzáférési hálózat (RAN) 20
6.2 Maghálózat (Core Network) 20
6.3 Peremhálózati (Edge) infrastruktúra: 21
6.4 Végponti eszközök 21

6.5 Backhauling infrastruktúra 21
7 Hálózattervezési modellek 23
7.1 Teljesen önálló (standalone) modell 23
7.2 Hibrid modell 23
7.3 Network-as-a-Service (NaaS) modell 24
7.4 Megosztott infrastruktúra modell 25
8 Szabályozási és engedélyezési folyamatok 26
8.1 Spektrumhasználati engedélyek 26
8.2 Telepítési engedélyek 26
8.3 Berendezések megfelelősége 26
8.4 Adatvédelmi és biztonsági előírások 27
8.5 Nemzetbiztonsági szempontok 27
9 Kihívások és korlátok 28
9.1 Kezdeti beruházási költségek 28
9.2 Integrációs nehézségek 28
9.3 Szakértelem hiánya 29
9.4 Biztonsági kockázatok 30
10 Jövőbeli trendek és fejlődési irányok 31
10.1 5G-Advanced és 6G felé 31
10.2 Edge computing és AI integráció 31
10.3 Ipari ökoszisztémák fejlődése 32
11 Összegzés és következtetések 33
Források 34

1. Bevezetés

A digitális transzformáció korában a vállalatok versenyképességének egyik kulcsfontosságú eleme a megbízható, nagy sebességű és biztonságos kommunikációs infrastruktúra. A privát 5G hálózatok kiépítése egyre nagyobb figyelmet kap az ipari és üzleti szektorban, mivel olyan technológiai lehetőséget kínál, amely számos előnnyel rendelkezik a hagyományos vezetékes és vezeték nélküli megoldásokkal szemben.

Ezek a dedikált 5G hálózatok lehetővé teszik a vállalatok számára, hogy saját, testreszabott kommunikációs infrastruktúrát működtessenek, amely kizárólag az ő igényeiket szolgálja.

A privát 5G hálózatok jelentősége különösen felértékelődik az Ipar 4.0 és a digitális átállás kontextusában, ahol a valós idejű adatáramlás, az alacsony késleltetés és a nagy megbízhatóság kritikus tényezőkké váltak. A technológia lehetővé teszi az ipari folyamatok hatékonyabb automatizálását, az Internet of Things (IoT) eszközök zökkenőmentes integrációját, valamint a mesterséges intelligencia és a fejlett analitikai megoldások szélesebb körű alkalmazását.

Jelen dolgozat célja, hogy átfogó képet nyújtson a privát 5G hálózatok jelentőségéről, megvalósítási lehetőségeiről és kihívásairól, valamint támpontokat adjon a technológia gyakorlati implementációjához. Elemzésünk kiterjed a technológiai alapokra, a főbb előnyökre, az alkalmazási területekre, a szükséges eszközökre és beszállítókra, valamint a gyakorlati megvalósítás szempontjaira és kihívásaira.

1 Az 5G technológia elméleti alapjai

1.1 Az 5G technológia általános jellemzői

Az 5G, vagyis az ötödik generációs mobilhálózati technológia jelentős előrelépést hoz a korábbi generációkhoz képest, különösen az adatátvitel sebessége, késleltetése, kapacitása, megbízhatósága és energiahatékonysága terén. Az 5G hálózatok akár 20 Gbps-os letöltési sebességet is lehetővé tesznek, amely nagyságrendekkel gyorsabb a 4G által nyújtott sebességnél.

Emellett ultraalacsony, akár 1 milliszekundum alatti késleltetés érhető el, szemben a 4G-nél jellemző 50-100 milliszekundumos értékkel. További jelentős előnye, hogy akár egymillió eszköz is csatlakozhat egyidejűleg egyetlen négyzetkilométeren belül, ami óriási kapacitásnövekedést jelent a korábbi hálózatokhoz képest.

Kritikus alkalmazásokhoz az 5G hálózatok rendkívül magas, akár 99,999%-os rendelkezésre állást tudnak biztosítani, továbbá energiahatékonyságuk révén az IoT (Internet of Things) alkalmazásokban használt eszközök akár 10 éves akkumulátor-élettartamot is elérhetnek.

Az 5G technológia működése három fő frekvenciasávban valósul meg, amelyek különböző előnyökkel és hátrányokkal rendelkeznek. Az alacsony frekvenciasáv (1 GHz alatt) nagyobb lefedettséget és jobb épületpenetrációt tesz lehetővé, viszont az adatátviteli sebessége ebben a tartományban alacsonyabb.

A közepes frekvenciasáv (1–6 GHz) kiegyensúlyozott kompromisszumot nyújt a lefedettség és a kapacitás között. Ezzel szemben a magas frekvenciasávok (24 GHz felett, úgynevezett mmWave) rendkívül nagy adatátviteli sebességet biztosítanak, viszont korlátozott a hatótávolságuk, és az épületpenetrációjuk is gyengébb.

1. ábra

https://www.origo.hu/techbazis/2021/02/lassabban-terjed-az-5g

1.2 A privát 5G hálózatok definíciója és jellemzői

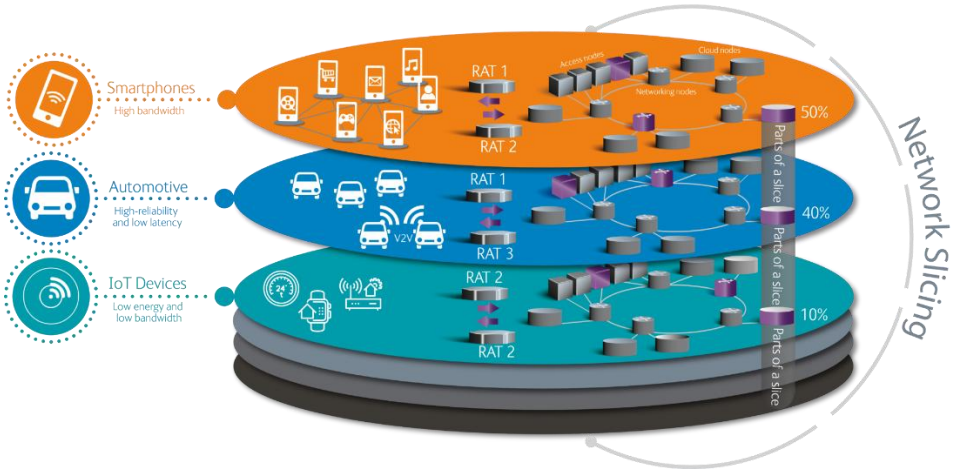
A privát 5G hálózatok olyan dedikált infrastruktúrára épülnek, amelyek saját rádióhálózati és maghálózati komponensekkel rendelkeznek. Ezek a hálózatok fizikailag vagy logikailag elkülönülnek a nyilvános mobilhálózatoktól, így izolált, biztonságos működést biztosítanak. Jelentős előnyük a testreszabhatóság, hiszen a hálózat konfigurációja teljes mértékben igazítható a szervezet egyedi igényeihez.

Az adatok feldolgozása helyben, a szervezet saját infrastruktúráján történik, ami növeli az adatbiztonságot és a működési hatékonyságot. A privát 5G hálózatok emellett garantált szolgáltatásminőséget (QoS) kínálnak, ami lehetővé teszi a teljesítmény pontos tervezését és biztosítását. Végezetül, ezek a hálózatok fokozott biztonságot nyújtanak, mivel a szervezet számára jobb kontrollt és szigorúbb biztonsági mechanizmusokat tesznek lehetővé.

1.3 Network slicing és egyéb kulcsfontosságú technológiák

Az 5G hálózatok további kulcsfontosságú technológiákat alkalmaznak a teljesítmény és hatékonyság növelésére. Az egyik ilyen a Multi-access Edge Computing (MEC), amelynek lényege, hogy az adatfeldolgozás közelebb kerül a végfelhasználókhoz, ezáltal csökken a késleltetés és a hálózati terhelés. Fontos elem a Software-Defined Networking (SDN) is, amelynek révén a hálózati infrastruktúra programozhatóvá válik, jelentősen javítva annak rugalmasságát és skálázhatóságát.

Hasonlóan lényeges a Network Function Virtualization (NFV), ami lehetővé teszi, hogy a korábban kizárólag hardver-alapú hálózati funkciók szoftveres formában működjenek, egyszerűsítve a hálózatok kezelését. További kulcstechnológia a Massive MIMO (Multiple Input Multiple Output), amely nagyszámú antenna használatával növeli a hálózat kapacitását és adatátviteli hatékonyságát. Ehhez kapcsolódik a beamforming technológia, amely célzottan irányítja az antennák jeleit a felhasználók felé, javítva a jelminőséget és csökkentve az interferenciát.



2. ábra
https://blog.viavisolutions.com/2017/08/22/network-slicing-enabling-the-5g-future/

2 A privát 5G hálózatok főbb előnyei

2.1 Nagy adatátviteli sebesség

A privát 5G hálózatok egyik legnagyobb előnye a kiemelkedő adatátviteli sebesség, amely akár 20 Gbps csúcssebességet is elérhet, jelentősen felülmúlva a korábbi vezeték nélküli technológiák, sőt bizonyos esetekben még a vezetékes megoldások teljesítményét is. Ez a rendkívül magas sebesség számos ipari alkalmazás előtt nyitja meg az utat. Lehetővé válik például nagy felbontású videóstreaming és valós idejű monitoring ipari környezetekben, továbbá a nagy adathalmazok gyors továbbítása gyártósorok, raktárak és logisztikai központok között.

A privát 5G infrastruktúra képes támogatni a zökkenőmentes Augmented Reality (AR) és Virtual Reality (VR) alkalmazásokat is, valamint elősegíti a valós idejű adatelemzést és a Big Data-alapú döntéshozatalt. Mivel a dedikált privát hálózat esetén a sávszélesség nem oszlik meg nagyszámú ismeretlen felhasználó között, mint a nyilvános hálózatoknál, a teljesítmény konzisztens, kiszámítható és jól tervezhető marad.

2.2 Alacsony késleltetés

Az 5G technológia egyik legforradalmibb aspektusa az ultra-alacsony késleltetés (latency), amely kiemelt jelentőséggel bír számos ipari és üzleti alkalmazás számára. A privát 5G hálózatok akár 1 milliszekundum alatti késleltetést is biztosíthatnak, ami gyakorlatilag valós idejű működést tesz lehetővé. Ez lehetővé teszi többek között a valós idejű gépvezérlést, robotikai alkalmazásokat, távműtétek lebonyolítását és egyéb kritikus egészségügyi rendszerek biztonságos és pontos irányítását.

Ezen túlmenően jelentősen hozzájárul az autonóm járművek és más önálló eszközök precíz és biztonságos vezérléséhez, illetve olyan gépi döntéshozatalhoz és beavatkozáshoz, amely gyorsabb az emberi reakcióidőnél, például vészhelyzetek során. Ez a rendkívül alacsony késleltetés alapvető változást hoz olyan területeken, ahol minden egyes milliszekundum kritikus jelentőséggel bír, különösen a fejlett ipari gyártási folyamatokban, ahol a gépek közötti kommunikáció sebessége közvetlenül befolyásolja a termelékenységet, a hatékonyságot és a minőséget.

2.3 Nagyszámú eszközkapcsolat

A privát 5G hálózatok egyik legimpozánsabb tulajdonsága a rendkívül magas eszközsűrűség kezelése: négyzetkilométerenként akár egymillió csatlakoztatott készüléket is képesek kiszolgálni. Ennek köszönhetően ideális megoldást nyújtanak olyan környezetekben, ahol nagyszámú szenzor, robot vagy automatizált berendezés kommunikációjára van szükség: a gyártóüzemekben a minőségellenőrző rendszerektől és robotkaroktól kezdve, a logisztikai központokban az árukövető rendszereken és automata targoncákon át, az okos városokban a közlekedési, közbiztonsági és közüzemi hálózatok összehangolt működéséig.

Ugyancsak lehetővé teszik a precíziós mezőgazdaság eszközeinek együttműködését, így a vállalati környezetben a dolgok internetének (IoT) teljes körű kiépítését támogatják, minden eddiginél több adatgyűjtési ponttal és automatizálási lehetőséggel.

2.4 Biztonság és adatvédelem

A privát 5G hálózatok egyik legnagyobb előnye a megerősített biztonság és adatvédelem, hiszen a hálózat fizikailag vagy logikailag elkülönül a nyilvános infrastruktúrától, így lényegesen csökken a kibertámadások és adatszivárgások kockázata. A szervezetek teljes körű kontrollt gyakorolnak a hálózati hozzáférés felett, miközben az érzékeny adatok végig a saját, zárt infrastruktúrán belül maradnak, soha nem haladnak át külső hálózatokon.

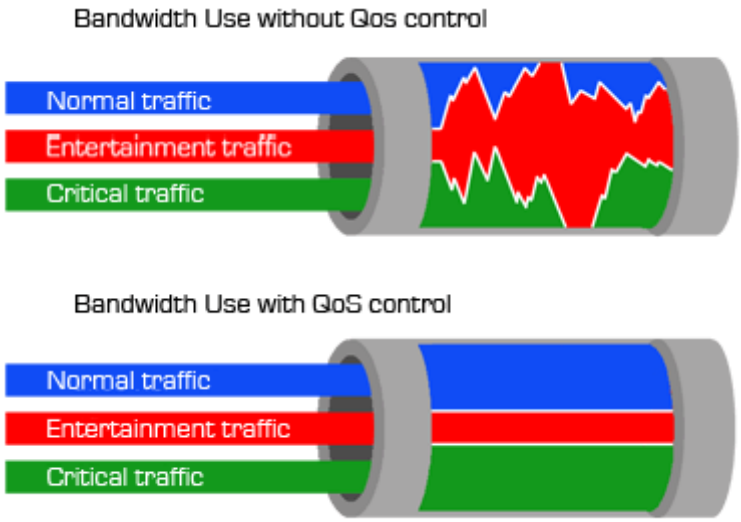
A rendszerben alkalmazott fejlett titkosítási protokollok, a szigorúbb hitelesítési mechanizmusok és a finomhangolt hozzáférés-szabályozás együttesen garantálják, hogy csak a jogosult eszközök és felhasználók férhessenek hozzá az erőforrásokhoz. Emellett a valós idejű biztonsági monitoring lehetővé teszi a fenyegetések azonnali észlelését és gyors reagálást, ami különösen kritikus olyan ágazatokban, mint az egészségügy, a pénzügyi szolgáltatások vagy a védelmi ipar, ahol a legszigorúbb adatvédelmi előírások betartása elengedhetetlen.

2.5 Testreszabhatóság

A privát 5G hálózatok egyik legnagyobb előnye a nagyfokú testreszabhatóság, amely lehetővé teszi, hogy a hálózat minden részlete a szervezet egyedi igényeihez igazodjon. A telepítés során a lefedettség pontosan megtervezhető az adott fizikai környezet például gyártócsarnok, raktár vagy irodaépület feltételeihez, miközben a hálózati teljesítmény és szolgáltatásminőség (QoS) finomhangolása révén biztosítható, hogy az egyes alkalmazások mindig a szükséges sávszélességet és késleltetést kapják.

A sávszélesség elosztása optimalizálható a különböző felhasználási területek között például videómonitoring, IoT-szenzorok és mobil gépek számára és egyedi biztonsági protokollokkal, hozzáférési szabályokkal tovább emelhető a védelem szintje.

A privát infrastruktúrában akár olyan speciális funkcionalitások is bevezethetők például dedikált üzemmódok vagy privát slices , amelyek a publikus hálózatokban nem elérhetők, és az egész rendszer skálázhatósága rugalmasságot biztosít a jövőbeli üzleti igények, például új gyártósorok vagy bővülő IoT-állomány kiszolgálásához. Így a szervezetek teljes mértékben a saját prioritásaik szerint alakíthatják ki és üzemeltethetik privát 5G hálózatukat, maximalizálva annak értékét és támogatva üzleti folyamataikat.



3. ábra
https://prohardver.hu/tudastar/qos_quality_of_service.html

3 Iparági alkalmazások

3.1 Gyártóipar és Ipar 4.0

A privát 5G hálózatok az Ipar 4.0 megvalósításának gerincét jelentik a gyártóiparban, lehetővé téve az intelligens gyártósorok valós idejű kommunikációját, ami gyors adaptációt és személyre szabott tömeggyártást tesz lehetővé. A prediktív karbantartás során a berendezésekből folyamatosan érkező adatok elemzése előre jelzi a lehetséges meghibásodásokat, így csökkenthető az állásidő és a karbantartási költség.

A nagy felbontású videóalapú minőségellenőrzési folyamatokat mesterséges intelligenciával kiegészítve már a termelés közben elvégezhetjük, míg az alacsony késleltetésű kapcsolaton keresztül a robotok precíz, összehangolt működése és automatizált feladatok végrehajtása válik lehetővé.

A fizikai berendezések digitális ikreként működő valós idejű modellezés és szimuláció segítségével folyamatosan nyomon követhetjük és optimalizálhatjuk a teljes folyamatot, és az AR-alapú alkalmazások révén a karbantartók, operátorok minden szükséges információt közvetlenül a látóterükben kapnak meg. Mindez rendkívül előnyös ott, ahol a vezetékes hálózatok kiépítése bonyolult vagy költséges, és ahol a mobilitás, valamint a rendszer rugalmassága kulcsfontosságú.

3.2 Logisztika és ellátási lánc

A privát 5G hálózatok alkalmazása forradalmasíthatja a logisztikai ágazatot és az ellátási láncok működését az automatizálás, a követhetőség és az adatalapú optimalizáció terén. A raktárautomatizálás keretében autonóm targoncák, szállítórobotok és akár drónok is együtt dolgozhatnak zökkenőmentesen a tágas raktárépületekben, miközben a valós idejű eszközkövetés lehetővé teszi a készletek és rakományok pontos lokalizálását nagy pontosságú helymeghatározással. Az intelligens leltárkezelés során RFID- és egyéb szenzoralapú rendszerek automatikusan frissítik a készletinformációkat, így minimalizálható az emberi beavatkozás miatti hibák száma.

Ezzel párhuzamosan a privát 5G hálózatokon futó valós idejű adatelemzés segítségével az ellátási lánc minden szakasza optimalizálható: a készletek forgási sebessége és a szállítási útvonalak dinamikusan igazíthatók a pillanatnyi igényekhez. Az automatizált minőségellenőrzés mesterséges intelligencia és nagy felbontású kamerák együttes használatával garantálja a csomagok és áruk sértetlenségét és megfelelőségét. Végül a járműflotta-menedzsment funkciói – valós idejű követés, üzemanyag-felhasználás-optimalizálás és intelligens útvonaltervezés – hatékonyabbá teszik a fuvarozást, különösen nagy kiterjedésű logisztikai központokban, kikötőkben és repterekben, ahol a hagyományos WiFi-megoldások már nem nyújtanak elegendő lefedettséget vagy megbízhatóságot.

3.3 Egészségügy

A privát 5G hálózatok az egészségügyi szektorban számtalan területen kínálnak előnyt: a telemedicina révén ultramagas felbontású, valós idejű videókonzultációk és távdiagnosztikai megoldások válnak lehetővé, míg a távműtéteknél az alacsony késleltetés biztosítja a sebészeti robotok precíz, távoli irányítását. A hordható és beültethető eszközök folyamatos adatgyűjtése és elemzése révén a betegmonitorozás új szintre lép, és a nagy méretű diagnosztikai felvételek gyors továbbítása révén az orvosi képalkotás is jelentősen hatékonyabbá válik.

A kiterjesztett valóság (AR) alkalmazások a műtétek során valós idejű, kontextuális információkkal támogatják a sebészek munkáját, míg a robotizált gyógyszerkiadási rendszerek és a kórházi eszközkövetés révén a gyógyszerautomatizálás és a kritikus orvosi berendezések lokalizálása is gördülékenyebbé, biztonságosabbá válik. Mindezeknél a fejlesztéseknél a privát 5G hálózatok fokozott biztonsági előnyei – az elkülönített infrastruktúra és a szigorú adatvédelmi mechanizmusok – illetve az ultramegbízható működés olyan kritikus tényezők, amelyek életmentő beavatkozások esetén is garantálják a folyamatos, zavartalan szolgáltatást.

4. ábra
https://www.pannondoktor.hu/2023/12/kiterjesztett-valosagot-alkalmazo-orvosi-eszkoz-fejlesztett-a-zmed-a-hun-ren-sztaki-es-a-pte/

3.4 Intelligens városi alkalmazások

Az okos városok digitális infrastruktúrájának kulcsfontosságú eleme lehet a privát 5G hálózat, amely lehetővé teszi az intelligens közlekedésirányítást így a forgalomoptimalizálást, a jelzőlámpák adaptív vezérlését és a torlódások előrejelzését , továbbá fokozott közbiztonsági rendszerek kiépítését fejlett megfigyelő- és vészhelyzeti kommunikációs megoldásokkal, valamint katasztrófaelhárítási koordinációval. Az

energiafelhasználást, a vízhálózatok menedzsmentjét és a hulladékkezelést összefogó okos közművek is zavartalanul működhetnek a privát 5G nyújtotta sávszélesség és megbízhatóság mellett.

A környezeti monitorozás valós idejűvé válik, így a lég- és vízminőség, valamint a zajszint folyamatosan ellenőrizhető, miközben az adaptív utcai világítás a forgalomhoz és az időjárási viszonyokhoz igazodva működik. Végezetül a tömegközlekedés is új szintre léphet: valós idejű járműkövetés, dinamikus útvonaltervezés és kapacitástervezés teszi hatékonyabbá a buszok, villamosok és városi vasutak működését. A privát 5G hálózatok bevezetésével a városok saját kezükbe vehetik digitális infrastruktúrájuk irányítását, csökkenthetik külső szolgáltatóktól való függőségüket, és integrált, testreszabott megoldásokat hozhatnak létre a modern városi kihívások kezelésére.

4 Eszközök és beszállítók

4.1 Ericsson megoldások

Az Ericsson a privát 5G hálózatok terén piacvezető megoldásokat kínál vállalati ügyfelei számára. Portfóliójának alapját az Industry Connect adja, amely előre integrált, felhasználóbarát privát 5G rendszert biztosít ipari környezetekre szabva, így a telepítés is gyors és egyszerű.

A teljes rugalmasságot igénylő vállalatok számára az Ericsson Private 5G egy testreszabható hálózati keretrendszert nyújt, amely minden üzleti követelményhez illeszthető. A rádiós hozzáférést az Ericsson Radio System moduláris, skálázható RAN-rendszere biztosítja, amely különböző frekvenciasávokban és telepítési forgatókönyvekkel egyaránt működik.

A hálózat intelligens funkcióit és vezérlését az Ericsson Cloud Core felhőalapú maghálózati megoldása kezeli, míg az Ericsson Local Packet Gateway a helyi adatfeldolgozást végzi, csökkentve a késleltetést és növelve a biztonságot. Ezekkel a komponensekkel az Ericsson már a gyártóipar, a bányászat, a kikötők és a logisztikai központok területén is számos sikeres privát 5G implementációt valósított meg világszerte.

4.2 Nokia privát 5G portfólió

A Nokia a privát 5G hálózatok piacán szintén meghatározó szereplő, átfogó termékportfóliójával és iparági tapasztalatával. A Nokia Digital Automation Cloud (DAC) teljes körű, felhőalapú privát vezeték nélküli megoldást kínál, amely magában foglalja a rádiós hálózatot, a maghálózatot és az alkalmazásplatformot. A Modular Private Wireless (MPW) rugalmas, moduláris felépítése lehetővé teszi a hálózat fokozatos kiépítését és bővítését az igényeknek megfelelően, míg az AirScale Radio kompakt és energiahatékony bázisállomásai különböző telepítési és teljesítménykövetelményekhez is illeszthetők.

A Nokia Industrial Edge peremhálózati számítási megoldása gondoskodik az adatok helyi feldolgozásáról, a Nokia Industrial DevOps pedig eszközöket és szolgáltatásokat nyújt az ipari alkalmazások fejlesztéséhez és telepítéséhez a privát hálózaton. A Nokia különösen erős az Ipar 4.0 megoldások terén, és számos referenciával rendelkezik a gyártás, az energiaipar és a közlekedés területén, emellett 4.9G/LTE és 5G megoldásokat egyaránt kínál a fokozatos átállás támogatására.

4.3 Cisco hálózati megoldások

A Cisco a privát 5G területén főként felhőalapú, szolgáltatásként nyújtott megoldásokat kínál, amelyek jól illeszkednek a meglévő hálózati környezetbe. A Private 5G as-a-Service előfizetéses modellje csökkenti a kezdeti beruházási költségeket, míg az Ultra Cloud Core felhőalapú maghálózat zökkenőmentesen integrálható a Cisco SD-WAN-nal és az egyéb IT-eszközökkel.

Az IoT Control Center platform központi felületet biztosít az eszközök menedzseléséhez és monitorozásához, miközben az Identity Services Engine (ISE) finomhangolt hozzáférés-szabályozást és folyamatos biztonsági ellenőrzést tesz lehetővé a hálózaton.

Ezzel a portfólióval a Cisco az end-to-end integrációban, a meglévő infrastruktúra hasznosításában és a gyorsan skálázható, előfizetéses szolgáltatások nyújtásában emelkedik ki, gyakran együttműködve vezető rádiós berendezésgyártó partnerekkel a teljes körű privát 5G élmény érdekében.

4.4 AWS és Microsoft Azure felhőintegrációs lehetőségek

4.4.1 AWS privát 5G megoldások:

Az AWS privát 5G portfóliója teljesen menedzselt szolgáltatásokat kínál, amelyek egyszerre segítik a hálózat gyors telepítését és zökkenőmentes üzemeltetését, valamint az alkalmazások késleltetésének csökkentését és az eszközök nagyszámú csatlakoztatását.

Az AWS Private 5G automatikusan kezeli a hálózat felállítását és karbantartását, míg az AWS Wavelength a peremhálózati számítási infrastruktúrát biztosítja a mobilfelhasználók számára, ezzel minimálisra csökkentve a késleltetést.

Az AWS Outposts lehetővé teszi az AWS felhő szolgáltatásainak kihelyezését a saját adatközpontokba, így a privát 5G megoldásokkal is integrálható, míg az AWS IoT Core platform milliónyi IoT-eszköz egyidejű csatlakoztatását és központosított kezelését teszi lehetővé.

4.4.2 Microsoft Azure privát 5G integrációk:

A Microsoft Azure privát 5G kínálatának központi eleme az Azure Private 5G Core, amely felhőalapú maghálózati szolgáltatásként zökkenőmentesen illeszkedik a helyi rádiós infrastruktúrához, így biztosítva a teljes hálózati folyamatok felhő és élszis támogatását. Az Azure Edge Zones azokra a feladatokra fókuszál, ahol az ultran alacsony késleltetés kritikus, hiszen közvetlenül a távközlési hálózat közelében nyújt konténerizált számítási kapacitást.

Az Azure Stack Edge lehetővé teszi a helyi adatfeldolgozást peremhálózati környezetben, így a szenzoroktól és IoT-eszközöktől érkező adatokat közvetlenül a telephelyen elemezhetjük, mielőtt azokat a felhőbe továbbítanánk.

Végül az Azure IoT Hub skálázható platformot kínál IoT-megoldások fejlesztéséhez és üzemeltetéséhez, milliószámra csatlakozó eszközök menedzselésével és üzenetközvetítésével. Mindkét felhőszolgáltató – az AWS és az Azure – jelentős előnyt biztosít az adatelemzés, a mesterséges intelligencia és a gépi tanulás területén, amelyek szorosan integrálhatók a privát 5G hálózatokkal a legfejlettebb ipari és üzleti alkalmazások támogatására. Gyakorlati megvalósítás

5 Spektrumhasználati lehetőségek

5.1 Dedikált spektrum

Számos országban külön frekvenciasávokat különítettek el a privát 5G hálózatok számára: például Németországban a 3,7–3,8 GHz-es, Japánban pedig a 4,6–4,9 GHz-es tartományban. Ezek a dedikált sávok garantálják az interferenciamentes működést és teljes körű kontrollt biztosítanak a hálózat felett, mivel kizárólag a jogosult üzemeltető használhatja őket.

Ugyanakkor a sávhasználatért licencdíjat kell fizetni, és az országonként eltérő szabályozási keretek korlátozhatják a frekvenciák elérhetőségét, így a privát 5G kiépítése tervezést és helyi engedélyezést igényel.

5.2 Megosztott spektrum

Az Egyesült Államokban a CBRS (Citizens Broadband Radio Service) 3,5 GHz-es sávjához háromszintű hozzáférési modell kapcsolódik: az incumbent (elsődleges) felhasználók, a prioritási hozzáférésű licenctulajdonosok és az általános hozzáférésű felhasználók.

Ez a struktúra alacsonyabb költségeket és könnyebb spektrumhozzáférést tesz lehetővé a privát hálózatok számára, ugyanakkor összetettebb spektrummenedzsmentet igényel, és fennáll a potenciális interferencia kockázata is.

5.3 Spektrumbérlés mobilszolgáltatóktól:

A meglévő mobilszolgáltatóktól történő frekvenciasáv-bérlés a privát 5G kiépítés egyik könnyen elérhető módja, amely elsődlegesen a gyors telepítést és a szabályozási követelmények egyszerűbb kezelését teszi lehetővé. Ebben az esetben a vállalat nem sajátítja ki közvetlenül a spektrumot, hanem szolgáltatói szerződés keretében kap hozzáférést a szükséges kapacitáshoz, ami jelentősen lerövidíti a projekt indítási idejét és tehermentesíti az engedélyeztetési folyamatot.

Ugyanakkor a szolgáltatótól függő spektrumhasználat hosszabb távon akár magasabb költségekkel is járhat, és korlátozhatja a hálózat teljesítményének és szabályozásának rugalmasságát, hiszen a gyakorlati alkalmazás a szolgáltató hálózati kapacitásától és üzleti döntéseitől is függ.

5.4 Engedélymentes spektrum:

Bizonyos 5G-technológiai megoldások engedélymentes sávokban (például az 5 GHz-es vagy a 6 GHz-es tartományban) is működhetnek, ami azt jelenti, hogy ezeknél a frekvenciáknál nem kell licencdíjat fizetni, és az üzemeltetés szabályozási folyamata is egyszerűbbé válik.

Ugyanakkor az engedélymentes spektrum használata nagyobb interferencia-kockázattal jár, hiszen más rendszerek is igénybe vehetik ugyanazokat a sávokat, ami korlátozhatja a hálózat teljesítményét és megbízhatóságát. A spektrum kiválasztása ezért erősen függ az adott alkalmazás területétől, a helyi szabályozási környezettől, a rendelkezésre álló költségvetéstől és a kívánt teljesítményszinttől.

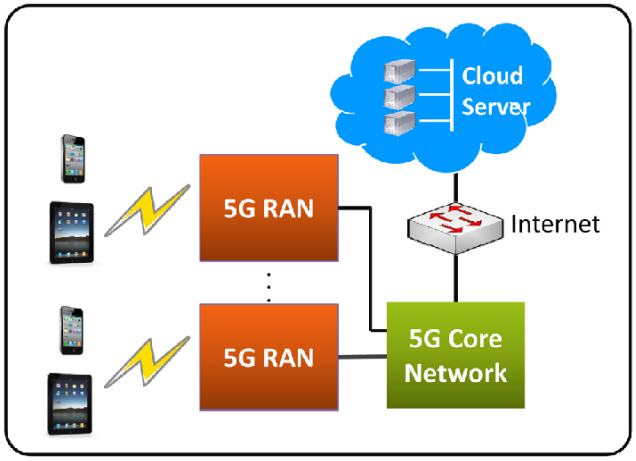
Kritikus ipari feladatoknál általában a dedikált, licencelt frekvenciasávok használata a preferált megoldás, míg kisebb, kevésbé érzékeny projektek esetén az engedélymentes vagy megosztott spektrum is kielégítő lehet.

6 Infrastrukturális követelmények

6.1 Rádiós hozzáférési hálózat (RAN)

A privát 5G hálózatok gerincét a különböző méretű és kapacitású gNodeB (bázisállomás) elemek képezik, amelyek a lefedettségi igényeknek megfelelően telepíthetők – a nagyobb beltéri egységektől a kültéri makrocella-eszközökig. Az antennák lehetnek passzívak vagy aktívak, és mindkét esetben alkalmazzák a MIMO (Multiple Input Multiple Output) technológiát a kapacitás és a jelszilárdság növelése érdekében.

A rájuk érkező adatforgalom továbbításához elengedhetetlen a megfelelő kábelezés és az optikai összeköttetések kiépítése, amelyek biztosítják a bázisállomások közötti zökkenőmentes adatátvitelt, valamint a rádióhálózat és a maghálózat közötti nagysebességű backhaul kapcsolatot.



5. ábra
https://www.researchgate.net/figure/C-RAN-architecture-in-5G-mobile-network_fig1_305805805

6.2 Maghálózat (Core Network)

A privát 5G hálózatok maghálózatát a 5G Core architektúra kulcselemei alkotják, mint az AMF (Access and Mobility Management Function), az SMF (Session Management Function) és az UPF (User Plane Function), amelyek együtt biztosítják a felhasználói kapcsolatok kezelését, az ülések menedzselését és az adatforgalom irányítását.

Ezek a maghálózati funkciók általában virtualizált infrastruktúrán futnak – nagy teljesítményű szervereken, skálázható tárolókon és rugalmas hálózati eszközökön –, így könnyen méretezhetők és gyorsan telepíthetők.

A rendszer működését és karbantartását szoftveres komponensek támogatják: hálózatmenedzsment-platformok, valós idejű monitorozó eszközök és átfogó biztonsági rendszerek együtt gondoskodnak arról, hogy a privát 5G hálózat megbízható, látható és védett legyen a napi üzemeltetés során.

6.3 Peremhálózati (Edge) infrastruktúra:

A privát 5G hálózatban a Multi Access Edge Computing (MEC) szerverek lehetővé teszik, hogy az adatfeldolgozás és az alkalmazások futtatása közvetlenül a végpontok közelében, helyben történjen, ezzel minimalizálva a hálózati késleltetést.

Ugyanakkor a lokális adattárolás keretében az érzékeny adatok végig a saját infrastruktúrán belül maradnak, biztosítva a maximális adatvédelmet és gyors hozzáférést. Mindezt a privát 5G alacsony késleltetésű kapcsolatai egészítik ki, amelyek garantálják, hogy a felhasználók és eszközök között zajló adatforgalom valós időben, megszakítás nélkül zajlik.

6.4 Végponti eszközök

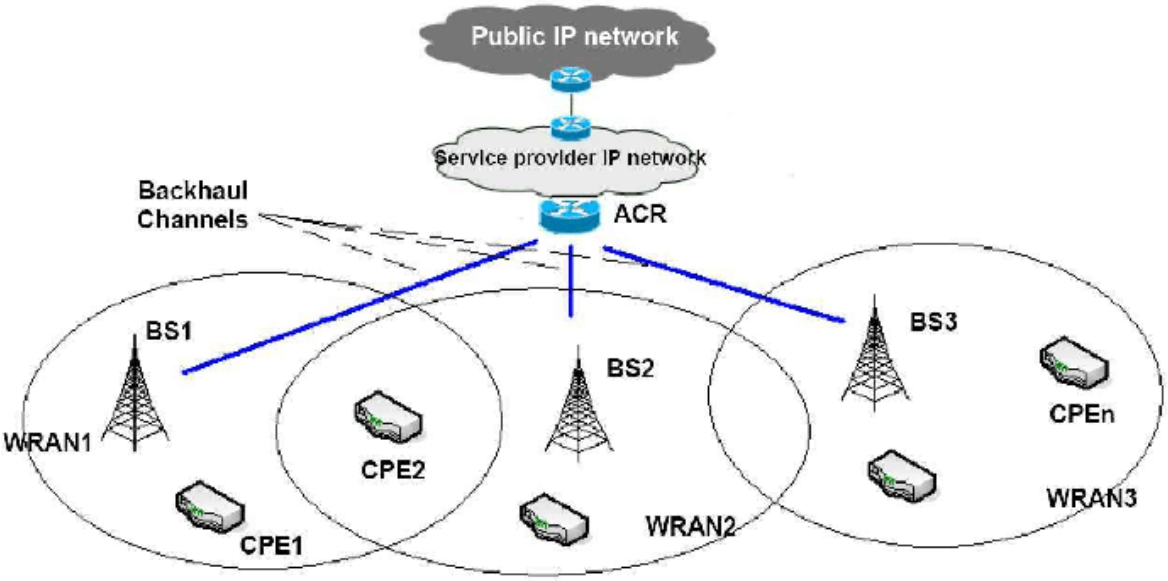
A privát 5G hálózatokban a végponti eszközök ugyanúgy kiemelt szerepet kapnak: az okostelefonok, táblagépek és ipari terminálok mellett egyre több IoT-szenzor és –aktuátor is 5G-modulokkal szerelve csatlakozik a hálózathoz, lehetővé téve a valós idejű adatgyűjtést és vezérlést.

Ezen felül speciális, nagy teljesítményt igénylő eszközök – például AR/VR headsetek, ipari robotok és autonóm járművek – is kihasználják az 5G alacsony késleltetését és nagy sávszélességét, hogy megbízhatóan és biztonságosan működjenek kritikus alkalmazásokban.

6.5 Backhauling infrastruktúra

A privát 5G hálózatok kialakításánál elengedhetetlen, hogy az optikai gerinchálózat biztosítsa a nagysebességű, alacsony késleltetésű összeköttetést a külvilággal. A magas rendelkezésre állás érdekében több, redundáns vonalon keresztül kell csatlakozni, míg a különböző forgalomtípusok zökkenőmentes együttműködését és az üzleti kritikus alkalmazások prioritását Quality of Service (QoS) mechanizmusok garantálják.

Az infrastruktúra méretezése és komplexitása azonban erősen függ a lefedettségi területtől, a csatlakoztatott felhasználók és eszközök számától, valamint a szolgáltatási követelményektől: míg kisebb telephelyeken néhány kompakt bázisállomás és egy egyszerűsített maghálózat is elegendő lehet, nagy ipari komplexumokban többrétegű, redundáns elemekből álló, skálázható rendszer kiépítése válik szükségessé.



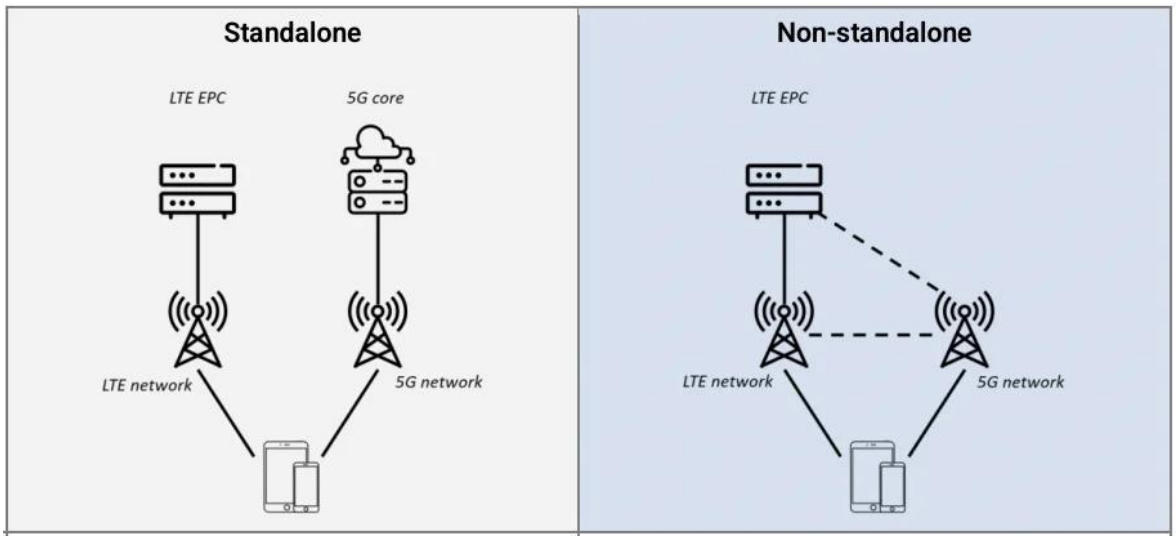
6. ábra
https://www.researchgate.net/figure/A-backhaul-infrastructure-for-80222-WRANs_fig7_221441713

7 Hálózattervezési modellek

7.1 Teljesen önálló (standalone) modell

A teljesen önálló privát 5G hálózat esetén minden egyes komponens a rádiós hozzáférési hálózat (RAN), a maghálózat és a menedzsment rendszerek is – helyben kerül telepítésre és üzemeltetésre, így a vállalat teljes autonómiát és kontrollt gyakorolhat a hálózat felett.

Ez a megközelítés a legmagasabb szintű adatvédelmet és biztonságot biztosítja, amit különösen érzékeny adatokat kezelő szervezetek például védelmi vállalatok vagy kutatóintézetek értékelnek, ugyanakkor számolni kell a nagyobb kezdeti beruházási igénnyel és az összetettebb üzemeltetési feladatokkal is.



7. ábra
https://www.researchgate.net/figure/A-backhaul-infrastructure-for-80222-WRANs_fig7_221441713

7.2 Hibrid modell

A hibrid privát 5G megközelítésben a hálózat kritikus elemei – például a rádiós hozzáférési hálózat (RAN) és a User Plane funkciói – helyben kerülnek telepítésre, míg egyes maghálózati szolgáltatások a felhőben vagy szolgáltatói környezetben futnak.

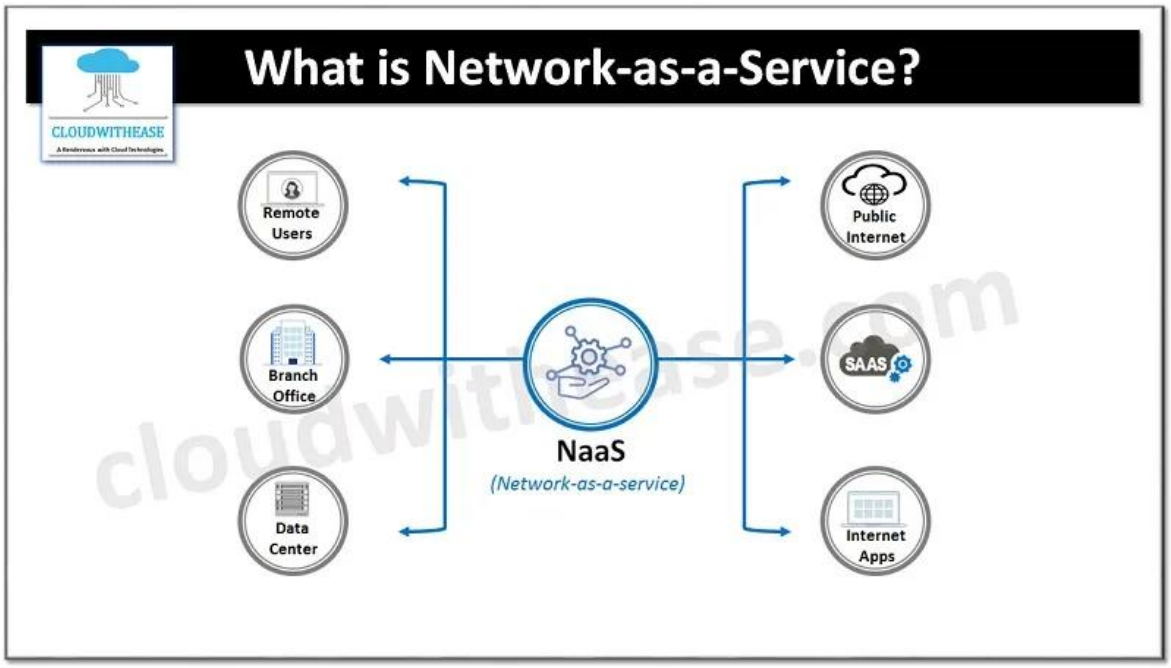
Ez a felépítés optimális egyensúlyt teremt a vállalat tulajdonosi kontrollja és a hálózat üzemeltetési komplexitása között, hiszen nem kell minden funkciót saját infrastruktúrán kezelni, ugyanakkor a legérzékenyebb adatforgalom és felhasználói műveletek helyben maradhatnak. A mérsékelt kezdeti beruházási igény lehetővé teszi, hogy a szervezetek gyorsabban indíthassák el a privát 5G-t, miközben a skálázhatóság és rugalmasság megmarad.

Ez a megoldás különösen jól illeszkedik gyártóüzemek, logisztikai központok és más olyan környezetek igényeihez, ahol a teljesítmény és a költséghatékonyság egyaránt kulcsfontosságú.

7.3 Network-as-a-Service (NaaS) modell

A teljesen menedzselt privát 5G megoldás esetén a szolgáltató biztosítja és üzemelteti az egész hálózati infrastruktúrát, előfizetés-alapú fizetési modell mellett, így a kezdeti beruházási költségek minimálisra csökkennek.

Ennek köszönhetően a hálózat gyorsan kiépíthető és egyszerűen skálázható is, ugyanakkor a testre szabási lehetőségek korlátozottak. Ez a konstrukció különösen vonzó lehet kis- és középvállalatok, valamint ideiglenes telephelyek számára, ahol a gyors üzembe állás és az alacsony belépési küszöb az elsődleges szempont.



8. ábra
https://cloudwithease.com/what-is-naas-network-as-a-service/

7.4 Megosztott infrastruktúra modell

Több vállalat közös privát 5G-infrastruktúrája – például egy ipari parkban – lehetővé teszi a költségek megosztását és az erőforrások hatékonyabb kihasználását, miközben a résztvevők közös irányítással, előzetes megállapodások alapján konfigurálják a hálózat paramétereit. Ilyen megosztott modell különösen előnyös technológiai klaszterek vagy ipari parkok esetében, ahol a tagvállalatok hasonló igényekkel rendelkeznek, de egyedileg túl költséges lenne a teljes infrastruktúra kiépítése.

A privát 5G-megoldások bevezetésekor azonban minden szervezetnek alaposan mérlegelnie kell a biztonsági követelményeket, a rendelkezésre álló költségvetést, a szakértelmet, a rugalmassági igényeket és a hosszú távú stratégiát. Gyakran a fokozatos bevezetés hozza a legnagyobb előnyt: először egy kisebb, korlátozott funkciókészletű hálózattal érdemes kezdeni, majd lépésről lépésre bővíteni a lefedettséget és a képességeket.

8 Szabályozási és engedélyezési folyamatok

8.1 Spektrumhasználati engedélyek

Az 5G spektrumhoz való hozzáférés jelentősen eltérő lehet országonként: egyes államok dedikált frekvenciasávokat különítenek el, amelyekre formális pályázati vagy licenckérési eljárás keretében lehet licencet szerezni, míg más területeken megosztott spektrummodellek például az Egyesült Államok CBRS-sávja – használata esetén Spektrumhozzáférési Rendszerekhez (SAS) kell csatlakozni a szabályozott, priorizált hozzáférés érdekében.

Még az engedélymentes sávokban (például 5 GHz-en vagy 6 GHz-en) való működéskor is előírások szabályozzák a maximális kimenő teljesítményt és az interferencia minimalizálását, így a spektrumválasztás során mind a technikai, mind a szabályozási követelményeket, továbbá a várt teljesítményt és a működési környezetet is figyelembe kell venni.

8.2 Telepítési engedélyek

A privát 5G hálózatok telepítése során számos jogi és szabályozási követelményt kell teljesíteni: a bázisállomások és antennák kihelyezéséhez építési és környezetvédelmi engedélyek beszerzése szükséges, míg védett épületek vagy területek esetén további, speciális jóváhagyásokra is lehet szükség.

Emellett minden esetben igazolni kell, hogy a létesítmény megfelel az elektromágneses sugárzásra vonatkozó határértékeknek, és nem veszélyezteti a környezetet vagy az emberi egészséget.

8.3 Berendezések megfelelősége

A privát 5G hálózatok rádiós és hálózati eszközeinek minden esetben meg kell felelniük az adott régióra vonatkozó előírásoknak és tanúsítványoknak Európában például a CE-jelölés, az Egyesült Államokban pedig az FCC-engedély a mérvadó, továbbá bizonyos, szigorúbb minőség- és biztonsági követelményeket támasztó ágazatokban (például a gyógyszergyártásban vagy az élelmiszeriparban) további iparági szabványoknak is meg kell felelniük.

8.4 Adatvédelmi és biztonsági előírások

A privát 5G hálózatok üzemeltetése során az adatkezelésre és kiberbiztonságra vonatkozó előírások betartása elengedhetetlen. Európában a hálózatoknak szigorúan meg kell felelniük a GDPR követelményeinek, amelyek a személyes adatok gyűjtésének, tárolásának és feldolgozásának minden fázisát szabályozzák, míg más régiókban hasonló adatvédelmi törvények – például az amerikai CCPA vagy Ázsiában a PDPA – írják elő a megfelelőséget.

Az egyes iparágak speciális előírásai tovább növelik a komplexitást: az egészségügyi alkalmazásoknál a HIPAA garantálja a betegadatok védelmét, a pénzügyi tranzakciók esetén pedig a PCI DSS szabvány felügyeli a kártyaadatok biztonságát. Emellett a kritikus infrastruktúrákat üzemeltető szervezeteknek például energiatermelőknek vagy közműveknek az iparág-specifikus kiberbiztonsági követelményeket (például az NIS2 irányelvet vagy az amerikai CISA ajánlásait) is teljesíteniük kell, biztosítva a hálózat folytonosságát és a szolgáltatások magas rendelkezésre állását.

8.5 Nemzetbiztonsági szempontok

Bizonyos országokban a privát 5G hálózatokat nemzetbiztonsági szempontból is átvilágíthatják, és előfordulhat, hogy csak meghatározott gyártók eszközei használhatók, illetve a titkosítási megoldásokra is külön jogszabályi előírások vagy korlátozások vonatkoznak.

Mivel az engedélyezési folyamat különösen a spektrumlicencek megszerzése hónapokig is eltarthat, már a tervezés során érdemes egyeztetni a releváns hatóságokkal és szakértőkkel. Ráadásul a szabályozási környezet folyamatosan alakul, ahogy egyre több ország dolgozza ki a privát 5G hálózatokra vonatkozó keretrendszereit, ezért a helyi előírások rendszeres nyomon követése elengedhetetlen.

9 Kihívások és korlátok

9.1 Kezdeti beruházási költségek

A privát 5G hálózatok kiépítése jelentős kezdeti beruházási költséget igényel, amelynek fő tételei közé tartoznak a rádiós infrastruktúra hardverkomponensei (bázisállomások, antennák, maghálózati elemek, szerverek és kábelezés), a hálózat működését és felügyeletét biztosító szoftverek (menedzsmentplatformok, biztonsági megoldások és speciális alkalmazások), valamint a dedikált spektrumlicencek díjai, amelyek egyszeri vagy rendszeres fizetési kötelezettséget jelentenek.

A telepítés során mérnöki munka, helyszíni felmérések, az elektromos hálózat bővítése és építészeti módosítások is növelik a költségeket, miközben a meglévő rendszerekkel való integráció, a belső folyamatok átalakítása és a szakértői szolgáltatások (tervezés, implementáció, képzés) további kiadásokkal járnak. Egy közepes méretű üzem esetén a teljes beruházás akár több százezer euró is lehet, míg nagyobb létesítményekben gyakran milliós nagyságrendű ráfordításra van szükség, ami különösen a kis- és középvállalatok számára jelenthet belépési korlátot.

A költségek mérséklésére érdemes fokozatos kiépítési stratégiát követni, először a legkritikusabb területeket lefedve, vagy hibrid modellben csak a leglényegesebb komponenseket helyben telepíteni, valamint Network-as-a-Service (NaaS) konstrukciókat alkalmazni, ahol a beruházás előfizetési díjakra oszlik. Emellett érdemes kihasználni a kormányzati támogatásokat és iparági együttműködéseket is.

Az üzleti megtérülés (ROI) alapos elemzése amelybe be kell számítani a termelékenység növekedését, a minőségjavulást, az állásidő csökkenését és az egyéb üzleti előnyöket kulcsfontosságú a költségek indokoltságának és a befektetés hosszú távú értékének megítéléséhez.

9.2 Integrációs nehézségek

A privát 5G hálózatok bevezetésekor a meglévő rendszerekkel való integráció során több nehézség merül fel. A régebbi gyártórendszerek és vezérlők nem mindig kompatibilisek közvetlenül az 5G technológiával, ezért gondos felmérést igényel, hogy mely legacy elemek kerülhetnek hiba nélkül az új hálózatra. Az információs technológiai és az operatív technológiai világ összehangolása számos technikai és szervezési kihívással jár, hiszen ipari környezetben különböző kommunikációs protokollokat és szabványokat kell egyszerre kezelni.

Emellett a meglévő biztonsági infrastruktúrát, a felhasználóazonosítási rendszereket és a hozzáférés-vezérlést is össze kell hangolni a privát 5G-vel, miközben a vezetékes vagy a WiFi hálózatról való zökkenőmentes átállás is gondos menedzsmentet igényel.

Végül a vállalati alkalmazások optimalizálása az új hálózati környezetre szintén

elengedhetetlen ahhoz, hogy a rendszerek a lehető legjobb teljesítményt nyújtsák.

Az integrációs kihívások kezelésére először részletes előzetes felmérés és gondos tervezés javasolt, amely alapján pilot projektek és Proof of Concept fázisok segítségével tesztelhetők a kritikus kapcsolódási pontok. A hálózatot érdemes fokozatosan bevezetni, közben middleware és API rétegekkel kötve össze az új és a meglévő rendszereket. Szakértői partnerek bevonása is hatékony módszer, hiszen olyan csapatokra van szükség, amelyek egyszerre értenek az 5G technológiához és az iparági rendszerekhez.

Hosszabb távon pedig érdemes olyan új gépeket és szoftvereket választani, amelyek már a tervezés során támogatják az 5G-t, ezzel egyszerűsítve a jövőbeni bővítéseket és a teljes körű integrációt.

9.3 Szakértelem hiánya

A privát 5G hálózatok tervezéséhez kiépítéséhez és üzemeltetéséhez olyan speciális tudásra van szükség, amely sok vállalatnál még nem áll rendelkezésre. Elengedhetetlenek a rádiótechnikai ismeretek a maghálózati architektúra és a frekvenciatervezés területén, továbbá a hálózatbiztonsági szakértelem, amely kiterjed az 5G specifikus titkosítási és hitelesítési kihívásokra.

A sikeres megvalósításhoz szükség van az információtechnológiai és az operatív technológiai rendszerek összehangolására, valamint az iparági alkalmazások fejlesztésére vonatkozó tapasztalatokra, hogy az 5G képességeit maximálisan ki lehessen használni.

A spektrummenedzsment terén szabályozási és műszaki tudásra van szükség a frekvenciák hatékony használatához, végül pedig folyamatos üzemeltetési szakértelemre van szükség a hálózat monitorozásához karbantartásához és optimalizálásához. A hiányzó kompetenciák pótlására a vállalatok támogathatják a meglévő IT és hálózati szakemberek 5G képzéseit, létrehozhatnak partnerkapcsolatokat technológiai beszállítókkal rendszerintegrátorokkal és tanácsadókkal, valamint igénybe vehetnek menedzselt szolgáltatásokat ahol a hálózat egy része vagy egésze külső szakértő kezében van.

Hasznos továbbá a tudásmegosztási kezdeményezésekben való részvétel iparági konzorciumokban és fórumokon, valamint az akadémiai együttműködések kiépítése egyetemekkel és kutatóintézetekkel az innovációs kapacitás bővítése érdekében. Középtávon a privát 5G szakértelem szélesebb körben elérhetővé válik, de addig is a legtöbb szervezet számára a belső kapacitásfejlesztés és a külső szakértők bevonása együttes alkalmazása jelenti a leghatékonyabb megoldást.

9.4 Biztonsági kockázatok

A privát 5G hálózatok alapvetően biztonságosabbak a nyilvános mobilhálózatoknál, ugyanakkor számos specifikus kihívással kell szembenézniük. Az 5G architektúra új komponenseket és interfészeket vezet be, amelyek növelik a kibertámadási felületet, miközben a virtualizált hálózati funkciók és konténerizált alkalmazások további biztonsági kockázatokat hordoznak.

A hálózati szeletelés mechanizmusai sérülékeny pontokat jelenthetnek, amelyek szelet-közti támadásokhoz adnak lehetőséget. A nagyszámú, gyakran korlátozott biztonsági képességekkel rendelkező IoT-eszközök jelentős kockázatot képviselnek, akárcsak az insider fenyegetések és a beszállítói láncban rejlő problémák, amelyek a hálózati berendezések és szoftverek eredetével és integritásával kapcsolatosak. Ráadásul a zero-day sebezhetőségek, azaz a korábban ismeretlen és ezért még nem javított biztonsági hibák is folyamatos fenyegetést jelentenek.

A kockázatok kezelésére a biztonságot már a tervezési fázisban érdemes beépíteni, alkalmazva a security by design elvét, és minden hozzáférést folyamatosan ellenőrizni a zero trust architektúra szabályai szerint. Többrétegű védelmi modellt kell kialakítani, többszörös védelmi vonalakkal a hálózat különböző szintjein, és rendszeresen végrehajtani biztonsági auditokat, valamint penetrációs teszteket a gyengeségek proaktív feltárására. A folyamatos monitorozás, anomália-detekció és fejlett SIEM rendszerek alkalmazása lehetővé teszi a biztonsági események gyors felderítését és kezelését.

Fontos, hogy minden komponens frissítési és javítási stratégiája naprakész legyen, és a rendszeres biztonsági tudatosság-fejlesztés során a felhasználók és üzemeltetők is elsajátítsák a fenyegetések felismerésének és kezelésének legjobb gyakorlatait. A privát 5G biztonsága folyamatosan fejlődik, ezért a stratégia rendszeres felülvizsgálata és az iparági legjobb gyakorlatok követése elengedhetetlen a változó fenyegetési környezethez való alkalmazkodáshoz.

10 Jövőbeli trendek és fejlődési irányok

10.1 5G-Advanced és 6G felé

A 5G technológia következő evolúciós lépcsője az úgynevezett 5G-Advanced, amely a 3GPP Release 17-18 szabványfázisokban számos olyan újítást hoz, amelyek a privát hálózatok teljesítményét és képességeit is tovább emelik. A késleltetés akár 0,5 milliszekundumra csökken, a megbízhatóság eléri a 99,9999 százalékot, miközben a spektrumhatékonyság javul és a hálózati szeletelés képességei is tovább fejlődnek. A mesterséges intelligencia és a gépi tanulás mélyebb integrációja a hálózati működésbe lehetővé teszi az önoptimalizáló folyamatokat, a helymeghatározás pontossága pedig centiméteres szintre javul.

A 2030 körül várható 6G generáció a terrahertz frekvenciasávok alkalmazásával akár 1 terrabit per másodperces elméleti adatátviteli sebességet is kínál majd, gyakorlatilag nulla késleltetés mellett. A tervezett fejlődés során a kommunikáció és az érzékelés integrálódik, megjelenik a holografikus adatátvitel, a kvantumkommunikációs elemekkel fokozottan védett átviteli csatornák jönnek létre, és az egész hálózat autonóm működésre kerül.

Ezek az előre lepések olyan új alkalmazási lehetőségeket nyitnak meg a privát hálózatok számára, amelyek ma még a jelenlegi 5G kereteit is jócskán túllépik. Elképzelhető teljesen önálló gyártórendszer, amely emberi beavatkozás nélkül végzi a termelést, haptikus távvezérlés bonyolult műtétek vagy veszélyes munkakörnyezetek esetén, valós idejű digitális érzékelés és környezeti modellezés, valamint a kvantumtitkosítással védett ultrabiztonságos kommunikáció, amely új szintre emeli az adatvédelem és az üzembiztonság kombinációját.

10.2 Edge computing és AI integráció

Az edge computing és a mesterséges intelligencia privát 5G hálózatokba való szoros integrálása forradalmi változásokat hoz majd. Az edge AI keretében az MI algoritmusok már a hálózat peremén futnak, így valós időben, központi felhő nélkül hozhatók meg döntések. A peremeszközökön megvalósított fejlett gépi látás és mintafelismerés lehetővé teszi a prediktív karbantartást és az anomáliadetekciót minimális késleltetéssel, miközben az algoritmusok folyamatosan tanulnak és alkalmazkodnak a helyi környezethez.

A federated learning modellek segítségével az adatokat helyben, a peremeszközökön kezelik, így a nyers adatok nem hagyják el a saját domaint, ami fokozza az adatvédelmet és csökkenti a központosított adattárolási igényt. Ez a kollaboratív tanulási megközelítés lehetővé teszi személyre szabott és kontextus specifikus MI-megoldások kialakítását anélkül, hogy óriási adatforgalom terhelné a maghálózatot.

Az autonóm hálózatmenedzsment keretében a privát 5G hálózatok önoptimalizálóvá válnak: a rendszer automatikusan észleli és javítja a hibákat, erőforrásokat oszt ki a proaktív kapacitástervezés alapján, és folyamatosan optimalizálja az energiafelhasználást a forgalmi minták függvényében. Mindenhez emberi beavatkozásra csak a kivételesesetekben van szükség.

Ezek a fejlesztések jelentősen mérséklik a hálózatok üzemeltetési költségeit és komplexitását, miközben új képességeket nyitnak meg olyan kritikus környezetekben, mint az autonóm járművek, az ipari robotika és a fejlett biztonsági rendszerek, ahol a valós idejű adatfeldolgozás létfontosságú.

10.3 Ipari ökoszisztémák fejlődése

A privát 5G ökoszisztéma dinamikus fejlődése számos új lehetőséget teremt az implementáció terén. Az O-RAN (Open Radio Access Network) szabványosított, nyílt interfészei és protokolljai révén egyre nagyobb rugalmasságot kapunk különböző gyártók rádiós komponenseinek kombinálásában, ami a verseny felerősödésével és költségcsökkenéssel jár, miközben innovatívabb megoldások jelennek meg a diverzifikált beszállítói bázisnak köszönhetően.

Egyre inkább előtérbe kerülnek az iparág-specifikus 5G csomagok, amelyek célhardvereket és szoftvereket tartalmaznak konkrét felhasználási esetekhez, valamint a vertikális integrációk, amikor például a gyártási rendszerek közvetlenül támogatják a 5G-t.

Ugyanakkor új üzleti modellek is kialakulnak: terjednek a 5G-as-a-Service konstrukciók, létrejönnek iparági konzorciumok a közös privát 5G infrastruktúra fejlesztésére, és megjelennek a hibrid tulajdonosi formák, ahol a vállalatok és a mobilszolgáltatók szoros együttműködésben üzemeltetik a hálózatot.

A semleges hostok új piaci szereplőkként több vállalat számára kínálnak privát 5G kapacitást. A hardverinnovációk közé tartoznak az energiahatékonyabb, kompaktabb bázisállomások és a plug-and-play jellegű rendszerek, amelyek gyors telepítést tesznek lehetővé, míg a szoftverizált és virtualizált komponensek elterjedése egyszerűsíti a hálózatkezelést. A beépített biztonsági megoldások révén pedig a privát 5G rendszerek megbízhatósága is folyamatosan nő, csökkentve a belépési korlátokat és lehetővé téve, hogy a kisebb szervezetek is élvezhessék a technológia előnyeit.

11 Összegzés és következtetések

A privát 5G hálózatok kiépítése forradalmi lehetőséget kínál a vállalatok és intézmények számára, hogy egy dedikált, magas teljesítményű, biztonságos és rugalmas kommunikációs infrastruktúrát hozzanak létre, amely teljesen az egyedi igényeikhez igazodik. Amint a dolgozatban bemutattuk, ezek a hálózatok számos előnyt kínálnak a hagyományos vezetékes és vezeték nélküli megoldásokkal szemben, különösen az olyan kritikus területeken, mint a nagy adatátviteli sebesség, az alacsony késleltetés, a masszív eszközkapcsolat, a fokozott biztonság és a testreszabhatóság.

Az iparági alkalmazások széles skálája bizonyítja, hogy a privát 5G technológia nem csupán elméleti koncepció, hanem már jelenleg is értékteremtő megoldás számos szektorban. A gyártóipar, a logisztika, az egészségügy és az intelligens városok területén bemutatott esettanulmányok szemléltetik a kézzelfogható üzleti előnyöket és a transzformatív hatást, amelyet ezek a hálózatok biztosíthatnak.

Ugyanakkor fontos figyelembe venni a kihívásokat és korlátokat is. A jelentős kezdeti beruházási költségek, az integrációs nehézségek, a szakértelem hiánya és a biztonsági kockázatok mind olyan tényezők, amelyeket gondosan mérlegelni kell a tervezési fázisban. A sikeres implementáció kulcsa a megfelelő hálózattervezési modell kiválasztása, a szabályozási követelmények alapos megértése, és a fokozatos, jól megtervezett bevezetési stratégia.

A jövőbeli trendek azt mutatják, hogy a privát 5G technológia folyamatosan fejlődni fog, integrálódva az edge computing, a mesterséges intelligencia és az iparág-specifikus megoldások ökoszisztémájába. Az 5G-Advanced és később a 6G technológiák megjelenése további lehetőségeket nyit majd meg, miközben az ipari ökoszisztéma fejlődése várhatóan csökkenti a belépési korlátokat és bővíti az elérhető megoldások körét.

Összességében a privát 5G hálózatok kiépítése stratégiai jelentőségű döntés, amely messze túlmutat egy egyszerű technológiai választáson. Ez a digitális transzformáció alapinfrastruktúrájának megteremtéséről szól, amely képes támogatni a jövő intelligens műveleti környezetét és üzleti modelljeit. A szervezeteknek érdemes már most elkezdeniük az 5G stratégiájuk kidolgozását, akár fokozatos bevezetéssel, akár pilot projektekkel, hogy felkészülhessenek a technológia által kínált lehetőségek kihasználására és versenyelőny megszerzésére a digitális gazdaságban.

Források

[1] T. Cinkler, L. Simon, R. Szabó, A. Székely, és L. Jakab, „5G hálózatok architektúrája”, *Híradástechnika*, sz. 1, o. 22–29, 2016.

[2] EU4Digital, „5G private networks development”. 2024. [Online]. Elérhető: https://eufordigital.eu/wp-content/uploads/2024/03/EU4D-Telecom-Rules-Report-on-5G-private-network-development.pdf

[3] E. Számvevőszék, „5G roll-out in the EU”. 2022. [Online]. Elérhető: https://www.eca.europa.eu/lists/ecadocuments/sr22_03/sr_security-5g-networks_hu.pdf

[4] M. Tudomány, „5G-mobilrendszer”. 2021. [Online]. Elérhető: https://mersz.hu/magyar-tudomany-202106/

[5] A. Unknown, „A Fully Open-Source End-to-End Private 5G Network Operating in a Globally Unlicensed Frequency Band”, *arXiv preprint arXiv:2407.20652*, 2024, [Online]. Elérhető: https://arxiv.org/abs/2407.20652

[6] L. Blog, „A kapcsolódás átalakítása: hogyan változtatják meg a magán 5G hálózatok a brit vállalkozásokat?” 2024. [Online]. Elérhető: https://blog.lebara.co.uk/hu/a-csatlakoztathatosag-atalakitasa-hogyan-valtoztatjak-meg-a-magan-5g-halozatok-a-brit-vallalkozasokat/

[7] S. K. Sharma, X. Wang, és X. Li, „A Survey on the Past, Present, and Future of Private Networks: Device Ecosystem, Use Cases, Architecture, Spectrum, and Deployment”, *arXiv preprint arXiv:2408.03817*, 2024, [Online]. Elérhető: https://arxiv.org/abs/2408.03817

[8] HTE, „Az 5G magánhálózatok technológiája és alkalmazásai”. 2023. [Online]. Elérhető: https://www.hte.hu/documents/10180/0/5G+mag%C3%A1nh%C3%A1l%C3%B3zatok.pdf

[9] M. REAL, „Az 5G- technológia jellemzői és a kialakításában rejlő kihívások”. 2023. [Online]. Elérhető: https://real.mtak.hu/175140/1/1155_%C3%9Aj%20t%C3%ADpus%C3%BA%20kih%C3%ADv%C3%A1sok%20az%20infokommunik%C3%A1ci%C3%B3ba-52-98.pdf

[10] HVG, „Működik Magyarország első ipari 5G-magánhálózata”. 2021. [Online]. Elérhető: https://hvg.hu/tudomany/20210610_5g_maganhalozat_mobilkommunikacio

[11] B. Insight, „Over 4700 private LTE/5G networks deployed globally by end of 2024”. 2024. [Online]. Elérhető: https://www.iot-now.com/2024/12/06/148416-over-4700-private-lte-5g-networks-deployed-globally-by-end-of-2024/

[12] I. C. S. Blog, „Privát 5G hálózatok kiberbiztonsága”. 2024. [Online]. Elérhető: https://icscybersec.blog.hu/2024/02/17/privat-5g-halozatok-biztonsaga

[13] I. C. T. Global, „Privát 5G hálózatok: üzleti érték, szabályozás, jövő”. 2023. [Online]. Elérhető: https://ictglobal.hu/cikk/privat-5g-halozatok-uzleti-ertek-szabalyozas-jovo

[14] I. C. T. Global, „Privát mobilhálózat: a gazdaság láthatatlan szuperereje”. 2025. [Online]. Elérhető: https://ictglobal.hu/print/privat-mobilhalozat-a-gazdasag-lathatatlan-szuperereje/

[15] PrivateLTEand5G.com, „Private 5G Market Report 2024: Global Trends Unveiled”. 2024. [Online]. Elérhető: https://www.privatelteand5g.com/reports/2024-private5g-market-report/

[16] R. Nester, „Private 5G Network Market Growth | $311.35 billion by 2037 with CAGR 44.5%”. 2025. [Online]. Elérhető: https://www.researchnester.com/reports/private-5g-network-market/5654
[17] Research és Markets, „Private 5G Network Market Report and Forecast 2024-2032”. 2024. [Online]. Elérhető: https://www.researchandmarkets.com/reports/5944431/private-5g-network-market-report-forecast
[18] A. Mason, „Private 5G networks are emerging in sectors beyond manufacturing and transport”. 2023. [Online]. Elérhető: https://www.analysysmason.com/research/content/articles/private-networks-sectors-rma17/
[19] S. T. & IT, „Private 5G Networks: 2024 – 2030”. 2023. [Online]. Elérhető: https://www.snstelecom.com/private5g
[20] M. Wen *és mtsai.*, „Private 5G Networks: Concepts, Architectures, and Research Landscape”, *IEEE Journal on Selected Topics in Signal Processing*, köt. 16, sz. 1, o. 7–25, 2022, doi: 10.1109/JSTSP.2021.3137669.
[21] A. Unknown, „Real-Time Monitoring of Private 5G Networks to Educate Future Engineers”, *SSRN*, 2023, [Online]. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4471402
[22] I. Analytics, „State of private 5G in 2024: Key growth trends, use cases, and forecast”. 2024. [Online]. Elérhető: https://iot-analytics.com/private-5g-2024-key-growth-trends-use-cases-forecast/
[23] D. S. & A. Networks, „Success in Private Networks Through Multi-Vendor Open Infrastructure”. 2022. [Online]. Elérhető: https://druidsoftware.com/wp-content/uploads/2023/09/Success-in-Private-Networks-through-Multi-vendor-Open-Infrastructure.pdf
[24] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, és J. Folgueira, „The Use of 5G Non-Public Networks for Industry 4.0”, *IEEE Communications Magazine*, köt. 57, sz. 8, o. 28–33, 2019, doi: 10.1109/MCOM.2019.1800879.
[25] GlobeNewswire, „U.S. Private 5G Networks Market Forecast 2024-2030: Key Trends, Industry Insights, and Growth Opportunities”. 2025. [Online]. Elérhető: https://www.globenewswire.com/news-release/2025/01/23/3014025/28124/en/U-S-Private-5G-Networks-Market-Forecast-2024-2030-Key-Trends-Industry-Insights-and-Growth-Opportunities-A-3-7-Billion-Growth-Opportunity.html

Ábrajegyzék

1. ábra 5
2. ábra https://blog.viavisolutions.com/2017/08/22/network-slicing-enabling-the-5g-future/ 8
3. ábra https://prohardver.hu/tudastar/qos_quality_of_service.html 11
4. ábra https://www.pannondoktor.hu/2023/12/kiterjesztett-valosagot-alkalmazo-orvosi-eszkoz-fejlesztett-a-zmed-a-hun-ren-sztaki-es-a-pte/ 13
5. ábra https://www.researchgate.net/figure/C-RAN-architecture-in-5G-mobile-network_fig1_305805805 20
6. ábra https://www.researchgate.net/figure/A-backhaul-infrastructure-for-80222-WRANs_fig7_221441713 22
7. ábra https://www.researchgate.net/figure/A-backhaul-infrastructure-for-80222-WRANs_fig7_221441713 23
8. ábra https://cloudwithease.com/what-is-naas-network-as-a-service/ 24

2.30. Az ipar kezdetei – Ókori Egyiptom Ha az iparról beszélünk a történelem kezdeti időszakaiban, akkor Egyiptom az egyik legkorábbi civilizáció, ahol már egész jól szervezett és sokféle „ipari tevékenység” zajlott – persze nem abban az

Oskar Schinfler hatása az iparra

Az ipar kezdetei – Ókori Egyiptom

Ha az iparról beszélünk a történelem kezdeti időszakaiban, akkor Egyiptom az egyik legkorábbi civilizáció, ahol már egész jól szervezett és sokféle „ipari tevékenység” zajlott – persze nem abban az értelemben, ahogy ma gondolunk az iparra, hanem sokkal inkább kézműves- és állami termelési formákban.

1. Építőipar – a korai „ipari nagyüzem”

Talán a legismertebb egyiptomi ipari tevékenység a **kőépítészet**, gondoljunk csak a piramisokra vagy a monumentális templomokra. Ezekhez hatalmas mennyiségű munkaerőre, szerszámokra és szervezésre volt szükség. Bár nem voltak gépeik, a munkaszervezés és a logisztika már itt megjelent. A kövek szállítása, faragása, a munkások ellátása, a raktározás – mind-mind egyfajta „ipari rendszerként” működött.

2. Fém- és üvegipar

Az egyiptomiak már korán használtak különféle fémeket, mint a **réz, bronz**, később pedig a vas is megjelent. Ezeket fegyverekhez, szerszámokhoz, ékszerekhez használták. Emellett ők voltak az elsők között, akik **üveget** is tudtak előállítani – ez eleinte dísztárgyak, gyöngyök formájában jelent meg.

3. Textilipar

A **lenvászon** készítése komoly iparággá vált. A len termesztése, szálakká fonása, majd szövése szintén jelentős szerepet játszott a gazdaságban, főleg mivel a fehér vászonruha vallási és társadalmi szempontból is fontos volt.

4. Élelmiszer-feldolgozás

Egyiptomban a mezőgazdaság központi szerepet töltött be, de a termények feldolgozása is fontos volt: **sörfőzés, kenyérsütés, halak tartósítása**, stb. Ezek részben a munkásokat ellátó rendszerekhez tartoztak, részben a kereskedelmi csereeszközként is funkcionáltak.

5. Papírgyártás (papirusz)

A **papirusz** készítése volt az egyik legismertebb „egyiptomi találmány”. Ez nemcsak a közigazgatás és az írásbeliség alapját képezte, hanem fontos exportcikk is volt, amiből más civilizációk is profitáltak.

6. Állami szerep

Fontos kiemelni, hogy az egyiptomi ipari tevékenységek döntő többsége **állami irányítás alatt** állt. A fáraó rendszere hierarchikusan irányította a munkát: állami raktárak, központilag szervezett munkaerő, adózás természetben – mindez megteremtette a nagy volumenű termelés és az erőforrás-újraelosztás alapjait.

Az ipar szerepe az ókori Görögországban

1. Kézműves ipar és városi specializáció

Az ókori görög városállamokban (mint Athén, Korinthosz, Spárta) az ipar elsősorban **kisüzemi** kézművesség formájában volt jelen. Voltak városok, amelyek bizonyos termékekre specializálódtak. Például:

Athén híres volt a kerámiáiról – a fekete- és vörösalakos vázák nemcsak esztétikai szempontból voltak fontosak, hanem kereskedelmi cikként is népszerűek voltak a Földközi-tenger térségében.

Korinthosz inkább a bronzmunkáiról, dísztárgyairól és hajóépítéséről volt ismert.

2. Fémmegmunkálás és haditechnika

A bronz- és vasmegmunkálás fejlett volt, főként a fegyvergyártás és a szerszámkészítés miatt. A városállamok közötti állandó konfliktusok és háborúk miatt a hadiipar egyfajta folyamatos háttértevékenységgé vált – bár ezt nem központosított módon, hanem inkább független kovácsok, mesterek végezték.

3. Hajóépítés és tengeri kereskedelem

A görög ipar egyik húzóágazata a hajóépítés volt. Mivel a görög vidék nem volt különösebben gazdag termőföldekben, a tengeri kereskedelem és a kolonizáció révén pótolták a szükséges javakat. Ehhez viszont megbízható hajók kellettek – és ez a hajógyártás technológiai fejlődését is magával hozta.

A triremek – három evezősoros hadihajók – például komoly technológiai újításnak számítottak a korukban, gyorsak és fordulékonyak voltak, és fontos szerepet játszottak például a perzsa háborúkban.

4. Bányászat

A Lavrion-i ezüstbányák Athén közelében fontos gazdasági és ipari szerepet töltöttek be. Az innen származó ezüst fedezte többek között Athén hadiflottájának kiépítését is. A bányászat kemény, veszélyes munka volt, amit leginkább rabszolgák végeztek.

5. Munkaerő és társadalmi háttér

Az ipari munkák döntő részét rabszolgák és felszabadítottak végezték. A szabad polgárok inkább földbirtokosként vagy politikai/társadalmi szereplőként működtek, így a termelés szinte teljes mértékben a nem szabad státuszú emberek vállán nyugodott. Ez megint csak azt mutatja, hogy bár volt ipari jellegű tevékenység, a társadalmi rendszer miatt nem fejlődhetett úgy, mint későbbi korokban.

6. Technológiai gondolkodás

A görögök közül többen (pl. Arkhimédész, Hérón) már a technológiai problémák elméleti megközelítését is elkezdték. Hérón például olyan szerkezeteket tervezett, amelyek gőz erejével működtek – igaz, ezek nem terjedtek el széles körben, de mutatják, hogy a műszaki gondolkodás már itt jelen volt, csak épp a gazdasági és társadalmi környezet nem tette lehetővé az ipari forradalom-szerű fellendülést.

Az ipar szerepe a Római Birodalomban

1. Állami és magánipar – nagyléptékű termelés

A Római Birodalom alatt az ipari tevékenység már nemcsak kis műhelyek szintjén zajlott, hanem nagyüzemi jellegű termelés is megjelent, különösen az állami megrendelésekhez kapcsolódóan. Ezek közé tartoztak:

építőanyag-ipar (téglaégetés, cementgyártás),

hadifelszerelés-gyártás (fegyverek, páncélzatok, sisakok, hadi kocsik),

textilipar (katonai ruházat, sátorvászon),

kerámiagyártás (nagy mennyiségű, szabványosított agyagedények – pl. terra sigillata típusú áruk).

A hadsereg ellátásához masszív ipari háttér kellett, és ennek egy részét központilag irányították.

2. Bányászat és fémmegmunkálás

A rómaiak hatalmas léptékben űzték a bányászatot. A birodalom szerte működtek arany-, ezüst-, vas-, réz- és ólomlelőhelyek – Hispániában, Galliában, Britanniában vagy Dáciában. A bányák munkásait gyakran rabszolgák és hadifoglyok adták, a munka pedig rendkívül veszélyes és embertelen volt.

A bányákból kinyert fémeket aztán kohókban olvasztották és dolgozták fel fegyverekké, pénzérmékké, építkezési elemekké vagy használati tárgyakká. Róma például Európa egyik legnagyobb ólomtermelője volt.

3. Építőipar és mérnöki tudás

A rómaiak mérnöki tevékenysége szinte ipari méretű volt. Az utak, vízvezetékek (aquaeductus), fürdők, amfiteátrumok és más középületek megépítéséhez óriási mennyiségű építőanyagra és munkásra volt szükség. Az építkezéseket a hadsereg is aktívan támogatta (főleg az ún. *legionárius mérnökök*).

Fontos technikai újításuk volt a pozzuolani cement, amivel tartósabb és vízállóbb építményeket tudtak létrehozni – ennek köszönhetően épülhettek például olyan kikötők, amik évszázadokon át fennmaradtak.

4. Mezőgazdasági iparszerű termelés

Bár nem ipar a szó klasszikus értelmében, fontos megemlíteni, hogy a rómaiak hatalmas latifundiumokat (nagybirtokokat) működtettek, ahol rabszolgamunkával folyt az élelmiszer-termelés – szinte ipari mennyiségben. Ezek biztosították az ellátást a városok és a hadsereg számára, és szintén nagy szervezettséget igényeltek.

5. Szállítás, logisztika és kereskedelem

A római ipari és gazdasági rendszer gerincét a kiváló úthálózat és **tengeri szállítás** alkotta. A Via Appia, Via Augusta és társaik lehetővé tették a nyersanyagok, félkész termékek és kész áruk gyors eljuttatását a Birodalom egyik végéből a másikba.

A központok – mint Róma, Alexandria, Epheszosz – nemcsak politikai, hanem ipari és kereskedelmi központok is voltak.

6. Munkaerő és társadalmi háttér

Mint az előző korszakokban, itt is a rabszolgamunka dominált az ipari termelésben. A rabszolgák gyakran nagy csoportokban, kegyetlen körülmények között dolgoztak a bányákban, műhelyekben vagy hajógyárakban. Voltak ugyanakkor felszabadítottak is, akik később saját vállalkozásokat indítottak, különösen a kereskedelemben és kézművességben.

A középkor ipara – az átalakulás és lassú fejlődés kora

1. A kora középkor (kb. 5–10. század): visszaesés és önellátás

A Római Birodalom bukása után Európában az ipar visszaesett. A korábbi, központosított és szervezett ipari struktúrák szétestek, a városok elnéptelenedtek, és a társadalom újra a földesúri birtokokon alapuló önellátásra rendezkedett be.

Az ipari tevékenységek jórészt uradalmi keretek között folytak: kovács, molnár, takács, fazekas a földesúri birtokon dolgozott.

A mezőgazdaság uralta a gazdaságot, és kevésbé volt szükség nagy mennyiségű árucikk előállítására.

Az emberek leginkább helyi szinten termeltek mindent, amit használtak.

2. A virágzó középkor (kb. 11–13. század): városfejlődés és kézművesség fellendülése

Ez a korszak már sokkal izgalmasabb ipari szempontból is. A népesség növekedésével, a kereskedelem újraindulásával és a városok kialakulásával újra megjelent az igény a kézműves termékek iránt.

A városok lettek a középkori ipari termelés központjai. Itt jelentek meg a kézműves műhelyek, ahol szabók, kovácsok, cipészek, tímárok, fazekasok és sok más mester dolgozott.

A kézműveseket céhekbe szervezték, amelyek meghatározták a termelés módját, a tanonc- és mesterré válás útját, és gyakran a minőséget is szabályozták.

Megjelentek a specializált ipari központok, például:

Flandriában és Itáliában textilipari központok (gyapjú- és selyemszövés),

Nürnberg és Milánó híres lett a fémművességéről,

Velence és Genova a hajóépítésben és üveggyártásban jeleskedtek.

3. A bányászat és fémipar fellendülése

A középkor második felében újra fellendült a bányászat:

A német területeken (pl. Harz-hegység, Cseh-érchegység) arany-, ezüst-, vas- és rézbányákat nyitottak.

A bányák technikai fejlődése is megindult, például vízkiemelő szerkezetek, csörlők, és a szellőztetés javítására szolgáló eszközök megjelenésével.

A kinyert fémeket azután fegyvergyártásra, páncélkészítésre, érmék verésére és mezőgazdasági szerszámokra használták fel.

4. Vízenergia és malmok – a gépesítés első jelei

A középkorban a vízimalmok elterjedése volt az egyik legnagyobb technikai előrelépés. Ezek nemcsak gabonát őröltek:

léteztek fűrészmalmok, posztóverő malmok, papírmalmok, sőt kalapácsműhelyek is, amelyeket vízenergia hajtott.

Ez már a mechanikus ipar előfutára volt: egyre több munkafolyamatot gépek vettek át az emberi erő helyett.

5. Hadjászati ipar és technikai fejlődés

A középkori ipar egyik mozgatórugója a háborúskodás volt. Az állandó konfliktusok és lovagi hadjáratok miatt megnőtt az igény:

fegyverekre (kardok, nyílvesszők, számszeríjak),

védőfelszerelésekre (páncélok, sisakok),

ostromgépekre (katapultok, faltörő kosok, később ágyúk).

Ezek gyártása szintén a városok iparosaira vagy uralkodói megrendelésre létrehozott műhelyekre hárult.

A kora újkor ipara – az ipari forradalom előszobája

1. Földrajzi felfedezések és gyarmatosítás hatása az iparra

A 15–16. századi nagy földrajzi felfedezések (Kolumbusz, Vasco da Gama, Magellán) alapjaiban változtatták meg a gazdaságot:

Az európai országok (pl. Spanyolország, Portugália, később Anglia, Hollandia, Franciaország) gyarmatokat szereztek, ahonnan aranyat, ezüstöt, fűszereket, cukrot, dohányt, gyapotot, később kávét és kakaót is hoztak be.

Ezek az alapanyagok új lendületet adtak az európai feldolgozóiparnak – különösen az élelmiszer-, textil- és fémipar fejlődött.

2. Manufaktúrák megjelenése – az ipari szervezés előfutára

A középkor céhes kézműipara helyett megjelentek a manufaktúrák:

Ezek nagyobb léptékű termelést tettek lehetővé.

Az alapelv: munkamegosztás és tömegtermelés, de még kézi eszközökkel.

A munkafolyamatokat részekre bontották – minden munkás csak egy részt végzett, így gyorsabban készült el egy termék.

Tipikus példák: textilmanufaktúrák (gyapjú, len, selyem), fegyvergyártás, papírkészítés, üveggyártás.

A manufaktúrák gyakran **állami támogatással** jöttek létre, különösen a merkantilista államokban, ahol az erős gazdaságot nemzeti érdeknek tekintették.

3. Textilipar – a legfontosabb iparág

A korszak legjelentősebb iparága a textilipar volt:

Főleg Angliában, Flandriában, Franciaországban és Itáliában volt erős.

A gyapjúból és gyapotból készült textiltermékek iránti kereslet világszinten megnőtt.

Ez az iparág lesz az ipari forradalom egyik legfontosabb kiindulópontja.

4. Bányászat és kohászat – nyersanyagok új hulláma

A felfedezések után özönlött az amerikai arany és ezüst, de közben Európában is megugrott a **bányászat**:

Németországban, Csehországban, Lengyelországban és Erdélyben új bányák nyíltak, különösen ezüst-, réz- és vaslelőhelyeken.

A kohászat fejlődése lehetővé tette a jobb minőségű fémtárgyak, szerszámok és fegyverek gyártását.

A vas és acél szerepe nőtt, ahogy a hadseregek is egyre több fémeszközt és ágyút használtak.

5. Hadipar – állandó hadseregek, új igények

A középkori lovagság helyét az állandó hadseregek vették át, ami hatalmas igényt teremtett:

egyenruhákra,

fegyverekre (kardok, puskák, ágyúk),

hajókra és lőszerekre.

Ez ipari méretű fegyvergyártást indított el, különösen Franciaországban és Angliában. A hadipar fejlődése mindig húzta magával a bányászatot, fémipart és vegyipart is.

6. Technikai újítások – még kézieszközökkel, de már hatékonyabban

Bár még nem beszélhetünk gépesítésről, sok technikai újítás született:

orsók, szövőszékek új típusai,

hatékonyabb malmok,

egyszerűbb szivattyúk a bányászatban.

Ezek az újítások előkészítették a terepet a gőzgépek és gépi gyártás megjelenéséhez.

Az ipari forradalom kora (kb. 1760–1850)

1. Mi is az ipari forradalom?

Ez nem egy hirtelen esemény volt, hanem egy fokozatos gazdasági és technológiai átalakulás, amely először Angliában kezdődött, majd átterjedt Európa többi részére és Észak-Amerikába. A változások főként az iparban és a mezőgazdaságban jelentek meg.

2. Kulcsfontosságú találmányok és technológiák

Gőzgép (James Watt) – lehetővé tette a gépek hajtását víz vagy állati erő nélkül.

Fonó Jenny, repülő vetélő, mechanikus szövőgép – forradalmasították a textilipart.

Gépgyártás, vasöntés, kohászat – a vas és acélgyártás óriási mértékben megnőtt.

Gőzmozdony és vasút – az áruszállítás és közlekedés gyorsabbá és olcsóbbá vált.

Szén mint energiahordozó – a vízi energia helyett egyre inkább szénnel működtek a gyárak.

3. Fontos iparágak

Textilipar – ez indította be az egész forradalmat, főleg Angliában. A gépesítés itt jelent meg először.

Bányászat – különösen a szén- és vaskitermelés nőtt meg, ezekre nagy szükség volt a gőzgépekhez és gyárakhoz.

Kohászat és fémipar – a gépgyártás, fegyvergyártás, vasútépítés igényei miatt hatalmas fejlődésen mentek át.

Vegyipar – eleinte a textilipar festékei és a szappangyártás, később a robbanóanyagok miatt is erősödött.

4. A gyáripar megszületése

Ez az időszak hozta létre az első modern gyárakat:

Munka már nem otthon vagy kis műhelyekben zajlott, hanem központosított üzemekben.

A munkarend szigorúvá vált, időhöz kötötték – megszületett a gyári munkás fogalma.

A városok rohamosan nőttek, mivel sokan költöztek be dolgozni.

5. Társadalmi hatások

Megjelent egy új társadalmi réteg: a munkásosztály.

A gyári munka nehéz, sokszor veszélyes volt, gyerekek és nők is dolgoztak alacsony bérért.

A kapitalista és tőkés rendszer megerősödött, a gyár- és földtulajdonosok (polgárság) meggazdagodtak.

A munkások körében megindultak az első sztrájkok, munkásmozgalmak, szakszervezetek kialakulása.

6. A mezőgazdaság átalakulása

Az ún. agrárforradalom párhuzamosan zajlott: új földművelési módszerek, gépesítés, vetésforgó.

Ez hatékonyabbá tette a termelést, és kevesebb emberre volt szükség – sokan így kerültek át az iparba.

A második ipari forradalom (kb. 1870–1914)

1. Új energiaforrások: elektromosság, olaj, vegyipar

Elektromosság: A villanymotor, a villanyvilágítás (pl. Edison izzólámpája) és az elektromos hálózat lehetővé tette a gépek rugalmasabb elhelyezését, gyorsabb termelést, és új iparágak létrejöttét.

Kőolaj: Az olajmeghajtású motorok (pl. Otto-motor, majd a dízelmotor) új korszakot nyitottak a közlekedésben és az iparban.

Vegyipar: Megindult a mesterséges anyagok (műtrágya, festék, robbanószerek, gyógyszerek, műanyagok) ipari gyártása.

2. Új iparágak születése

Gépjárműgyártás: Megjelentek az első autók (Benz, Ford), és elindult a tömeggyártás (pl. Ford T-modell).

Elektronika és elektromos ipar: Villamosenergia-termelés, elektromos háztartási eszközök, telefon (Bell), rádió (Marconi) stb.

Acélipar: A Bessemer-eljárás és más technikák révén az acélgyártás olcsóbb és hatékonyabb lett, amit az építőipar (hidak, vasút, felhőkarcolók) és a hadipar is kihasznált.

3. Tömegtermelés és a futószalag

A gyártásban megjelent a futószalagos termelés (Henry Ford), amely drasztikusan lecsökkentette a termékek árát, és lehetővé tette a tömeges fogyasztást.

A gyárak hatékonysága ugrásszerűen megnőtt, és egyre több embert foglalkoztattak.

4. Közlekedés és kommunikáció forradalma

Autók, villamosok, metrórendszerek: Városi közlekedés átalakulása.

Vasút fejlesztése, illetve a hajózásban a gőzhajók és a dízelhajók elterjedése.

Telefon, távíró: az információáramlás villámgyorssá vált, ami segítette a gazdaságot és a tőzsdét is.

5. Társadalmi változások

Városiasodás még intenzívebbé vált, mivel a munkalehetőségek főleg városokhoz kötődtek.

Középosztály megerősödött – a mérnökök, technikusok, irodai dolgozók száma megnőtt.

Munkásvédelem és jogok: a munkások szervezkedni kezdtek, több országban megjelentek a munkásvédelmi törvények (pl. munkaidő-szabályozás, gyermekmunka tiltása).

6. Nemzetközi gazdasági verseny és gyarmati háttér

A második ipari forradalom idején a nagyhatalmak ipari versenybe kezdtek (Anglia, Németország, Franciaország, USA).

A gyarmatok olcsó nyersanyaggal és piacokkal támogatták az európai országok iparának növekedését.

Amikor 1914-ben kitört az első világháború, az ipar szinte egyik napról a másikra átalakult. Az addig békés célokat szolgáló gyárakat – például mezőgazdasági gépeket, járműveket vagy háztartási eszközöket előállító üzemeket – tömegesen állították át haditermelésre. Ez azt jelentette, hogy innentől fegyvereket, lőszereket, katonai járműveket, egyenruhákat és hadi felszerelést kezdtek gyártani.

Főbb változások az iparban:

1. Haditermelésre való gyors átállás

Állami utasításra vagy megrendelésre a gyárak új gépeket telepítettek, vagy a meglévőket alakították át, hogy lőszert, gránátokat, puskákat vagy tankokat tudjanak előállítani.

Sok helyen éjjel-nappal folyt a termelés, hogy ki tudják elégíteni a frontokon harcoló csapatok igényeit.

2. A nők megjelenése az ipari munkában

Mivel a férfiak nagy részét besorozták, rengeteg nő állt munkába a gyárakban, sokan életükben először dolgoztak fizikai munkát.

Ez társadalmi szempontból is jelentős változás volt, mivel a nők egyre nagyobb szerepet kaptak a gazdaságban.

3. Új technológiák és fegyverek gyors fejlesztése

A háborús szükségletek miatt sok új találmány és technológiai újítás született (pl. harckocsik, géppuskák, vegyi fegyverek).

A hadiparban való versenyzés gyorsította az ipari kutatást is.

4. Állami irányítás erősödése

A kormányok közvetlenül beleszóltak a termelésbe: meghatározták, mit kell gyártani, mennyiért, és mennyi nyersanyagot lehet felhasználni.

Az állam gyakran központilag osztotta el az erőforrásokat, így hatékonyabban lehetett kezelni a háborús helyzetet.

5. Közlekedési és logisztikai háttér kiépítése

A vasutak és teherautók szerepe megnőtt, hiszen gyorsan kellett mozgatni az utánpótlást a frontokra.

Az ipari logisztika is fejlődött: hogyan lehet hatékonyan, időre, nagy mennyiségben szállítani fegyvereket vagy ellátmányt.

A háború után az ipar lassan állt vissza a hétköznapi állapotába. Ez köszönhető annak, hogy rengeteg országban káosz uralkodott ami kihatással volt az extrémebb nézetű emberek hatalomra jutásában. Az egyik ilyen volt a német nemzetszocialista párt. Németország annak ellenére, hogy háborút vesztett és rengeteg kártérítést kellet fizetnie viszonylag gyorsan talpra állt mivel amerikai segítséget kaptak ehez.

A Weinmar köztársaság alatt a hiperinfláció mindennapi volt. Az áruk egyiknapról a másikra többszörösbe kerültek. Ilyen környezetben az ipar nehezen állt volna talpra ha nincs külső beavatkozás. Említettem, hogy amerikai segítséget kaptak a németek ennek köszönhetően pedig elégé kötődtek az amerikai gazdasághoz.

1929-ben be ütött a katasztrófa. Összeomlott a New York-i tőzsde és vele együtt rengeteg európai ipar is. Munkanélküliség az egekbe szökött és az extrém ideológiájú emberek ismét alternatívát jelentettek az ehező munkanélküli tömegeknek. Ekkor került hatalomra egy bizonyos Adolf Hitler aki az elején tényleg normális hozzáértő embernek tűnt. Volt baj a fejében de ez egyenlőre megtartotta magának. Alatta kezdett szárnyalni a német ipar újra. Ekkor épült mega z Autobahn amit mai napig használnak a németek. A had ipar is fellendült, a békeszerződés tiltása ellenére. És ekkor törekedett fell egy bizonyos Oskar Schindler is.

Oskar Schindler 1908. április 28-án született az Osztrák–Magyar Monarchia területén, Zwittau nevű kisvárosban, amely ma Csehországban található (cseh nevén Svitavy). A családja német származású volt, és középosztálybeli életet éltek. Apja, Hans Schindler mezőgazdasági gépek és motorok kereskedelmével foglalkozott, anyja, Louisa egy hagyományosabb, vallásos családhoz tartozott, és nagy szerepet játszott Oskar nevelésében.

Gyerekként Schindler egyáltalán nem tűnt ki különösebb tehetséggel – sem tanulásban, sem viselkedésben. Kifejezetten élénk, sőt néha kezelhetetlen gyerek volt. Iskolai évei alatt nem volt kifejezetten jó tanuló, de fiatal korától kezdve látszott, hogy könnyen teremt kapcsolatokat, gyorsan alkalmazkodik, és jól tudja használni a személyes varázsát. Ezek a tulajdonságok később kulcsfontosságúak lettek a túléléséhez – és mások megmentéséhez is.

A húszas éveiben, az első világháború után, Csehszlovákiában élt, ahol sok német anyanyelvű ember – köztük ő és családja is – kisebbségbe került. Az ország ekkor gazdasági és politikai átalakuláson ment keresztül, ami kihívásokkal járt mind a helyi németek, mind a többségi lakosság számára. A fiatal Schindler ebben a helyzetben nemcsak dolgozott, hanem megfigyelte, hogyan működik a gazdaság és a politika – különösen érdekelte, hogy kinek hogyan van hatalma vagy befolyása.

Mivel apja vállalkozása nem ment mindig zökkenőmentesen, Oskar több munkát is kipróbált. Dolgozott értékesítőként, ügynökként, később egy cseh telefoncég alkalmazottja lett. Ezekben az években tanulta meg, hogyan lehet "eladni magát", hogyan kell tárgyalni, és hogyan lehet meggyőzni embereket – ami később a túlélési stratégiáinak része lett. Közben elég mozgalmas életet élt: szerette a társasági eseményeket, az autókat, a motorokat, és nem vetette meg a női társaságot sem.

A harmincas években csatlakozott a német hírszerzéshez (Abwehr), ahol kémtevékenységet folytatott a csehszlovák kormány ellen. Ezért később le is tartóztatták, de rövid idő után elengedték, miután Németország bekebelezte a Szudéta-vidéket. Ekkorra már aktív tagja lett a náci pártnak (NSDAP), de későbbi tettei alapján azt mondhatjuk, hogy ez inkább karrierlépés volt, mint meggyőződés.

Fontos megjegyezni, hogy Schindler fiatalkorában nem volt hős, és nem is feltétlenül „jó emberként” indult. Inkább olyan valaki volt, aki mindig tudta, hogyan kell túlélni, és hogyan kell a rendszert a saját előnyére fordítani. Ami viszont igazán érdekessé teszi őt, az az, hogy egy ilyen háttérrel is képes volt változni, és a későbbiekben olyan döntéseket hozott, amik emberek ezreinek életét mentették meg.

Oskar Schindler vállalkozásának felépítése

Miután Németország 1939-ben lerohanta Lengyelországot, Schindler is követte a német hadsereget Krakkóba, a megszállt területekre. Ekkorra már jól kiismerte magát a rendszerben – voltak pártkapcsolatai, és tudta, hol lehet hasznot húzni egy adott helyzetből. Az egyik ilyen lehetőség a lengyel zsidók vagyonának kisajátítása és az államosított gyárak átvétele volt.

Krakkóban Schindler 1939 végén megszerezte az Emalia nevű zománcozó gyárat, amely korábban egy zsidó tulajdonosé volt. Ez volt az első lépés a vállalkozásának felépítésében. A gyár eredetileg főként edényeket és háztartási eszközöket gyártott, de Schindler hamarosan hadiipari megrendeléseket is el tudott nyerni – például lőszerhüvelyek és egyéb kisebb katonai felszerelések gyártását.

A háborús helyzetben a német hadsereg minden beszállítót örömmel fogadott, főleg ha gyorsan és olcsón dolgoztak. Schindler ebben volt jó: jó kapcsolatokat épített ki a Wehrmacht tisztjeivel és a náci párttal, cserébe megrendeléseket kapott, amitől a gyára egyre jobban ment.

A munkások között eleinte lengyelek is dolgoztak, de Schindler hamar felismerte, hogy a zsidó munkaerő olcsóbb – és könnyebben „szabályozható” a nácik szerint. Ezért kapcsolatba lépett az SS-szel, és megszerezte az engedélyt, hogy zsidó munkásokat alkalmazzon, akiket a helyi gettóból vagy később a plaszówi koncentrációs táborból hoztak a gyárba.

Ekkor viszont valami megváltozott. Schindler nem csak mint „olcsó munkaerőre” tekintett ezekre az emberekre. Lassan személyesen is megismerte őket, együtt élt velük nap mint nap, látta a szenvedésüket, és egyre jobban kezdte védeni őket. A gyár egyre inkább menedékké vált, ahol viszonylag emberi körülmények között dolgozhattak a zsidó munkások, és ahová nem volt könnyű csak úgy „bevinni” őket a haláltáborba.

Vállalkozása tehát papíron egy sikeres hadiipari gyár volt, a valóságban viszont egyre inkább egy fedősztori lett arra, hogy embereket mentsen meg. Schindler rengeteg pénzt költött kenőpénzekre, ajándékokra és luxuscikkekre, hogy a tiszteket maga mellé állítsa, és védje a munkásait. Végül, amikor a háború végéhez közeledtek, és a helyzet egyre veszélyesebb lett, sikerült elérnie, hogy a gyárát átköltöztessék Csehországba, így sok munkást a biztos haláltól mentett meg.

1. A gyárak humanitárius célú átalakítása – az ipar szerepének újraértelmezése

Oskar Schindler egyik legmeghatározóbb hatása az iparra az volt, hogy a náci Németország hadigépezetének részét képező ipari rendszert részben humanitárius célokra kezdte használni. Ez radikálisan eltért attól, ahogyan a korszakban a gyártási kapacitásokat általában alkalmazták – hiszen a legtöbb üzem a háború gépezetét szolgálta ki teljes mértékben. Schindler viszont úgy alakította át

gyárát, hogy az nemcsak a hadiipar számára termelt, hanem menedékként is szolgált a zsidó munkások számára.

A krakkói Deutsche Emailwarenfabrik (más néven: Emalia) nevű zománcáru-gyárban olyan "hasznos munkásokat" alkalmazott, akiket egyébként deportáltak volna koncentrációs táborokba. A hivatalos indoklás szerint ezek az emberek kulcsfontosságúak voltak a háborús termelés szempontjából, de valójában Schindler kifejezetten azért "foglalkoztatta" őket, hogy életben tartsa őket. Ez az átalakított szemlélet, hogy a gyár ne csupán profittermelésre és hadiszolgálatra legyen alkalmas, hanem emberéletek védelmére is, alapjaiban kérdőjelezte meg az ipari funkciók kizárólagos céljait a korszakban.

Ez a hozzáállás a gazdasági racionalitás és a morális felelősségvállalás határán mozgott – Schindler rengeteg pénzt áldozott a megmentett emberek ellátására, étkeztetésére, ruházására, miközben sok esetben szándékosan alultervezte a termelést, hogy ne "tűnjön ki" túl hatékony gyárként a náci rendszer szemében.

Ez a humanitárius iparhasználat az ipari szemléletmód egyfajta történelmi kivételének is tekinthető: míg más gyárak a halál ipari logikáját követték (pl. vasúti szállítás, fegyvergyártás, koncentrációs táborok építése), Schindler gyára a túlélés eszközévé vált.

2. Az ipari logisztika tudatos manipulálása a túlélés érdekében

A második fontos pont Oskar Schindler iparra gyakorolt hatásában az, ahogyan kihasználta és átformálta a korszak logisztikai rendszereit. A náci Németország ipari rendszere egy rendkívül szigorú és hatékony bürokratikus-logisztikai hálózaton keresztül működött: a munkaerő-elosztás, az alapanyag-ellátás, a szállítás, és a termelés mind központi ellenőrzés alatt álltak. Schindler ezt a gépezetet tudatosan kezdte kijátszani.

Az egyik legismertebb példa erre a híres „Schindler-lista”. Ebben a dokumentumban szereplő több mint 1 000 zsidó munkás nevét úgy jegyezték fel, mint „elengedhetetlenül szükséges munkaerő”, annak ellenére, hogy közülük sokan valójában nem rendelkeztek ipari szaktudással. A lista összeállítása, a hivatalos papírok, a munkaszerződések és engedélyek beszerzése mind olyan ipari és logisztikai rendszereken keresztül történt, amelyek a náci állam hadigépezetét szolgálták, de Schindler ezeket a rendszereket saját céljai – az emberéletek megóvása – érdekében használta fel.

A termeléshez szükséges nyersanyagok, gépek és szállítási eszközök biztosítása is olyan logisztikai kihívást jelentett, amelyet Schindler gyakran kreatívan, sokszor szabálytalanul oldott meg. A brünnlitzi gyárba való átköltözéskor például nemcsak gépeket és berendezéseket szállíttatott át, hanem magukat a munkásokat is – mindezt hivatalosan „ipari átszervezés” címén. Ez a fajta logisztikai bűvészkedés példaértékű abban az értelemben, hogy megmutatta: egy szigorúan szabályozott ipari rendszerben is van lehetőség a humanitás érvényesítésére – ha valaki hajlandó kockázatot vállalni és ügyesen manőverezni a szabályok között.

Schindler tehát nemcsak gyárakat üzemeltetett, hanem újraértelmezte azt, hogy mit jelent az ipar logisztikai gépezetének részeként működni – nem a hatalom, hanem az élet szolgálatában.

3. Az ipar emberközpontú újraértelmezése a munkaerő védelmében

A harmadik kiemelhető pont Oskar Schindler iparra gyakorolt hatásában az, hogy ő volt az egyik első olyan iparvállalkozó a korszakban, aki – legalábbis a gyakorlat szintjén – az embert állította a középpontba, nem pedig a termelést vagy a profitot.

A náci Németországban az ipar szigorúan a háborús célokat szolgálta: a munkaerő szinte kizárólagos szerepe a minél gyorsabb és nagyobb mennyiségű termelés volt, minden más – különösen az emberi méltóság – másodlagos vagy egyáltalán nem is számított. Ebben a közegben Schindler teljesen más megközelítést alkalmazott.

A brünnlitzi gyárában nem az volt az elsődleges cél, hogy valódi, működőképes lőszereket gyártson. Sőt, számos forrás szerint tudatosan hibás termékeket állítottak elő, hogy ne járuljanak hozzá ténylegesen a háborús pusztításhoz. Ezzel párhuzamosan viszont a gyár valódi célja az volt, hogy menedéket nyújtson az ott dolgozó zsidó munkásoknak. Az ipari tevékenység így eszközzé vált az életben maradásért folytatott küzdelemben – nem pedig öncélú gazdasági vagy politikai cél megvalósításává.

Schindler rendszeresen túlfizette a munkásait a náci előírásokhoz képest, élelmet és gyógyszert szerzett nekik a feketepiacon, és gondoskodott az alapvető higiéniai feltételekről is. Ezek az intézkedések egy átlagos vállalkozó részéről elképzelhetetlenek lettek volna akkoriban – főleg, hogy Schindlernek ez személyes anyagi veszteséget is jelentett. A gyára végül veszteségessé vált, és teljes vagyonát elköltötte a munkások ellátására és megmentésére.

Ezzel nemcsak a zsidó munkások számára jelentett reményt és túlélést, hanem egyfajta alternatívát is mutatott arra, hogyan lehet egy embertelen rendszerben emberként viselkedni. Schindler ipari működése így morális példává vált: megmutatta, hogy a termelés nem kell, hogy kizárólag a pusztítás eszköze legyen, hanem akár az élet védelmének színtere is lehet.

4. A brünnlitzi gyár mint az ipar humanizálásának szimbóluma

A következő fontos szempont Oskar Schindler iparra gyakorolt hatásában az, hogy a brünnlitzi gyár (Csehországban, a mai Brněnec településen) szinte jelképévé vált annak, hogyan válhat egy ipari létesítmény az embermentés eszközévé.

Amikor Schindler 1944-ben felismerte, hogy a krakkói gettó felszámolása és a plaszówi koncentrációs tábor működése után a zsidó munkások élete végveszélybe került, lépésre szánta el magát. Elérte, hogy a gyárát áthelyezzék Lengyelországból a nála viszonylag „biztonságosabb” Protektorátus területére, Csehországba. Ez önmagában is szokatlan lépés volt: háborús időkben, a hadiipari termelés csúcsán senki nem „költöztetett” gyárat csak azért, hogy megmentse a munkaerőt.

A gyár fizikai működése sokkal inkább szolgálta az embermentést, mint a termelést. A berendezések ugyan ott voltak, de a termékek nem működtek, vagy szándékosan selejtesek voltak. A lényeg nem az volt, hogy lőszert állítsanak elő, hanem hogy jogilag fenntartható módon alkalmazhassa a listáján szereplő embereket – és így életben tartsa őket.

Ez a gyár tehát sokkal több volt, mint egy üzem: egy bujtatott menedékhely, egy „élő fedőcég”, ahol az emberiesség kapott főszerepet. A munkások számára ez a hely jelentette az utolsó esélyt az életre, az élelemhez jutásra és a relatív biztonságra. A gyár falai között kialakult közösség és viszonylagos nyugalom egy egészen másfajta ipari működés modelljét mutatta meg – amely nem a nyers termelési számokban mérte a sikert, hanem az emberéletekben.

Ez a szimbolikus jelentőség később, a háború után is fennmaradt: a brünnlitzi gyár a Schindler-listával együtt az egyik legismertebb példájává vált annak, hogy az ipart is lehet úgy használni, hogy az az emberi értékeket szolgálja – még akkor is, amikor a világ éppen ezek ellen fordul.

5. Az ipari kapcsolatok és hálózatok átalakulása Schindler munkássága nyomán

Egy másik jelentős hatása Oskar Schindler tevékenységének az volt, hogy megváltoztatta és újragondolta az ipari kapcsolatok és hálózatok szerepét a háborús időszakban. Schindler nem csak egy gyár tulajdonosa volt, hanem egyfajta közvetítő, aki képes volt az összekötő kapocs lenni különböző érdekcsoportok között — a nácik, a munkások, az ipari beszállítók és a helyi közösségek között.

Ez a szerep azért volt fontos, mert a háborús ipar működése során a termelési láncok nagyon összetettekké váltak, és a túléléshez elengedhetetlen volt, hogy valaki képes legyen finoman lavírozni az egyes szereplők között. Schindler azzal, hogy befolyásos kapcsolatait felhasználva megvédte a zsidó munkásokat, példát mutatott arra, hogy az ipari vezetői szerep túlmutathat a tiszta üzleti érdekeken, és emberségességgel is párosulhat.

Ugyanakkor ez a fajta kapcsolatépítés átalakította a hadiipari termelés szervezését is: a gyár működésében megjelent egyfajta rugalmasság és emberközpontúság, ami szokatlan volt akkoriban. Schindler képes volt alkalmazkodni a folyamatosan változó háborús körülményekhez, és azzal, hogy embereket mentett meg, egy újfajta ipari vezetői magatartást is formált — olyat, amelyben a morális szempontoknak is helye van a gazdasági döntések mellett.

Ez a hálózatépítés és emberközpontú menedzsment hozzájárult ahhoz, hogy a hadiipar ne csupán egy gépezet legyen, hanem egy élő, emberi tényezőket is figyelembe vevő rendszer. Ez az attitűd pedig később más ipari vezetők számára is mintaként szolgált.

6. A munkavállalói szemlélet és munkaerő-felfogás átalakítása

Oskar Schindler munkásságának egyik legmélyebb és legmaradandóbb ipari hatása az volt, ahogyan a munkaerőhöz viszonyult — különösen a második világháború idején. Míg a náci Németország iparában sok helyen a munkások csak „erőforrásként” szerepeltek, akiket kizsákmányoltak és embertelen körülmények között dolgoztattak, Schindler ezzel szöges ellentétben járt el.

A Schindler-listán szereplő zsidó munkásokat nemcsak megvédte a deportálástól, hanem emberhez méltó bánásmódban részesítette őket. Ez nemcsak morális tett volt, hanem olyan ipari szemléletváltást is jelentett, amely a munkaerőt nem kizárólag eszközként kezelte, hanem értékes emberi tőkének tekintette.

A gyára, az "Emalia" (azaz a Deutsche Emailwarenfabrik), ahol edényeket és lőszereket is gyártottak, egyfajta menedékké vált. Az ott dolgozó emberek képzést kaptak, jobbak voltak a munkakörülmények, és Schindler aktívan dolgozott azon, hogy ne kelljen őket veszélyes vagy embertelen munkába küldeni. Ez a hozzáállás a humánus munkáltatói magatartás egyik korai példája lett.

Ez a szemlélet, amely figyelembe veszi a dolgozók jólétét, emberi méltóságát és biztonságát, a háború után fokozatosan beépült a modern ipari gondolkodásba. A jóléti intézkedések, munkavállalói jogok, céges felelősségvállalás egy része történelmi távlatból visszatekintve olyan egyéni példákhoz vezethető vissza, mint amilyen Schindleré.

Bár Schindler munkássága nem hozott létre új ipari technológiákat, az általa képviselt értékrend és vezetési stílus olyan irányokat jelölt ki, amelyek ma is alapvetőnek számítanak a modern iparban: az etikus üzleti magatartás, a munkahelyi biztonság, az emberi méltóság tiszteletben tartása és a társadalmi felelősségvállalás terén.

2.31. Digitális ikrek a jövő iparában: Architektúrák, kihívások és alkalmazások az autóiparban Digitális ikrek az autóiparban

Digitális ikrek a jövő iparában: Architektúrák, kihívások és alkalmazások az autóiparban

Digitális ikrek az autóiparban

A kiber-fizikai rendszerek fejlődése és integrációja az Ipar 4.0 keretrendszerében

Szabó Bence

Mérnökinformatikus BSc, szabobence392@gmail.com

A tanulmány első része áttekinti a digitális ikrek fogalmát, eredetét és elhelyezését a kiber-fizikai rendszerek (CPS), valamint az Ipar 4.0 kontextusában. Külön figyelmet kap a digitális ikrek és az IoT eszközök közötti kapcsolat, valamint a valós idejű adatgyűjtés és -feldolgozás jelentősége, továbbá bemutatásra kerülnek a kulcsfontosságú kommunikációs protokollok (pl. OPC-UA, MQTT).

A második fejezet a digitális iker rendszerek architektúráját és működését vizsgálja. Részletesen elemzi a fő komponenseket – a fizikai objektumokat, érzékelőket, kommunikációs infrastruktúrát, digitális modelleket, adatfeldolgozó algoritmusokat és vizualizációs eszközöket –, valamint bemutatja a gépi tanulás, a prediktív karbantartás és az adatvizualizáció szerepét.

A harmadik rész esettanulmányokon keresztül mutatja be a technológia gyakorlati alkalmazásait, különös tekintettel az autóiparra, a gyártásautomatizálásra, a logisztikára és a karbantartásra. Ismertetésre kerülnek olyan vállalati megoldások, mint a Siemens, a Bosch, a Tesla vagy a GE Predix platformja.

Végül a dolgozat kitekint a digitális ikrek jövőbeli lehetőségeire: az MI-integrációra, a fejlettebb szimulációs modellekre, valamint a fenntarthatóság és energiahatékonyság szempontjából betöltött szerepükre az ipari digitalizáció fejlődő ökoszisztémájában.

Kulcsszavak: Ipar 4.0, digitális ikrek, fenntarthatóság, autóipar, kiber-fizikai rendszerek, IoT, digitalizáció, mesterséges intelligencia, BMW, Tesla

Tartalom

1 Bevezetés 3

2 Elméleti háttér és definíciók 4

2.1 A digitális iker fogalma 4

2.2 Digitális iker a kiber-fizikai rendszerekben 4

2.3 IoT, szenzorhálózatok és kommunikációs technológiák 5

3 Digitális ikrek architektúrája és technológiái 6

3.1 A digitális iker általános architektúrája 6
3.2 Használt technológiák 7
3.2.1 Érzékelők és IoT-platformok 7
3.2.2 Kommunikációs protokollok 8
3.2.3 Modellezési és szimulációs eszközök 8
3.3 A digitális ikrek időbeli aspektusai 8
3.4 Az interoperabilitás és szabványosítás kihívásai 8
3.5 Felhő és peremhálózat (Edge/Fog Computing) szerepe 10
4 Digitális ikrek ipari alkalmazásai 11
4.1 A digitális ikrek szerepe az autóiparban 12
4.1.1 Terméktervezés és szimuláció 12
4.1.2 Gyártósorok optimalizálása (Smart Factory) 12
4.1.3 Járműfenntartás és üzemeltetés 12
4.1.4 Tesztelés autonóm járműveknél 12
4.2 Előnyök, korlátok és kihívások a digitális ikrek alkalmazásában az autóiparban 13
4.2.1 Előnyök 13
4.2.2 Korlátok 13
4.2.3 Kihívások 13
5 A jövő lehetőségei és fejlesztési irányok: Digitális ikrek és mesterséges intelligencia integrációja 14
5.1 A digitális ikrek evolúciója: statikustól az intelligens rendszerekig 14
5.2 Az MI integráció fő területei 14
5.2.1 Gépi tanulás (Machine Learning) 14
5.2.2 Mélytanulás és neurális hálók 14
5.2.3 Autonóm döntéshozatal 14
5.3 Autóipari jövőkép: MI + digitális iker szinergiában 15
5.4 Kihívások az MI integráció során 15
6 Esettanulmány: Digitális ikrek az autóiparban – a BMW és a Tesla példája 15
6.1 Bevezetés 15

6.2 BMW – Digitális iker a gyártás minden szintjén 15
6.3 Tesla – Digitális ikrek a járművekben és a flottakezelésben 16
6.4 Összegzés és összehasonlítás 17
7 A digitális ikrek jövője az autóiparban – lehetőségek és fejlesztési irányok 18
7.1 Dinamikusan tanuló digitális ikrek 18
7.2 Mesterséges intelligencia integrációja 18
7.3 Virtuális validáció és szimulált járműfejlesztés 19
7.4 Szabványosítás és interoperabilitás 19
7.5 Kihívások a jövőben 20
8 Összegzés és jövőbeli kilátások 20
9 KÖSZÖNETNYILVÁNÍTÁS 21

1 BEVEZETÉS

A digitális iker (Digital Twin, DT) technológia az Ipar 4.0 egyik legmeghatározóbb innovációja, amely lehetővé teszi a fizikai rendszerek digitális reprezentációjának létrehozását, valós idejű adatkapcsolattal és folyamatos visszacsatolással. A koncepció lényege, hogy egy adott fizikai objektum vagy rendszer működését, állapotát és környezeti viszonyait egy virtuális modell segítségével lehet nyomon követni, szimulálni és optimalizálni.

A digitális ikrek alkalmazása különösen nagy jelentőséggel bír az iparban, mivel lehetővé teszik a gyártási folyamatok, logisztikai láncok és berendezések megbízható, költséghatékony és prediktív üzemeltetését. Az olyan iparágakban, mint az autóipar, a repülőgépgyártás vagy az energetika, a DT technológia hozzájárul a termékminőség javításához, a karbantartási költségek csökkentéséhez és az üzemidő növeléséhez [1], [2].

Az autóiparban a digitális ikrek alkalmazása különösen előnyös, mivel lehetővé teszi a járművek és gyártási folyamatok valós idejű monitorozását, szimulációját és optimalizálását. Ez hozzájárul a termékminőség javításához, a karbantartási költségek csökkentéséhez és az üzemidő növeléséhez.

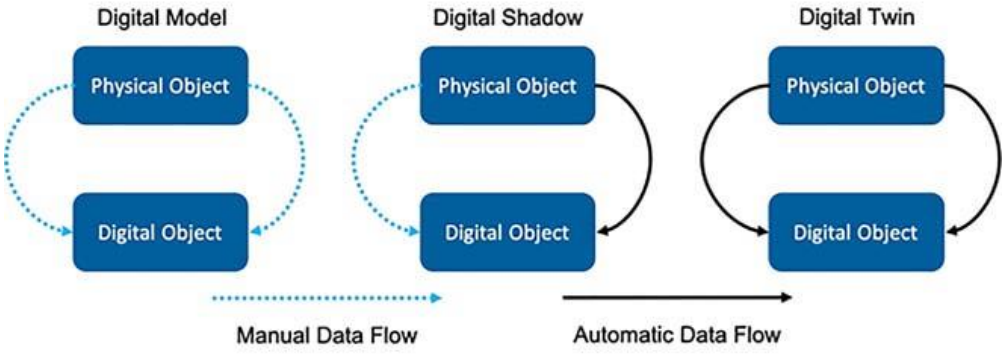
A jelen dolgozat célja, hogy átfogó képet adjon a digitális ikrek technológiájáról, különös tekintettel a kiber-fizikai rendszerek (CPS) és az ipari IoT szerepére. A dolgozat először bemutatja a digitális iker fogalmi és technológiai alapjait, majd kitér az architektúrákra, a kommunikációs megoldásokra, valamint a kapcsolódó adatfeldolgozó és gépi tanulási rendszerekre. A technológiai áttekintést követően konkrét ipari alkalmazásokat mutat be, különös tekintettel az autóiparra és a gyártási folyamatok digitalizációjára. A dolgozat végül megvizsgálja a technológia előnyeit és kihívásait, valamint a jövőbeli fejlődési irányokat.

2 ELMÉLETI HÁTTÉR ÉS DEFINÍCIÓK

2.1 A digitális iker fogalma

A digitális iker (Digital Twin, DT) egy olyan virtuális modell, amely szorosan integrált egy fizikai eszközzel, és képes annak működését valós időben tükrözni. A koncepció először a NASA-nál jelent meg 2010-ben, ahol a digitális ikreket a fizikai rendszerek virtuális reprezentációjaként definiálták, amelyek képesek a rendszer állapotának és működésének valós idejű tükrözésére [3].
A digitális ikrek három fő szintje különböztethető meg:

- **Digitális modell (Digital Model):** Egy statikus modell, amely nem rendelkezik valós idejű adatkapcsolattal a fizikai rendszerrel.
- **Digitális árnyék (Digital Shadow):** Egyirányú adatkapcsolat a fizikai rendszerből a digitális modell felé, amely lehetővé teszi az adatok valós idejű megjelenítését, de nem teszi lehetővé a visszacsatolást.
- **Digitális iker (Digital Twin):** Kétirányú adatkapcsolat a fizikai és a digitális rendszer között, amely lehetővé teszi a valós idejű adatcserét és a rendszer állapotának folyamatos szinkronizálását [4](lásd 1. ábra).

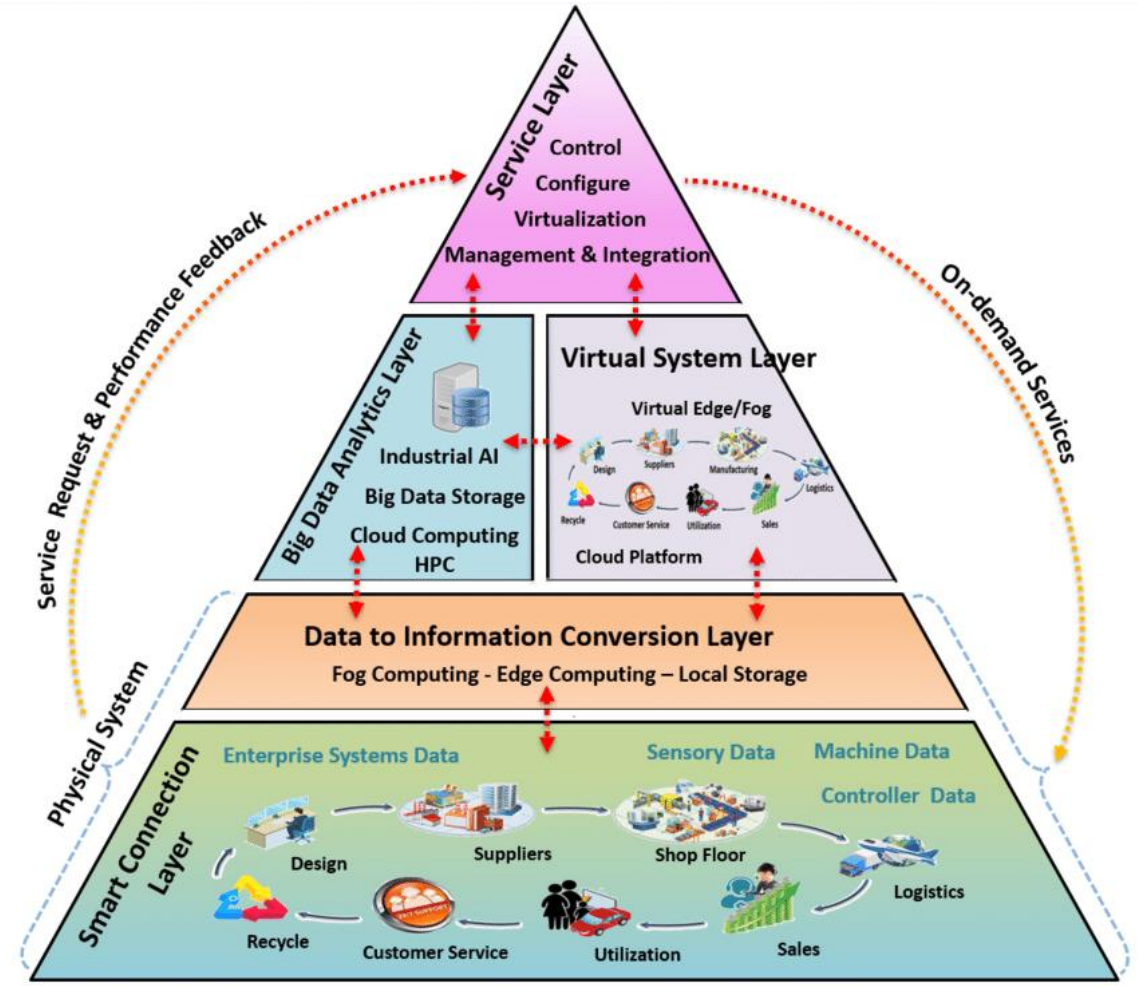


1. ábra A digitális ikrek három fő szintje (https://ieeexplore.ieee.org/document/9103025)

2.2 Digitális iker a kiber-fizikai rendszerekben

A digitális ikrek szorosan kapcsolódnak a kiber-fizikai rendszerek (Cyber-Physical Systems, CPS) koncepciójához, ahol a fizikai és digitális komponensek szorosan integrált rendszert alkotnak, valós idejű adatcserével és autonóm döntéshozatallal. A digitális iker lényegében a CPS „digitális magja", amely a fizikai valóságból származó adatok feldolgozásával támogatja az intelligens működést [5].

A CPS-ek és a digitális ikrek integrációja lehetővé teszi a rendszerek valós idejű monitorozását, szimulációját és optimalizálását, ami különösen fontos az ipari alkalmazásokban, például az autóiparban, ahol a gyártási folyamatok és a járművek működésének optimalizálása kulcsfontosságú (lásd 2. ábra).



2. ábra Digitális ikerrel támogatott kiber-fizikai rendszer architektúrája (https://www.researchgate.net/figure/Digital-Twin-enabled-CPS-DT-CPS-architecture-for-smart-manufacturing-systems-red_fig5_339563643)

2.3 IoT, szenzorhálózatok és kommunikációs technológiák

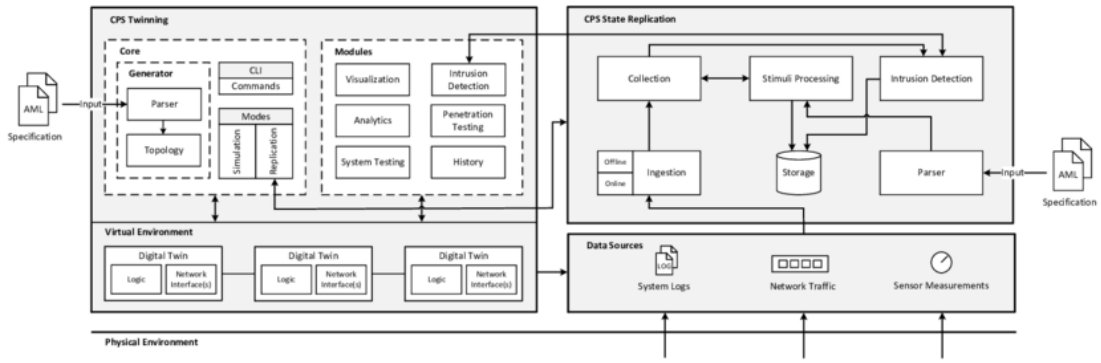
A digitális iker alapját az Internet of Things (IoT) és a szenzorhálózatok biztosítják. A szenzorok adatokat gyűjtenek a fizikai rendszer állapotáról (pl. hőmérséklet, vibráció, nyomás), amelyeket edge computing vagy felhőalapú platformok dolgoznak fel. Az adatátvitelhez olyan ipari protokollokat használnak, mint:

- MQTT (Message Queuing Telemetry Transport): Kis sávszélességű, megbízható adatküldés.
- OPC-UA (Open Platform Communications Unified Architecture): Ipari gépek közötti szabványos kommunikáció.
- ROS 2 (Robot Operating System 2): Robotikai rendszerek integrációjára alkalmas keretrendszer [6], [7].

Az 5G és alacsony késleltetésű hálózatok új dimenziókat nyitnak a digitális ikrek valós idejű működtetésében, különösen az autóipari alkalmazásoknál (pl. önvezető járművek, gyártósori szinkronizáció).

3 DIGITÁLIS IKREK ARCHITEKTÚRÁJA ÉS TECHNOLÓGIÁI

A digitális ikrek architektúrája jellemzően többrétegű, és kiber-fizikai rendszerek (CPS) struktúrájára épül, amelyekben a fizikai és digitális elemek szoros, kétirányú kapcsolatban állnak. A digitális iker architektúrája különböző komponensekből áll össze, amelyek mindegyike specifikus feladatot lát el az adatok gyűjtésétől a modellezésen át a predikcióig (lásd 3. ábra).

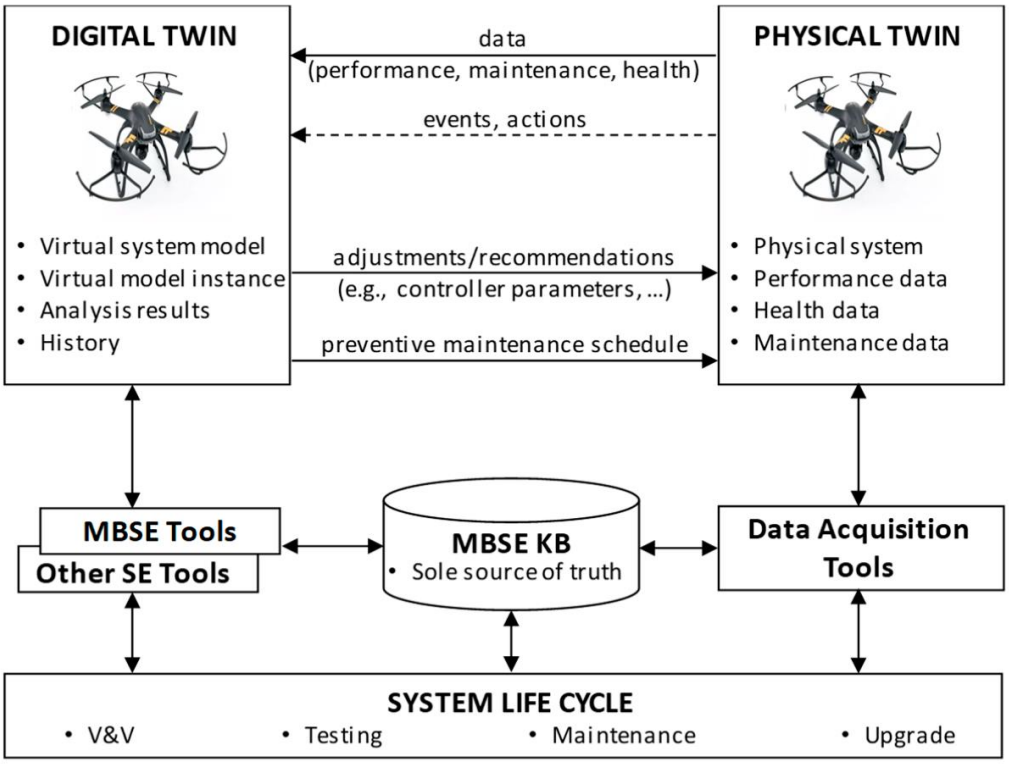


3. ábra Egy kiber-fizikai rendszer digitális iker másának architektúrája (https://www.researchgate.net/figure/Architecture-of-CPS-Twinning-7-and-CPS-State-Replication_fig3_328328509)

3.1 A digitális iker általános architektúrája

A leggyakrabban alkalmazott struktúra az alábbi fő rétegekre tagolható [8][9] (lásd 4. ábra):

- **Fizikai réteg (Physical Layer):** A valódi objektum, eszköz, gép vagy folyamat, amelyhez a digitális iker tartozik. Itt történik az érzékelés és a digitális modell frissítése.
- **Adatgyűjtő réteg (Data Acquisition Layer):** Szenzorok és IoT-eszközök segítségével történik a rendszerállapotok (pl. hőmérséklet, nyomás, sebesség) valós idejű begyűjtése.
- **Kommunikációs réteg (Network Layer):** Az adatokat valós időben továbbítja edge/felhő rendszerekhez. Alkalmazott protokollok: MQTT, OPC-UA, DDS stb.
- **Adatfeldolgozó és modellező réteg (Processing & Modeling Layer):** A digitális iker virtuális modellje itt található. Itt történik a szimuláció, gépi tanulási algoritmusok alkalmazása, valamint a prediktív analitika.
- **Alkalmazási réteg (Application Layer):** Itt zajlik a felhasználói interakció, vizualizáció, döntéstámogatás és visszacsatolás a fizikai rendszer felé.



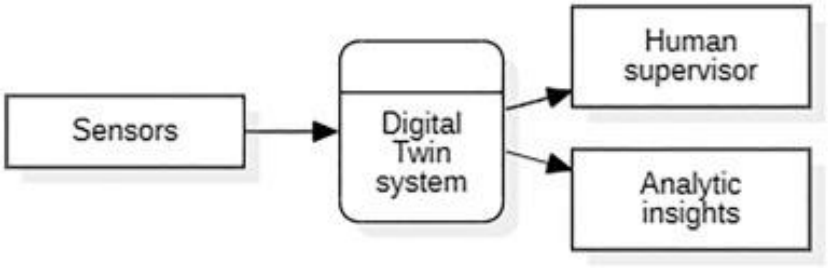
4. ábra A digitális iker a modellezésben (https://www.mdpi.com/systems/systems-07-00007/article_deploy/html/images/systems-07-00007-g001.png)

3.2 Használt technológiák

A digitális ikrek működéséhez többféle technológiai komponens szükséges, ezek integrációja adja meg az eszköz funkcionalitását.

3.2.1 Érzékelők és IoT-platformok

- Fizikai eszközökbe ágyazott szenzorok gyűjtik az adatokat: hőmérséklet, vibráció, nyomás, kopás stb. (lásd 5. ábra)
- Az adatok gyakran edge számítástechnikai eszközön keresztül kerülnek feldolgozásra (pl. NVIDIA Jetson, Raspberry Pi + Yocto), vagy felhőbe továbbítva (pl. AWS IoT, Microsoft Azure Digital Twins).



5. ábra Digitális iker-alapú előrejelző karbantartási rendszer funkciódiagramja (https://ars.els-cdn.com/content/image/1-s2.0-S0360835223001237-fx2.jpg)

3.2.2 Kommunikációs protokollok

- **MQTT**: Könnyű, publish/subscribe alapú üzenetküldő protokoll, ideális alacsony sávszélességű eszközökhöz.
- **OPC-UA**: Platformfüggetlen ipari szabvány a gépek közötti biztonságos kommunikációra.
- **DDS (Data Distribution Service)**: Valós idejű elosztott rendszerekhez tervezett kommunikációs protokoll.
- **ROS 2**: Robotikai rendszerek digitális ikres szimulációjához használható keretrendszer [10].

3.2.3 Modellezési és szimulációs eszközök

- **CAD / CAE rendszerek**: Siemens NX, PTC Creo, Autodesk Fusion 360.
- **Fizikai modellezés**: MATLAB/Simulink, ANSYS, vagy Unity/Unreal Engine alapú real-time szimulációk.
- **Gépi tanulás és analitika**: TensorFlow, PyTorch, Scikit-learn, Apache Spark.

3.3 A digitális ikrek időbeli aspektusai

A digitális ikreknek különféle idődimenziói is vannak:

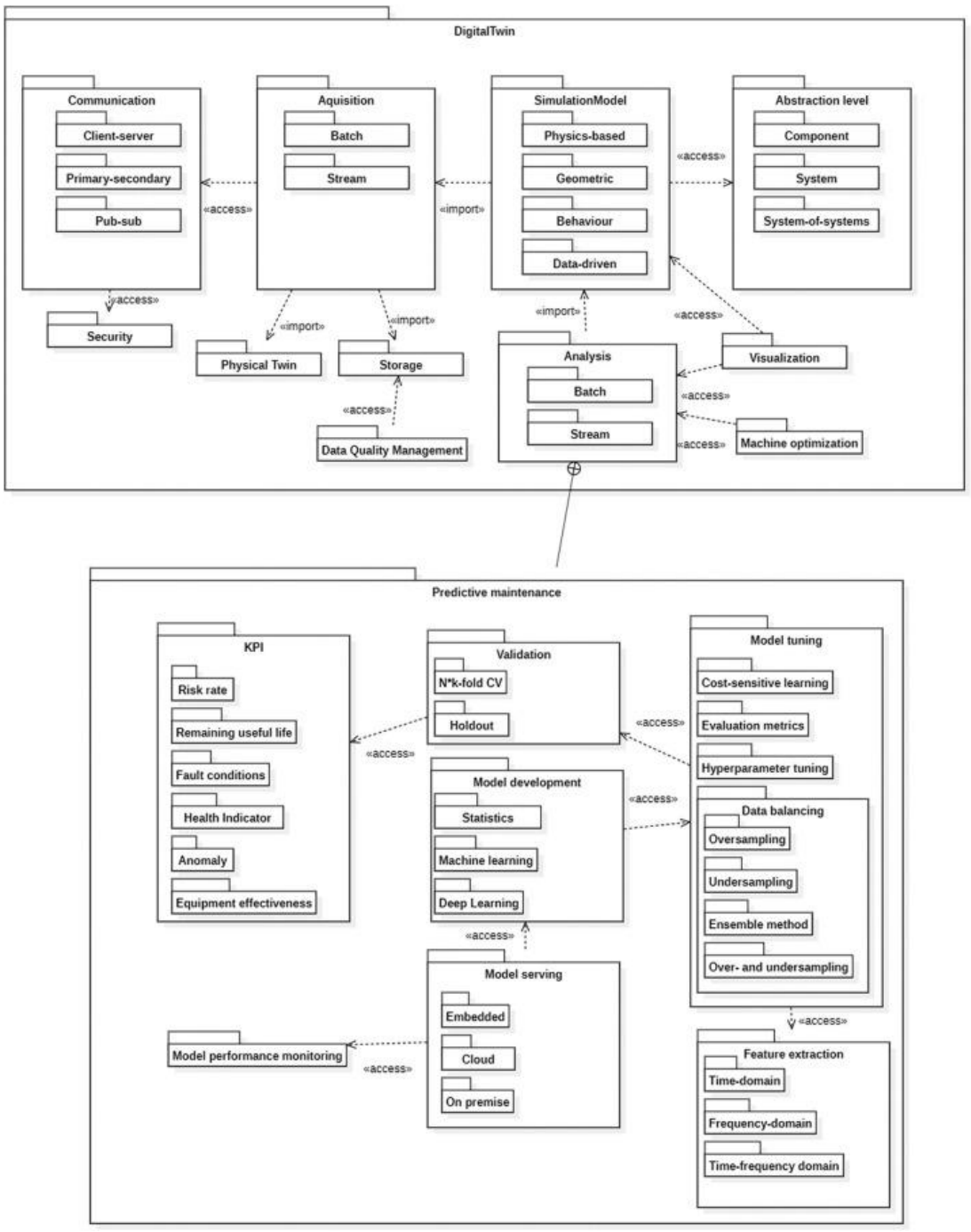
- **Múlt** – korábbi adatok elemzése (pl. hibák visszakeresése)
- **Jelen** – valós idejű monitorozás, vezérlés
- **Jövő** – szimulációk, prediktív karbantartás (Predictive Maintenance)

Ezek az aspektusok lehetővé teszik a teljes életciklus-menedzsmentet (PLM – Product Lifecycle Management).

3.4 Az interoperabilitás és szabványosítás kihívásai

A digitális ikrek heterogén rendszerekből épülnek fel, így fontos a különféle komponensek közötti interoperabilitás biztosítása:

- Adatformátumok egységesítése (pl. XML, JSON, OPC-UA modellek)
- Metaadat-kezelés (ontológiák, szabványos modellezési nyelvek: SysML, UML) (lásd 6. ábra)
- API-alapú rendszerek: RESTful API-k, GraphQL

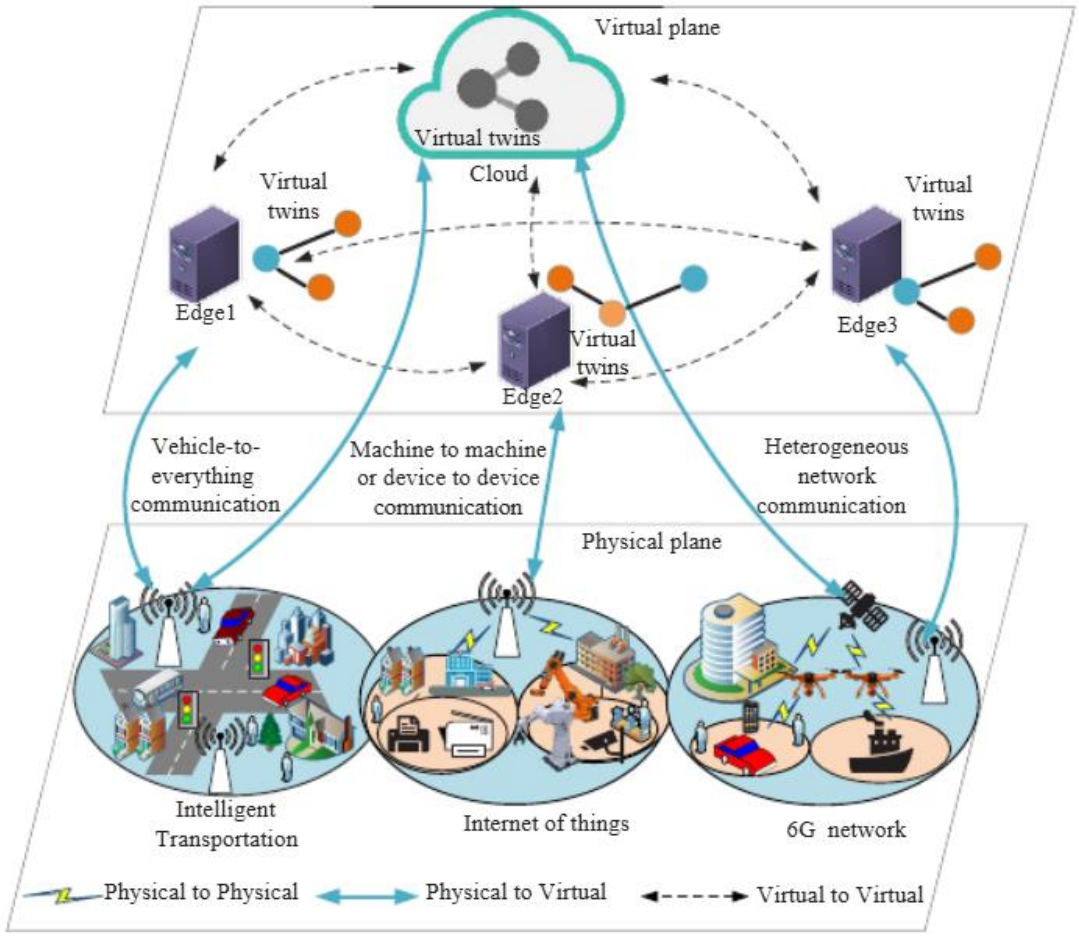


6. ábra Digitális iker leírása egységes, modellezési nyelven (https://ars.els-cdn.com/content/image/1-s2.0-S0360835223001237-gr5.jpg)

3.5 Felhő és peremhálózat (Edge/Fog Computing) szerepe

A digitális ikrek gyakran nagy mennyiségű adatot kezelnek, ezért az edge és felhő alapú feldolgozás kombinációja a legelterjedtebb megközelítés.

- **Edge Computing**: Lokálisan, gyors válaszidővel, alacsony késleltetéssel (pl. járművekben) (lásd 7. ábra).
- **Cloud Computing**: Nagy számítási kapacitás, hosszú távú adattárolás, ML modellek képzése.



7. ábra A digitális ikerhálózatok hierarchikus architektúrája
(https://www.researchgate.net/publication/378090236_Edge_Computing_for_Digital_Twin)

4 DIGITÁLIS IKREK IPARI ALKALMAZÁSAI

A digitális ikrek egyik legfontosabb és legnagyobb hozzáadott értéket képviselő alkalmazási területe az ipar, azon belül is kiemelkedően az autóipar. A digitalizáció ezen formája lehetővé teszi a fizikai rendszerek valós idejű leképezését, a gyártási folyamatok optimalizálását, karbantartási igények előrejelzését, és az új termékek fejlesztésének gyorsítását.

A digitális ikrek alkalmazása az **Ipar 4.0** paradigmájának egyik alappillére, amely a termelési rendszerek intelligens, adaptív, és önoptimalizáló működését célozza meg [11].

4.1 A digitális ikrek szerepe az autóiparban

4.1.1 Terméktervezés és szimuláció

A digitális iker lehetővé teszi az új járműmodellek fejlesztését és tesztelését a fizikai prototípus elkészítése előtt. A szimulációk során figyelembe vehetők:

- aerodinamikai tulajdonságok (CFD-analízis),
- strukturális integritás (FEM),
- járműdinamika, ütközési szimulációk,
- elektromos rendszerek működése.
- **Példa**: A BMW digitális ikreket használ a járműszerkezetek töréstesztjeinek szimulációjára, így csökkentve a fizikai prototípusok számát [12].

4.1.2 Gyártósorok optimalizálása (Smart Factory)

A digitális ikrek a gyártósor elemeinek (robotkarok, szállítószalagok, szenzorok) digitális másolatait tartalmazzák. Segítségükkel lehetőség nyílik:

- gyártás szimulációjára még az indulás előtt,
- az anyagáramlás optimalizálására,
- prediktív karbantartásra,
- a gépek együttműködésének elemzésére.
- **Példa**: A Tesla gyáraiban valós időben frissülő digitális iker-modell figyeli a gépek teljesítményét és segít gyorsan reagálni az esetleges kiesésekre [13].

4.1.3 Járműfenntartás és üzemeltetés

Az okosjárművek digitális ikrei nem csupán a gyártósoron, hanem a használat során is „élnek”. Valós időben követik a jármű állapotát, és az alábbi funkciókat teszik lehetővé:

- Prediktív karbantartás (olajcsere, fékek, akkumulátorok),
- Távoli diagnosztika,
- Szoftverfrissítések tesztelése,
- Felhasználói viselkedés alapján történő járműoptimalizáció.
- **Példa**: A General Motors digitális ikreket alkalmaz flottakezelésre, ahol egyes járművek állapotát a rendszer automatikusan monitorozza és javaslatot tesz szervizelésre [14].

4.1.4 Tesztelés autonóm járműveknél

Az önvezető járművek fejlesztése során a digitális ikrek lehetőséget biztosítanak a következőkre:

- valós közlekedési helyzetek szimulációja,
- szenzorfúzió (kamera, radar, LiDAR) tesztelése,
- MI algoritmusok tréningje biztonságos környezetben,
- edge és cloud alapú koordináció.
- **Példa**: A Waymo és a NVIDIA DRIVE Sim rendszerei digitális iker környezeteket alkalmaznak az önvezető szoftverek tesztelésére több millió virtuális mérföldön keresztül [15].

4.2 Előnyök, korlátok és kihívások a digitális ikrek alkalmazásában az autóiparban

4.2.1 Előnyök

A digitális ikrek alkalmazása az autóiparban számos előnyt nyújt, mind a termékfejlesztés, mind a gyártás, üzemeltetés és karbantartás során:

- **Költségcsökkentés**: A digitális prototípusok alkalmazásával jelentősen csökken a fizikai prototípusokra fordított költség és idő. Egy jármű új modelljének fejlesztése során akár több millió dollár takarítható meg a szimulációs tesztek révén [16].
- **Gyorsabb fejlesztési ciklusok**: A digitális ikrek segítségével iteratív és párhuzamos fejlesztési folyamatok valósíthatók meg. A visszacsatolás folyamatos, így a tervezési hibák korán kiszűrhetők [17].
- **Valós idejű monitoring és prediktív karbantartás**: A digitális ikrek valós idejű adatkapcsolaton keresztül képesek követni a járművek és gyártósorok állapotát, lehetővé téve az előrejelzéseken alapuló karbantartást. Ez csökkenti az állásidőt és növeli a berendezések megbízhatóságát [18].
- **Minőségellenőrzés és hibadetektálás**: A gyártási folyamat minden lépését digitálisan leképezve az esetleges minőségi eltérések gyorsan észlelhetők és orvosolhatók, akár automatizált módon is.
- **Fenntarthatóság és környezetterhelés csökkentése**: A virtuális szimulációk révén csökkenthető az anyag- és energiafelhasználás. Az optimalizált folyamatok kevesebb hulladékot eredményeznek, hozzájárulva a körforgásos gazdaság céljaihoz [19].
- **Ügyfélélmény javítása**: A végfelhasználók igényeihez igazított személyre szabott karbantartási, vezetési és frissítési javaslatokat is lehetővé tesznek az egyedi digitális ikrek.

4.2.2 Korlátok

Bár a digitális ikrek jelentős potenciállal rendelkeznek, bevezetésük és működtetésük számos technikai és szervezeti kihívással jár:

- **Komplexitás**: Egy digitális iker teljes körű megvalósítása összetett feladat, amely integrálja a fizikai modellezést, adatgyűjtést, szimulációt és kommunikációt. A rendszer heterogenitása és sokféle forrásból származó adatok kezelése komoly szakértelmet igényel [20].
- **Infrastruktúraigény**: A valós idejű adatfeldolgozás és a nagyméretű digitális modellek működtetése jelentős számítási kapacitást, felhőalapú vagy edge infrastruktúrát igényel. A kis- és középvállalkozások számára ez komoly beruházást jelenthet.
- **Kezdeti beruházási költség**: A digitális ikrek kiépítése nagy kezdeti ráfordítást igényel hardverre, szoftverre és humán erőforrásra. A megtérülés csak hosszú távon érvényesül.
- **Modellek hitelessége**: A digitális modell csak akkor lehet hasznos, ha pontosan tükrözi a valós rendszert. Ennek elérése érdekében folyamatos kalibrálásra és verifikációra van szükség, amely nehézkes és költséges lehet.

4.2.3 Kihívások

A digitális ikrek alkalmazása során számos jövőbeli és jelenlegi kihívással is szembe kell nézni:

- **Adatintegráció és interoperabilitás**: A különböző gyártók és beszállítók rendszerei gyakran eltérő adatstruktúrákat, formátumokat és protokollokat használnak. Az adatcsere és integráció akadályai jelentősen lassíthatják a digitális iker létrehozását [21].

- **Adatbiztonság és kiberbiztonság**: A digitális ikrek sok esetben érzékeny üzleti vagy működési adatokat tartalmaznak, így célpontjai lehetnek kiberbiztonsági támadásoknak. A valós idejű adatkapcsolat különösen sebezhető lehet – például az önvezető járművek szenzoradatai esetében.
- **Szervezeti kultúra és humán tényezők**: A digitális iker technológia bevezetése átalakítja a munkafolyamatokat és új képességeket kíván meg a dolgozóktól. Az elfogadás hiánya, vagy az új rendszerekhez való adaptációs nehézségek szintén akadályozhatják a bevezetést.
- **Etikai és jogi kérdések**: Az adatgyűjtés és feldolgozás során felmerülhetnek adatvédelmi aggályok, különösen, ha a digitális ikrek a végfelhasználók viselkedését is monitorozzák. A szabályozási környezet e téren még fejlődés alatt áll.

5 A JÖVŐ LEHETŐSÉGEI ÉS FEJLESZTÉSI IRÁNYOK: DIGITÁLIS IKREK ÉS MESTERSÉGES INTELLIGENCIA INTEGRÁCIÓJA

5.1 A digitális ikrek evolúciója: statikustól az intelligens rendszerekig

A digitális ikrek fejlődése egyre összetettebb irányt vesz, melyben az MI központi szerepet tölt be. A kezdeti, statikus modellezési megközelítések már nem elegendőek a komplex, dinamikusan változó rendszerek szimulálására. A jövő digitális ikrei adaptívak, prediktívek és önfejlesztőek lesznek [22]. Ezt a fejlődést három fő irány jellemzi:

1. **Adaptivitás** – A digitális ikrek képesek alkalmazkodni a változó környezeti feltételekhez és valós idejű adatok alapján automatikusan újratanulni.
2. **Predikció** – MI-algoritmusok segítségével előrejelzések készíthetők nemcsak a rendszer működéséről, hanem a felhasználói viselkedésről, környezeti hatásokról, hibalehetőségekről is [23].
3. **Önoptimalizálás** – A rendszer képes saját működésének elemzésére és a paraméterek finomhangolására a hatékonyság növelése érdekében [24].

5.2 Az MI integráció fő területei

5.2.1 Gépi tanulás (Machine Learning)

A gépi tanulás (ML) algoritmusai – például neurális hálók, döntési fák vagy SVM-ek – képesek a digitális ikrek által gyűjtött nagy mennyiségű adatból tanulni, ezzel növelve a modell pontosságát. Az ML lehetőséget ad hibadetektálásra, prediktív karbantartásra, termékélettartam-előrejelzésre [25].

5.2.2 Mélytanulás és neurális hálók

A mélytanulás (deep learning) rendszerei képesek feldolgozni a komplex szenzoradatokat, például képeket, hangokat, mozgásmintákat – mindezt a digitális iker részévé téve. Az autóiparban ez különösen fontos az önvezető rendszerek, prediktív vezetéssegítés és hibadetektálás szempontjából.

5.2.3 Autonóm döntéshozatal

A MI lehetővé teszi a digitális ikrek számára, hogy meghatározott határokon belül önálló döntéseket hozzanak. Ilyen lehet például egy autógyárban a karbantartási sorrend újratervezése egy alkatrész hibajelzése alapján.

5.3 Autóipari jövőkép: MI + digitális iker szinergiában

A digitális ikrek és MI kombinációja forradalmasítja az autóipart az alábbi területeken:

- Autonóm járművek szimulációja: A valós és virtuális vezetési adatok kombinálásával fejleszthetők az önvezető algoritmusok, miközben csökkenthető a valós tesztelés költsége és kockázata.
- Okos karbantartás: A jármű digitális ikre folyamatosan monitorozza az állapotot, és MI segítségével képes előre jelezni a szükséges szervizelést.
- Gyártósori optimalizálás: A robotok, gyártócellák és logisztikai rendszerek digitális ikerének egyesítésével intelligens, önhangoló gyártási rendszerek jöhetnek létre.
- Ügyfélspecifikus testreszabás: A digitális ikrek képesek a felhasználói szokások elemzésére, így az MI egyéni ajánlásokat készíthet – például vezetési stílushoz optimalizált járműbeállításokat.

5.4 Kihívások az MI integráció során

Az MI integrációja a digitális ikrekbe számos új kihívást is felvet:

- **Adatminőség és adatetika**: A döntések minősége az adatminőségtől függ. Az adatmanipuláció, torz mintavétel vagy hiányos adathalmazok veszélyesek lehetnek.
- **Magyarázhatóság**: Az MI rendszerek, különösen a mélytanulási modellek „feketedoboz" -szerű működése átláthatatlanná teszi a döntési folyamatokat.
- **Költség és számítási igény**: A valós idejű, nagy pontosságú MI-vezérelt digitális ikrek jelentős erőforrásokat igényelnek – mind hardver, mind szoftver oldalról.

6 ESETTANULMÁNY: DIGITÁLIS IKREK AZ AUTÓIPARBAN – A BMW ÉS A TESLA PÉLDÁJA

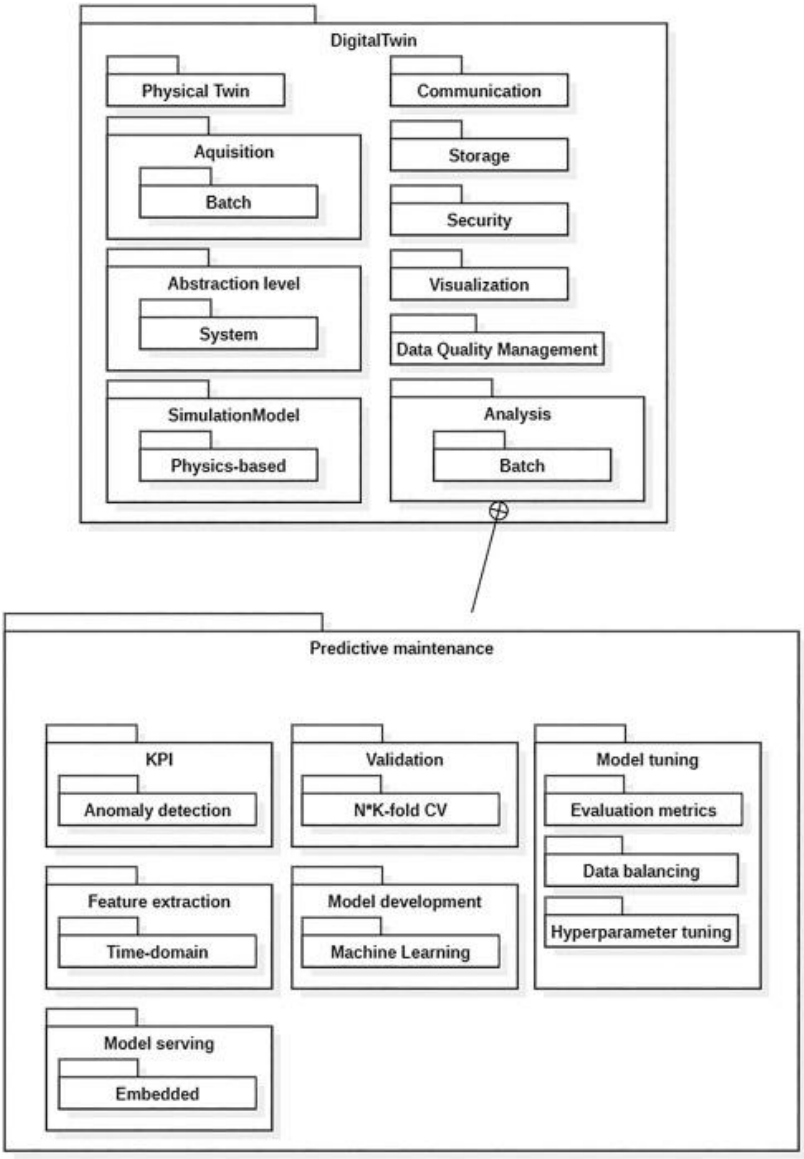
6.1 Bevezetés

Az autóipar az Ipar 4.0 egyik legérettebb ágazata, amely élen jár a digitális ikrek alkalmazásában. A modern járműgyártás rendkívül komplex rendszerek koordinált működését igényli – a tervezéstől a gyártáson át a karbantartásig. Ebben a környezetben a digitális ikrek alkalmazása kulcsszerepet tölt be a folyamatok optimalizálásában, predikciók készítésében és az autonóm rendszerek támogatásában [26].

6.2 BMW – Digitális iker a gyártás minden szintjén

A BMW Group már 2020-ban bejelentette, hogy a **Németországban található regensburgi gyárában** digitális ikertechnológiát alkalmaz a teljes gyártósorra. A cél: a gyártási folyamatok szimulációja, a lehetséges zavarok előrejelzése és az erőforrások optimalizálása. A rendszert **Siemens NX és Teamcenter** szoftverekkel integrálták, és folyamatosan szinkronizálják az adatokat az Edge és a Cloud között [27].
Kulcspontok:

- **Virtuális gyártási környezet**: A teljes gyártósor digitalizálva van, amely lehetővé teszi a valós idejű ellenőrzést, szimulációkat és hibaanalízist.
- **Prediktív karbantartás**: Szenzoradatok alapján az MI előrejelzi az alkatrészek meghibásodásának valószínűségét, ezzel minimalizálva az állásidőt (lásd 8. ábra).
- **Energiahatékonyság**: A digitális iker segítségével az energiafogyasztás optimalizálható, akár 10–15%-os csökkenés is elérhető [28].



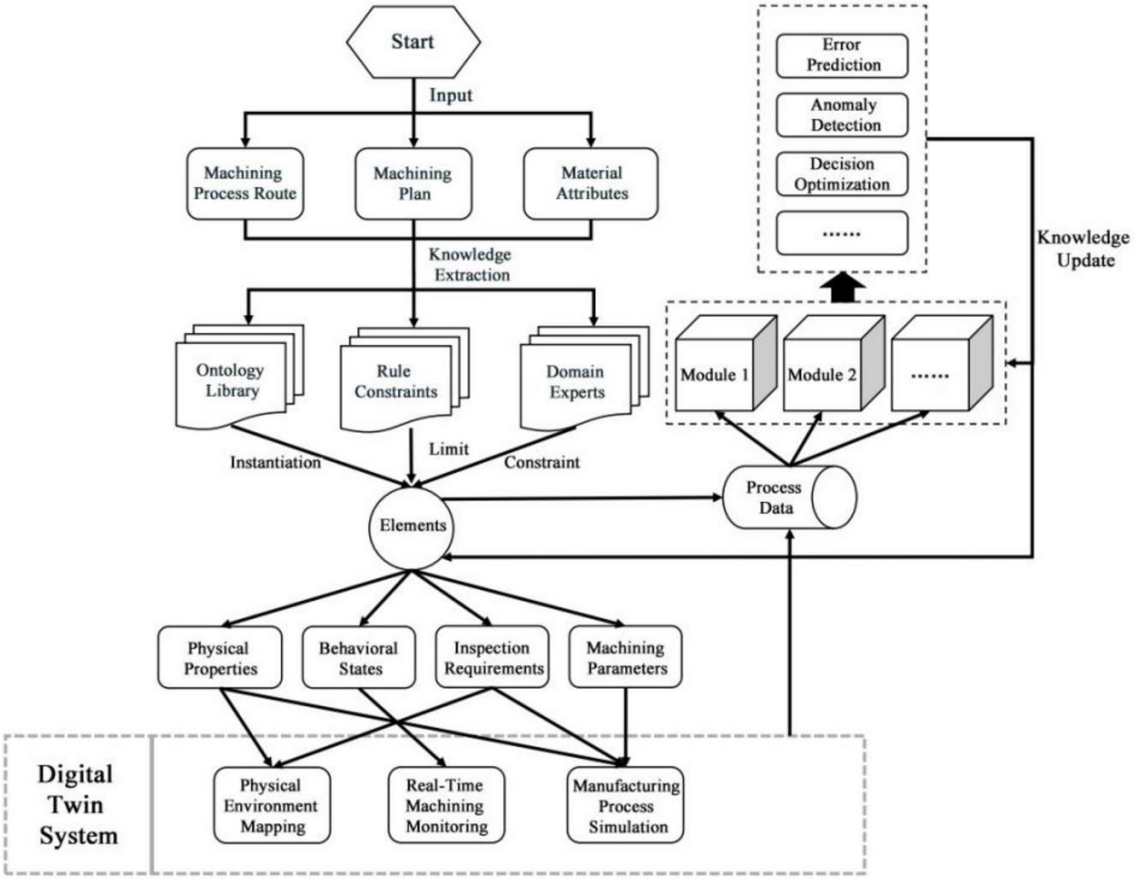
8. ábra Digitális iker-alapú előrejelző karbantartási rendszer összefüggésdiagramja (https://ars.els-cdn.com/content/image/1-s2.0-S0360835223001237-fx3.jpg)

6.3 Tesla – Digitális ikrek a járművekben és a flottakezelésben

A Tesla nemcsak a gyártási folyamatokban, hanem a járművek teljes életciklusán keresztül alkalmaz digitális ikreket. Minden Tesla modell saját digitális ikerrel rendelkezik, amely folyamatosan adatokat gyűjt a jármű viselkedéséről, karbantartási szükségleteiről és vezetési szokásokról [29].

Kulcspontok:

- **Autonóm tanulás**: Az önvezető rendszer fejlesztése során a digitális ikrek kulcsfontosságú szerepet játszanak a valós és szimulált adatok kombinálásában (lásd 9. ábra).
- **Over-the-air (OTA) frissítések**: A digitális ikrek visszacsatolása alapján személyre szabott szoftverfrissítések érkeznek a járműre.
- **Flottaszintű optimalizálás**: A Tesla minden egyes jármű adatait aggregálja és elemzi a gyártás utáni folyamatos fejlesztésekhez – ez a digitális iker „kollektív intelligenciája” [29].



9. ábra Többrétegű tudásgráf modellen alapuló digitális iker rendszer (https://www.nature.com/articles/s41598-024-85053-0/figures/5)

6.4 Összegzés és összehasonlítás

1. táblázat: Összehasonlítás a digitális ikrek alkalmazásában a BMW és a Tesla között

Szempont	BMW	Tesla
Fókusz	Gyártási folyamatok optimalizálása	Teljes járműéletciklus nyomon követése
Alkalmazás területe	Gyár (belső folyamatok, energia, karbantartás)	Jármű (felhasználói adatok, OTA, autonómia)
Szoftveres háttér	Siemens NX, Teamcenter	Saját fejlesztésű MI és adatplatform

Szempont	BMW	Tesla
Prediktív funkciók	Karbantartás, gyártástervezés	Vezetési minták, szerviz, vezetéssegítő rendszerek
Adatintegráció	Szenzorok, gyártósor, edge/cloud	Teljesen integrált jármű és felhőkommunikáció

7 A DIGITÁLIS IKREK JÖVŐJE AZ AUTÓIPARBAN – LEHETŐSÉGEK ÉS FEJLESZTÉSI IRÁNYOK

7.1 Dinamikusan tanuló digitális ikrek

A jövő digitális ikrei az autóiparban nem statikus modellek lesznek, hanem **adaptív, tanuló rendszerek**, amelyek képesek önállóan fejlődni a begyűjtött adatok alapján. Ez azt jelenti, hogy a digitális iker nemcsak a kezdeti járműmodellt tükrözi, hanem folyamatosan frissül az alapján, hogy hogyan használják az adott autót, milyen környezetben működik, és milyen hibák vagy teljesítményváltozások jelennek meg az idő során [30].

Ez különösen fontos az **önvezető járművek** esetében, ahol a digitális iker akár **valós idejű döntéstámogatásra** is képes lehet, ha szinkronizálva van a jármű fedélzeti MI-rendszerével.

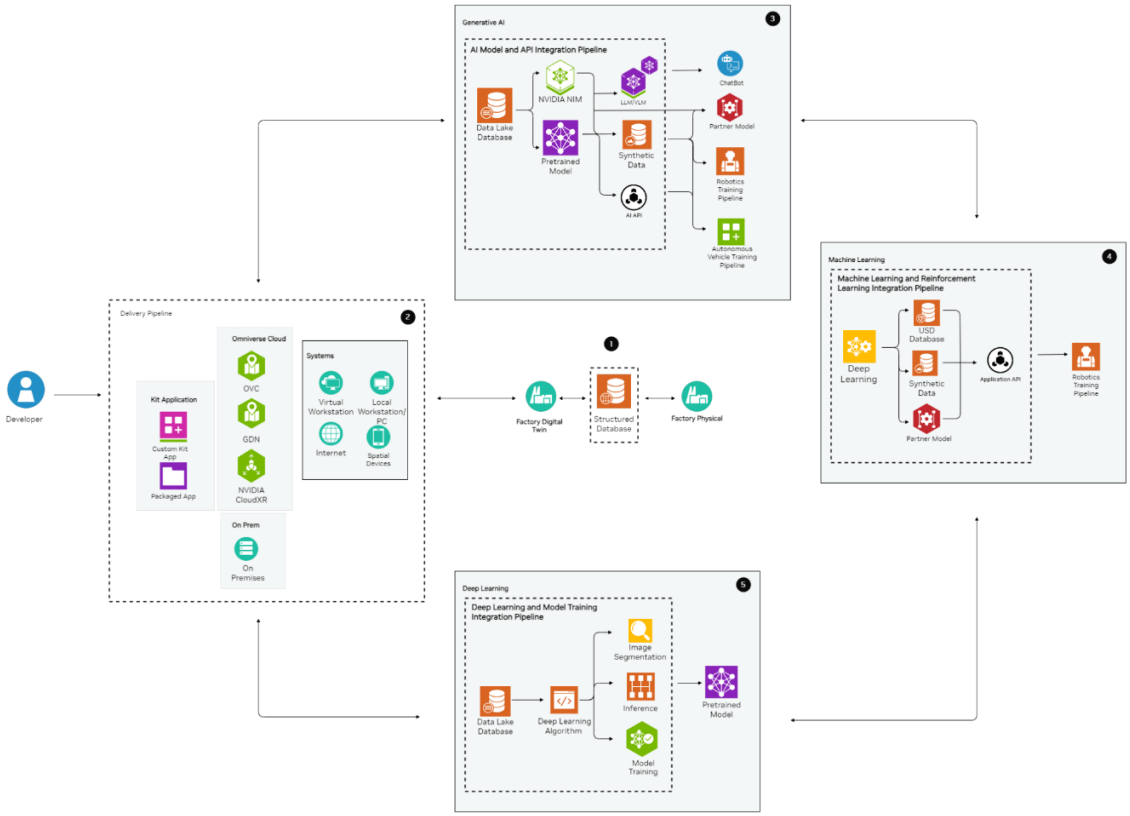
7.2 Mesterséges intelligencia integrációja

A mesterséges intelligencia (MI) beépítése a digitális ikrekbe lehetővé teszi az **önoptimalizáló gyártósorokat**, **intelligens karbantartási rendszereket** és **proaktív járműdiagnosztikát**. Az MI algoritmusok képesek mintázatokat felismerni az érzékelők adataiban, előre jelezni a problémákat, és automatikusan javaslatokat tenni a változtatásokra (lásd 10. ábra).

Az MI és digitális ikrek kapcsolata különösen erős az alábbi területeken:

- **Gyártási folyamatok optimalizálása** (pl. anyagáramlás, logisztika)
- **Üzemidő maximalizálás** gépi tanulással támogatott karbantartással
- **Fogyasztói élmény javítása** személyre szabott frissítésekkel és ajánlásokkal

A Tesla példája már most jól demonstrálja ezt az irányt: a járművek viselkedése alapján készült digitális ikrek segítik a vezetéstámogató rendszerek tanítását és fejlesztését is [31].



10. ábra Mesterséges intelligencia integrációja a gyár digitális ikreihez (https://docs.omniverse.nvidia.com/arch-diagrams/latest/_images/factory-digital-twin-ai2.png)

7.3 Virtuális validáció és szimulált járműfejlesztés

A jövő autóinak tervezése egyre inkább a **virtuális térben zajlik majd**. A digitális ikrek lehetővé teszik, hogy új járműmodelleket teljes mértékben digitálisan tervezzünk, szimuláljunk, teszteljünk – és csak a végső fázisban valós prototípust építsünk.

Ez jelentősen lerövidítheti a **time-to-market** időt, csökkenti a fejlesztési költségeket, és növeli az innovációs képességet. A jövőben várható, hogy a teljes fejlesztési folyamat – CAD, szimuláció, AI-tréning, gyártástervezés – egyetlen digitális ökoszisztémában zajlik majd [32].

7.4 Szabványosítás és interoperabilitás

Ahogy a digitális ikrek egyre elterjedtebbek, kulcsfontosságúvá válik a **szabványos adatcsere és interoperabilitás**. Az autóipari beszállítók és gyártók csak akkor tudják hatékonyan használni a digitális ikereket, ha a rendszerek képesek egymással együttműködni – például a BMW digitális gyártósora és egy Bosch szenzorrendszer adatai zökkenőmentesen kapcsolódnak [33].

Ebben az irányban az olyan nyílt platformok, mint az **OPC-UA**, a **Digital Twin Consortium ajánlásai** vagy a **FIWARE** ökoszisztéma kulcsszerepet játszanak.

7.5 Kihívások a jövőben

A digitális ikrek további fejlődése azonban **jelentős kihívásokkal** is szembesül:

- **Adatbiztonság és adatvédelem**: a járművek szenzitív adatok ezreit generálják, amelyek megfelelő védelme kritikus.
- **Valós idejű adatfeldolgozás**: az 5G és edge computing nélkül a digitális ikrek valós idejű szinkronizálása nem megvalósítható.
- **Komplex rendszerintegráció**: a digitális ikrek rendszereinek integrálása a meglévő gyártási és üzemeltetési rendszerekkel továbbra is jelentős kihívás.

8 ÖSSZEGZÉS ÉS JÖVŐBELI KILÁTÁSOK

A digitális ikrek technológiája az utóbbi évek egyik legdinamikusabban fejlődő területévé vált az ipari digitalizációban, különösen az Ipar 4.0 kontextusában. A dolgozat célja az volt, hogy feltárja ennek az összetett és sokoldalú koncepciónak az alapjait, architektúráját, alkalmazási lehetőségeit, valamint kihívásait, különös tekintettel az autóiparra mint esettanulmányra.

A dolgozat első része bemutatta a digitális iker fogalmát, fejlődését, valamint azokat a technológiai komponenseket, amelyek lehetővé teszik a működését: érzékelők, adatgyűjtés, szimuláció, felhő- és peremalapú számítási kapacitás, valamint mesterséges intelligencia. Ezek együttesen alkotják azt az ökoszisztémát, amelyben egy digitális iker nem csupán statikus modell, hanem **interaktív, tanuló, prediktív rendszer** lehet.

Az ipari alkalmazási területek vizsgálata során világossá vált, hogy a digitális ikrek nemcsak a gyártási folyamatok hatékonyságát növelhetik, hanem hozzájárulnak az energiahatékonysághoz, a fenntarthatósághoz és a termékminőség állandó kontrolljához is. A különböző példák – a Siemens, a BMW vagy a Tesla – jól illusztrálják, hogy a technológia nemcsak elméleti lehetőség, hanem konkrét üzleti értéket teremt a valóságban.

Az autóipari esettanulmány részletesebben megvilágította, hogyan épül be a digitális iker a járműtervezésbe, a szimulációba, a karbantartásba, sőt akár a járművezetési élménybe is. A jövőben várható, hogy a digitális ikrek szoros szimbiózisban működnek majd mesterséges intelligenciával, így olyan rendszerek jönnek létre, amelyek önállóan képesek optimalizálni saját működésüket – a fejlesztés első fázisától a jármű életciklusa végéig.

Ugyanakkor a fejlődés nem mentes a kihívásoktól: az adatbiztonság, a valós idejű adatfeldolgozás, valamint a rendszerek közötti interoperabilitás még mindig komoly akadályt jelentenek a technológia széles körű adaptációjában.

A jövő kulcsszava tehát az **integráció** – a digitális ikrek összehangolt működése más intelligens rendszerekkel, például MI-vel, edge computinggal vagy felhőalapú szolgáltatásokkal. A siker kulcsa az átfogó ipari ökoszisztéma kialakítása lesz, amelyben a digitális ikrek központi szerepet játszanak az adatalapú döntéshozatalban, az automatizációban és a fenntartható ipari fejlődésben.

A digitális ikrek többé nem csupán egy technológiai trend, hanem egy **stratégiai eszköz** a vállalatok kezében. A jövő iparában – különösen az autóiparban – azok a szereplők lesznek versenyelőnyben, akik nemcsak alkalmazzák, hanem képesek is adaptálni és újraértelmezni a digitális iker-technológia lehetőségeit.

9 KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném megköszönni Hajdu Csaba Tanár Úrnak, valamint a Széchenyi István Egyetemnek, hogy az Ipar 4.0 tantárgy keretein belül lehetőséget biztosítottak számomra a tanulmány megírására.

IRODALOMJEGYZÉK

[1] M. Grieves and J. Vickers, “Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems,” Transdisciplinary Perspectives on Complex Systems, Springer, 2017.

[2] A. Fuller, Z. Fan, C. Day, and C. Barlow, “Digital Twin: Enabling Technologies, Challenges and Open Research,” IEEE Access, vol. 8, pp. 108952–108971, 2020.

[3] NASA, “Modeling, Simulation, Information Technology & Processing Roadmap,” NASA Technology Area 11, 2010.

[4] M. Kritzinger et al., “Digital Twin in manufacturing: A categorical literature review and classification,” IFAC-PapersOnLine, vol. 51, no. 11, pp. 1016–1022, 2018.

[5] E. Negri, L. Fumagalli, and M. Macchi, “A review of the roles of Digital Twin in CPS-based production systems,” Procedia Manufacturing, vol. 11, pp. 939–948, 2017.

[6] H. Kagermann et al., “Recommendations for implementing the strategic initiative INDUSTRIE 4.0,” German National Academy of Science and Engineering, 2013.

[7] A. Slama et al., “Enterprise IoT: Strategies and Best Practices for Connected Products and Services,” O’Reilly Media, 2015.

[8] Object Management Group, “OPC UA and DDS Interoperability,” white paper, 2021.

[9] A. Fuller, Z. Fan, C. Day, and C. Barlow, “Digital Twin: Enabling Technologies, Challenges and Open Research,” *IEEE Access*, vol. 8, pp. 108952–108971, 2020.

[10] E. Negri, L. Fumagalli and M. Macchi, “A Review of the Roles of Digital Twin in CPS-based Production Systems,” *Procedia Manufacturing*, vol. 11, pp. 939-948, 2017.

[11] G. Coulson et al., “A Software Architecture-Based Approach to ROS 2-Based System Integration Using Digital Twins,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 1012–1023, 2021.

[12] M. Grieves and J. Vickers, “Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems,” in *Transdisciplinary Perspectives on Complex Systems*, Springer, 2017.

[13] A. Gabor et al., “Digital Twin Solutions in Manufacturing: A Survey,” *Procedia CIRP*, vol. 91, pp. 131–136, 2020.

[14] R. Stark et al., “Digital Twins for Industrial Applications: A Review,” *CIRP Annals*, vol. 68, no. 2, pp. 1–20, 2019.

[15] NVIDIA, “NVIDIA DRIVE Sim,” [Online]. Elérhető: https://developer.nvidia.com/drive/drive-sim

[16] M. Grieves, “Digital Twin: Manufacturing Excellence through Virtual Factory Replication,” *White Paper*, 2014.

[17] R. Rosen, G. von Wichert, G. Lo, and K. D. Bettenhausen, “About The Importance of Autonomy and Digital Twins for the Future of Manufacturing,” *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.

[18] G. Tao, Z. Zuo, and H. Ren, “Digital Twin Driven Smart Maintenance: Framework and Case Study,” *IEEE Access*, vol. 8, pp. 183019–183032, 2020.

[19] A. Jones et al., “Sustainable Manufacturing Enabled by Digital Twins,” *Procedia CIRP*, vol. 81, pp. 155–160, 2019.

[20] F. Tao et al., “Digital Twin in Industry: State-of-the-Art,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2405–2415, 2019.

[21] J. Negri et al., “A Review of the Roles of Digital Twin in CPS-Based Production Systems,” *Procedia Manufacturing*, vol. 11, pp. 939–948, 2017.

[22] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, “Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0,” *IEEE Access*, vol. 5, pp. 11013–11022, 2017.

[23] M. Kritzinger, W. Karner, G. Traar, J. Henjes, and W. Sihn, “Digital Twin in manufacturing: A categorical literature review and classification,” *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 1016–1022, 2018.

[24] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, “Characterising the Digital Twin: A systematic literature review,” *CIRP Journal of Manufacturing Science and Technology*, vol. 29, pp. 36–52, 2020.

[25] F. Tao et al., “Digital twin driven smart manufacturing: Connotation, reference model, applications and research issues,” *Robotics and Computer-Integrated Manufacturing*, vol. 61, 2020.

[26] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, “Characterising the Digital Twin: A systematic literature review,” *CIRP Journal of Manufacturing Science and Technology*, vol. 29, pp. 36–52, 2020.

[27] BMW Group, “Digitalization in Production,” [Online]. Available: https://www.bmwgroup.com/en/company/production.html (letöltve: 2024.12.10)

[28] Siemens, “Digital Twin for Automotive Industry,” Siemens White Paper, 2021.

[29] Tesla, “Tesla Impact Report 2022,” [Online]. Available: https://www.tesla.com/ns_videos/2022-tesla-impact-report.pdf

[30] J. Leng et al., “Digital twins-based smart manufacturing system design in Industry 4.0: A review,” *Journal of Manufacturing Systems*, vol. 60, pp. 119–132, 2021.

[31] Tesla, “Autopilot AI Day,” [Online]. Available: https://www.tesla.com/AI (letöltve: 2024.11.15)

[32] Siemens, “Virtual Commissioning with Digital Twin,” White Paper, 2022.

[33] OPC Foundation, “OPC UA for Automotive Applications,” 2021. [Online]. Available: https://opcfoundation.org

2.32. Parkolóház kapuvezérlése Arduino Nano segítségével

Parkolóház kapuvezérlése Arduino Nano segítségével

Varga Dorina

mechatronikai mérnök szak, email.: varga.doda@gmail.com

Kulcsszavak: sorompó, LCD kijelző, modellezés, hardver, szoftver, kódolás, szimuláció

1 BEVEZETÉS

A megvalósítandó beágyazott rendszernek egy kapuvezérlést választottam. Úgy gondolom, hogy a modern világban a megnövekedett gépjármű vezetőknek köszönhetően egyre nagyobb szükség van az automatizált beléptető rendszerekre. Alkalmazását tekintve széleskörű felhasználják többek között parkolóházakban, ipari területeken, amit azt az 1 ábra is illusztrálja.

1. ábra: Parkolóházi sorompó (https://sorompo.aas.hu/parkolo-rendszer)

1.1 Rendszer által ellátott feladat ismertetése

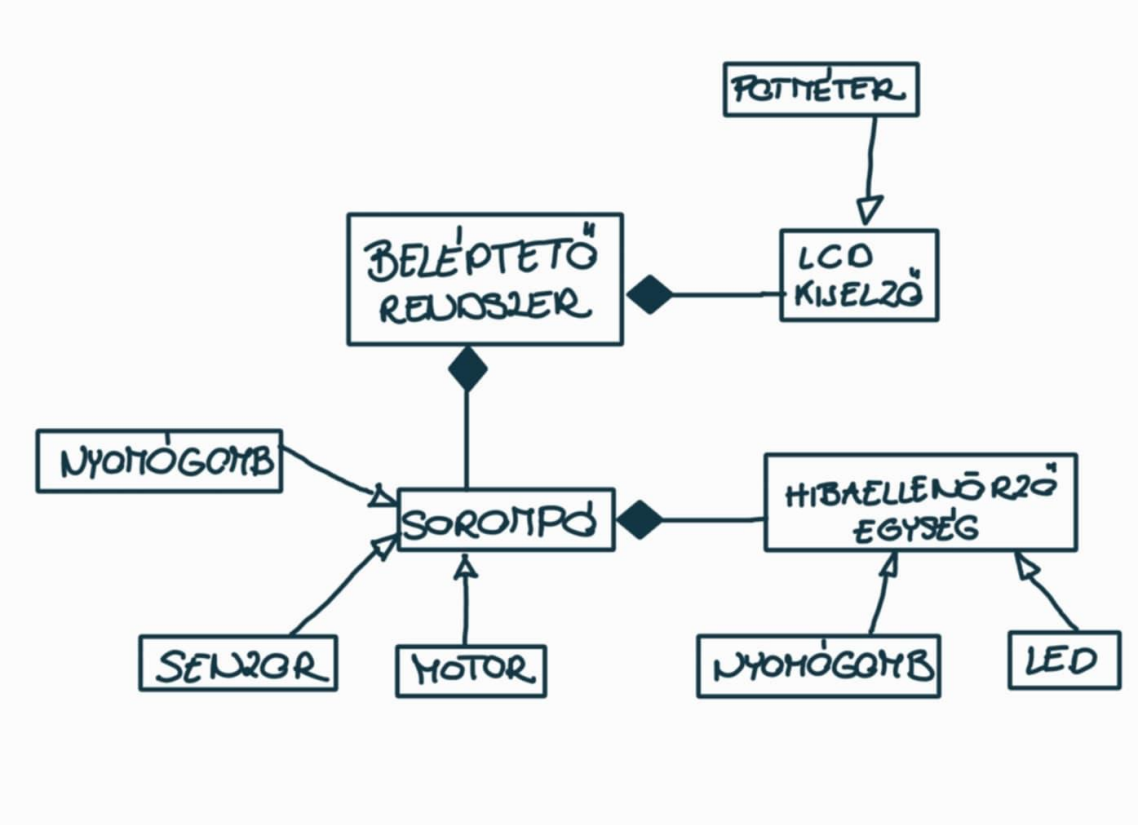
2 sorompó működését írja le, amelyből az egyik a területre beérkező, a másik a területről kihajtó autósokat detektálja. A kapuk nyomógombok segítségével nyithatók és a gépjárművek áthaladását érzékelőkkel figyeljük. A parkolóház aktuális kapacitása egy LCD kijelzőn folyamatosan frissül ezáltal időben tájékoztatva az embereket az aktuális állapotról és elkerülve a területen kialakuló dugókat. Ezt megerősítve azzal a funkcióval, hogy ha nincs rendelkezésre álló szabad hely a beérkező gépjárművet már nem engedi be a sorompó mindaddig, míg a másik kapu egy távozót ki nem engedett. Egyéb

biztonsági feladatot is szükséges volt beépíteni a szenzor végett, mivel hibás működés esetén anyagi károkat és személyi sérüléseket okozhat az átmenő forgalmon. A hiba esetén az a karbantartói irodában jelentkezésre kerül és javítás után egy nyugtázó funkcióval tud folytatódni a működés.

2 TERVEZÉS MENETE

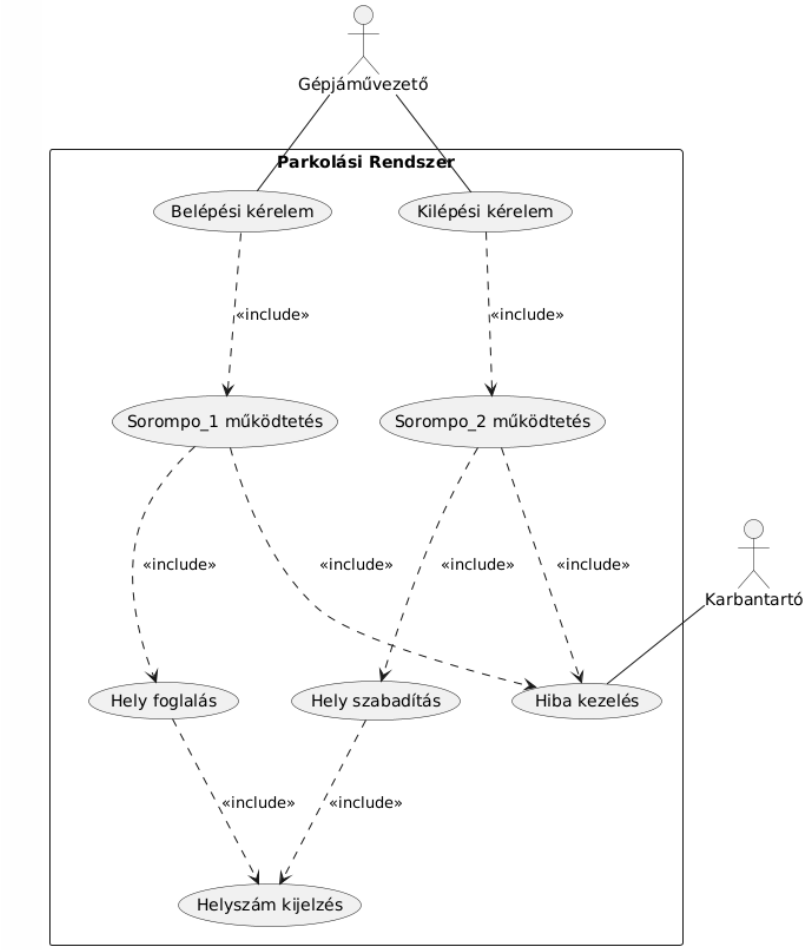
A következő alszakaszok útmutatást adnak a beágyazott rendszer tervezési szakaszáról. A modellezéshez UML és SysML alapokat használtam és elkészítettem a projekthez egy architektúra ábrát és háromfajta diagramot: használati esetről, állapotokról és tevékenységekről (folyamatábrát).

2.1 Architektúra ábra



2. ábra: Parkolási rendszer architektúra ábrája – saját készítés

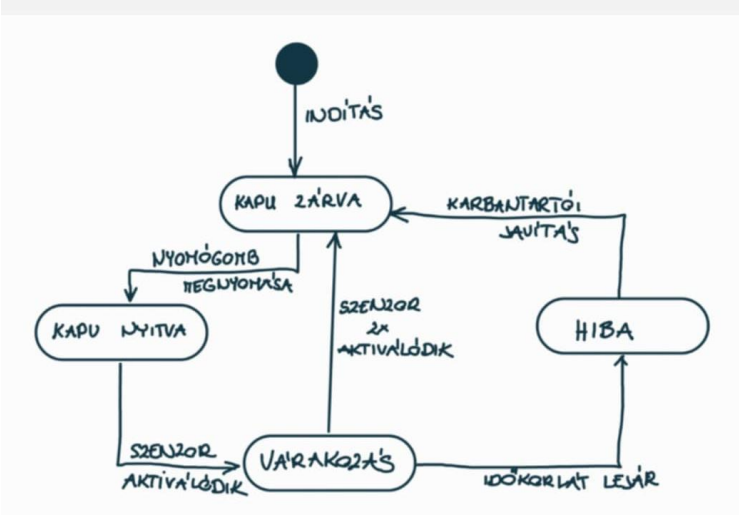
2.2 Használati eset diagram



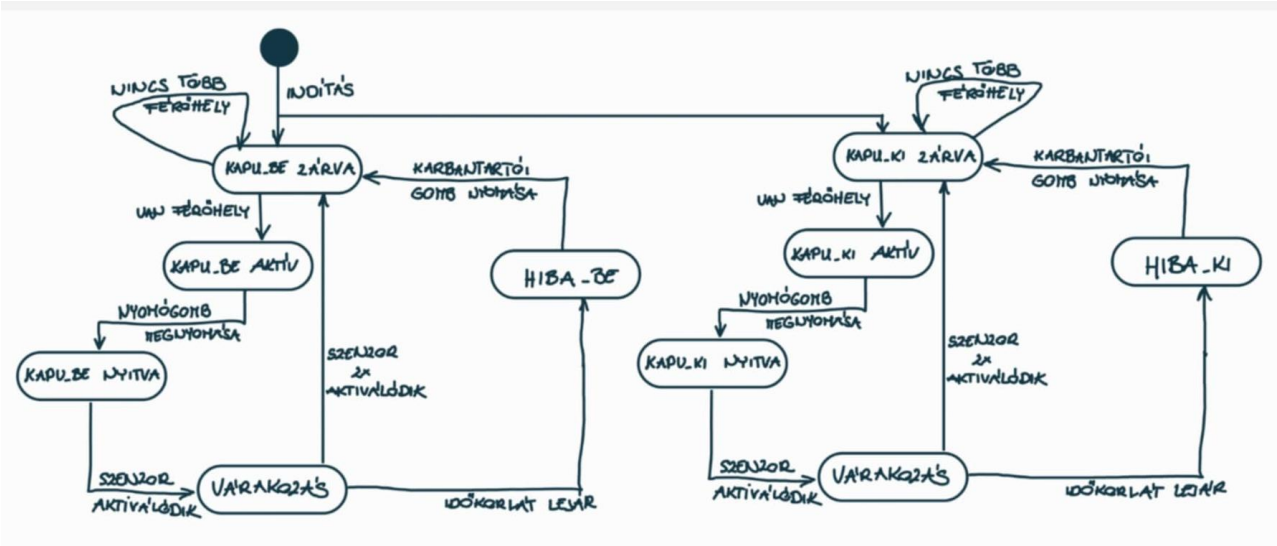
3. ábra: Parkolási rendszer használati eset diagramja - saját készítés a PLANT UML Web Server-ben [2]

A rendszerben 2 aktor vesz részt a gépjárművezető, aki a parkolót igénybe veszi és a karbantartó, aki a felmerülő hibák esetén közbeavatkozik. A használati esetek között include kapcsolatok állnak fel. A két kapu használati esetei megegyeznek, mivel egy kérelemre kezd el működni a sorompó és az magában foglalja a férőhely változását, ami a kijelzőn megjelenik. Ezeken felül még egy használati esetet kell felvenni a hiba kezelésére. A 3. ábra mutatja a teljes használati eset diagramot.

2.3 Állapotdiagram



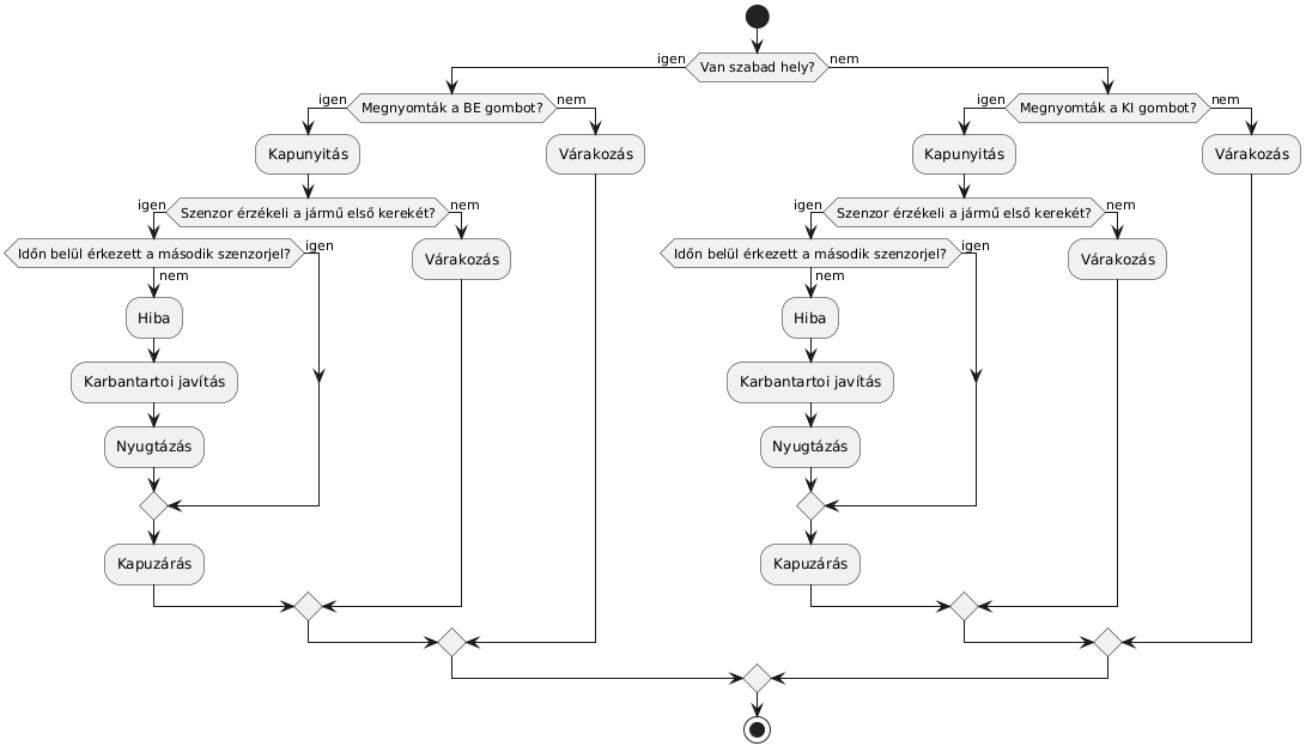
4. ábra: Sorompó állapotdiagramja - saját készítés



5. ábra: Parkolási rendszer állapotdiagramja - saját készítés

A 4. ábra a sorompó megvalósítható általános állapotdiagramját, míg a 5. ábra a teljes rendszer állapotdiagramját tartalmazza.

2.4 Tevékenységdiagram



6. ábra: Parkolási rendszer tevékenységdiagramja - saját készítés a PLANT UML Web Server-ben [2]

Az 6. ábra mutatja milyen elágazások találhatók a rendszer működése közben. A teli kör a belépési pontot, a másik kör a kilépési pontot jelzi, de mivel a projektemben folyamatosan figyeli a szabad helyek számát, így ezt elérve újraindul a folyamat.

3 RENDSZER KOMPOZÍCIÓJA

A következő alszakaszok útmutatást adnak a felhasznált hardver- és szoftver eszközökről.

3.1 Hardverkomponensek

1.táblázat: Beléptető rendszer hardverkomponensei

Név	Kódban megválasztott név	Lábkiosztás	Arduino konfiguráció	Feladata
Arduino UNO	-	-	-	Mikrokontroller: A központi vezérlő

Szervo 1	myServo	D3	PWM kimenet	Belépő kapu
Szervo 2	myServo2	D11	PWM kimenet	Kilépő kapu
Nyomógomb 1	NYOMOGOMB	D2	Digitális bemenet	Belépés kezdeményezése
Nyomógomb 2	NYOMOGOMB_KI	D12	Digitális bemenet	Kilépés kezdeményezése
Karbantartói gomb 1	NYOMOGOMB_KARBANTARTO	A1	Digitális bemenet	Belépő kapunál javítás nyugtázása
Karbantartói gomb 1	NYOMOGOMB_KARBANTARTO_KI	A3	Digitális bemenet	Kiléptető kapunál javítás nyugtázása
Optikai érzékelő 1	OPTIKAI_ERZEKELO	D4	Digitális bemenet	Belépő kapunál szenzor
Optikai érzékelő 2	OPTIKAI_ERZEKELO_KI	D13	Digitális bemenet	Kilépő kapunál szenzor
Figyelmeztető LED 1	FIGYELMEZTETO_LED	A0	Digitális kimenet	Belépő kapunál hiba jelzése
Figyelmeztető LED 2	FIGYELMEZTETO_LED_KI	A2	Digitális kimenet	Kilépő kapunál hiba jelzése
LCD kijelző (16x2)	-	D5-D10	Digitális kimenet	Szabad férőhelyek kijelzése
Potméter	-	LCD 3-as (VO)	-	LCD kijelző kontraszt változtatása
Ellenállás	-	-	-	Eszköz védelem

3.2 Szoftvermodulok

2.táblázat: Beléptető rendszer legfontosabb szoftvermoduljai

Modul neve	Feladat
Főmodulok	
Beengedes	Gombfigyelés, kapunyitás, szenzorok értelmezése, időzített hibaellenőrzés, kapuzárás
Kienged	Hasonló a belépéshez, de a kilépési oldalon
FrissitLCD	Férőhelyek kijelzése
Almodulok	

Hibakezeles	Timeout érzékelése, LED kapcsolás, karbantartási visszaállítás + nyugtázás
Szenzor	Jel érzékelés, visszaszámláló indítás

4 KÓDRÓL

A projektet C++ nyelven a wokwi fejlesztői környezetben készítettem el. A kódoláshoz kétféle könyvtárat a Servo.h, amit a szervok és a LiquidCrystall.h, amit az LCD kijelző beüzemeléséhez használtam fel. Definiáltam az Arduino UNO lábaihoz bekötött hardvereket és létrehoztam a szervo könyvtár által két motor objektumot. Meghatároztam a kezdeti pozíciókat, ami a sorompóknál a zárva, a változóknál pedig a férőhely kivételével a 0 értéket jelentette. A jelenlegi rendszerben a maximális férőhelyek száma 6, azonban ez megváltoztatható, így kompaktá téve a rendszert. A setup részben minden egyes gombhoz egyes alapállapotot detektáltam, amely azt jelentette, hogy a gomb megnyomására 0 értéket vegyen fel. Beirattam a szervo lábaihoz a kezdeti szervo pozíciókat, végül az LCD inicializálásával a kijelző első sorába “szabad helyek”, a második sorában a férohely változó, éppen aktuális értékét adtam meg. A Beengedes és a Kienged szoftver modulok felépítésüket tekintve nagyon hasonlóak, ezek határozzák meg, hogy a kapuk mikor záródhatnak és nyitódhatnak. Legelső lépésben megvizsgálják azt a feltételt, hogy a szervonak milyen az éppen aktuális állapota. Ha zárva van, ellenőrzi a férőhelyek számát és ha a NYOMOGOMB éppen aktuális állapota alacsony, a sorompó felnyílik. Ha a szervo nyitva van, azt jelenti, hogy a gépjármű vezető éppen a sorompó alatt szeretne átjutni. A gépjármű első kerekének érzékelésekor erzekeloSzamlalo változót eggyel növelve és az időzítőt elindítva várja a második kerék megérkezését. Ha a kerék nem érkezik meg az időzítő lejártáig, a sorompó hibára áll ki, amelyet egy led felkapcsolásával jelzésre kerül. Azonban, ha időn belül megérkezik az OPTIKAI_ERZEKELO alacsony jele, a sorompó bezáródik. A hiba esetén a kapu addig nem nyitódik és záródik, míg a javítást a NYOMOGOMB_KARBANTARTO alacsony szintjével le nem nyugtázták. A FrissitLCD részben minden egyes lefutáskor frissül a parkolóházban található szabad helyek száma. Végül a loop teszi lehetővé a program folyamatos futtatását és soros kommunikáción történő változók ellenőrzését.

5 SZIMULÁCIÓ / TESZTELÉS

A szimulációt a wokwi környezetben végeztem. Részegységenként építettem fel a kódot, és minden egység elkészítése után szimulációval teszteltem.

Részegységek:

1. a kapu nyitása, zárása
2. férőhelyek feltételének meghatározása
3. LCD kijelző
4. hiba fellépése
5. hiba jelzése és javítása

6 FEJLESZTÉSI LEHETŐSÉGEK

A biztosabb működés érdekében a kód átírható állapotgép modell alapján.

PROJEKTEM KÓDJA ÉS SZIMULÁCIÓJA ELÉRHETŐ: https://wokwi.com/projects/414816900939651073

IRODALOMJEGYZÉK

[1] https://people.inf.elte.hu/molnarba/Informaciorendszerek_ELTE/Use_case/he.pdf

[2] https://www.plantuml.com/plantuml/uml/TP0zIWH148NpEaKn-GRkJogB9k8c8dY0sjb2ngcPbQfUmHOFq-441h97ABoNBNJG3cpMh_jxpUFRMY0Dfq60sd1KlFUamyztIJlIFOr_X9y1bDj0uxCmDW-a_L7yZ8yy7YooDlW1Y2VZbYo_tx3uzEgJTTZxf2myD4Y6JxTNDRRhBc7B6hjZUKUBjAU3VmLFLg1L3LLRa-5RPxdWIUHVOpt_rgAd0VlkXINc7GNRm2T0KO6BnJNctREydEKDrBBAvHeoMCuhs6PNsVGl

[3] https://www.arduino.cc/en/Tutorial/HomePage/

2.33. vezérlésében szerelősoron

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

IPAR 4.0 Technológiák

Digitális ikrek szerepe és hatása ipari robotkarok vezérlésében szerelősoron

Igali Marcell Károly

[redacted]

(GKNB_INTM087)

2024/2025/2

Tartalom

1. Bevezetés 4
1.1 Az Ipar 4.0 jelentősége 4
1.2 A digitális ikrek technológiájának rövid áttekintése(1.1 Ábra) (1.2 Ábra) 4
1.3 Az esszé célja és felépítése 4
2. A digitális iker fogalma és jelentősége az Ipar 4.0 kontextusában 6
2.1 A digitális iker definíciója 6
2.2 Kiber-fizikai rendszerek (CPS) bemutatása 6
2.3 A valós és virtuális rendszerek kapcsolata (2.2 Ábra) 8
2.4 Előnyök és kihívások 10
3. Ipari robotkarok működése és felépítése 12
3.1 Általános szerkezeti elemek (3.1. Ábra) 12
3.2 Szenzorok szerepe (pozíció-, nyomaték-, sebesség-érzékelők) 13
3.3 Aktuátorok működése és típusai 14
3.4 Tipikus alkalmazási környezetek 15
4. A robotkar mozgásának monitorozása és visszacsatolása 16
4.1 Szenzoros adatok valós idejű gyűjtése 16
4.2 Mérés és adatértelmezés folyamata 18
4.3 Visszacsatolás szerepe a precíz mozgásvezérlésben 19
4.4 Hibaforrások és kompenzálási technikák 21
5. Digitális iker modell és valós idejű vezérlés 22
5.1 Valós idejű adatátvitel folyamata (5.1 Ábra) 22
5.2 A digitális modell és a fizikai rendszer közötti szinkronizáció 24
5.3 Diagnosztika és prediktív karbantartás digitális modellen keresztül 25
5.4 Adatvizualizáció szerepe 26
6.1 Mozgáspálya-optimalizálás algoritmusai 27
6.2 Torlódás- és ütközéselkerülési stratégiák 28
6.3 Tanuló rendszerek integrálása 29
6.4 Valós idejű alkalmazkodás változó környezethez 31
7.Felhőalapú háttérszolgáltatások integrációja 31
7.1 Felhőszolgáltatások szerepe (pl. AWS, Azure IoT) 31
7.2 Adatelemzés és gépi tanulás 34
7.3 Hibadetektálás és prediktív karbantartás felhőn keresztül 34

7.4 Biztonsági kérdések a felhőben 35
8. Kommunikációs protokollok és adatkapcsolatok 36
8.1 OPC-UA alapjai és ipari alkalmazása 36
8.2 MQTT és más IoT-protokollok 37
8.3 Protokollválasztás szempontjai 38
8.4 Interoperabilitás és kompatibilitás 39
9. Esettanulmány: Digitális ikrek alkalmazása egy elektronikai szerelősoron 40
9.1 A szerelősor felépítése és működése 41
9.2 A digitális iker rendszer implementációja 43
9.3 Robotkarok szerepe az adott környezetben 46
9.4 Elért eredmények és tanulságok 47
10. Összefoglalás és jövőbeli kilátások 49
10.1 Főbb tanulságok összegzése 49
10.2 A technológia jövőbeli irányai 49
10.3 További kutatási lehetőségek 49
Források 50

1. Bevezetés

1.1 Az Ipar 4.0 jelentősége

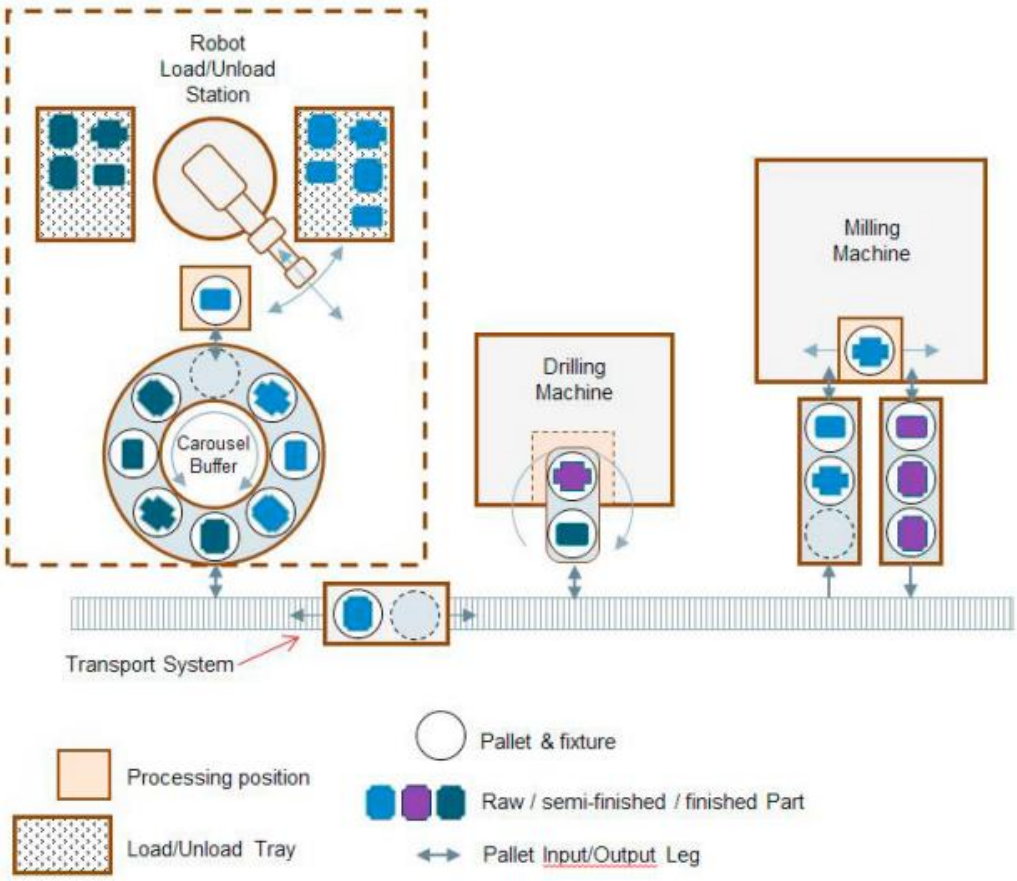
Az ipar napjainkban jelentős átalakuláson megy keresztül, amelyet az Ipar 4.0-nak nevezett koncepció határoz meg. Ez a negyedik ipari forradalom a digitalizációra, az automatizációra, a mesterséges intelligencia integrálására és az intelligens rendszerek összekapcsolására épül. Az Ipar 4.0 lehetővé teszi a gyártási folyamatok valós idejű monitorozását, optimalizálását és adaptív irányítását, ami jelentős hatással van a termelékenységre és a versenyképességre [4].

1.2 A digitális ikrek technológiájának rövid áttekintése(1.1 Ábra) (1.2 Ábra)

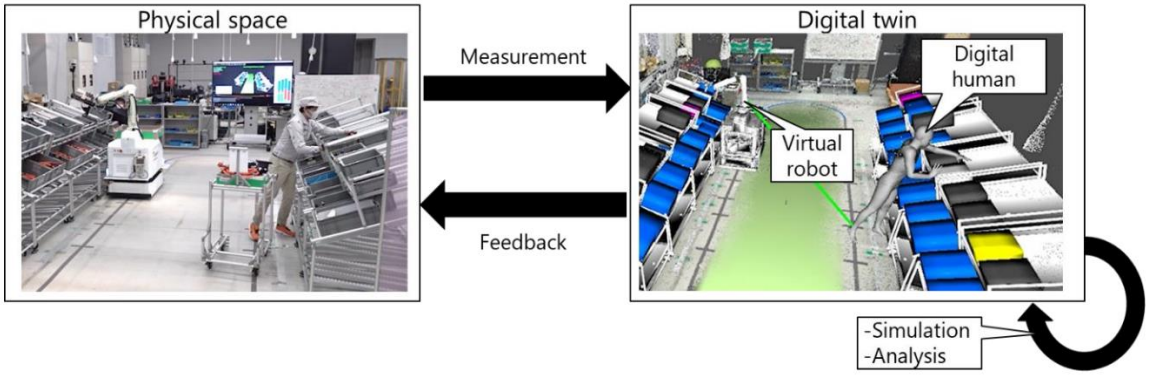
A digitális iker (Digital Twin) olyan virtuális modell, amely egy valós eszköz, folyamat vagy rendszer digitális reprezentációját jelenti. E modell képes tükrözni a fizikai megfelelőjének állapotát, viselkedését és teljesítményét valós időben, amelyhez szenzoradatok és vezérlési utasítások folyamatos áramlása szükséges [1][2]. Az ipari alkalmazások terén a digitális ikrek elősegítik az előrejelzéseket, diagnosztikát és a rendszeroptimalizálást is [3].

1.3 Az esszé célja és felépítése

Az esszé célja, hogy bemutassa a digitális ikrek szerepét és hatását az ipari robotkarok vezérlésében, különösen a szerelősorokon történő alkalmazások kontextusában. Az esszé tíz fejezeten keresztül vezeti végig az olvasót a technológia elméleti alapjaitól kezdve, a technikai részleteken át, egészen a konkrét esettanulmányig. A főbb témák között szerepelnek a digitális ikrek architektúrája, a robotkarok felépítése és működése, valós idejű vezérlés, felhőalapú rendszerek, valamint kommunikációs protokollok és alkalmazási példák is.



1.1 Ábra Robotkar CPS([3] p. 4 Fig. 6)



1.2. Ábra Digitális iker környezet ([8] p. 2. Fig. 1)

2. A digitális iker fogalma és jelentősége az Ipar 4.0 kontextusában

2.1 A digitális iker definíciója

A digitális iker egy dinamikus, adatvezérelt digitális reprezentáció, amely egy fizikai objektum vagy rendszer életciklusát valós időben tükrözi. Grieves és Vickers [1] megfogalmazása szerint a digitális iker három fő komponenst foglal magába: a fizikai rendszert, a digitális reprezentációt és a köztük lévő adatkapcsolatot. A digitális ikrek lehetővé teszik a szimulációkat, elemzéseket és optimalizálásokat anélkül, hogy közvetlenül be kellene avatkozni a valós rendszerbe [5].

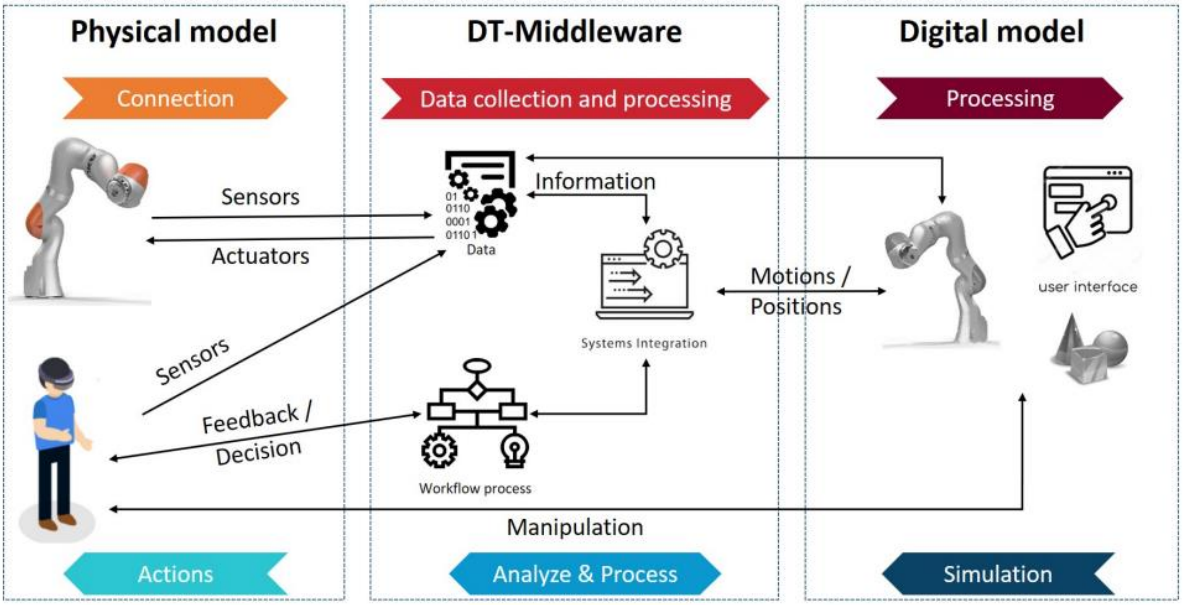
2.2 Kiber-fizikai rendszerek (CPS) bemutatása

A kiber-fizikai rendszer (Cyber-Physical System, CPS) olyan integrált architektúra, amelyben a fizikai komponensek (gépek, berendezések, robotkarok stb.) és az informatikai réteg (szoftverek, hálózati összeköttetések, felhőszolgáltatások) szoros együttműködésben valós időben cserélnek adatot és reagálnak a környezeti változásokra. A CPS-ek célja, hogy egyesítsék a beágyazott rendszerek determinisztikus vezérlését a nagy teljesítményű adatfeldolgozással, így a fizikai valóság és a digitális modell folyamatosan szinkronban legyen egymással [4].

Egy kiber-fizikai rendszer tipikus felépítése három rétegre bomlik (2.1. Ábra):

1. **Fizikai réteg**
   - Szenzorok*:* mérik a környezeti és működési paramétereket (hőmérséklet, nyomaték, sebesség, helyzet, rezgés stb.).
   - Aktuátorok*:* mechanikai hajtások, amelyek a vezérlő utasítására végrehajtják a fizikai változtatásokat (például robotkar mozgatása).
2. **Kommunikációs réteg**
   - Helyi hálózatok: EtherCAT, PROFINET és OPC UA protokollok biztosítják a determinisztikus, valós idejű adatcserét a gyártórendszeren belül [7].
   - Felhőkapcsolat*:* MQTT vagy HTTPS alapú csatornák segítségével a helyi vezérlők és a felhőszolgáltatások között küldenek adatot, ahol nagyteljesítményű elemzések futnak [26].
3. **Digitális réteg**
   - Edge computing*:* helyben végzett előfeldolgozás, amely csökkenti a késleltetést és a hálózati terhelést.
   - Felhőszolgáltatások: felhőalapú adatbázisok, nagy teljesítményű gépi tanulási modellek és prediktív karbantartó algoritmusok futnak, elemezve a beérkezett szenzoradatokat [27].

- Digitális iker modul*:* a fizikai rendszer virtuális másolatát tartja karban, és valós időben frissíti a memóriában tárolt modellt, hogy szimulációkat és előrejelzéseket készítsen [1][2].



2.1. Ábra CPS felépítése ([10] p. 9 Fig. 5)

A CPS-ek kulcseleme a zárt hurkú vezérlés (closed-loop control), ahol a fizikai réteg jelzései (pl. pozíció vagy nyomatékadatok) azonnal visszacsatolódnak a feldolgozó egységbe, és real-time módon módosítják az aktuátorok vezérlőjeleit. Ez a modell lehetővé teszi a reactive (valós idejű reakció) és a proactive (előrejelző) vezérlési stratégiák kombinálását: a CPS nem csupán reagál a fizikai változásokra, de előre is jelezheti a lehetséges hibákat és karbantartási igényeket [6].

Az Ipar 4.0 környezetében a CPS-ek jelentik az adatvezérelt automatizálás gerincét. Egy robotkar CPS-be ágyazva képes:

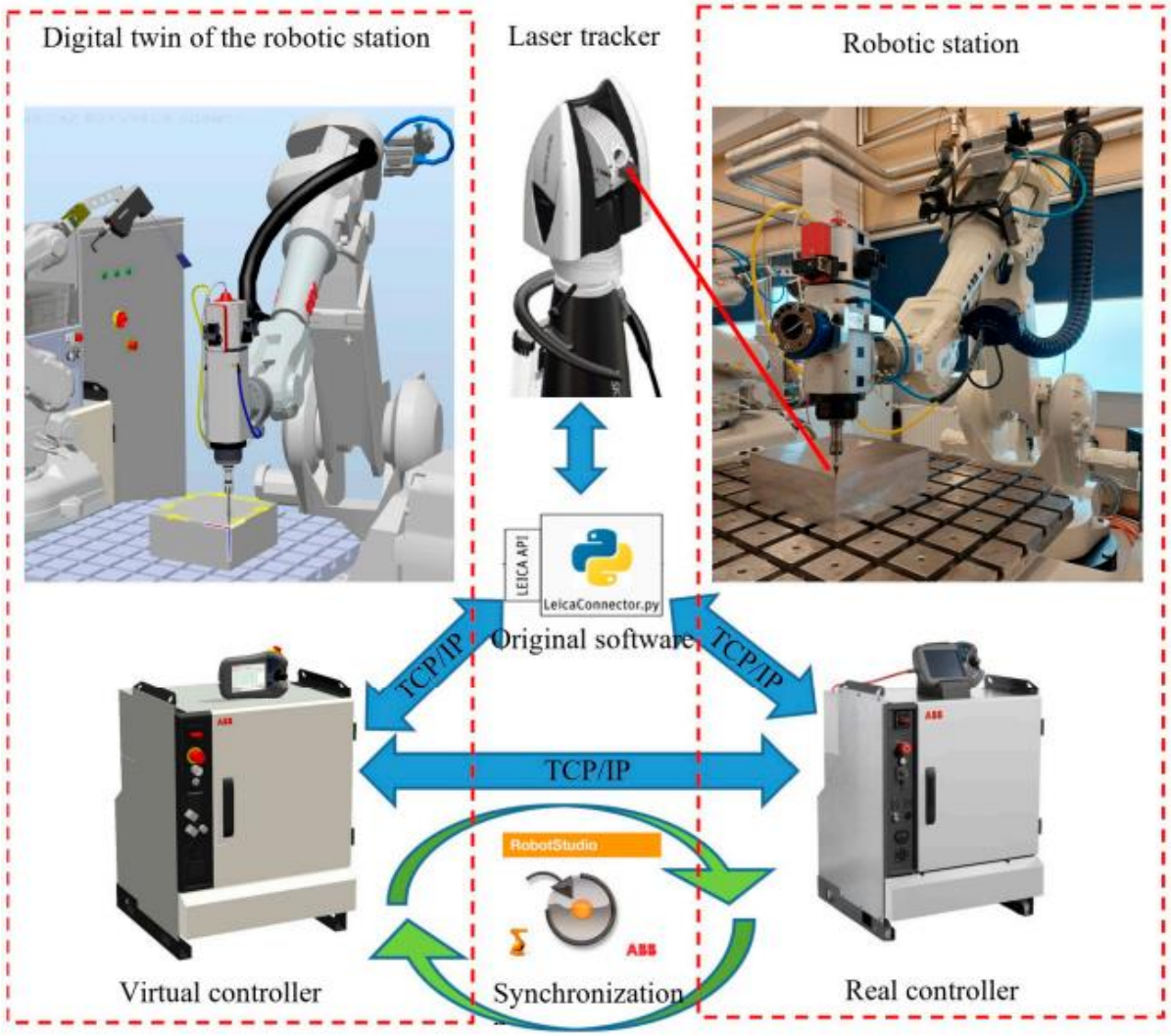
- Valós idejű monitoringra, ahol a terepi szenzorok folyamatos adatot küldenek a központi felügyeletnek.
- Prediktív karbantartásra, mely során a digitális iker előre jelzi a kopás jeleit és ütemezett karbantartást javasol.
- Adaptív vezérlésre, amikor a rendszer – például egy hirtelen terhelésnövekedés vagy környezeti zavar esetén – valós időben módosítja a mozgáspályákat vagy sebességprofilokat a minőség és biztonság megőrzése érdekében [3].

Mindezek alapján a CPS olyan intelligens architektúrát hoz létre, amelyben a fizikai és digitális világ összekapcsolódik, és egységes keretrendszert alkot az ipari gépek, robotkark és szerelősorok vezérléséhez és optimalizálásához.

2.3 A valós és virtuális rendszerek kapcsolata (2.2 Ábra)

A digitális iker lényege, hogy a fizikai és a virtuális rendszerek valós időben szoros kölcsönhatásban álljanak egymással. Ezt a kapcsolatot két, egymást kiegészítő fogalom írja le: a digitális árnyék (digital shadow) és a digitális ikerszál (digital thread) [1], [2].

- **Digitális árnyék** alatt azt az automatikusan frissülő adatfolyamot értjük, amely a fizikai eszköz (például egy robotkar) szenzorai által gyűjtött valós idejű mérési adatokat közvetíti a virtuális modell felé. Ez a folyamatos adatkapcsolat biztosítja, hogy a digitális iker minden pillanatban a legfrissebb állapotot tükrözze.
- **Digitális ikerszál** az a folytonos információsor, amely összeköti a tervezési, gyártási és üzemeltetési fázisokat: a CAD-modellektől és gyártásirányító rendszerektől a szenzoradatok gyűjtéséig, elemzéséig és a vezérlőparancsok visszaküldéséig terjedő folyamat [4].



2.2 Ábra Digitális iker és Fizikai világ közti kölcsönhatás ([13] p. 10. Fig. 6)

E két fogalom megvalósítása szempontjából a következő komponensek kulcsfontosságúak:

1. **Időszinkronizáció**

   A fizikai és a virtuális rendszerek között a mérési és vezérlési adatok millimásodperces pontossággal kell, hogy cserélődjenek. Ehhez ipari környezetben gyakran alkalmaznak precíz hálózati időszinkronizációt (pl. IEEE 1588 PTP), amely garantálja, hogy a szenzoradatok és a szimulációs modul egységes idővonalon fusson [12].

2. **Késleltetés és adatkonzisztencia**

   A valós idejű vezérléshez elfogadhatatlanul nagy késleltetés (latency) gyártási selejtet és biztonsági kockázatot okozhat. Ezért élvonalbeli CPS-architektúrákban (edge computing) előfeldolgozás történik a gyártósor közelében, a kritikus döntések pedig helyben, minimális hálózati késleltéssel születnek [12], [15].

3. **Modellefok (fidelity)**

   A virtuális modellnek reprodukálnia kell a fizikai rendszer dinamikáját, beleértve a robotkar mechanikáját, tömegeloszlását és vezérlési nemlinearitásait. A magasabb modellefok azt jelenti, hogy a virtuális tesztek és előrejelzések pontosabban tükrözik a valós viselkedést, ugyanakkor nagyobb számítási kapacitást igényelnek [5].

4. **Kétirányú visszacsatolás**

   A szenzoroktól érkező adatokat a digitális iker folyamatosan elemzi (diagnosztika, prediktív karbantartás), majd vezérlési parancsok formájában visszaküldi a fizikai rendszer felé. Ez a zárt hurkú architektúra teszi lehetővé, hogy a robotkar a tényleges állapotváltozásokhoz adaptív módon igazítsa a mozgástervezést [1], [2].

5. **Middleware és szabványos interfészek**

   Az interoperabilitás biztosításához elengedhetetlenek a szabványos protokollok (például OPC UA), valamint olyan middleware-rétegek, amelyek elrejtik a hardware-specifikus részleteket, és egységes API-kat biztosítanak a virtuális modellek és a fizikai eszközök között [7].

6. **Biztonság és adatvédelmi megfontolások**

   A valós és virtuális rendszerek közötti adatforgalom védelme kritikus, hiszen a vezérlőparancsok manipulálása akár súlyos üzemzavarokat is okozhat. A titkosított kommunikáció és a jogosultságkezelés mellett a belső auditnaplók és integritás-ellenőrzések biztosítják, hogy az adatok ne változhassanak meg illetéktelenül [19].

Összefoglalva, a valósidejű és kétirányú kapcsolat egy olyan CPS-architektúrát hoz létre, ahol a fizikai robotkar és a digitális iker folyamatos, szinkronizált párbeszédben áll. Ez a szoros integráció teszi lehetővé az Ipar 4.0-ban az adaptív, prediktív és intelligens vezérlési stratégiákat, amelyek révén a gyártási folyamatok hatékonyabbá és megbízhatóbbá válhatnak.

2.4 Előnyök és kihívások

A kiber-fizikai rendszerek és digitális ikrek integrációja az ipari gyártásban számos jelentős előnnyel jár, ugyanakkor komoly műszaki és szervezeti kihívásokat is támaszt.

Előnyök:

1. **Folyamatoptimalizálás és rugalmasság**

   A digitális iker segítségével a gyártási paramétereket valós időben lehet követni és finomhangolni, ami növeli a termelési sebességet és csökkenti a holtidőt. Előre jelezhetővé válnak a szűk keresztmetszetek, így adaptív újraütemezés alkalmazható a szerelősor kapacitásának jobb kihasználása érdekében [2], [6].

2. **Prediktív karbantartás**

   A folyamatos szenzoradat-elemzés (pl. vibráció, hőmérséklet, nyomaték) lehetővé teszi a kopáshelyzetek korai felismerését, amivel minimalizálhatók a váratlan leállások és a kapcsolódó veszteségek. A digitális iker jobb karbantartási ütemezést biztosít, csökkentve a karbantartási költségeket akár 20–30%-kal [3].

3. **Minőségjavítás**

   A valós idejű visszacsatolás és szimuláció révén a gyártási folyamat során korán detektálhatók a minőségi eltérések, ami kevesebb selejtet és utólagos javítást eredményez. Így a termékek konzisztensen megfelelnek a specifikációknak, és csökken a vevői reklamációk aránya [5].

4. **Gyorsabb piacra lépés (time-to-market)**

   Virtuális tesztkörnyezetekben a termékek és gyártósor-tervek iteratív tesztelése lényegesen gyorsabb, mint a hagyományos fizikai prototípusok gyártása. A digitális iker támogatja az úgynevezett „first-time-right” elvet, amely csökkenti a drága tervezési újrafuttatásokat [1], [4].

5. **Energia- és erőforrás-hatékonyság**

   A digitális iker valós idejű adatainak elemzése révén optimalizálható a gépek energiafogyasztása és anyagfelhasználása, ami nemcsak költségmegtakarítást, hanem fenntarthatóbb üzemeltetést is eredményez [6].

Kihívások:

1. **Rendszerintegráció és szabványosítás hiánya**

   A gyártóberendezések többsége eltérő kommunikációs protokollokat és interfészeket használ. A CPS-ekbe való integrálás igényli az OPC UA, MQTT vagy egyedi middleware megoldások bevezetését, ami hosszú fejlesztési és tesztelési ciklusokat vonhat maga után [7].

2. **Adatkezelés és -minőség**

   A nagymennyiségű, heterogén szenzoradat tisztítása, normalizálása és valós idejű feldolgozása komoly informatikai erőforrásokat és szakértői know-how-t igényel. Az adatintegritás biztosítása kritikus, hiszen egy pontatlan adat rontja a digitális iker prediktív képességeit [19].

3. **Kiberbiztonság és adatvédelem**

   A fizikai rendszerekhez való távoli hozzáférés és a felhőszolgáltatások felé irányuló adatforgalom új támadási felületet nyit. Biztosítani kell a titkosított kommunikációt, a jogosultságkezelést és a folyamatos auditálást, hogy elkerülhető legyen a vezérlőparancsok manipulációja vagy az ipari kémkedés [19].

4. **Késleltetés és valós idejű követelmények**

   Az adaptív vezérléshez alacsony mikroszekundumos késleltetésre van szükség, amit nehéz elérni nagy távolságú felhőhöz való csatlakozás esetén. Edge computing megoldásokkal lehet csökkenteni a hálózati késleltetést, de ez extra beruházást és üzemeltetési komplexitást jelent [12].

5. **Szakmai kompetenciahiány**

   A CPS-ek és digitális ikrek üzemeltetéséhez átfogó tudásra van szükség mind gépészeti, mind informatikai területen. Jelenleg világszerte hiány mutatkozik olyan mérnökökből és fejlesztőkből, akik mindkét szakirányban jártasak lennének, ezért a vállalatoknak képzési programokat és külső szakértői támogatást kell igénybe venniük [6].

Összességében a digitális ikrek és CPS-ek alkalmazása jelentős üzleti és műszaki előnyökkel kecsegtet, de csak átgondolt, holisztikus megközelítés és megfelelő szakértelem mellett lehet sikeresen megvalósítani. A következő fejezetekben részletesen vizsgáljuk a technológia ipari robotkarok vezérlésében rejlő gyakorlati lehetőségeket és esettanulmányokat.

3. Ipari robotkarok működése és felépítése

Az ipari robotkarok olyan automatizált manipulátorok, amelyek meghatározott tevékenységek (hegesztés, festés, összeszerelés stb.) elvégzésére specializáltak. A robotkar felépítése és működése szorosan kapcsolódik a mozgástervezéshez, a vezérlőrendszerekhez és a beépített szenzorokhoz, amelyek együttesen biztosítják a precíz és megbízható működést [28].

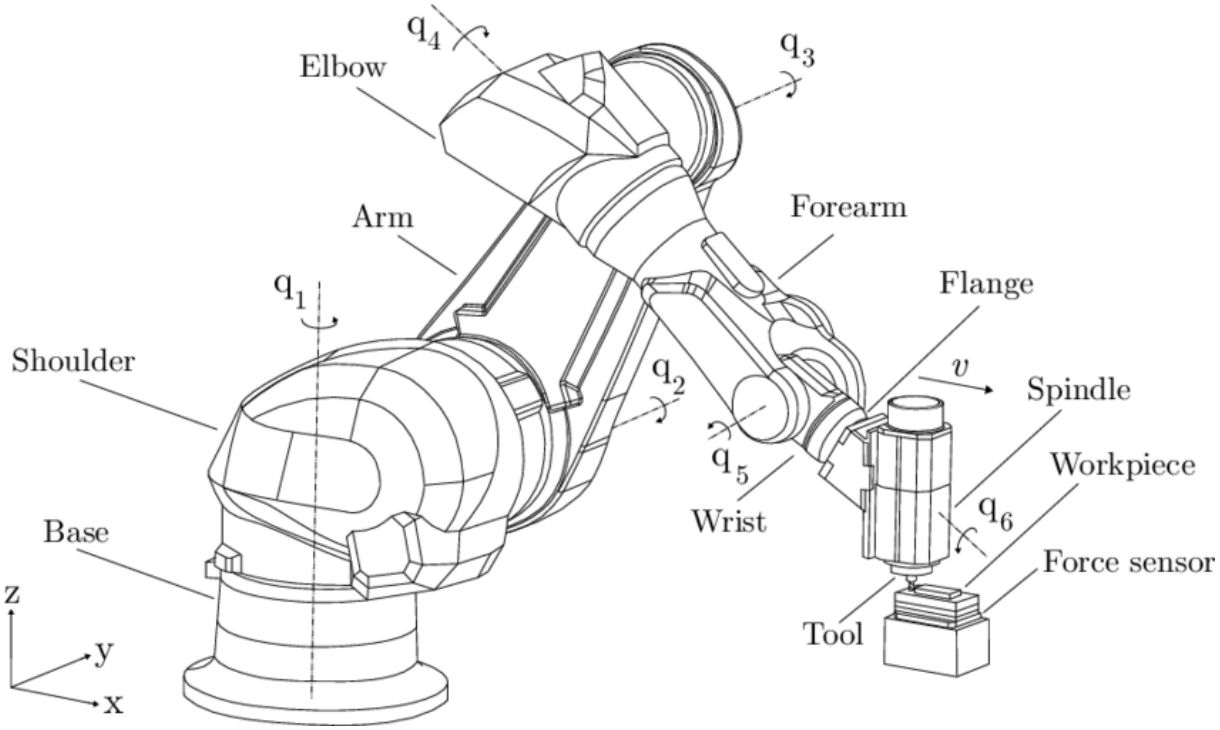
A robotkar fő célja, hogy a végszerszám (*end effector*) pozícióját és orientációját a háromdimenziós térben határozott pontokra és irányokra mozgassa. Az ipari robotok általában hat szabadságfokkal (6 DOF) rendelkeznek, amely lehetővé teszi bonyolult térbeli pályák követését és a különböző irányból történő munkavégzést. A szabadságfokok száma és elrendezése (pl. karos, SCARA, delta) határozza meg a robot mozgásgeometriáját, elérési tartományát és teherbírását [28].

A robotkar vezérlőegysége egy beágyazott ipari PC, amely valós időben futtatja a mozgástervező algoritmusokat és a zárt hurkú szabályozást. A vezérlő a beprogramozott feladatot ütemezi, és koordinált parancsokat küld az aktuátoroknak, miközben folyamatosan figyeli a szenzoroktól érkező visszajelzéseket. A modern robotokban egyre gyakrabban használják a PLC-k (Programmable Logic Controller) és a valós idejű operációs rendszerek kombinációját, hogy a meghajtás és biztonsági rétegek elkülönüljenek [29].

3.1 Általános szerkezeti elemek (3.1. Ábra)

1. **Alap (Base):** A robotkar fix alapszerkezete, amelyhez a többi elem csatlakozik. Tartja a robotot és szolgáltatja a támasztékot valamint az energiát és adatkapcsolatot.
2. **Váll (Shoulder):** Az első forgástengely, amely a kar fő mozgását biztosítja oldalirányban.
3. **Könyök (Elbow):** A második tengely, amely lehetővé teszi a kar előre-hátra mozgatását, s ezzel a hatótávolság beállítását.
4. **Csukló (Wrist):** A kar végén található több tengely, amelyek a végszerszám orientációját pontosan szabályozzák (forgás, dőlés, billenés).
5. **Linkek:** A tengelyeket összekötő mechanikai karok, amelyek lehetnek hengeres profilúak vagy merev keretszerkezetűek az erőátvitel biztosítására.
6. **Végszerszám (End Effector):** A konkrét feladatot végzi (pl. fogó, hegesztőpisztoly). Modulárisan cserélhető, a munkafolyamat igénye szerint [28].

A robotkar statikai és dinamikai analízise során modellezik a linkek tömegét, a csapágyak súrlódását és a hajtómotorok nyomatékát, hogy a vezérlőrendszer pontosan előre tudja jelezni a kar reakcióit. A teherbírás – maximális terhelőmomentum – meghatározása kulcsfontosságú a biztonságos és hosszú élettartamú működéshez.



3.1. Ábra Robotkar részei

(https://www.researchgate.net/figure/axis-industrial-robot-Staeubli-TX200-robot_fig1_326106790)

3.2 Szenzorok szerepe (pozíció-, nyomaték-, sebesség-érzékelők)

A zárt hurkú vezérlés alapja a valós idejű szenzoradat, amelynek fő típusaival a robotkar megbízhatósága és pontossága garantálható:

- Pozícióérzékelők**:**
    - Forgó enkóderek (optikai vagy mágneses) méri a tengelyek pontos szöghelyzetét, akár 0,01° pontossággal. Ezek szolgáltatják a legfontosabb visszajelzést a tengelyek aktuális állásáról.
    - Lineáris mérőelemek (pl. LVDT) a lineáris mozgásokhoz, bár ipari robotkarnál ritkábbak, ha kiegészítő lineáris tengely van beépítve.
- Sebességérzékelők**:**
    - A forgó enkóderekből differenciálással számolható a tengelyek aktuális fordulatszáma.
    - Tachométerek vagy hall-szenzorok esetén közvetlenül mérik a motorfordulatot, különösen a gyors dinamikájú mozgásoknál hasznosak [29].
- Nyomatékérzékelők**:**

- Nyomatékszenzorok (elektromos vagy piezoelektromos) a hajtóműben érzékelik a tényleges terhelést, segítve az ütközések detektálását és az ember-robot együttműködés biztonsági elemeit [30].
- Erő/nyomaték-tomopárok (FT-szenzorok) a végszerszám közelében mérik a fogóerőt vagy a hegesztés közbeni erőhatásokat.

A szenzorokból érkező jelek magas mintavételi frekvenciájú A/D átalakítókon mennek keresztül, majd a vezérlőegység FPGA- vagy DSP-alapú gyors jelfeldolgozásban dolgozza fel őket. Ez a folyamat biztosítja, hogy a zárt hurkú PID- vagy adaptív szabályozók rendelkezésére álljanak a valós idejű hibajelek.

3.3 Aktuátorok működése és típusai

Az ipari robotkar mozgatását végző aktuátorok felelősek a mechanikai energia előállításáért és szabályozott átadásáért. A leggyakoribb típusok közé a villamos szervomotorok, a pneumatikus és a hidraulikus hajtások tartoznak [11].

- Villamos szervomotorok
  - Legelterjedtebbek az ipari robotkarokban nagy pontosságuk és gyors reakciójuk miatt. A motorok belsejében állandó mágnes és tekercsek találhatók, melyek között a vezérlő áramgenerátorral állítja be a kívánt forgónyomatékot és fordulatszámot. A beépített enkóder visszajelzi a tengely pontos pozícióját, így zárt hurkú (closed-loop) szabályozás valósul meg [11].
  - Előnyük a tiszta működés (nincs folyadék), könnyű hűthetőség és karbantarthatóság. Hátrányuk, hogy nagyobb terhelés esetén több motorra vagy sebességváltó egységre van szükség.
- Pneumatikus aktuátorok
  - Sűrített levegővel működnek, erő-súly arányuk kedvező, és rendkívül gyors bekapcsolás-kikapcsolás jellemzi őket. Általában kisebb pontosságú pozícionálást tesznek lehetővé (±0,1–1 mm). Óriási előnyük a robusztusság, illetve a gyúlékonyság- és szikramentesség (kémiai vagy tűzveszélyes környezetben) [11].
  - Hátrányuk a sűrített levegő ellátásának energiaigénye és a viszonylag alacsony pontosság.
- Hidraulikus aktuátorok
  - Nagy erőkifejtésre képesek kis méretben, hiszen a folyadék nem összenyomható, így nagyon pontos nyomásszabályozás révén nagy nyomatékot adhatnak át. Gyakoriak olyan alkalmazásokban, ahol nagy terhelés vagy ütő-ütő mozgás szükséges (pl. préselés, hajlítás) [11].
  - Hátrányuk a folyadékszivárgás, karbantartási igény és a zaj.

A modern robotkarok gyakran kombinált rendszereket alkalmaznak: a fő mozgásokhoz villamos szervomotorok, a speciális erőhatásokhoz nyomatékszenzorral ellátott hidraulikus egységek vagy gyors pneumatikus modulok integrálódnak. A hajtásrendszerhez tartoznak még a sebességváltók (harmónikus hajtóművek vagy bolygóművek), amelyek fokozzák a torziós merevséget és csökkentik a motorfordulat-tartományt a kívánt tengelysebességre [11]. Az aktuátorok összjátéka biztosítja a robotkar dinamikus pontosságát, terhelhetőségét és tartósságát, ami kritikus a szerelősoron végzett precíziós feladatoknál.

3.4 Tipikus alkalmazási környezetek

Az ipari robotkarok sokféle gyártási környezetben alkalmazhatók, ahol magas sebesség, ismételhetőség és megbízhatóság szükséges. A leggyakoribb szektorok:

1. Autóipar
    - Festőcellák, hegesztőállomások és összeszerelő sorok, ahol a robotkarok egymást követő elemeket precízen illesztenek vagy hegesztenek. A nagy mozgástartomány és teherbírás miatt jellemzőek a többrobot-konfigurációk, ahol minden kar speciális feladatot lát el [11].
2. Elektronikai gyártás
    - PCB-k összeszerelése és forrasztás, ahol milliméteres pontosság és finom erőszabályozás szükséges. Gyakran alkalmaznak SCARA karokat az alacsonyabb tényleges terhelés és nagy ciklussebesség miatt [14].
3. Élelmiszer- és csomagolóipar
    - Csomagoló-sorok, palackozás és válogatás, ahol a higiéniai követelmények miatt előny a könnyen tisztítható pneumatikus vagy speciális bevonatú robotkar [6].
4. Farmácia és vegyipar
    - Aszeptikus környezetben, ahol a robbanásveszély és a szigorú tisztítási előírások meghatározzák az aktuátortípusokat (például szenvedélymentes, zárt pneumatikus hajtások) [6].
5. Kutatás és oktatás
    - Robotikai laborokban, ahol moduláris, könnyen programozható cobotok segítik a hallgatók és kutatók prototípus-fejlesztési feladatait [8].
6. Humán-robot együttműködés (HRC)
    - Együttműködő robotok (cobotok) biztosítják a munkaterület megosztását a kezelővel, erő-nyomaték korlátok és szoftveres biztonsági zónák alkalmazásával [8].

A tipikus ipari alkalmazási környezetekben a robotkark telepítésekor fontos a padlóteherbírás, a védőkerítések és biztonsági zónák kialakítása, valamint az automatizált

anyagmozgató rendszerek integrációja (pl. futószalagok, AGV-k). A környezet dust- és splash-proof, valamint EMC-kompatibilis kialakítása biztosítja a folytonos, megbízható termelést. A jövő iránya az adaptív üzem felé mutat, ahol a robotkarok a digitális ikrek révén automatikusan újratervezik a munkapályáikat, ahogy a gyártási rendelés változik [23].

4. A robotkar mozgásának monitorozása és visszacsatolása

A digitális iker alapú kiber-fizikai rendszerben (CPS) a robotkar mozgásának folyamatos monitorozása és visszacsatolása elengedhetetlen a precíz és megbízható működéshez. A beágyazott szenzorok valós idejű adatokat szolgáltatnak a kar pozíciójáról, sebességéről és erőhatásairól, amelyeket zárt hurkú vezérlőalgoritmusok dolgoznak fel [12]. Ezek az adatok táplálják a virtuális modellt, így a digitális iker mindig naprakészen tükrözi a fizikai eszköz állapotát és dinamikáját [1]. A visszacsatolás révén a rendszer képes azonnal korrigálni az eltéréseket és adaptív módon reagálni a váratlan terhelés- vagy környezeti változásokra. Ezzel a módszerrel a szerelősoron dolgozó robotkarok hatékonysága, biztonsága és termelékenysége egyaránt jelentősen növelhető.

4.1 Szenzoros adatok valós idejű gyűjtése

A digitális iker és a CPS-k működésének alapja a valós idejű szenzoradat-gyűjtés, amely lehetővé teszi a fizikai robotkar állapotának folyamatos megfigyelését és a digitális modell pontos szinkronizációját. A szenzoradatok gyűjtése több szinten és több protokollon keresztül valósul meg, ahol az adatok első lépésben a robotkar beágyazott vezérlőegységéhez, majd innen az edge és felhő rétegekbe jutnak.

1. Perifériás szenzorhálózat kialakítása

    - Minden forgástengelyhez optikai vagy mágneses enkóder tartozik, melyek 1 kHz és 10 kHz közötti mintavételi frekvenciával képesek pozíció- és sebességadatokat szolgáltatni. A nyomaték- és erőmérő szenzorok (FT-csuklók) mintavétele szintén nagysebességű (500–1 000 Hz), hogy az ütközések vagy terhelésváltozások azonnal detektálhatók legyenek.

    - A hőmérséklet-, rezgés- és hűtőközeg-áramlás-mérők egészítik ki a mozgásadatokat, lehetővé téve a robotkar környezeti és mechanikai állapotának teljességre törekvő monitorozását.

2. Edge computing és adatgyűjtő szoftverek

    - A helyszínen (edge) telepített számítási csomópont(ok) feladata a szenzoradatok előfeldolgozása és hibamentesítése, mielőtt azok a felhő felé továbbítódnának. Az Apache NiFi mint adatintegrációs eszköz biztosítja az adatfolyamok dinamikus kezelését, prioritásos továbbítását és az eredetkövetését.

- Az OPC UA szolgáltatásai lehetővé teszik a szenzoradatok standardizált lekérdezését és eseményalapú publikálását, ami kulcsfontosságú a digitális iker valós idejű szinkronizációjához. Többgyártós eszköz környezetben az OPC UA beágyazott szerverek automatikusan továbbítják a friss értékeket a CPS middleware rétegbe [20], [17].

3. Valós idejű adatátvitel

    - A helyi vezérlőegységek (PLC vagy valós idejű PC) által összegyűjtött szenzoradatok először a robotkar vezérlőbuszán (pl. EtherCAT) mozognak, majd az edge csomópontokon keresztül TCP/IP, MQTT vagy HTTPS protokollokon jutnak el a felhőbe.

    - A magasabb szintű adatgyűjtő réteg az Azure Digital Twins platformot is használhatja a CPS-ben, ahol a különböző forrásból érkező adatokat egységesen tárolják, és a digitális iker komponenseinek szolgáltatják (adatbázis-szolgáltatások, stream-analízis)[21].

4. Adatminőség és szűrés (4.1 Ábra)

    - A beérkező nyers adatok zajcsökkentését és kalibrálását a helyi egységek végzik (pl. FIR/ IIR szűrők, kompenzációs függvények), így a digitális iker már megbízható, konzisztens adatokat kap.

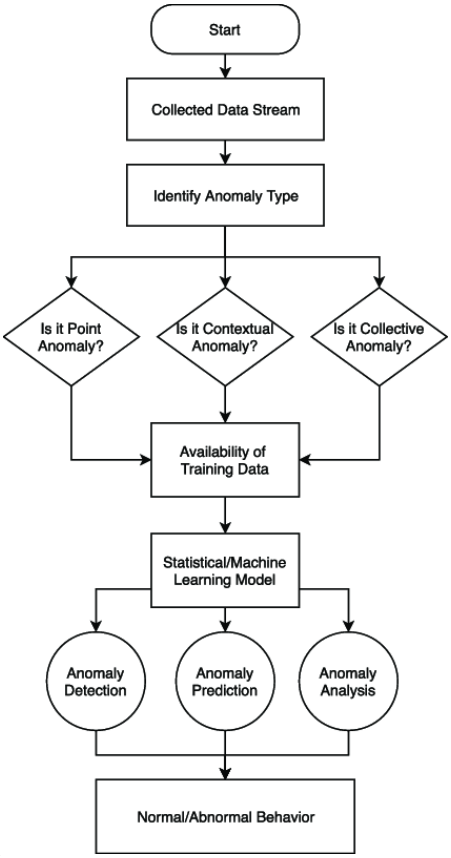
    - Anomália-észlelő algoritmusok valós időben kiszűrik a kiugró értékeket, és riasztást generálnak a hasonló CPS-ekben alkalmazott felügyeleti rendszerek felé [17].

5. Digitális iker frissítés

    - A feldolgozott szenzoradatok az edge csomópontokból a digitális ikerhez kötődő stream-be kerülnek, ahol REST API vagy MQTT topic segítségével folyamatosan frissítik a virtuális modellt.

    - A digitális iker elemző moduljai (diagnosztika, prediktív karbantartás) ezekre az adatfolyamokra építve hajtanak végre valós idejű szimulációkat és előrejelzéseket, melyek visszacsatolható vezérlőparancsokat generálnak a robotnak.

A valós idejű szenzoradat-gyűjtés kulcsfontosságú ahhoz, hogy a CPS és digitális iker integrációja az ipari robotkarok vezérlésében megbízható, adaptív és prediktív legyen. A szenzoradatok magas mintavételi gyakorisága, a megbízható edge computing infrastruktúra és a szabványos adatcsere-protokollok együttesen garantálják a digitális iker pontosságát és a vezérlési hurkok hatékonyságát.



4.1 Ábra Anomália detektálás folyamat diagram

(https://www.researchgate.net/figure/The-flow-chart-of-anomaly-detection-systems_fig1_344737972)

4.2 Mérés és adatértelmezés folyamata

A robotkar mozgásának pontos vezérléséhez elengedhetetlen a szenzorokból érkező nyers jelek megfelelő mérése, majd ezek értelmezése a digitális iker számára. A folyamat három fő lépésre bontható: adatgyűjtés és kalibráció, jelfeldolgozás (szűrés és adat-fúzió), valamint a fizikai állapot modellezése és diagnosztikája.

1. Adatgyűjtés és kalibráció

    - A pozíció-, sebesség- és erőmérő szenzorok analóg vagy digitális jeleit valós időben mintavételezik (1–10 kHz tartomány), majd A/D átalakítók digitalizálják.

    - Minden szenzort rendszeresen kalibrálni kell: a gyártó specifikációinak megfelelően nullpont-beállítást és linearizálást végeznek, hogy a digitális ikerbe továbbított értékek pontosan tükrözzék a fizikai mennyiségeket [12].

2. Jelfeldolgozás és adat-fúzió

    - A nyers jelek zajcsökkentését digitális szűrők (pl. FIR, IIR) végzik, amelyek megszűrik a mechanikai rezgések és elektromos interferenciák által okozott kitéréseket.

- Több szenzor–pl. enkóder és giroszkóp–adatainak fúziója segít a helyzet- és sebességbecslés pontosságának növelésében: Kalman-szűrő vagy kiterjesztett Kalman-szűrő alkalmazásával a digitális iker egyesíti a különböző mintavételi frekvenciájú adatfolyamokat [17].

3. Állapotmodellezés és diagnosztika

    - A megtisztított adatok a digitális iker dinamikai modelljébe kerülnek, ahol a robotkar kinematikai és dinamikai egyenletek alapján számítják a várt állapotokat (pozíció, sebesség, nyomaték) [3].

    - A várt és a mért állapotok közötti eltérésekből a hiba-vektor képződik, amelyet hibabecslő algoritmusok (PID-hurkok, adaptív szabályozók) felhasználnak az azonnali korrekcióhoz. Ugyanez a hiba-vektor táplálja a prediktív karbantartási modulokat: ha tartósan jelentős eltérés mutatkozik, a digitális iker előrejelzi a kopási folyamatot és karbantartási riasztást generál [16].

4. Értelmezés és visszacsatolás

    - A digitális iker dashboard-ja vizualizálja a legfontosabb mutatókat (helyzet, sebesség, nyomaték, hőmérséklet), és valós idejű riasztásokat küld a rendszergazdának vagy a felhőalapú felügyeleti szolgáltatásnak.

    - A diagnosztikai modul kiegészülhet gépi tanulási technikákkal (anomália-észlelés, klaszterelemzés), amelyeket offline tanítottak a korábbi üzemadatokon. Ezek az algoritmusok automatikusan felismerik a szokatlan működési mintákat, és javaslatot tesznek a vezérlési paraméterek finomhangolására vagy karbantartási beavatkozásra [19].

E munkafolyamat eredményeként a robotkar és a digitális iker közötti zárt hurkú visszacsatolás a fizikai mozgások és a virtuális szimulációk között folyamatosan friss és pontos információkat cserél, biztosítva a rendszer adaptivitását, megbízhatóságát és hosszú távú stabilitását.

4.3 Visszacsatolás szerepe a precíz mozgásvezérlésben

A precíz mozgásvezérlés alapja a zárt hurkú visszacsatolás (closed-loop feedback), ahol a vezérlő folyamatosan összeveti a kívánt és a tényleges állapotot, majd a hiba alapján korrigálja az aktuátorok bemenetét. Ebben a folyamatban a digitális iker kiber-fizikai rendszerként (CPS) tovább fokozza a pontosságot és megbízhatóságot, mivel a visszajelzések nemcsak a helyi vezérlőhöz, hanem a virtuális modellhez is eljutnak, amely valós idejű szimulációk segítségével segíti a korrekciót [12].

A visszacsatolás két fő komponense a pozicionálási hiba és a dinamikai eltérés. A pozíció- és sebességérzékelők által szolgáltatott jeleket a vezérlő PID-algoritmusa dolgozza fel, amely három paraméter (arányos, integráló, deriváló) hangolásával minimalizálja a hiba-vektort. A digitális iker ebben a hurkú rendszerben előre jelzi a várt viselkedést a fizikai modell alapján, így előrekompenzációval csökkenti a késleltetések és nemlineáris torzítások hatását [3]. Ennek

eredményeként a robotkar képes mikrométeres pontosságra és alacsony jitter-re (kis pozícióingadozás) [12].

A dinamikai visszacsatolás ugyancsak kulcsfontosságú: a robotkar mozgása során fellépő gyors gyorsulások, terhelésváltozások vagy ütközések hirtelen nyomatékigényt generálnak az aktuátorokban. A nyomaték- és erőérzékelők (FT-szenzorok) folyamatosan mérik ezeket az eltéréseket, és a digitális iker biztosítja, hogy a virtuális modell is kövesse a dinamikai változásokat. Ezáltal a vezérlő adaptív stratégiákat alkalmazhat—például erőalapú pályakorrekciót—, ami különösen fontos az együttműködő robotoknál (cobotok), ahol az ember-robot interakció során hirtelen fellépő külső erők automatikus kompenzációja elengedhetetlen [13].

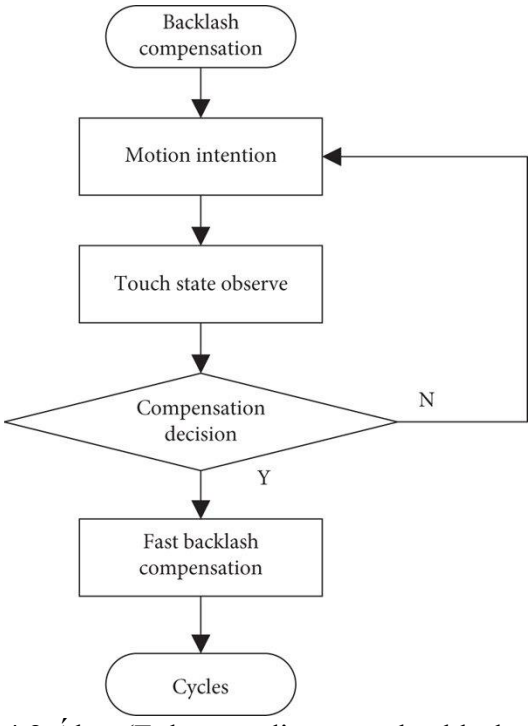
A digitális iker a visszacsatolási hurkot tovább bővíti azzal, hogy a fizikai, valósidejű adatokat egy prediktív modellben is futtatja. A digitális iker előrejelzései alapján a vezérlő már a hiba kialakulása előtt képes módosítani a mozgásterveket (feed-forward + feedback kombináció), ezzel csökkentve a stabilizációs időt és a túllövést [17]. A Tripathy és munkatársai által javasolt architektúrában a digitális iker a helyi vezérlőhöz hasonló zárt hurkot alkot, de ráépül a felhőalapú elemző réteg is, ahol gépi tanuló modellek finomhangolják a vezérlési paramétereket hosszabb távú üzemadatok alapján [17].

A visszacsatolás minőségét nagyban befolyásolja a kommunikációs késleltetés és az adatcsomag-veszteség. A digitális iker és a CPS esetében kulcsfontosságú, hogy a visszacsatolt jelek edge rétegen előszűrés után, alacsony késleltetésű protokollokon (pl. EtherCAT, OPC UA PubSub) érkezzenek a vezérlőhöz [20]. A Mourtzis és munkatársai által bemutatott valós idejű adatgyűjtés- és vezérlési keretrendszer pontosan ezt valósítja meg, így a precíz mozgásvezérlés feltételei – alacsony lateráció és magas adatminőség – egyaránt teljesülnek [12].

Összefoglalva, a zárt hurkú visszacsatolás a digitális ikerrel kiegészülve az ipari robotkarok vezérlésének gerincét alkotja. A fizikai szenzoradatok és a virtuális szimulációk párhuzamos kezelése lehetővé teszi a gyorsabb korrekciót, csökkenti a hibákat, és támogatja az adaptív és prediktív vezérlési stratégiákat, amelyek elengedhetetlenek a modern szerelősori automatizálásban.

4.4 Hibaforrások és kompenzálási technikák

A robotkar mozgásvezérlésében számos hibaforrás csökkenti a pontosságot és a megbízhatóságot. Ezek közé tartoznak a szenzorok pontatlanságai (kvantálási zaj, drifts, kalibrációs eltérések), a mechanikai szabadságfokok holtjátéka (backlash (4.2 Ábra)), a termikus deformációk, valamint a kommunikációs késleltetések és adatcsomag-veszteségek a CPS hálózatokban [12], [19]. A digitális iker segítségével azonban fejlett kompenzálási technikák alkalmazhatók, amelyek holisztikusan kezelik ezeket a hibákat.



4.2 Ábra (Folyamat diagram a backlash-ről)

(https://www.researchgate.net/figure/Process-diagram-of-backlash-compensation_fig11_347046788)

Először is, a szenzorkalibráció rendszeres futtatása csökkenti a driftszerű eltolódásokat. A digitális ikerben futó kalibrációs modul automatikusan összehasonlítja a szenzorok által mért adatokat a fizikai modell várt értékeivel, és kidolgozza a korrekciós függvényeket, amelyeket a helyi vezérlőegység alkalmaz [12]. Másodszor, a mechanikai holtjáték és súrlódás hatását backlash-kompenzációs algoritmusok kezelik: ezek a digitális iker segítségével prediktíven módosítják a mozgásterveket, hogy a visszacsatolt helyzetminimális eltolásokat tükrözhessen [13].

A termikus hatások (pl. a motorhőmérséklet növekedése miatt fellépő anyagdeformáció) kezelésére a CPS-be épített hőmérséklet-szenzorok adatai alapján hőtágulási modell építhető. A digitális iker szimulációjában a valós hőmérséklet függvényében lineáris vagy nemlineáris korrekciót számít, így a fizikai kar a változó környezeti feltételek ellenére is megtartja pozíciós pontosságát [16].

A kommunikációban fellépő késleltetés és adatveszteség hibáját az előrekompenzációs (feed-forward) vezérlés és az állapotrekonstrukciós megfigyelők (pl. Kalman-szűrők)

együttesen csökkentik. A digitális iker folyamatosan futtatja a modellalapú megfigyelőt, amely a hiányzó vagy késedelmes szenzoradatokat prediktíven becsli, így a vezérlőben mindig rendelkezésre áll egy megbízható becslés [17].

Végül, a gépi tanulási alapú adaptív kompenzáció új dimenziót ad a hibakezelésnek: hosszabb távú üzemadatok elemzésével neurális hálók tanulják meg a könnyen előforduló nemlinearitásokat és kopási jellegzetességeket, majd a digitális iker valós időben alkalmazza a megtanult korrekciós mintákat. Ez a megközelítés különösen hatékony a prediktív karbantartás keretében, ahol a hibajelző mintázatok felismerése által megelőzhetőek a kritikus meghibásodások [19].

E kombinált, digitális ikerrel támogatott kompenzálási stratégia az ipari robotkarok mozgásvezérlésében jelentősen javítja a pontosságot, rugalmasságot és megbízhatóságot, lehetővé téve a szerelősorok folyamatos, zavarmentes működését.

5. Digitális iker modell és valós idejű vezérlés

5.1 Valós idejű adatátvitel folyamata (5.1 Ábra)

A digitális iker és a fizikai robotkar közötti valós idejű adatátvitel három rétegen zajlik: a perifériás, az edge, és a felhő rétegen. Minden réteg feladata a megbízható, alacsony késleltetésű adatgyűjtés, -feldolgozás és -átadás biztosítása, hogy a vezérlési hurkok és a prediktív modellek mindig naprakészek legyenek.

1. **Perifériás réteg – Szenzoradatok begyűjtése és előfeldolgozása**

A robotkar tengelyeihez szerelt optikai vagy mágneses enkóderek, nyomaték- és erőmérő szenzorok, valamint hő- és rezgésérzékelők adatátvétele gyakran 1–10 kHz-es mintavételi frekvenciával történik. Ezek a nyers jelek először az A/D átalakítókba kerülnek, majd közvetlenül a helyi vezérlőegység (PLC vagy beágyazott valós idejű PC) buszrendszerére (EtherCAT vagy PROFINET) jutnak, ahol a determinisztikus ciklusidő garantálja a konzisztens, időzített adatcserét [12]. A perifériás egységekben első körben zajszűrés (pl. digitális FIR/IIR szűrők) és kalibráció (offset- és skálabeállítás) történik, hogy a hibák már itt minimalizálódjanak.

2. **Edge réteg – Lokális aggregáció és integráció**

A vezérlőbuszról érkező, megtisztított adatcsomagokat az edge csomópontok – speciális ipari számítógépek vagy mini-szerverek – gyűjtik össze. Itt futnak a szoftveres adatintegrációs eszközök, például az Apache NiFi, mely biztosítja az adatfolyam származási nyomon követését, prioritáskezelését és gyors hibadetektálását [26]. Az edge réteg feldolgozási feladatai közé tartozik az OPC UA PubSub szolgáltatás beágyazott futtatása, amellyel a szenzoradatok egységesített objektumként publikus/előfizetéses modellben továbbíthatók [20]. A helyszíni

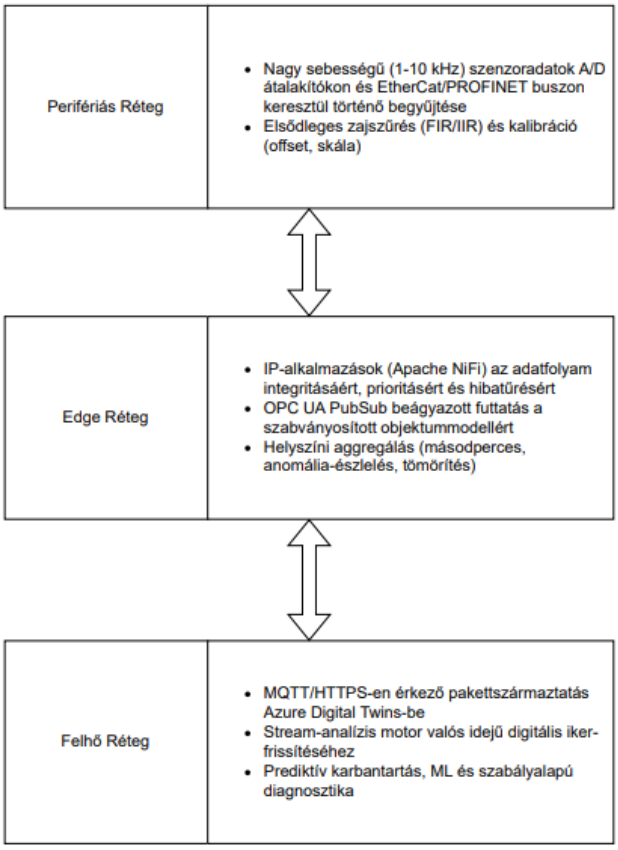
előfeldolgozás (másodperces szintű aggregálás, anomália-észlelés, tömörítés) csökkenti a hálózati forgalmat és a felhő terhelését.

3. Felhő réteg – Digitális iker és magas szintű analitika

Az edge csomópontokból a feldolgozott adatokat általában MQTT-n vagy HTTPS-en keresztül továbbítják a felhőbe. Az Azure Digital Twins platform fogadja az üzeneteket, és valós időben frissíti a digitális modellt [21]. A beérkező adatfolyamokat egy stream-analízis motor (pl. Azure Stream Analytics) dolgozza fel, amely feed-forward vezérlési jeleket generál a digitális iker számára. A felhőben futó prediktív karbantartó algoritmusok – gépi tanulás és szabályalapú diagnosztika kombinációja – folyamatosan elemezik az adatokat, és riasztásokat vagy korrekciós javaslatokat küldenek vissza az edge hurokhoz.

Teljes körű megvalósítási példa

Tripathy et al. egy hibrid OPC UA / ISO 10303 STEP alapú architektúrát ír le, ahol az edge és a felhő közötti adatcsere szigorúan szabványosított modellinformációs csomagokra épül, így a termékéletciklus-információk is konzisztensen átadhatók [17]. Matsive és munkatársai pedig bemutatnak egy soft actor-critic reinforcement learning alapú valós idejű vezérlési keretrendszert, amely 5–10 ms end-to-end késleltetéssel éri el a CPS rétegek közötti zökkenőmentes adatáramlást [18].



5.1 Ábra 3 Átviteli Réteg (Saját készítés)

5.2 A digitális modell és a fizikai rendszer közötti szinkronizáció

A digitális iker és a fizikai robotkar közötti szinkronizáció garantálja, hogy a virtuális másolat mindig a valós időben történő állapotváltozásokat tükrözze, és a vezérlési döntések mindkét oldalon konzisztensen érvényesüljenek. Ennek megvalósítása több összetevőt igényel:

A szenzoradatok időbélyegzése az első lépés: minden mérési értékhez pontosan rögzített időpont tartozik, amely lehetővé teszi a digitális iker számára a kronológiai sorrend szerinti visszajátszást és összevetést. A CPS környezetben alkalmazott IEEE 1588 PTP protokoll vagy az NTP-alapú megoldások biztosítják a rendszerszintű időszinkronizációt, hogy millimásodperces pontossággal lehessen összehasonlítani a helyi és felhőbeli időállapotokat [12].

A állapotreprezentáció egységes adattípusokra épül: a fizikai kar kinematikai és dinamikai paramétereit (pozíció, sebesség, nyomaték) JSON- vagy OPC UA modellobjektumokként tárolja, amelyeket az Azure Digital Twins JSON-sémák segítségével standardizál [21]. A digitális iker minden frissítésnél végrehajt egy állapotrekonziliációs eljárást, amelyben a bejövő szenzoradatok és a szimulációs modell kimenete közötti eltéréseket kiszámítja, és eldönti, szükséges-e a modellparaméterek (például súrlódási együttható, tömegeloszlás) automatikus korrekciója [2].

A edge és felhő közötti replikáció fontos láncszem: az edge rétegben futó digitális árnyék (digital shadow) folyamatosan rögzíti a fizikai kar valós idejű állapotát, majd periodikus snapshotok vagy eseményvezérelt frissítések formájában továbbítja a felhő felé. Itt a digitális iker központi szervere egy időben vett pillanatképet készít, amelyhez a teljes korábbi eseménytörténet is rendelkezésre áll az idősoros adatbázisban. Ez a részletes eseménytörténet lehetővé teszi az auditálást és az utólagos analitikát is [19].

A kétirányú állapotkonzisztencia fenntartásához a digitális iker a vezérlőparancsokat is regisztrálja. Amikor a felhőben egy prediktív algoritmus (gépi tanulás vagy model-alapú diagnosztika) új paraméterekkel javasol vezérlőbeállításokat, ezek a parancsok feed-forward üzenetként visszakerülnek az edge rétegbe, ahol a lokális zárt hurkú szabályozó végrehajtja őket. A végrehajtott állapotot ismét a szenzoradatok igazolják vissza, ezzel bezárul a kétirányú szinkronizációs hurkok láncolata [17].

Végül a modellfrissítés során a digitális iker képes automatikusan módosítani a szimulációs modellen alkalmazott paramétereket a fizikai rendszer viselkedése alapján. Ez a önkalibrációs folyamat folyamatosan finomhangolja a robotkar modellezését, így a digitális iker egyre pontosabbá válik, és a CPS egésze megbízhatóbb prediktív analitikát és vezérlést tesz lehetővé [1]. A Grieves által bevezetett architektúra alapján a digitális iker így nem csupán statikus tükör, hanem dinamikusan adaptálódó entitás, amely lökhárító a fizikai tér nemlineáris zavarai és a vezérlési algoritmus stabil működése között.

5.3 Diagnosztika és prediktív karbantartás digitális modellen keresztül

A digitális iker egyik legnagyobb üzleti értéke a diagnosztikai és prediktív karbantartási funkciók integrálása a gyártási folyamatba. A digitális modellen keresztül gyűjtött valós idejű és történeti szenzoradatok elemzésével a rendszer képes automatikusan felismerni a kopás, túlterhelés vagy rendellenes viselkedés kezdeti jeleit, még mielőtt az meghibásodáshoz vezetne.

A diagnosztika első lépéseként a digitális iker a szenzoradatokat összeveti a fizikai modell által szimulált elvárt állapotokkal. Amely szenzoradatok jelentős eltérést mutatnak (pl. növekvő rezgés- vagy hőmérsékletingadozás a kar csuklóján), a rendszer beágyazott anomália-észlelő algoritmus aktiválódik. Ezek lehetnek szabályalapú (threshold) ellenőrzések, de egyre gyakrabban alkalmaznak gépi tanulási alapú klaszterelemzést vagy neurális háló-specifikus detektorokat, amelyek a normálistól való finom eltolódásokat is képesek kiszűrni [16].

A prediktív karbantartás során a digitális iker nem csak észleli a hibákat, hanem előre is jelzi a várható meghibásodások időpontját. A prédiktív modulok statisztikai modelleket (pl. Weibull-eloszlás) vagy idősoros gépi tanulási algoritmusokat (pl. LSTM hálók) alkalmaznak a korábbi diagnosztikai események és üzemi adatok alapján [19]. Amikor a modell a várható élettartam közelgő végét vagy kritikus kopási küszöb átlépését jósolja, a rendszer automatikusan ütemezett karbantartási feladatot generál a vállalat erőforrás-tervező moduljában, minimalizálva a tervezetlen leállásokból adódó költségeket.

Az end-to-end karbantartási folyamat a digitális ikerrel így a következő elemekből áll:

1. Adatgyűjtés és előfeldolgozás edge és felhő réteg segítségével.
2. Anomália-észlelés a diagnosztikai modulban (szabály- vagy AI-alapú).
3. Élettartam-előrejelzés idősoros elemzéssel és statisztikai modellezéssel.
4. Karbantartási igény automatikus ütemezése és visszacsatolása a ERP/CMMS rendszerbe.
5. Visszajelzés és újratanulás, ahol az elvégzett karbantartás hatását visszavezetik a digitális modellbe, tovább finomítva a prediktív algoritmusokat [16][19].

A Yao et al. által bemutatott több-szintű feladat-újraütemezés esettanulmánya mutatja, hogy a prediktív karbantartás során keletkező karbantartási ablakokat a gyártási ütemezésbe integrálhatjuk, ezzel minimalizálva a termelés-kiesést és megszakítatlanul fenntartva a szerelősor teljesítményét [23].

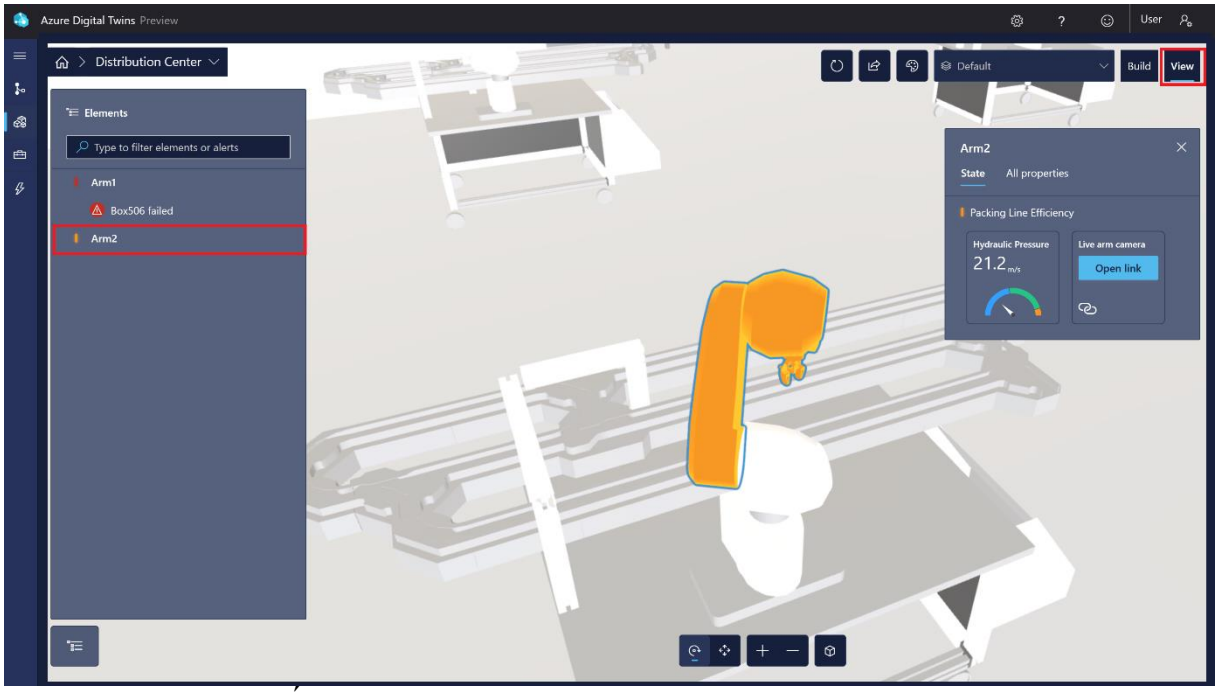
Ezek a digitális iker alapú diagnosztika és prediktív karbantartás megoldások jelentős költségmegtakarítást és megnövelt termelékenységet biztosítanak, hiszen a váratlan gépleállások helyett tervezett, optimalizált karbantartási ablakokat tesznek lehetővé, miközben a modell folyamatosan tanul a valós eredményekből, és egyre pontosabb előrejelzéseket produkál.

5.4 Adatvizualizáció szerepe

Az adatvizualizáció kulcsfontosságú a digitális iker és a CPS által gyűjtött nagymennyiségű, komplex adatok értelmezésében. A valós idejű és történeti adatok grafikus megjelenítése lehetővé teszi a mérnökök és üzemeltetők számára, hogy gyorsan felismerjék a trendeket, kiugró értékeket és potenciális problémákat, ezáltal támogatva a megalapozott döntéshozatalt.

Elsősorban a dashboardok szolgálnak felületként: ezek interaktív felületeken mutatják a legfontosabb kulcs teljesítménymutatókat (KPI), például a robotkarok pozíció és nyomatékprofilját, ciklusidőket, hibaüzeneteket és karbantartási riasztásokat. A dashboardokon alkalmazott idősoros diagramok segítségével követhető, hogyan változtak a szenzoradatok hosszabb időtávon, így a prediktív karbantartó modul által jelzett kopási trendek könnyen validálhatók a valós adatok alapján [21].

Emellett a 3D-s vizualizáció egyre inkább előtérbe kerül: olyan szoftverek, mint az Azure Digital Twins Explorer (5.2 Ábra), lehetővé teszik a fizikai környezet és a robotkar valós idejű, valósághű megjelenítését a böngészőben. A 3D-s ikernézetben a felhasználó virtuálisan bejárhatja a szerelősort, kiválaszthatja a kar egy-egy komponensét, és megtekintheti annak aktuális állapotát, hőmérsékletét vagy vibrációs mintázatait a digitális modellen ábrázolt szín- és formakódok segítségével [4].



5.2 Ábra Azure Digital Twins Explorer CAD környezet

(https://learn.microsoft.com/en-us/azure/digital-twins/quickstart-3d-scenes-studio)

Az eseményalapú vizualizáció (event-driven visualization) lehetővé teszi, hogy kritikus események – például hirtelen nyomatékemelkedés, szenzorhibák vagy hálózati kiesések – automatikusan kiemelve jelenjenek meg a felületen. A felugró (pop-up) értesítések és az “alert”

sávok segítenek abban, hogy az üzemeltetők azonnal reagáljanak a rendellenességekre, csökkentve a leállási időket és a selejtköltségeket.

Végül az analitikai műszerfalak (analytics dashboards) integrálják a gépi tanulási algoritmusok kimeneteit is: prediktív hőmapok, hajtóműállapoteloszlások és anomália-score-értékek jelennek meg vizuális formában, támogatva a hosszú távú karbantartási stratégiák kialakítását. A vizualizált adatok alapján a digitális iker felhasználói könnyedén összevethetnek különböző időszakokat, termelési műszakokat vagy konfigurációkat, és azonnali „mi lenne, ha" szimulációkat is futtathatnak a felületen a következő műszak optimalizálásához [7].

Összhangban a CPS alapelveivel, az adatvizualizáció nem pusztán statikus diagramok megjelenítése, hanem aktív interakciós felület a digitális ikerrel. Ez a vizualizált, jól áttekinthető formátum teszi lehetővé, hogy a műszaki csapat a digitális iker adatait hatékonyan alkalmazza a gyártási folyamatok finomhangolására, hibaelhárításra és stratégiai karbantartás tervezésére.

6.1 Mozgáspálya-optimalizálás algoritmusai

Az adaptív vezérlés egyik legfontosabb feladata a robotkarok mozgáspályáinak optimalizálása a digitális iker és a CPS segítségével. A cél a gyors, energiatakarékos és ütközésmentes mozgás megtervezése, amely figyelembe veszi a fizikai kar teljes dinamikáját, a szerelősor környezeti korlátait és a valós idejű szenzoradatokat. A digitális ikerben futó mozgáspálya-optimalizáló algoritmusok főbb típusai a következők:

1. Modell-predictív vezérlés (MPC)

A MPC iteratív optimalizációs eljárás, amely a dinamikai modell alapján előre számítja a robotkar következő mozgáspályáit, miközben valós idejű visszacsatolással korrigálja a pályagenerálást. A digitális ikerben futó MPC-algoritmus minden vezérlési ciklusban megold egy kisméretű, kvadratikus programozási (QP) feladatot, amely minimalizálja a következő időablakra vonatkozó költségfüggvényt (pl. energiafogyasztás + eltérés a célpozíciótól), miközben betartja a fizikai korlátokat (sebesség-, gyorsulás- és nyomatékhatárok) [4]. A modell-predictív hurok előnye, hogy a valós idejű szenzoradatok alapján adaptív módon módosítja a vezérlési stratégiát, csökkentve a túllövést és stabilizációs időt.

2. RRT és PRM alapú útfelderítés*

A gyorsan járható fastruktúrát (RRT*) és a probabilisztikus útfelderítőt (PRM) kiterjesztett változatban alkalmazva a digitális iker képes bonyolult, dinamikusan változó akadályterekben is megtalálni az optimális mozgáspályát. A szoftver a fizikai környezet 3D-s modelljét (pl. Azure Digital Twins környezeti modellje) használja, és valós idejű akadályfelderítést végez a szenzoradatok alapján. Az RRT* algoritmus iteratív optimalizációval közelíti a legrövidebb vagy legenergiatakarékosabb útvonalat, miközben biztosítja a folyamatos adaptációt, ha új akadályok (pl. leálló szállítószalag) jelennek meg [5].

3. Genetikus algoritmusok és populációs optimalizáció

A populációs metaheurisztikák – genetikus algoritmus (GA), differenciális evolúció (DE) – kombinálva a digitális iker szimulációs képességével lehetővé teszik, hogy több ezer alternatív mozgáspályát generáljanak és értékeljenek offline vagy részben online. A fitness-függvénybe beemelhetők a ciklusidő, az energiafogyasztás, az ütközés- és közelítési távolság, valamint a hőmérsékleti terhelés szempontjai. A GA-k folyamatosan frissítik a populációt a fizikai adatokat is visszajelző digitális iker szimulációk alapján, ami rugalmasságot ad a nemlineáris dinamikájú robotkarok vezérlésében [23].

4. Reinforcement learning (RL) alapú optimalizáció

A mély megerősítéses tanulás (deep RL) lehetővé teszi, hogy a digitális iker egy próbálkozásokra épülő tanulási környezetben alakítsa ki a legjobb mozgáspálya-stratégiákat. Matsive et al. egy Soft Actor-Critic (SAC) keretrendszert mutatnak be, amely offline és online azonnali visszajelzéssel (reward: pontos pozicionálás és energiahatékonyság) tanítja a rendszert. A digitális iker környezete szimulált és valós szenzoradatokat is tartalmaz, ezáltal a megtanult politika készen áll éles üzemre, minimalizálva az átállási időt és a fizikai tesztköltségeket [28].

5. Hibrid megközelítések

A legújabb kutatások kombinálják a vasbeton MPC-t a genetikus vagy RL-alapú módszerekkel, hogy először gyors közelítő útvonalat generáljanak (populációs vagy fastruktúrás algoritmussal), majd pezsgő MPC finomra hangolja a mozgáspályát a valós időben beérkező szenzoradatok alapján. Ezzel a hibrid stratégia a sebesség és pontosság optimális egyensúlyát éri el, megfelelő rugalmasságot biztosítva a dinamikus gyártási körülmények között [4] [18].

Az adaptív mozgáspálya-optimalizálás algoritmusai a digitális iker és CPS integrációja révén biztosítják, hogy a szerelősori robotkarok ne csak statikus, előre definiált útvonalakat kövessenek, hanem valós időben alkalmazkodjanak az ütemezési változásokhoz, környezeti zavarokhoz és a fizikai kar állapotváltozásaihoz. Ez a rugalmasság és hatékonyság kulcsfontosságú a modern, adatvezérelt gyártásban.

6.2 Torlódás- és ütközéselkerülési stratégiák

Az ipari robotkarok szerelősortól elkülönülő cellákban vagy kollaboratív környezetben gyakori kihívás a váratlan ütközések és torlódások elkerülése. A digitális iker által vezérelt CPS-ek az alábbi stratégiákat alkalmazzák a biztonságos és zavartalan működés érdekében:

1. Potenciálmező-alapú módszerek

A fizikai és virtuális objektumokat vonzó és taszító erőkkel modellezik. Minden akadály és a célpozíció egyaránt rendelkezik “töltéssel”: a robotkar virtuális modellje a vonzó mezőn belülmozdul, míg az akadályok taszító mezője tartja távol. A digitális iker folyamatosan szimulálja ezeket a mezőket, így a valós idejű szenzoradatok (pl. 3D LIDAR pontfelhő) alapján képes módosítani a pályát, ha egy új akadály lép be a térbe [13].

2. Velocity Obstacle (VO) és Dinamikus VO

A VO-algoritmusok a robot kar valós idejű sebesség- és helyzetadatait használják, hogy előre kiszámítsák, mely sebességvektorok vezetnének ütközéshez. A digitális iker modellező modulja ezt kiterjeszti dinamikus objektumokra (Emberek, AGV-k), és valós időben blokkolja az ütközésveszélyes mozgásokat, automatikus pályakorrekciót indítva [10].

3. Model-Predictive Collision Avoidance (MPCA)

A MPC-alapú stratégiák a rövid távú előrejelzés során beépítik az ütközéskorlátokat a QP-problémába. A digitális iker minden ciklusban lefuttat egy prediktív szimulációt a jövőbeli ütközések becslésére, és a vezérlőparancsokat úgy optimalizálja, hogy a dinamikai korlátok (gyorsulás, sebesség) és az ütközési marginok egyaránt teljesüljenek [4].

4. Sensor Fusion és Biztonsági Zónák

A robotkar környezetének megfigyelésére több szenzort (3D kamera, idő- és fáziseltolásos LIDAR, erő-/nyomatékszenzor) egyesítenek. A digitális iker a fúziós adatokat használva kialakít adaptív biztonsági zónákat, amelyek mérete a robot sebessége és a környezeti bizonytalanság (szenzorhang, modellpontatlanság) alapján változik. Ha a biztonsági zóna sérül, a rendszer azonnal csökkenti a sebességet vagy megállítja a mozgást [8].

5. Hibrid Tanuló Stratégiák

A gépi tanuláson alapuló megközelítés (deep RL, imitation learning) lehetővé teszi, hogy a digitális iker tanulja az optimális ütközéselkerülési manővereket. Egy Soft Actor-Critic (SAC) alapú RL-agent a digitális iker szimulált és valós ütközési adataiból tanulva egyre gyorsabb és biztonságosabb pályákat generál az új helyzetekben is [18].

Összegzés:

A fenti stratégiák együttesen biztosítják, hogy a digitális ikerrel vezérelt robotkarok folyamatosan elkerüljék az ütközéseket és torlódásokat, miközben a mozgáspálya-optimalizáció és adaptív vezérlés révén fenntartják a nagy termelékenységet és biztonságot a szerelősoron.

6.3 Tanuló rendszerek integrálása

A tanuló rendszerek (Machine Learning, ML és Reinforcement Learning, RL) integrációja a digitális ikerrel támogatott kiber-fizikai rendszerekben (CPS) forradalmasítja az ipari robotkarok vezérlését és üzemeltetését. A digitális iker univerzális, jól paraméterezhető szimulációs környezetként szolgál, amelyben a tanuló algoritmusok biztonságosan gyakorolhatnak, miközben a gyártósor valós adatain alapuló visszacsatolást is kapnak.

Offline tanulás és szupervízionált modellek

A tanulási folyamat első lépése gyakran az offline, történeti adatokon végzett szupervízionált tanítás. Az ipari robotkarok működése során összegyűlt szenzoradatokat (pozíció, sebesség, nyomaték, hőmérséklet, rezgés) előfeldolgozott, címkézett adatcsomagokban tároljuk. Gépi tanulási modellek – például döntési fák, támogatott vektorgépek (SVM) vagy egyszerűbb neurális hálók – ilyen adatokon tanulják meg a hibajelző mintázatokat és az energiafogyasztás

optimalizálásának összefüggéseit. Hananto és munkatársai [5] például részletesen elemezték, hogyan lehet szupervízionált tanulással előre jelezni a robotkar elektronikus hajtásainak kopását és energiahatékonyságát.

Sim-to-Real és Domain Randomization

A digitális iker egyik nagy előnye, hogy lehetővé teszi a Sim-to-Real (szimulációból a valós környezetbe) átvitelt. A szimulált környezetben úgynevezett *domain randomization*-t alkalmazunk, vagyis a modellparamétereket (súrlódás, tömeg, inerciák) és a környezeti jellemzőket (fényviszonyok, zajszintek) véletlenszerűen változtatjuk, hogy a tanuló algoritmus robusztusan megtanulja a feladatot. Ezután a megtanult politika a valós robotkaron is jól működik, minimális finomhangolást igényelve.

Reinforcement Learning és Online Finomhangolás

A Meleg Actor-Critic (SAC) vagy Proximal Policy Optimization (PPO) algoritmusok deep RL keretrendszerben olyan agenteket képeznek, amelyek valós idejű interakcióból és a digitális iker valósághű fizikai modelljéből tanulnak. Matsive és kollégái [18] bemutatták, hogy egy SAC-alapú rendszer képes akár 5–10 ms end-to-end késleltetéssel is optimális mozgáspályákat generálni, miközben a fizikai valóság számára is elfogadható stabilitást tart fenn. Az online finomhangolás során az RL-agent a valós üzem közben gyűjtött adatokkal folyamatosan frissíti a politikát, ezzel tovább javítva a teljesítményt és alkalmazkodóképességet.

Transfer Learning és Multi-Task Learning

A digitális iker platform lehetővé teszi, hogy a különböző típusú robotkarok és feladatok között transfer learning-et alkalmazzunk. Egy már betanított modell paramétereit át lehet vinni új, de hasonló környezetekbe, így a tanulási idő jelentősen csökken. Ezen túl a multi-task learning révén egyetlen hálózat több feladatot (pl. pályaoptimalizálás és erő-vezérlés) is képes megtanulni, mélyíteni a robotkar általános képességeit.

Mesterséges intelligencia a prediktív karbantartásban

A tanuló rendszerek a prediktív karbantartási modulokban is kulcsszerepet játszanak. LSTM alapú idősoros modellek és konvolúciós neurális hálók elemzik a diagnosztikai szenzoradatokat, hogy előre jelezzék a komponensek kopását vagy hibáit [19]. Az így kapott predikciók alapján a digitális iker automatizáltan ütemezi a karbantartást, helyettesítve a hagyományos, gyakran túlzottan konzervatív előírásokon alapuló karbantartási rendet.

Összességében a tanuló rendszerek integrálása a digitális ikerrel egy öntanuló, adaptív CPS-t hoz létre, amely képes a valós idejű és történeti adatok együttes feldolgozására, a gyors szimulációra és a folyamatos finomhangolásra. Ez a megközelítés lehetővé teszi, hogy a szerelősoron a robotkarok a változó termelési igényekhez, környezeti zavarokhoz és hosszú távú kopási folyamatokhoz is rugalmasan alkalmazkodjanak, miközben maximális hatékonyságot, pontosságot és rendelkezésre állást biztosítanak.

6.4 Valós idejű alkalmazkodás változó környezethez

A digitális iker egyik legnagyobb előnye, hogy a robotkarok képesek valós időben alkalmazkodni a környezeti változásokhoz, legyen az váratlan terhelésnövekedés, újonnan felbukkanó akadály vagy a gyártandó darabok geometriai eltérése. A CPS architektúrában az edge réteg folyamatosan monitorozza a szenzoradatokat (pozíció, sebesség, nyomaték, erő) és eseményvezérelt riasztásokat generál azonnali elemzésre. Amennyiben például egy munkaanyag súlya eltér a tervezettől, a nyomatékszenzorok azonnal magasabb terhelést jeleznek, és a digitális iker prediktív modelljében futó dinamika-szimuláció azonnal újraszámolja a mozgáspályákat, minimalizálva a késleltetést és elkerülve a túllövést vagy a meggörbülést [12].

Ha egy szerelősoron hirtelen feltorlódik egy szállítószalag, az új akadály a LIDAR és 3D-kamera jelei alapján azonnal bekerül az akadálytérképre, amelyet a digitális iker 3D-s környezetmodelljében frissít. Az RRT*-alapú vagy MPC-alapú pályauszítás immár az új körülményeknek megfelelően generál optimális útvonalat, megelőzve az ütközést [4]. Amikor az emberi operátor belép az együttműködési térbe, az erő-/nyomatékszenzorok azonnal detektálják a könnyed érintést, és a digitális iker valós idejű szabályozója átvált alacsony sebességű, biztonságos módra, garantálva az együttműködés biztonságát [13].

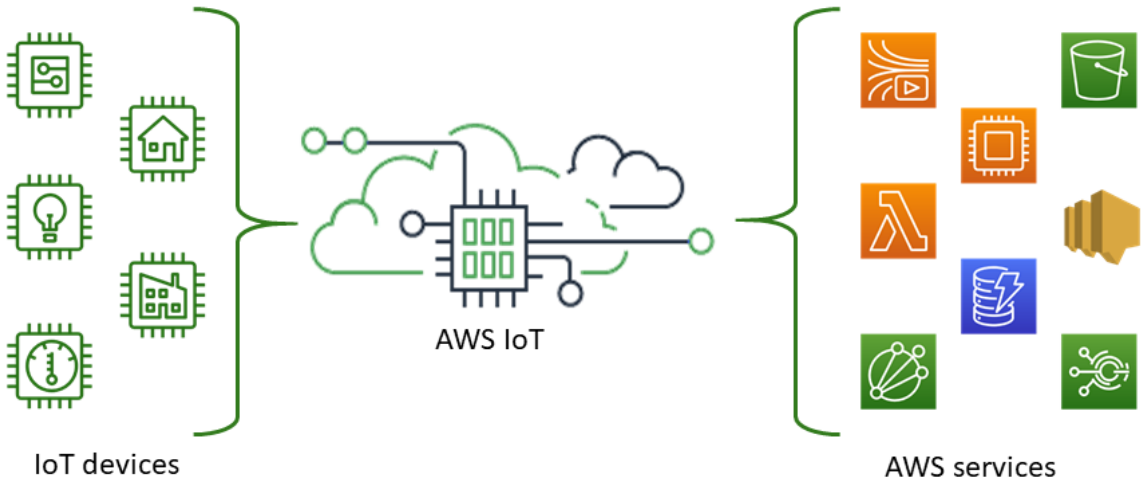
A soft actor-critic reinforcement learning rendszerek pedig képesek online finomhangolásra: a digitális iker szimulációban gyűjtött új tapasztalatok alapján a RL-agent frissíti politikáját, amelyet néhány ciklus alatt éles vezérlésre is át lehet ültetni [18]. Ez a hibrid megközelítés ötvözi a valós idejű visszacsatolás előnyeit az adaptív tanulás rugalmasságával, lehetővé téve, hogy a robotkarok azonnal alkalmazkodjanak a gyártási ütemezés, a munkaanyag tulajdonságainak vagy a munkakörnyezet változásaihoz.

Összességében a digitális ikerrel támogatott valós idejű alkalmazkodás révén a CPS-ben működő robotkarok magasabb fokú megbízhatóságot, termelékenységet és biztonságot érnek el, miközben minimalizálják a leállásokat és optimalizálják az üzemeltetési költségeket.

7.Felhőalapú háttérszolgáltatások integrációja

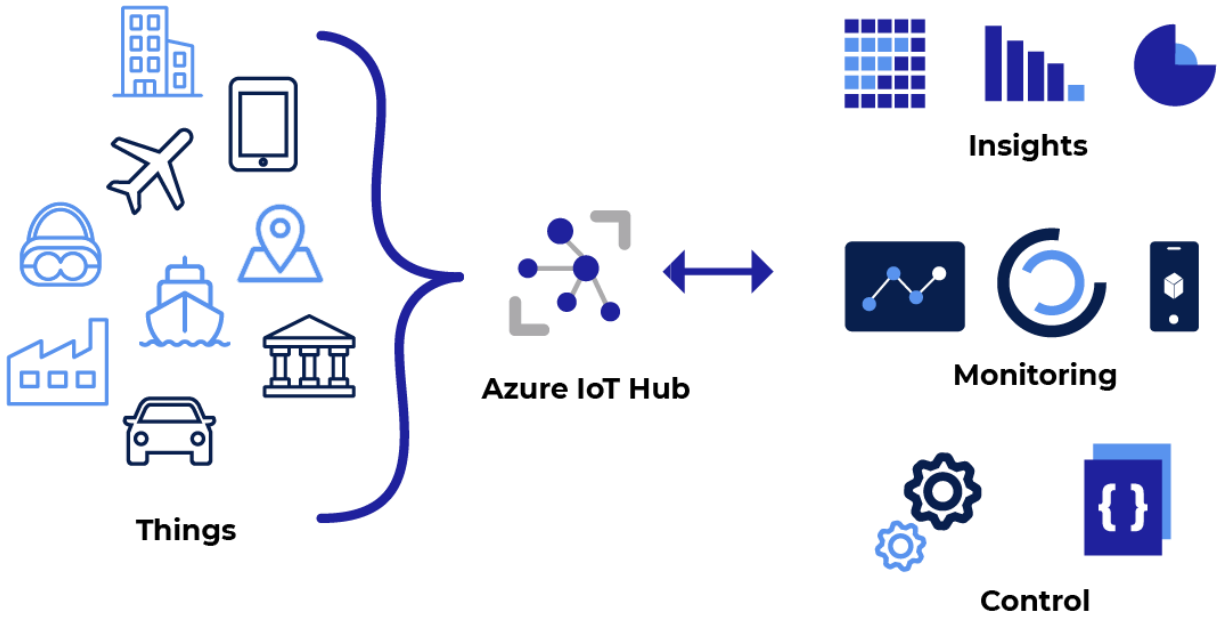
7.1 Felhőszolgáltatások szerepe (pl. AWS, Azure IoT)

A felhőalapú háttérszolgáltatások kulcsszerepet töltenek be a digitális ikerrel támogatott kiber-fizikai rendszerek (CPS) működésében, hiszen lehetővé teszik a skálázható adatgyűjtést, feldolgozást, tárolást és elemzést. A következőkben bemutatjuk a két vezető platform, az AWS IoT (7.1 Ábra) és az Azure IoT (7.2 Ábra) főbb komponenseit és funkcióit, valamint azok integrációs lehetőségeit az ipari robotkarok digitális ikerével.



7.1 Ábra AWS IoT

(https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html)



7.2 Ábra Azure IoT

(https://blog.cellenza.com/en/data/what-is-azure-iot-hub/)

1. Eszközkezelés és adatgyűjtés

   AWS IoT Core: Biztosítja a biztonságos, kétirányú kommunikációt a nagy számú edge-eszközzel (pl. PLC, szenzormodulok). A MQTT és HTTP protokollokat natívan támogatja, beépített eszköz-azonosítással (X.509 tanúsítványok) és hozzáférés-szabályozással. Az eszközök gyors regisztrációját és nagy rendelkezésre állást garantálja [30].

   Azure IoT Hub: Hasonló módon kezeli az eszközkapcsolatokat és üzenetközvetítést, integrált Identity Managementtel és Role-Based Access Control (RBAC) szolgáltatásokkal. Az üzeneteket Device Twins modellekben tárolja, ami egységes metaadat-sémát biztosít az eszközállapotokhoz és kívánt konfigurációkhoz [21].

2. Edge integráció és offline működés

   AWS IoT Greengrass: Lehetővé teszi, hogy a kritikus logikát és ML-modulokat az edge-eszközön futtassuk, csökkentve a felhő felé irányuló adatforgalmat és a késleltetést. A Greengrass Lambda funkciói képesek helyben előfeldolgozni a szenzoradatokat, majd csak a kiválasztott eseményeket továbbítani [30].

   Azure IoT Edge: Hasonlóan támogatja a konténerizált modulok futtatását az edge-gépeken, így a digitális iker lokális példánya is használhat ML-modulokat (pl. anomália-észlelés), offline környezetben is működőképes marad, és szinkronizálja a felhővel, amint hálózat elérhető.

3. Adatfeldolgozás és elemzés

   AWS IoT Analytics: Adatcsatornákat (pipeline-okat) definiálva tisztítja, transzformálja és tárolja a nagy mennyiségű üzenetet. Beépített idősoros elemzéseket és vizualizációs eszközöket kínál, melyek közvetlenül kapcsolhatók a digitális iker monitoring-dashboardjaihoz.

   Azure Stream Analytics & Time Series Insights: Valós idejű adatfolyam-analízist és interaktív, történeti idősoros vizualizációt tesznek lehetővé. A felhasználó könnyen definiálhat lekérdezéseket és riasztási szabályokat, amelyek azonnal visszacsatolható vezérlési parancsokat generálnak a digital twin vezérlő API-kon keresztül [21].

4. Digitális iker modell hosztolása és skálázás

   Azure Digital Twins: Kifejezetten digitális ikrek kezelésére tervezett szolgáltatás. Írás-olvasás API-kat biztosít a modell erőforrásaihoz (alrendszerek, komponensek, relációk), és natív integrációt aIoT Hub-bal, Stream Analytics-szel és Time Series Insights-szal. A DSL-alapú definíciók (DTDL) segítségével tetszőleges gyártási topológiák hozhatók létre és frissíthetők valós időben.

   AWS IoT TwinMaker: Hasonló szolgáltatás az AWS-en, amely lehetővé teszi a fizikai eszközök topológiai és viselkedési modelljének létrehozását. Integrációt nyújt a Kinesis Data Streams-szel és QuickSight-tal, így a digitális modell skálázható adatmegjelenítést és elemzést kínál [30].

5. Biztonság és megfelelőség

   Mindkét platform kiemelten kezeli a felhő-edge biztonságot: titkosított csatornák (TLS), finom szemcséjű IAM-szabályok és auditnaplók biztosítják, hogy a digitális iker csak jogosult entitásoktól fogadjon és küldjön adatot. Az AWS és Azure megfelelőségi keretrendszerei segítik a GDPR-, ISO- és IEC-szabványoknak való megfelelést is.

Összegzésképpen a felhőalapú szolgáltatások – AWS IoT és Azure IoT – biztosítják az end-to-end adatáramlást, valós idejű és történeti elemzéseket, valamint a digitális iker skálázható hosztolását és integritását. Ezek a komponensek együttépülnek a CPS-architektúrába, lehetővé téve a robotkarvezérlés adaptív, prediktív és biztonságos működését a szerelősoron.

7.2 Adatelemzés és gépi tanulás

A felhőalapú platfromok – AWS IoT Analytics és Azure IoT Hub/Azure Machine Learning – lehetővé teszik a szerveroldali nagyadat-elemzést és gépi tanulást (ML), amely túllép a hagyományos dashboardokon. Először a valós idejű adatfolyamokat tisztítják és normalizálják (pl. hiányzó értékek pótlása, outlier-szűrés), majd idősoros elemzéseket futtatnak, hogy azonosítsák a trendeket, szezonális ciklusokat és anomáliákat [21].

A következő lépésben ML-modelleket – lineáris regressziót, döntési fákat vagy neurális hálókat – használnak a teljesítmény-optimalizálás céljára. Hananto és munkatársai bemutatták, hogyan alkalmazható 3D digitális iker-alapú ML a gyártási minőségjavításra: a modell előre jelzi a potenciális selejt-képződési pontokat, és javaslatot tesz a paraméterek automatikus módosítására [5]. Azure ML-ben a Automated ML funkcióval gyakorlatilag programozás nélkül választhatók ki a legjobb algoritmusok és hiperparaméterek.

A stream-számítás (Azure Stream Analytics, AWS Kinesis Data Analytics) valós időben futtat SQL-szerű lekérdezéseket és beágyazott ML-modulokat, lehetővé téve az azonnali predikciót (pl. ciklusidő-előrejelzés, energiafogyasztás-optimalizálás). Ezek az eredmények automatikusan visszakerülnek a digitális ikerhez, amely feed-forward vezérlési jeleket generál az edge hurokba [21], [30].

7.3 Hibadetektálás és prediktív karbantartás felhőn keresztül

A felhőben kezelt diagnosztikai és prediktív karbantartási modulok képesek nagyméretű, heterogén szenzoradatokat hosszú távon elemezni. A National Academies jelentése hangsúlyozza, hogy a felhőalapú idősoros adatbázisok (pl. Azure Data Explorer, AWS Timestream) kritikusak a megbízható előrejelzésekhez [19].

Az Azure Digital Twins és IoT Hub integráció segítségével a felhőben futó ML-modellek – LSTM hálók vagy konvolúciós neurális hálók – képesek előre jelezni a robotkar alkatrészeinek kopását és meghibásodását. A Yao et al. által javasolt több-szintű feladat-újraütemezés integrálja a prediktív karbantartási ablakokat a gyártási ütemtervbe, minimalizálva a termelés-kiesést [23].

AWS oldalán az IoT Events és Lookout for Equipment szolgáltatások automatizálják az anomália-észlelést és prediktív karbantartást. A platformok egymást kiegészítve lehetővé teszik, hogy a diagnosztikai riasztások automatikusan generáljanak karbantartási feladatokat a CMMS rendszerekben, és kövessék nyomon a beavatkozások hatását [16].

7.4 Biztonsági kérdések a felhőben

A felhőalapú CPS-ekben a biztonság kritikus, hiszen a robotkar vezérlése és a vállalati adatbázis összekapcsolódik. A legfontosabb kihívások: adattitkosítás, identitás- és jogosultságkezelés, hálózati izoláció és naplózás.

- Titkosított kommunikáció: MQTT és HTTPS protokollok TLS-alapú végponti titkosítással védik az adatok integritását és bizalmasságát.
- Identity and Access Management (IAM): Azure RBAC és AWS IAM finom szemcséjű jogosultságkezelést tesz lehetővé, hogy csak a hitelesített eszközök és szolgáltatások férhessenek hozzá a digitális iker API-khoz [21], [30].
- Hálózati szegregáció: Virtuális magánhálózatok (VPC, VNet) és bejövő/kimenő biztonsági csoportok biztosítják, hogy a CPS hálózat elkülönüljön a vállalati IT rendszerektől.
- Audit és monitorozás: AWS CloudTrail és Azure Monitor naplózza a hozzáférési és konfigurációs eseményeket, támogatva a megfelelőségi (GDPR, ISO/IEC 27001) követelmények auditálását [19].

Ezek a biztonsági mechanizmusok együttesen garantálják, hogy a digitális iker és a CPS-komponensei biztonságosan működjenek, minimalizálva a kiberfenyegetések és adatvédelmi kockázatok esélyét.

8. Kommunikációs protokollok és adatkapcsolatok

A digitális ikerrel támogatott CPS-ben a hatékony és megbízható adatcsere létfontosságú a fizikai eszközök, edge-egységek és felhőszolgáltatások között. Két kiemelten fontos protokoll az OPC UA és az MQTT, de emellett számos más IoT-szabvány (AMQP, HTTP/REST, DDS) is használható specifikus igényekre.

8.1 OPC-UA alapjai és ipari alkalmazása

Az OPC Unified Architecture (OPC UA) egy platform- és gyártófüggetlen kommunikációs keretrendszer, amelyet kifejezetten az ipari automatizálás igényeire terveztek. Összhangban van az Ipar 4.0 céljaival: felhő-edge integráció, biztonság és interoperabilitás.

- Adattípusok és modellalapú felépítés

  Az OPC UA nem csupán értékcsere-protokoll, hanem egy teljes adatmodell-keretrendszer. A szerverek (pl. PLC, edge-eszköz) „Object” és „Variable” node-okat kínálnak, amelyekhez metaadatokat (műszaki jellemzők, units, történet) lehet rendelni. Ezek a node-ok hierarchikus fában rendeződnek, és a digitális iker JSON- vagy OPC UA-konform DTDL-sémák alapján lekérdezhetők [20].

- Biztonság

  Az OPC UA beépített biztonsági mechanizmusokat tartalmaz:

  1. Titkosítás: TLS-alapú védelem a kliens–szerver kommunikációnál.
  2. Hitelesítés: X.509 tanúsítványokkal vagy felhasználónév/jelszó párosokkal.
  3. Integritás és jogosultságkezelés: Hozzáférési szabályok fine-grain szabályozása node-szinten [20].

- Kommunikációs minták
  - Client–Server: Közvetlen lekérdezések (Read/Write) és publish események.
  - PubSub: Publish/Subscribe modell UDP-alapú multicast-tal (TSN-kompatibilis is), amely kimondottan alkalmas valós idejű CPS-adatfolyamokra.

- Ipari alkalmazások
  - Szenzoradat-gyűjtés: Minden digitális ikerhez kapcsolt edge-egység OPC UA szerverként publikálja a valós idejű szenzorértékeket, amelyeket a digitális iker felhőoldali komponensei konzisztensen lekérdeznek [17].

- Eszköz-monitoring és vezérlés: A digitális iker dashboard-ja OPC UA kliensként csatlakozik, és grafikusan megjeleníti a node-okon keresztül elérhető paramétereket (pozíció, nyomaték, hőmérséklet).
- Standardizált interfészek: Több gyártó robotkar-driverei és PLC-i egyaránt OPC UA-kompatibilisek, így a digitális iker egyszerre több forrásból tud adatot aggregálni.

8.2 MQTT és más IoT-protokollok

Az MQTT (Message Queuing Telemetry Transport) egy könnyű, publish/subscribe alapú üzenetprotokoll, amelyet kifejezetten korlátozott sávszélességű, magas késleltetésű vagy megbízhatatlan hálózatokra terveztek. Számos felhő-IoT szolgáltató – mint az AWS IoT Core és az Azure IoT Hub – támogatja natívan.

- MQTT fő jellemzők
  1. Publish/Subscribe modell: A device-ok témákra (topic) küldenek üzeneteket, az előfizetők pedig ezeket valós időben megkapják.
  2. QoS szintek:
     - QoS 0: „At most once” – egyszeri kézbesítés, nem garantált.
     - QoS 1: „At least once” – legalább egyszer, duplikátum lehetséges.
     - QoS 2: „Exactly once” – garantáltan egyszeri, legmagasabb overheaddel.
  3. Könnyűsúlyúság: Minimális fejléc-méret, alacsony CPU- és memóriaterhelés.
- Alkalmazás a digitális ikerben
  - Edge–Felhő kommunikáció: A szenzoradatok (pl. pozíció, hőmérséklet) MQTT-vel kerülnek továbbításra az edge eszközökről a felhő-brokerre, ahol a digitális iker feliratkozik a releváns témákra.
  - Értesítések és riasztások: A diagnosztikai modul MQTT-üzeneteket publikál (pl. „fault/robotarm1”), amelyeket a CMMS-szel vagy dashboard-dal integrált előfizetők azonnal feldolgoznak.
  - Device Shadows / Twins: Azure IoT Hub és AWS IoT Core támogatja a shadow/twin koncepciót: minden eszközhöz egy reprezentációs objektum (shadow) tartozik, amely a kívánt és aktuális állapotot tartalmazza, így a digitális iker és a physical device állapota konzisztensen szinkronizálható.
- Egyéb IoT-protokollok
  - AMQP: Célszerű komplexabb üzenet-routing és tranzakcióvezérelt alkalmazásokhoz, magasabb overheaddel.

- DDS (Data Distribution Service): Alacsony késleltetésű, peer-to-peer modell nagy megbízhatóságot és szelektív QoS-t kínál, elsősorban kritikus valós idejű rendszerekben.
- HTTP/REST: Bár nem ideális valós időhöz, egyszerűsége miatt sok konfigurációs és menedzsment feladat (pl. firmware-update, provisioning) helyetti megoldás.

Az OPC UA és MQTT egyaránt nélkülözhetetlenek a digitális ikerrel működő CPS-ekben: az OPC UA strukturált, standardizált interfészt biztosít a helyi gyártóberendezések és a digitális modell között, míg az MQTT tömör, megbízható üzenetküldést tesz lehetővé edge és felhő közt alacsony sávszélességű környezetben. Ezeket kombinálva a CPS építőkövei megteremtik az adaptív, prediktív és skálázható ipari automatizálás feltételeit.

8.3 Protokollválasztás szempontjai

A megfelelő kommunikációs protokoll kiválasztása a CPS-ekben kritikus a rendszer teljesítménye, megbízhatósága és biztonsága szempontjából. Elsődleges szempontok:

- Késleltetés és sávszélesség

Valós idejű vezérlésnél a hálózati késleltetésnek szigorú határok között kell maradnia. Az EtherCAT vagy OPC UA Pub/Sub alacsony késleltetésű, determinisztikus adatcserét tesz lehetővé, míg az MQTT inkább nagyobb késleltetésű, de alacsony sávszélességű IoT-csatornákra optimalizált [2], [20].

- Üzenetméret és overhead

Az MQTT kis fejlécmérete és minimalizált protokoll-overheadje akkor előnyös, ha az eszközök erőforrás-korlátosak és a hálózati sávszélesség korlátozott [5]. Ezzel szemben az OPC UA részletes metaadat-támogatása nagyobb üzenetméretet és komplexitást jelent [2].

- Biztonság

A titkosítás, hitelesítés és jogosultságkezelés beépítettsége fontos. Az OPC UA beépített TLS- és tanúsítványkezelése, valamint finomabb hozzáférés-szabályozása erősebb védelmet nyújt a nagy értékű ipari rendszerekben [20]. Az MQTT esetén külön szolgáltatásokra (pl. AWS IAM, Azure RBAC) kell támaszkodni [4].

- Interoperabilitás

A szabványos adatmodellek (OPC UA Information Model, DTDL) és a protokollon áthidalható gateway-megoldások (OPC UA–MQTT bridge) biztosítják, hogy különböző gyártók eszközei egyszerűen integrálhatók legyenek a CPS-be [2], [21].

- Skálázhatóság

Nagy eszközparkok kezelése esetén a publish/subscribe architektúrák (MQTT, OPC UA PubSub) jobban skálázódnak, mint a kliens–szerver modellek [7]. Az AWS IoT Core és Azure IoT Hub felhőalapú broker-megoldásai automatikus skálázódást tesznek lehetővé [4].

- Fejlesztési és üzemeltetési költség

Az egyszerűséget igénylő vagy prototípus-fázisban az MQTT/HTTP alacsonyabb belépési küszöböt jelent, míg nagyvállalati környezetben az OPC UA szabványosítás, dokumentáció és támogatás hosszú távon költségmegtakarítást eredményez [1], [3].

8.4 Interoperabilitás és kompatibilitás

Az ipari digitalizáció sikerének kulcsa az interoperabilitás – a rendszerek és eszközök közötti zökkenőmentes együttműködés – valamint a kompatibilitás – a visszafelé és előrefelé történő könnyű csatlakozhatóság biztosítása.

- Szabványos adatmodellek

  Az OPC UA Information Model és a DTDL (Digital Twins Definition Language) egységes séma segítségével írja le az eszközök és komponensek tulajdonságait, viselkedését és relációit. Ez garantálja, hogy a digitális iker komponensei és az ipari eszközök ugyanarról az adattérképről „beszéljenek” [20], [21].

- Gateway- és adapter-megoldások

  Régebbi, nem OPC UA-kompatibilis eszközök esetén protokoll-átalakító gatewayek (pl. OPC DA → OPC UA, Modbus → MQTT) biztosítják, hogy a digitális iker minden releváns adatot elérjen [2]. Ezek a middleware-ek kezelik a formátum- és üzenettranszformációkat, valamint a prioritás- és biztonsági szabályokat.

- Visszafelé kompatibilitás

  A gyártósor élettartama alatt újabb kommunikációs szabványok jelennek meg. Az OPC UA tervezi, hogy megőrzi az OPC DA funkcióit szolgáltatás-rétegen, és OPC UA-on keresztül biztosít teljes kompatibilitást [20].

- Hibrid protokoll-architektúrák

  A CPS-ekben gyakran alkalmazzák együtt az OPC UA-t a gyártási cellákban és az MQTT-t az IoT-periférián. A digitális iker middleware-e (pl. Azure IoT Edge, AWS Greengrass) képes mindkét protokollt kezelni, és automatikusan kiválasztani a legoptimálisabb adatútvonalat [7], [8].

- Szabványos API-k és SDK-k

  Mind az Azure, mind az AWS rendelkezik kész SDK-kkal és REST/SDK-alapú API-kkal, amelyek lehetővé teszik, hogy a digitális iker alkalmazásfejlesztői több programozási nyelvből és keretrendszerből (Python, .NET, Java) egyszerűen csatlakozzanak a CPS-hez [11].

Az interoperabilitás és kompatibilitás fenntartása biztosítja, hogy a digitális ikerrel működő CPS-ek hosszú távon rugalmasak és bővíthetők maradjanak, minimalizálva a fejlesztési kockázatokat és támogatva a folyamatos technológiai fejlődést.

9. Esettanulmány: Digitális ikrek alkalmazása egy elektronikai szerelősoron

A felhasznált esettanulmány: [14]

Rövid ismertető róla: A Kousi et al. (2021) tanulmány egy ember–robot kollaboratív szerelősor digitális iker alapú tervezési és újratervezési módszerét mutatja be az autóiparban, konkrétan egy jármű első tengelyének összeszerelésére fókuszálva [14]. A szerzők egy szolgáltatás-orientált architektúrát dolgoztak ki, amelyben a fizikai erőforrások (robotkarok, AGV-k, szenzorok) ROS-alapú interfészeken keresztül kommunikálnak a felhő- és edge-réteg szolgáltatásaival. A digitális iker folyamatosan szinkronizálja a CAD- és szenzoradatokat, lehetővé téve a valós idejű újratervezést AI-vezérelt feladat- és mozgástervező modulokkal. A megközelítés hatékonyságát Gazebo-szimulációk és WITNESS diszkrét eseményalapú modellezés segítségével validálták, kimutatva jelentős termelékenység- és rugalmasság-növekedést.

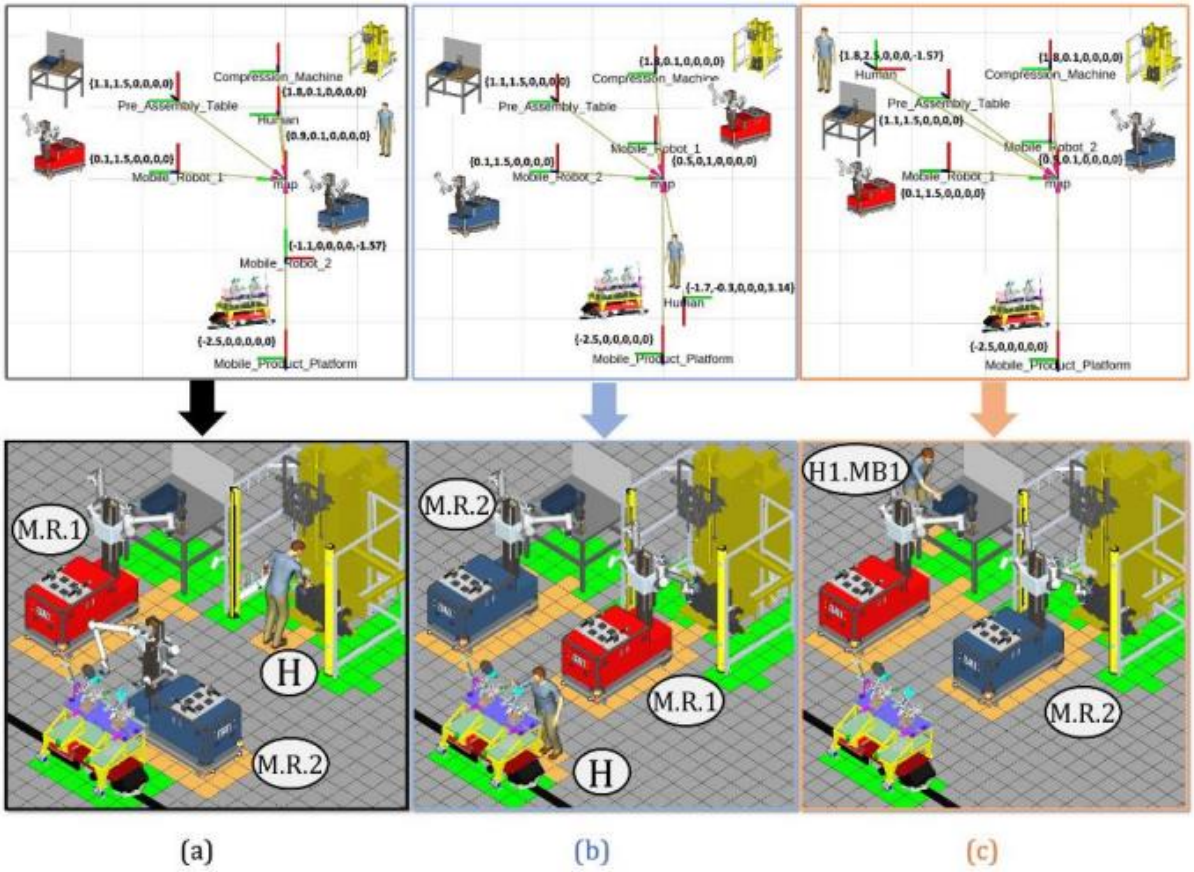
9.1 A szerelősor felépítése és működése

A tanulmány esettanulmánya egy autóipari első tengely összeszerelésére szolgáló moduláris szerelősort vizsgál, melyet a Patrasz Egyetem laboratóriumában telepítettek. A gyártósor három munkaterületre tagolódik – pre-assembly, compression és AGV area –, amelyeken a feladatokat automatizált és emberi erőforrások egyaránt végzik ([14144. Case Study) :

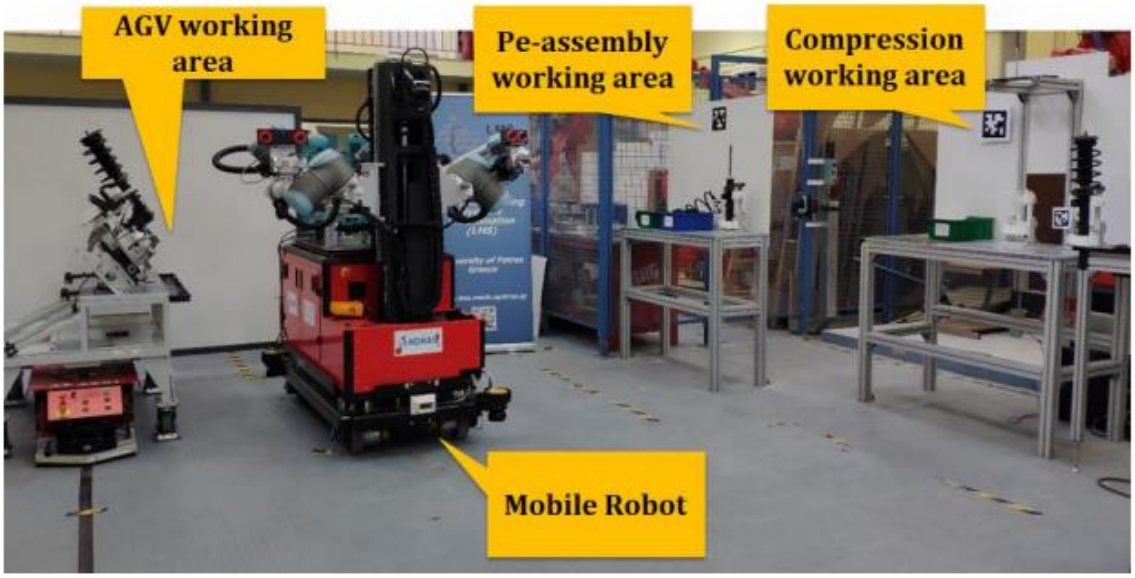
1. Pre-assembly working area
    - Itt történik a jobb oldali lengéscsillapító előösszeszerelése. A nyers alkatrész AGV-ről kerül a pre-assembly állomásra, ahol egy emberi operátor és egy mobil robotkar közösen helyezik be és pozícionálják az alkatrészt (9.1.a Ábra).
2. Compression working area
    - A pre-assemblált lengéscsillapítót a mobil robot átviszi a kompressziós állomásra, ahol a gép megnyomja és rögzíti azt. Ezt követően a robotkar eltávolítja az illesztőhüvelyt, helyezi be anyát és felhelyezi a csavarokat a tengelyre. (9.1.b Ábra)
3. AGV working area
    - A végszerelés után az alkatrész egy automata vezetésű járműre (AGV) kerül, amely elszállítja a kész tengelyt a következő gyártószakaszba.

A sor hosszát, az állomások számát és azok fizikai elhelyezkedését a (9.1 Ábra) mutatja be három alternatív konfigurációban, amelyek közül a kiválasztott elrendezést a (9.2 Ábra) szemlélteti.

- Mobil erőforrások: Két darab autónóm, kerekes mobil robotkar (Mobile Robot, M.R.) mozog a munkaterületek közt. Egyikük az AGV-hez hasonlóan szállítja az alkatrészeket, míg a másik a kompressziós és csavarozási műveleteket végzi.
- Robotkarok: Mindkét mobil robot 6 tengelyes, ipari szabványú manipulátor, melyek URDF-leírása a DT „Resource Manager” moduljában tárolt kinematikai és tömegparaméterekkel együtt.
- Szenzorok: A munkaterületek fölött felülről két 2D lézerscanner és egy robot-torzóra szerelt stereo kamera biztosítja a valós idejű környezeti és emberi jelenlét adatokat, amelyeket a „Sensor Manager” aggregál.



9.1 Ábra Különböző konfigurációi az összeszerelő rendszernek ([14] p. 9. Fig. 10)



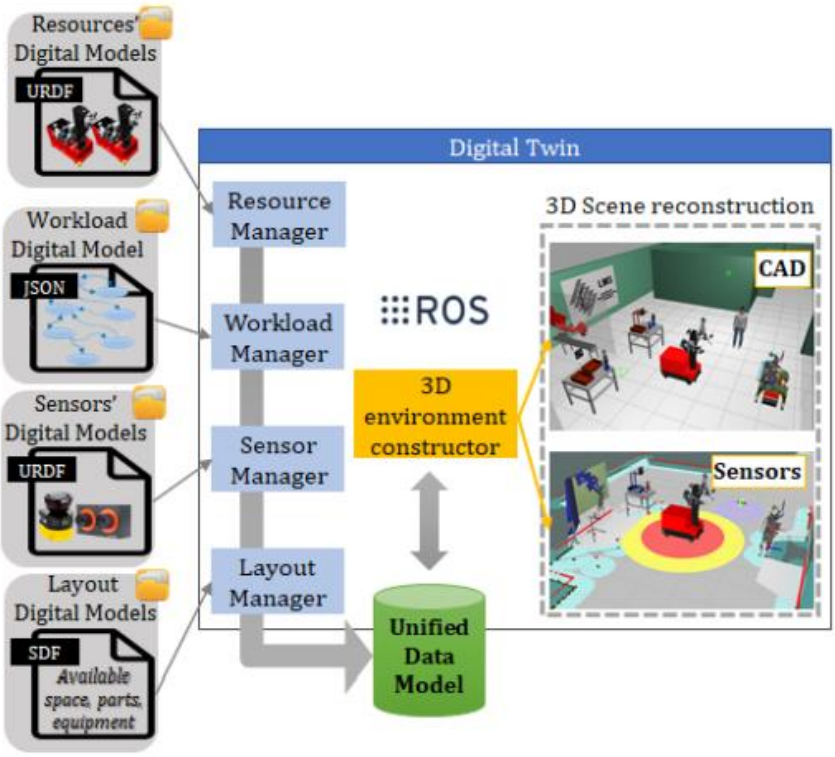
9.2 Ábra Fizikai elhelyezése az állomásokról (9.1 Ábra) ([14] p. 10 Fig. 11)

9.2 A digitális iker rendszer implementációja

A digitális iker (DT) rendszer architektúráját a 9.3 Ábra mutatja be, amely Ubuntu 16.04 és ROS Kinetic környezetben futtatott modulok hierarchiáját ábrázolja .

1. Fő komponensek és modulok (9.3 Ábra)

    - Resource Manager: Tárolja és publikálja a robotkarok, AGV-k és egyéb erőforrások URDF- és SRDF-leírásait, valamint jellemző paramétereiket (payload, maximális sebesség) ([14] o. 6) .
    - Workload Manager: A gyártási feladatokat JSON formátumban kezeli hierarchikus modellként, melyhez a DT-modell AI-algoritmusokkal rendel alternatív konfigurációkat ([14] o. 6) .
    - Sensor Manager: Integrálja a 2D lézerscannerek és a stereo kamera konfigurációs adatait, és publikálja a nyers szenzoradatokat ROS-topikokon keresztül ([14] o. 6) .
    - Layout Manager: Betölti a CAD-fájlokat (.sdf), definiálja az ütközések, tömeg és inercia paramétereket, és készíti elő a statikus elemek virtuális modelljét ([14] o. 6) .
    - 3D Environment Constructor: A Resource és Sensor Managerből származó adatok alapján felépíti a valós idejű 3D világmodellt ROS tf-transzformációkkal, és fenntart egy folyamatosan frissített „planning scene” topikot ([14] o. 6).

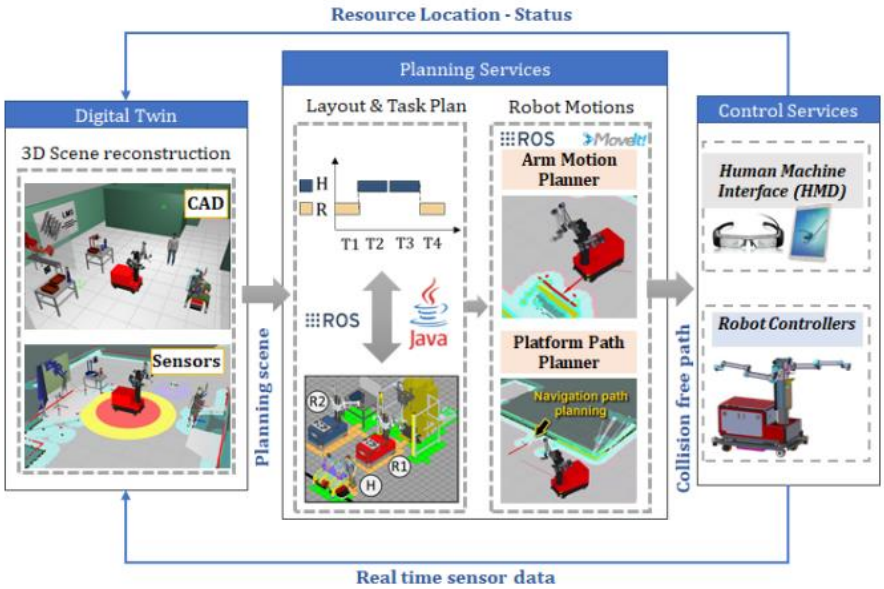


9.3 Ábra Digitális Iker rendszer architektúra ([14]. p. 6 Fig. 6)

2. Tervező és vezérlő szolgáltatások integrációja

A 9.4 Ábra mutatja a DT és az AI-alapú planning/control modulok közötti kapcsolatot:

- Layout & Task Planning (Java): AI-vezérelt modul generál alternatív elrendezési és feladatterveket a real-time planning scene és a DT egyedi entitásmodelljei alapján.
- Motion Planning: gmapping, amcl és OMPL könyvtárak segítségével végzi a mobil robotok és a karok trajektória-tervezését, a DT-ből kapott 3D térképen.
- ROSDriver & ROSBridge: A tervezett utasítások ROS-driveren keresztül jutnak el a robotvezérlőkhöz, míg az emberi műveletek felé ROSBridge szolgáltatás publikálja az értesítéseket smart eszközökön.

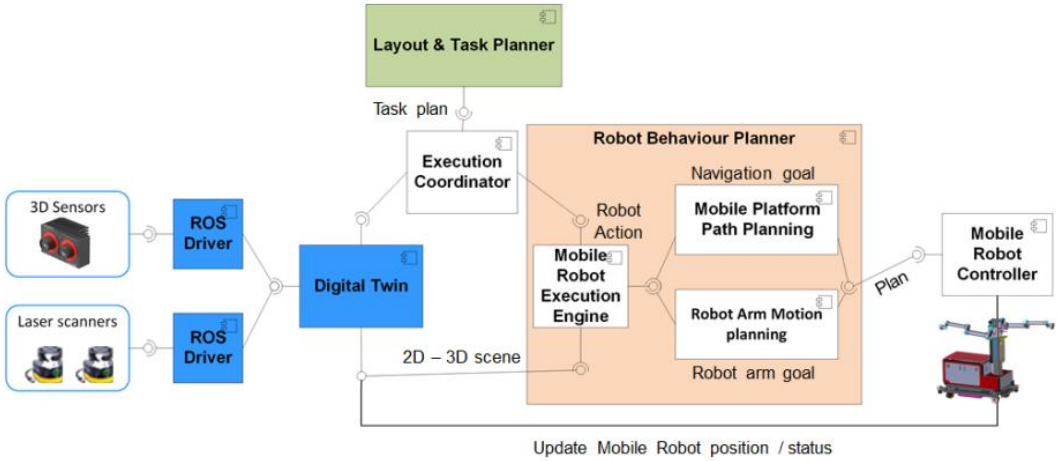


9.4 Ábra Digitális iker re-design rendszer architektúra ([14] p. 7 Fig. 7)

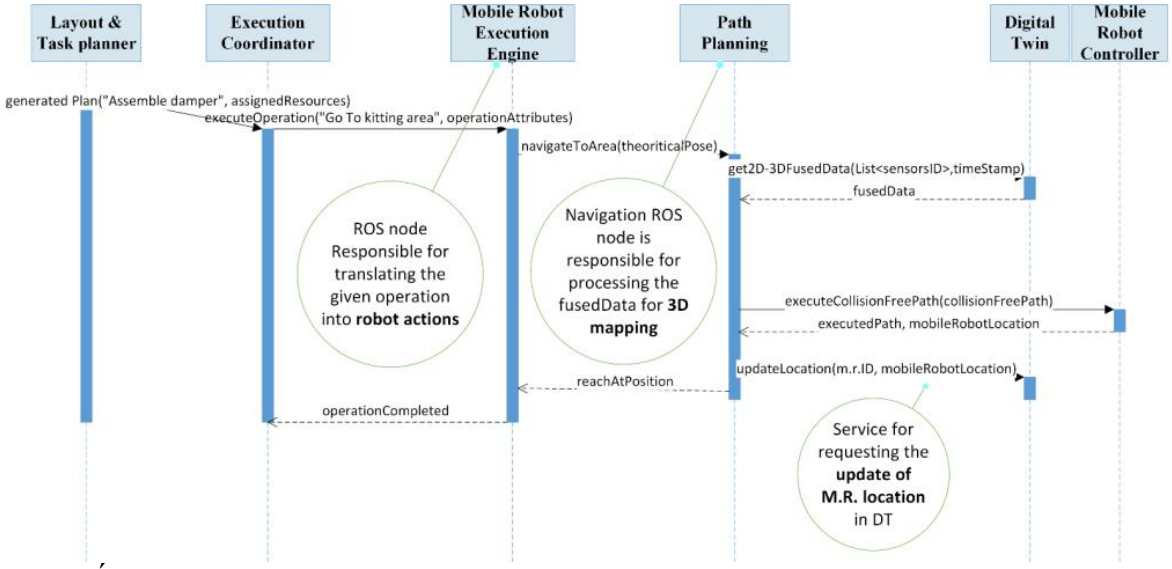
3. Komponens-diagram és futásidejű művelet

- A 9.5 Ábra részletesen ábrázolja a planning és control szolgáltatások valamint a DT modulok közötti peer-to-peer szolgáltatáshívásokat .
- A 9.6 Ábra példaszekvencia-diagramon mutatja be, hogyan történik egy Navigation Task végrehajtása: a Planning Service lekéri a current planning scene-et, kiválasztja a mobil robot útvonalát, majd a ROSDriver-en keresztül kiadja a MoveBase-utasításokat, és végül a Sensor Manager visszacsatolja a helyzetfrissítéseket.

Ez az implementációs felépítés biztosítja, hogy a digitális iker valós idejű, kétirányú kapcsolatban álljon a fizikai szerelőcellával, lehetővé téve a dinamikus újratervezést és adaptív működést.



9.5 Ábra DT alapú rendszer komponens diagram ([14] p. 7 Fig. 8)



9.6 Ábra DT alapú rendszer szekvencia diagram a „Navigation Task” elvégzésére ([14] p. 8 Fig. 9.)

9.3 Robotkarok szerepe az adott környezetben

A Kousi et al. esettanulmányában a mobil dual-arm robotkarok (M.R.) az emberi operátorokat kiegészítve végzik a kritikus, ismétlődő és nehéz fizikai feladatokat az elektronikai szerelősoron. A Táblázat(9.7 Ábra) alapján a robotkarok felelősségi köre a következő feladatokra terjed ki :

Tasks	Working Area	M.R.	Human
Pre-assembly of right damper	Pre-assembly		X
Pick and place of pre-assembled damper	From pre-ass. to compress.	X	
Align damper in comp. machine	Compression		X
Remove alignment rod	Compression	X	
Pick and place nut	Compression	X	
Pick and place compressed damper	From comp. to AGV.	X	
Pick and insert cables/screws on the disk	Compression		X
Screwing damper on the disk	Compression	X	

9.7 Ábra (Táblázat) Felelősségi körök eloszlása ([14] p. 9 Table 1)

1. Pre-assembly of right damper

   A robotkar átveszi a nyers lengéscsillapítót az AGV-től, majd precízen pozícionálja a pre-assembly állomáson elhelyezett tartókon.

2. Pick and place of pre-assembled damper

   A robotkar a pre-assembly állomáson elkészített előegységet megfogja, és az automatizált kompresszorhoz viszi.

3. Align damper in compression machine

   A kar behelyezi és rögzíti a lengéscsillapítót a kompressziós gépben, biztosítva a megfelelő irányt és pozíciót.

4. Remove alignment rod & Pick and place nut

   A kompresszió befejezése után a robotkar eltávolítja az illesztőcsapot, majd behelyezi a rögzítő anyát.

5. Pick and place compressed damper

   A készített egységet a robotkar az AGV-ra helyezi, amely továbbítja a végszereléshez.

További jellemzők

A 6 tengelyes robotkarok URDF-fájlban definiált payload és kinematika paraméterei alapján működnek, amelyeket a “Resource Manager” modul kezel ([14] 3. Implementation) .

Erő- és nyomatékérzékelők garantálják a finom mozgásvezérlést és kollíziómentességet az ember közelsége esetén is ([14] 4. Case Study).

A Stereo kamera és a két lézerscanner adatait a “Sensor Manager” egyesíti a 3D tervkép létrehozásához, amely a robotkarok valós idejű mozgástervezését támogatja ([14] 3. Implementation) .

9.4 Elért eredmények és tanulságok

A Kousi et al. esettanulmánya két fő érdemi eredményt emel ki: a szerelősor kezdeti tervezésének hatékonyságnövelését és a futásidejű zavarok kezelésének jelentős gyorsulását.

1. Tervezési fázisban mért javulások (Discrete Event Simulation) (Táblázat(9.8 Ábra))

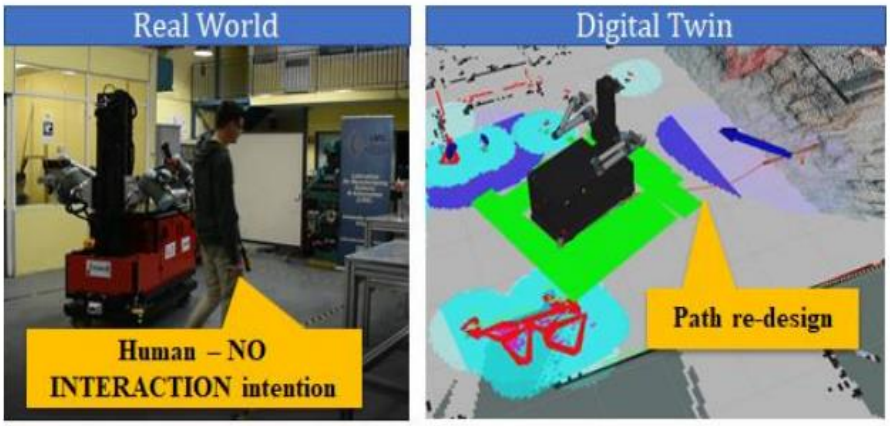
    - Az új DT-alapú kialakítás évente 394 997 darab alkatrész összeszerelését tette lehetővé a korábbi 315 353 helyett, ami 25 %-os növekedést jelent.
    - Az összeszerelésre fordított operátori idő aránya 34 %-ról 49 %-ra nőtt, ami 30 %-os hatékonyságjavulást mutat.

KPI	Current	DT Based Design	Increase
Annual production throughput—No. of Parts	315,353	394,997	25%
Time percentage allocated to performing assembly (%)	34	49	30%

9.8 Ábra Összehasonlító performansz táblázat ([14] p. 11. Table 2)

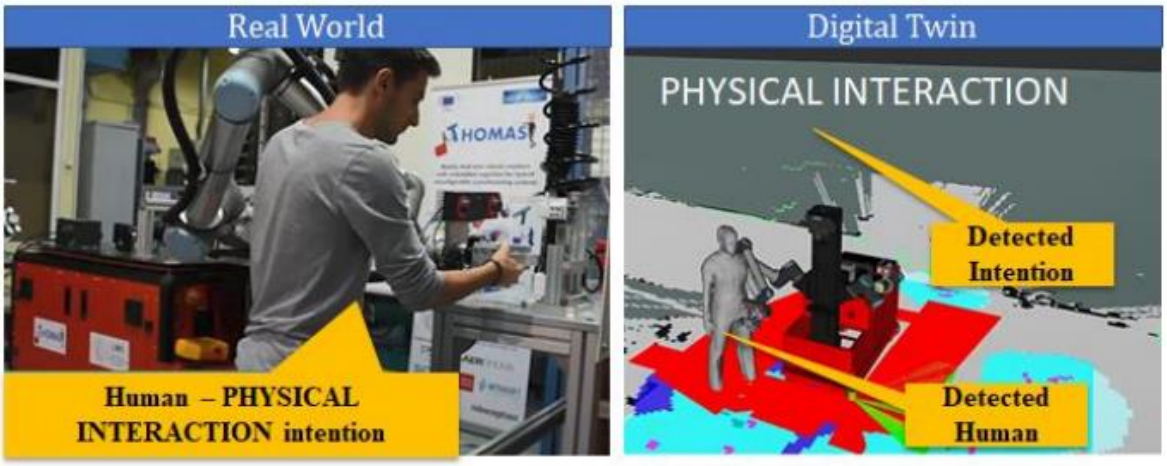
2. Futásidejű zavarok esetén elért rugalmasság

    - Case 1 (Robot viselkedés újratervezése): Ha egy operátor átlépi a robot útvonalát, a hagyományos rendszerben összesítésben 36 perc késleltetés keletkezik egy műszakban; a DT-alapú rendszerben ugyanez 7 percre csökken, ami 80 %-os javulás (Táblázat(9.11 Ábra)) . A robot ~2 másodperc alatt újratervezi az útvonalát, szemben a 1 másodperces újraindulással a hagyományos módszerben (9.9 Ábra).



9.9 Ábra Emberi beavatkozás nélkül([14] p. 11 Fig. 13)

- Case 2 (Állomásszintű újratervezés hiba esetén): A robotkar fogási hibája esetén a manuális beavatkozás 70 másodperc állásidőt okoz; a DT-rendszerben az operátor irányított beavatkozása 21 másodperc alatt helyreállítja a feladatot, így 69 %-kal csökken a leállás ideje (Táblázat(9.11 Ábra)). A "Physical Interaction" helyzetet a 14. ábra szemlélteti (9.10 Ábra).



9.10 Ábra Emberi beavatkozás ([14] p. 12. Fig. 14)

Time to Re-Design the Execution/Shift	Current	DT Based	Decrease
Case 1—Robot behavior re-design	36 (min)	7 (min)	80%
Case 2—Station level re-design	58 (min)	17.5 (min)	69%

9.11 Ábra Összehasonlító táblázat (responsiveness) a 2 rendszer között ([14] p. 12. Table 3)

Tanulságok

- A digitális iker bevezetése a tervezési és végrehajtási fázisban egyaránt jelentős produktivitás- és rugalmasság-növekedést eredményez.
- A valós idejű sensor fusion és a ROS-alapú architektúra együttesen lehetővé teszi a gyors újratervezést zavarok esetén, csökkentve a leállási és átszerelési időket.
- A mobil dual-arm robotkarok és az AGV integrációja minden munkaterületen hatékonyan kiegészíti az emberi munkaerőt, különösen a fizikai igénybevételt jelentő műveleteknél.

Ezek az eredmények alátámasztják, hogy a digitális iker koncepciója nem csupán elméleti keretrendszer, hanem ipari környezetben is mérhető és gyakorlati előnyöket hozó megoldás.

10. Összefoglalás és jövőbeli kilátások

A dolgozatban bemutatott esettanulmány rávilágított arra, hogy a digitális iker (DT) technológia miként teszi lehetővé a moduláris ember–robot kollaborációs szerelősorok rugalmas megtervezését és üzemeltetését. A PT Patrasz laboratóriumában telepített rendszer sikeresen integrálta a valós idejű szenzoradatokat, a ROS-alapú kommunikációt és az AI-alapú tervezőmodulokat, így a gyártósor hatékonysága és adaptivitása mind a tervezési, mind a futásidejű fázisokban jelentősen nőtt [14].

10.1 Főbb tanulságok összegzése

- A DT lehetővé teszi a tervezési és üzemeltetési fázisok közti zártláncú visszacsatolást, amellyel a gyártórendszer újratervezése akár valós időben is megtörténhet [1][2].
- A mobil dual-arm robotkarok és az AGV-k integrálása csökkenti az emberi operátorok fizikai terhelését és növeli a ciklusidők stabilitását [14][11].
- A valós idejű sensor fusion és a DT-alapú 3D planning scene kialakítása drasztikusan csökkenti a futásidejű zavarok okozta leállásokat (80 %-os csökkenés a robot viselkedés újratervezésében, 69 % a hiba utáni helyreállítás idejében) [14].

10.2 A technológia jövőbeli irányai

- A DT-képességek standardizálása és interoperabilitása (pl. OPC UA [20], Azure Digital Twins [21]) alapfeltétel a vállalati szintű elterjedéshez [19].
- A felhőhöz és edge-hez kapcsolt elosztott architektúrák (AWS IoT Core, Azure IoT Hub) tovább bővíthetik a DT-k skálázhatóságát és valós idejű analitikáját [4][5].
- A DT-k és kibervédelmi megoldások összekapcsolása kulcsfontosságú lesz a gyártási adatok biztonságos kezelése érdekében [19].

10.3 További kutatási lehetőségek

- Prediktív karbantartás fejlett DT-alapú modellezéssel és gépi tanulással, amelyek képesek korai anomália-detektálásra [16][17].
- Emberi tényezők beépítése a DT-kbe, például a kognitív állapot- és szándékfelismerés támogatása [8][10].
- Energia- és fenntarthatósági optimalizáció digitális ikerrel vezérelt SMT-PCB sorokon [31].
- Unity/ROS-alapú vizualizációs és szimulációs rétegek fejlesztése a felhasználói interakcióhoz és teszteléshez [32].
- A hibrid ember–robot munkaállomások biztonságosabbá tétele DT-alapú dinamikus kockázatértékeléssel [13][30].

A digitális iker technológia gyors fejlődése és széleskörű alkalmazhatósága új lehetőségeket nyit meg az ipari automatizálásban, különösen az ember–robot együttműködés és a rugalmas gyártórendszerek területén. Jövő-kutatások során a fenti irányok alapos vizsgálata hozzájárulhat a következő generációs, önadaptív gyártórendszerek megvalósításához.

Források

[1] M. Grieves, Digital Twin: Manufacturing Excellence through Virtual Factory Replication, 2014. https://www.researchgate.net/publication/275211047_Digital_Twin_Manufacturing_Excellence_through_Virtual_Factory_Replication

[2] M. Kritzinger et al., Digital Twin in manufacturing: A categorical literature review and classification, 2018. https://www.sciencedirect.com/science/article/pii/S2405896318316021

[3] R. Rosen et al., "About the importance of autonomy and digital twins for the future of manufacturing," 2015

https://www.sciencedirect.com/science/article/pii/S2405896315003808

[4] Jaskó, Szilárd; Ruppert, Tamás: *"The Future of Manufacturing and Industry 4.0."* Applied Sciences, 15(9), 4655 (2025). [DOI:10.3390/app15094655]

https://www.mdpi.com/2076-3417/15/9/4655#:~:text=the%20future%20of%20manufacturing%20and,time%20decision

[5] Hananto, April Lia et al.: *"Digital Twin and 3D Digital Twin: Concepts, Applications, and Challenges in Industry 4.0 for Digital Twin."* Computers, 13(4), 100 (2024). [DOI:10.3390/computers13040100]

https://www.mdpi.com/2073-431X/13/4/100/pdf?version=1713251230#:~:text=Citation%3A%20Hananto%2C%20A,3390%2F%20computers13040100

[6] Sass, Henrietta; Bányai, Tamás: *"A digitális iker logisztikai alkalmazásának lehetőségei a negyedik ipari forradalom keretében."* Multidiszciplináris Tudományok, 10(2): 43–47 (2020). DOI:10.35925/j.multi.2020.2.7

https://ojs.uni-miskolc.hu/index.php/multi/article/view/392#:~:text=A%20digitális%20iker%20logisztikai%20alkalmazásának,a%20negyedik%20ipari%20forradalom%20keretében

[7] Amthiou, Hanan; Arioua, Mounir; Benbarrad, Tajjedine: *"Digital Twins in Industry 4.0: A Literature Review."* ITM Web of Conferences 52, 01002 (2023). [DOI:10.1051/itmconf/20235201002]

https://www.itm-conferences.org/articles/itmconf/pdf/2023/02/itmconf_cocia2023_01002.pdf#:~:text=Digital%20Twins%20in%20Industry%204,date%20representation%20of%20a

[8] Maruyama, Tsubasa et al.: *"Digital Twin-Driven Human Robot Collaboration Using a Digital Human."* Sensors, 21(24), 8266 (2021). [DOI:10.3390/s21248266]

https://www.mdpi.com/1424-8220/21/24/8266#:~:text=The%20advent%20of%20Industry%204,with%20relatively%20low%20latency%2C%20and]

[9] Tarng, Wernhuar; Wu, Yu-Jung; Ye, Li-Yuan et al.: *"Application of Virtual Reality in Developing the Digital Twin for an Integrated Robot Learning System."* Electronics, 13(14), 2848 (2024). [DOI:10.3390/electronics13142848]

https://www.mdpi.com/2079-9292/13/14/2848#:~:text=Author%20to%20whom%20correspondence%20should,be%20addressed

[10] Gallala, Abderrahman; Kumar, Anil Anil; Hichri, Belhassen; Plapper, Peter: *"Digital Twin for Human–Robot Interactions by Means of Industry 4.0 Enabling Technologies."* Sensors, 22(13), 4950 (2022). [DOI:10.3390/s22134950]

https://www.mdpi.com/1424-8220/22/13/4950#:~:text=Interactions%20by%20Means%20of%20Industry,3390%2Fs22134950

[11] Urrea, Claudio; Kern, John: *"Recent Advances and Challenges in Industrial Robotics: A Systematic Review of Technological Trends and Emerging Applications."* Processes, 13(3), 832 (2025). [DOI:10.3390/pr13130773]

https://www.mdpi.com/2227-9717/13/3/832#:~:text=Urrea%2C%20C,3390%2Fpr13030832

[12] Elsevier B.V, " Real-time resilient scheduling by digital twin technology in a flow-shop manufacturing system" 2022.

https://www.sciencedirect.com/science/article/pii/S2212827122003274

[13] Szybicki, Dariusz et al.: *"Application of Digital Twins in Designing Safety Systems for Robotic Stations."* Electronics, 13(21), 4179 (2024). [DOI:10.3390/electronics13214179]

https://www.mdpi.com/2079-9292/13/21/4179#:~:text=by

[14] Kousi, Niki et al.: *"Digital Twin for Designing and Reconfiguring Human–Robot Collaborative Assembly Lines."* Applied Sciences, 11(10), 4620 (2021). [DOI:10.3390/app11104620]

https://www.mdpi.com/2076-3417/11/10/4620#:~:text=Digital%20Twin%20for%20Designing%20and,Reconfiguring%20Human–Robot%20Collaborative%20Assembly%20Lines

[15] Jaskó, Sz.; Ruppert, T. (2025) *(Ipar 4.0 vezérlőtechnológiák és IoT-eszközök robbanásszerű elterjedésének ismertetése.)*

https://www.mdpi.com/2076-3417/15/9/4655#:~:text=the%20future%20of%20manufacturing%20and,time%20decision

[16] Bofill et al. (2023). *(Digitális iker alapú hibamonitorozás általános áttekintése, prediktív karbantartással.)*

[17] Tripathy, Aparajita: *"Digital Twin-based Condition Monitoring with Distributed Data Mapping of OPC UA and ISO 10303 STEP Standard."* In: eSAAM/COCIS 2024 Proceedings, vol.58 (2024). [DOI:10.3390/proceedings2020580058]

https://ltu.diva-portal.org/smash/get/diva2:1908559/FULLTEXT01.pdf#:~:text=2,SOAP%2C%20making%20it%20more%20adaptable

[18] Matsive, Ali et al.: *"Digital Twin-Enabled Real-Time Control in Robotic Additive Manufacturing via Soft Actor-Critic Reinforcement Learning."* Preprint (arXiv:2501.18016, 2024).

https://arxiv.org/html/2501.18016v1#:~:text=

[19] National Academies of Sciences, Engineering, and Medicine: *"Foundational Research Gaps and Future Directions for Digital Twins."* The National Academies Press, Washington, D.C. (2024). [DOI:10.17226/26894]

https://nap.nationalacademies.org/catalog/26894/foundational-research-gaps-and-future-directions-for-digital-twins#:~:text=Across%20multiple%20domains%20of%20science%2C,many%20challenges%20remain%20before%20these

[20] OPC Foundation, "OPC-UA Specifications," 2018.

https://reference.opcfoundation.org

[21] Microsoft, Azure Digital Twins, 2020.

https://azure.microsoft.com/en-us/products/digital-twins/

[22] D. Yan et al., *"Digital twin-driven variant design of a 3C electronic product assembly line,"* Sci. Rep., vol. 12, Article 3846, 2022.

[23] B. Yao et al., *"Digital twin-based multi-level task rescheduling for robotic assembly line,"* Sci. Rep., vol. 13, Article 1769, 2023.

[24] Siemens Digital Industries, *"Automating and standardizing PCB engineering planning (Connect Group case study),"* 2020.

https://resources.sw.siemens.com/en-US/case-study-connect-group/ (elérés: 2023. ápr. 1.).

[25] Robots.com, *"What are the main parts of an industrial robot arm?"*

https://www.robots.com/articles/what-are-the-main-parts-of-an-industrial-robot-arm

[26] Apache NiFi, The Apache Software Foundation, 2023.

https://nifi.apache.org

[27] Microsoft Azure Data Factory, 2025.

https://azure.microsoft.com/en-us/products/data-factory/

https://learn.microsoft.com/en-us/azure/data-factory/

https://learn.microsoft.com/en-us/azure/data-factory/introduction

[28] Claudio Urrea és John Kern: "Recent Advances and Challenges in Industrial Robotics: A Systematic Review of Technological Trends and Emerging Applications," *Processes*, 13(3), 832 (2025).

https://www.mdpi.com/2227-9717/13/3/832

[29] D. Mourtzis et al.: "Real-time data acquisition and control in digital twin systems," *Procedia CIRP*, vol. 92, pp. 100–105 (2020).

[30] Dariusz Szybicki et al.: "Application of Digital Twins in Designing Safety Systems for Robotic Stations," *Electronics*, 13(21), 4179 (2024).

[31] Nehakaranjkar et al. (2018) – „Digital Twin for Energy Optimization in an SMT-PCB Assembly Line"

https://nehakaranjkar.github.io/publications/Digital_Twin.pdf#:~:text=operational%20state,described%20in%20detail%20in%20Section

[32] Singh (2024) – „Unity and ROS as a Digital and Communication Layer for Digital Twin Application: Case Study of Robotic Arm in a Smart Manufacturing Cell"

https://www.mdpi.com/1424-8220/24/17/5680#:~:text=reflects%20real,crucial%20for%20modern%20smart%20manufacturing

2.34. IoT-rendszerek szerepe az okosotthonok kommunikációjában és biztonságában az Ipar

Féléves beadandó

Ipar 4.0 és az okosotthonok: Nyílt forráskódú IoT-rendszerek szerepe az okosotthonok kommunikációjában és biztonságában az Ipar 4.0 környezetében

Murai Márk – [redacted]

Mérnökinformatikus BSc

2025

Tartalomjegyzék

ELŐSZÓ 3

OKOSOTTHONOK ÉS KIBER-FIZIKA RENDSZEREK AZ IPAR 4.0 KORSZAKÁBAN 4

A KIBER-FIZIKAI RENDSZEREK (CPS) ÉS IOT-ESZKÖZÖK SZEREPE AZ OKOSOTTHONOKBAN 4

SZENZOROK, AKTUÁTOROK ÉS FELHŐALAPÚ SZOLGÁLTATÁSOK INTEGRÁCIÓJA 5

A NYÍLT FORRÁSKÓDÚ SZEMLÉLET JELENTŐSÉGE AZ OTTHONI RENDSZEREKBEN 7

NYÍLT FORRÁSKÓDÚ IOT-MEGOLDÁSOK AZ OKOSOTTHONOKBAN 9

NÉPSZERŰ NYÍLT FORRÁSKÓDÚ SMART HOME PLATFORMOK BEMUTATÁSA 9

ELŐNYÖK ÉS KIHÍVÁSOK: TESTRESZABHATÓSÁG, KÖZÖSSÉGI TÁMOGATÁS, BIZTONSÁGI KÉRDÉSEK 10

KOMMUNIKÁCIÓS TECHNOLÓGIÁK ÉS ADATÁTVITEL AZ OKOSOTTHONOKBAN 13

PROTOKOLLOK ÖSSZEHASONLÍTÁSA 13

AZ IOT-ESZKÖZÖK KOMMUNIKÁCIÓS BIZTONSÁGA ÉS KIHÍVÁSAI 18

BIZTONSÁGI FENYEGETÉSEK: MITM, FIRMWARE-TÁMADÁSOK, JOGOSULATLAN HOZZÁFÉRÉS 18

VÉDEKEZÉSI LEHETŐSÉGEK: TITKOSÍTÁS, HITELESÍTÉS, RENDSZERES FRISSÍTÉS 21

BLOKKLÁNC-TECHNOLÓGIA ÉS ADATINTEGRITÁS 22

DECENTRALIZÁLT HITELESÍTÉS ÉS ADATVÉDELEM 22

ADATMANIPULÁCIÓ ELLENI VÉDEKEZÉS 25

EDGE COMPUTING ÉS LOKÁLIS ADATFELDOLGOZÁS AZ OKOSOTTHONOKBAN 26

AZ EDGE COMPUTING SZEREPE NYÍLT RENDSZEREKBEN 26

HELYI ADATFELDOLGOZÁS ELŐNYEI: GYORSASÁG, ADATBIZTONSÁG, FELHŐTŐL VALÓ FÜGGETLENSÉG ÉS VÁLASZIDŐ-OPTIMALIZÁLÁS 28

JÖVŐBELI TRENDEK ÉS KUTATÁSI IRÁNYOK 30

NYÍLT FORRÁSÚ AI-MODULOK, ÖNFEJLESZTŐ AUTOMATIZÁLÁSI SZABÁLYOK, ENERGIAHATÉKONYSÁGI TÖREKVÉSEK 30

KONKLÚZIO 32

IRODALOMJEGYZÉK 32

ÁBRAJEGYZÉK 38

Előszó

Az Ipar 4.0 korszakában az okosotthonok egyre nagyobb figyelmet kapnak, mivel az emberek törekednek az életminőségük javítására és a mindennapi tevékenységek automatizálására. Az Internet of Things (IoT) technológiák lehetővé teszik az eszközök közötti kommunikációt, ami új lehetőségeket teremt az otthoni rendszerek fejlesztésében.

A nyílt forráskódú IoT-megoldások, mint például a Home Assistant és az OpenHAB, lehetőséget biztosítanak a felhasználók számára, hogy testreszabott és költséghatékony okosotthon-rendszereket hozzanak létre. Ezek a platformok nemcsak a rugalmasságot növelik, hanem a közösségi fejlesztés révén folyamatosan bővülnek és fejlődnek.

Dolgozatom célja, hogy bemutassa a nyílt forráskódú IoT-rendszerek szerepét az okosotthonok kommunikációjában és biztonságában az Ipar 4.0 környezetében. Különös figyelmet fordítok a szenzorok és aktuátorok integrációjára, a kommunikációs protokollok összehasonlítására, valamint a biztonsági kihívásokra és azok lehetséges megoldásaira.

Ábra 1: Az okosotthonok alapvető komponensei és működési elve.

Okosotthonok és Kiber-fizika rendszerek az Ipar 4.0 korszakában

A kiber-fizikai rendszerek (CPS) és IoT-eszközök szerepe az okosotthonokban

Az okosotthonok kialakulása és fejlődése szorosan összefügg a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) és az Internet of Things (IoT) technológia térhódításával. A CPS rendszerek lényege, hogy a fizikai világot és a digitális rendszereket szorosan integrálják – valós idejű érzékelést, adatfeldolgozást és automatikus beavatkozást tesznek lehetővé [1].

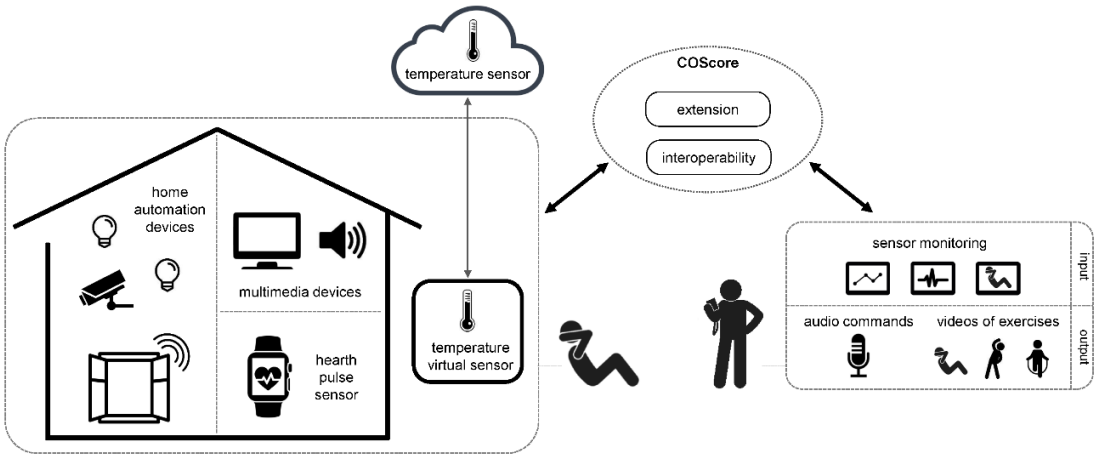
Az okosotthonok tehát olyan stacionárius CPS-eknek tekinthetők, amelyek IoT-eszközöket, szenzorokat, aktuátorokat, számítógépes rendszereket és szoftvereket kapcsolnak össze annak érdekében, hogy automatizálják és kényelmesebbé tegyék a lakók mindennapjait [2]. A rendszer képes adatokat gyűjteni a környezetről, a lakók szokásairól, majd ezek alapján döntéseket hozni és műveleteket végrehajtani.

A CPS rendszerek legfontosabb előnyei az okosotthonokban a következők:

- **Intelligencia**: A beépített érzékelőknek és vezérlőrendszereknek köszönhetően képesek a környezet és a lakók viselkedésének elemzésére.
- **Automatizálás**: A rendszer automatikusan reagál különböző eseményekre – például szabályozza a hőmérsékletet vagy aktiválja a világítást és a riasztót.
- **Erőforrás-hatékonyság**: Optimalizálja az energiafelhasználást, például kikapcsolja a feleslegesen működő készülékeket vagy szabályozza az öntözőrendszert.
- **Biztonság**: Érzékeli az illetéktelen behatolást vagy tűz esetén riasztást küld.
- **Interoperabilitás**: Az okosotthon különféle eszközei – például világítás, fűtés, biztonsági rendszerek – képesek összehangoltan működni.

A rendszerhez kapcsolódó konkrét eszközök például az intelligens termosztátok, világítási rendszerek, füst- és szén-monoxid érzékelők, okos zárak, videó kapucsengők, valamint hangvezérlésű asszisztensek (pl. Google Home, Amazon Echo) [2].

Ezek az eszközök valós idejű adatkommunikációt folytatnak egymással, gyakran felhőalapú szolgáltatásokon keresztül, ami lehetővé teszi a felhasználói szokásokhoz alkalmazkodó automatizálást és a biztonságos működést [1][3].



Ábra 2: Kiberfizikai rendszerek integrálása komponens alapú megközelítésben intelligens otthonok számára

Szenzorok, aktuátorok és felhőalapú szolgáltatások integrációja

A szenzorok és aktuátorok az okosotthonok működésének alapvető elemei, hiszen ezek biztosítják az adatok gyűjtését, feldolgozását és a környezeti változásokra adott automatikus reakciókat. Az IoT-technológia által lehetővé tett eszközintegráció révén az otthoni környezet intelligensen reagál a felhasználók szokásaira és igényeire.

A modern okosotthonokban gyakori megközelítés az ún. „**ubiquitous sensing**”, amelyben a szenzorok egy összetett hálózata kapcsolódik feldolgozó eszközökhöz, így létrehozva egy multimodális adathalmazt [4]. Az ilyen rendszerek képesek valós időben nyomon követni a lakók napi tevékenységeit, mint például a főzés, fürdés vagy gyógyszerbevétel, és ezek alapján mintázatokat azonosítanak. Ez a fajta viselkedésalapú adatfeldolgozás lehetővé teszi az eltérések azonnali észlelését, ami korai figyelmeztetést adhat például egészségügyi problémákra [4].

Az aktuátorok a szenzorok által begyűjtött adatok alapján végzik el a kívánt műveleteket. Ezek olyan eszközök, amelyek jelek hatására fizikai beavatkozást hajtanak végre – például egy

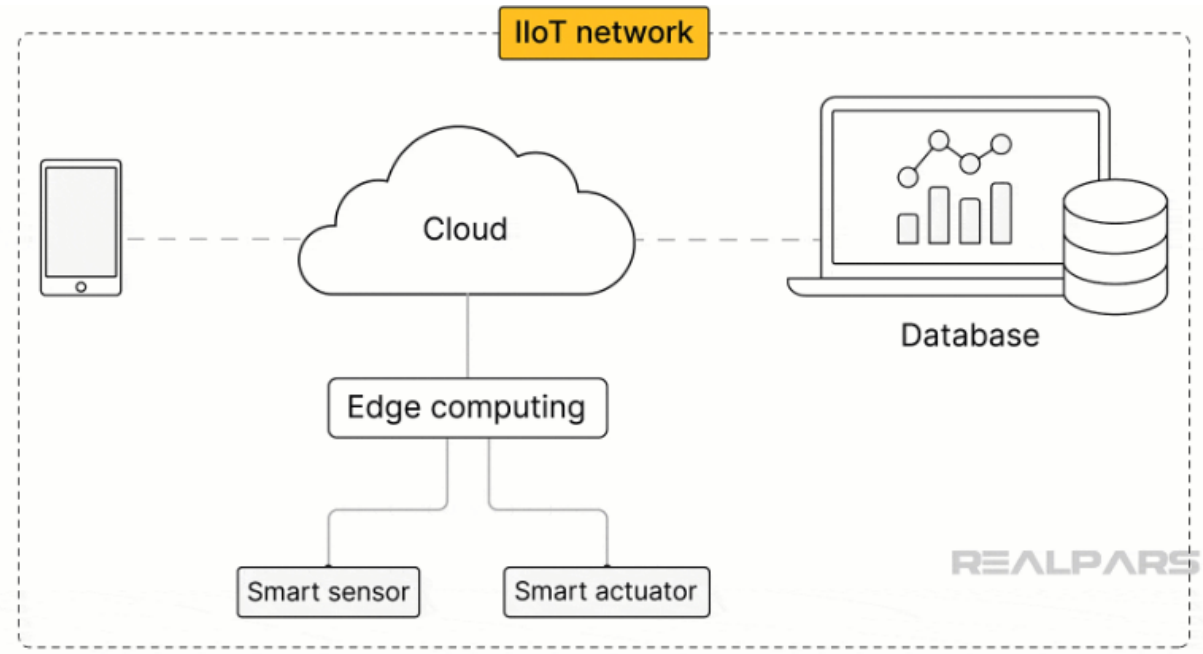
mozgásérzékelő jele alapján felkapcsolják a világítást [5]. Egyes rendszerek szenzorok és aktuátorok kombinációját alkalmazzák az automatizált vezérléshez: ha például egy szenzor érzékeli a napfelkeltét, akkor utasítja az aktuátort, hogy felhúzza a redőnyöket. Hasonlóképpen, ha a levegő minősége romlik, a rendszer automatikusan kinyitja az ablakokat, amennyiben azokat aktuátorral szerelték fel [5].

A felhőalapú szolgáltatások kulcsszerepet játszanak az okosotthonok működésében, mivel lehetővé teszik az eszközök számára, hogy az interneten keresztül kommunikáljanak és adatokat tároljanak. Ezáltal a felhasználók távolról is hozzáférhetnek és irányíthatják otthoni eszközeiket, növelve a kényelem és a funkcionalitás szintjét [6].

Például a Chameleon Smart Home rendszere lehetővé teszi a felhasználók számára, hogy távolról vezéreljék az otthoni eszközöket, mint a víz-, áram-, árnyékolás-, hűtés- vagy fűtésrendszereket, akár a világ másik feléről is, a felhőalapú technológiának köszönhetően [7].

Fontos megjegyezni, hogy bár a felhőalapú szolgáltatások számos előnnyel járnak, adatvédelmi és biztonsági szempontból kihívásokat is felvetnek. Egyes rendszerek, mint például a Loxone okos ház rendszere, nem használnak felhőalapú szolgáltatásokat, ezáltal biztosítva, hogy az összes adat helyben maradjon, növelve ezzel a biztonságot és az adatvédelmet [8].

Összességében a felhőalapú szolgáltatások integrációja az okosotthonokban jelentős mértékben hozzájárul a rendszer rugalmasságához és funkcionalitásához, ugyanakkor szükségessé teszi a megfelelő biztonsági intézkedések alkalmazását az adatvédelem érdekében.



Ábra 3: IIoT hálózati architektúra – okosszenzorok és aktuátorok kapcsolódása felhő- és edge computing rendszeren keresztül adatbázishoz

A nyílt forráskódú szemlélet jelentősége az otthoni rendszerekben

A nyílt forráskódú rendszerek egyre fontosabb szerepet töltenek be az okosotthonok fejlődésében, mivel lehetővé teszik a felhasználók és fejlesztők számára, hogy teljes mértékben átlássák, testreszabják és bővítsék a rendszereket saját igényeik szerint. Az ilyen rendszerek nyitottsága nemcsak a rugalmasságot növeli, hanem segít a biztonság fokozásában is, hiszen a forráskód átvizsgálható és közösségi auditnak vethető alá [9].

Az egyik legfőbb előny a testreszabhatóság. A felhasználók saját automatizálási szkripteket és integrációkat hozhatnak létre, amelyek megfelelnek napi rutinjuknak – például kombinálhatják a világítást a mozgásérzékelőkkel, vagy a hőmérséklet-szabályozást időjárási adatokkal [9], [10]. Illetve a közössége támogatás is a legfőbb előnyök közé sorolható, ugyais a fejlesztők hatalmas közössége járul hozzá a folyamatos fejlesztéshez és hibaelhárításhoz [9]. A Home Assistant és az OpenHAB két kiemelkedő példa, amelyek mögött aktív közösség áll. Ezek a platformok lehetővé teszik, hogy különböző gyártók eszközei egy egységes ökoszisztémában működjenek [11].

A nyílt forráskódú rendszerek másik fontos előnye az interoperabilitás. Mivel a legtöbb zárt rendszer gyártóspecifikus, nehézséget jelenthet az eszközök összekapcsolása. Ezzel szemben a

nyílt megközelítés a szabványos kommunikációs protokollokat (pl. MQTT, Zigbee, REST API-k) támogatja, így csökkenti a függőséget egyetlen beszállítótól [12].

Emellett a költséghatékonyság sem elhanyagolható szempont. A felhasználók licencdíjak nélkül férhetnek hozzá fejlett funkciókhoz és automatizálási lehetőségekhez, valamint a közösség által karbantartott bővítményekhez [9].

A biztonság és adatvédelem szempontjából is előnyös a nyílt forráskódú megközelítés. A nyitottság lehetőséget ad arra, hogy a felhasználók ellenőrizzék, hogyan történik az adatkezelés, illetve hogy kiküszöböljék azokat a rejtett kockázatokat, amelyek a zárt rendszerekben könnyen észrevétlenek maradhatnak. Megnézhetik a szoftverek forráskódját, a konfigurációt, a nyíltforrású Smart Home-ok megosztják a hardvereiket. A felhasználó akár saját szoftvert is írhat és telepíthet, hibajelentéseket küldhet, mi pedig meghallgatjuk [13].

Összességében a nyílt forráskódú szemlélet nemcsak technológiai, hanem filozófiai értelemben is jelentős, mivel a kontrollt visszaadja a felhasználónak, miközben a közösség támogatására épít. Ez különösen fontos az Ipar 4.0 korszakában, ahol a decentralizált, rugalmas és biztonságos rendszerekre egyre nagyobb szükség van.

Ábra 4: Google Nest Hub a Home Assistant felhasználói felülettel

Nyílt forráskódú IoT-megoldások az okosotthonokban

Népszerű nyílt forráskódú Smart Home platformok bemutatása

Az okosotthonok terjedésével párhuzamosan egyre nagyobb figyelmet kapnak a nyílt forráskódú automatizálási platformok, amelyek lehetőséget biztosítanak a felhasználók számára, hogy testreszabott, rugalmas és átlátható rendszereket alakítsanak ki otthoni környezetükben. Ezek a megoldások különösen népszerűek a technológiai közösségek körében, mivel nemcsak költséghatékonyak, hanem aktív közösségi támogatással és bővíthetőséggel is rendelkeznek [14].

OpenHAB (Open Home Automation Bus) az egyik legismertebb és legtöbbet használt nyílt forráskódú platform. Több mint 2000 eszközzel kompatibilis, és különösen népszerű robusztussága, stabilitása és nagy felhasználói közössége miatt. További előnye, hogy ingyenesen használható, támogatja az egyéni automatizálási szabályok létrehozását, és számos pluginnal bővíthető [14], [15].

Home Assistant szintén kiemelkedő szereplő az open-source világban. Támogat több mint 1000 márkát, és lehetőséget biztosít a teljes lokális adatkezelésre – ez különösen fontos az adatvédelem szempontjából. Az egyszerű, reszponzív felhasználói felület mellett mobilalkalmazással is rendelkezik, amellyel távolról is könnyedén vezérelhető a teljes rendszer [14], [15].

Domoticz elsősorban egyszerűsége és könnyű kezelhetősége révén kedvelt. HTML5-alapú, reszponzív felületének köszönhetően asztali számítógépen és mobileszközökön egyaránt kényelmesen használható. Számos operációs rendszerre telepíthető, és széles eszköztámogatási palettával rendelkezik [14], [15].

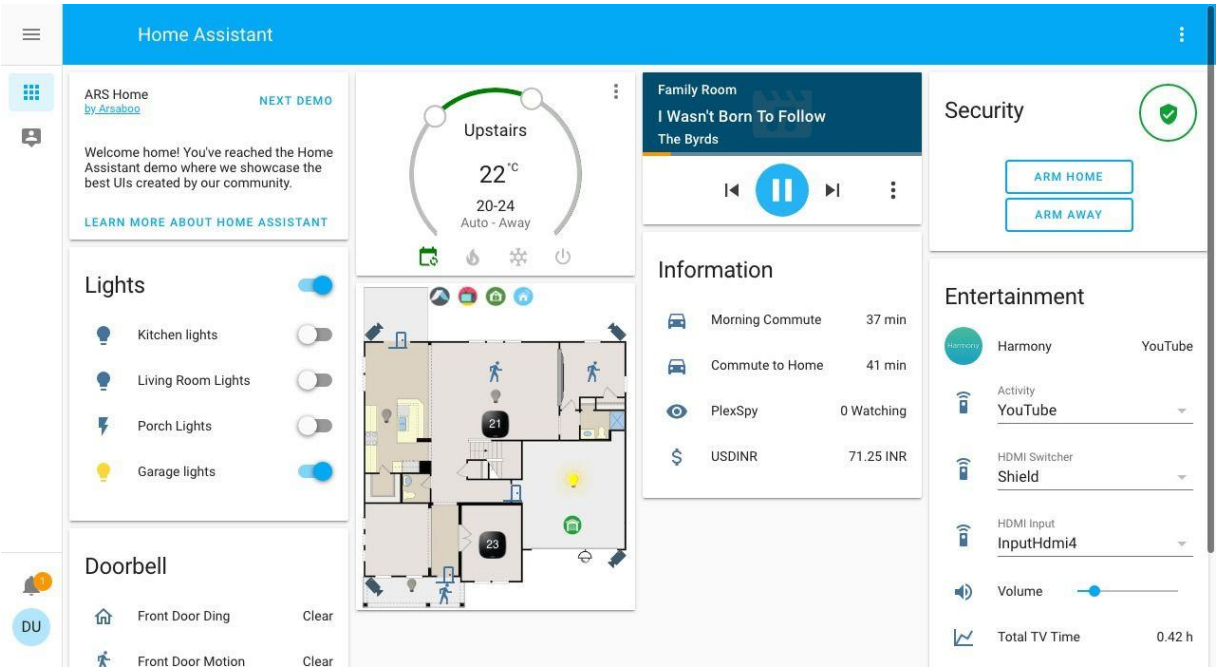
Calaos teljes körű, GPLv3 alatt elérhető open-source megoldás, amely saját érintőkijelzős felületet, webalkalmazást és mobilalkalmazást is kínál. Az előre konfigurált Linux-alapú operációs rendszerrel együtt egy komplett „csomagot” nyújt az okosotthon-automatizáláshoz [15].

OpenMotics esetében különösen érdekes, hogy hardveres modulokat is kínál, amelyek könnyedén integrálhatók a szoftverrel. A rendszer nyílt forráskódú, lehetővé teszi a saját modulok fejlesztését és teljes testreszabását. Több mint 1000 eszközt támogat, és több száz előre elkészített automatizálási szkripttel érkezik [14], [15].

HomeGenie egy másik fontos platform, amely webalapú kezelőfelületet, RFID-támogatást és programozható automatizálási lehetőségeket kínál. Bár a közösségi támogatás kissé visszafogottabb, technikai képességei mégis versenyképesek [14].

MisterHouse Perl-alapú rendszer, amelyet technológiai érdeklődésű felhasználók körében kedvelnek. Hangvezérléssel, eseményalapú automatizálással és széleskörű eszköztámogatással rendelkezik, beleértve az X10, Insteon és soros interfésszel ellátott eszközöket is [15].

Összességében ezek a platformok nemcsak az automatizálás rugalmasságát kínálják, hanem lehetőséget is adnak arra, hogy a felhasználók teljes mértékben ellenőrzésük alatt tartsák az otthoni rendszereiket – mindezt ingyenes, közösségi fejlesztésű környezetben.



Ábra 5: Home Assistant Demo

Előnyök és kihívások: testreszabhatóság, közösségi támogatás, biztonsági kérdések

Az okosotthonok és nyílt forráskódú rendszerek alkalmazása számos előnnyel jár, de ugyanakkor kihívásokat is rejt magában. A Mussab et al. által összegyűjtött szakirodalom alapján az okosotthon-rendszerek legfontosabb előnyei közé tartozik az energiafogyasztás optimalizálása, a biztonságérzet növekedése, az életminőség javulása, valamint az idő-, pénz- és energia-

megtakarítás [16]. Ezen kívül az ilyen rendszerek lehetőséget biztosítanak a kényelmi funkciók széleskörű testreszabására, így a felhasználók saját igényeikhez szabhatják otthonuk működését.

A nyílt forráskódú rendszerek különösen kiemelkednek a testreszabhatóság terén. A fejlesztők és a technikai ismeretekkel rendelkező felhasználók szabadon módosíthatják és bővíthetik a rendszert, így teljes mértékben kontrollálhatják annak működését. Ez azonban csak akkor előnyös, ha rendelkezésre áll a megfelelő technikai háttér és erőforrás [17].

A közösségi támogatás szintén a nyílt rendszerek egyik meghatározó jellemzője. Bár a fórumokon és blogokon keresztül elérhető tudásanyag hasznos lehet, a válaszok nem mindig gyorsak és megbízhatóak. A zárt forráskódú rendszerekkel szemben – ahol dedikált ügyfélszolgálat áll rendelkezésre – a nyílt rendszerek támogatása gyakran önkéntes közösségek munkájára épül [17].

A biztonság kérdése az egyik legkritikusabb kihívás. Mivel a nyílt forráskódú szoftverek bárki számára hozzáférhetők, potenciálisan nagyobb kockázatot jelentenek a sebezhetőségek szempontjából. A decentralizált fejlesztés és a különböző fejlesztői szintek miatt előfordulhat, hogy bizonyos biztonsági réseket nem vesznek időben észre. Emellett a nyílt forráskódú rendszerek fejlesztése nem mindig történik szigorúan ellenőrzött környezetben, ami megnehezíti az egységes minőségbiztosítást [17].

Ugyanakkor fontos megjegyezni, hogy a közösségi auditálás lehetősége – vagyis hogy bárki átvizsgálhatja a kódot – hosszú távon hozzájárulhat a biztonság növeléséhez. Emellett számos nyílt rendszer (pl. Home Assistant) már alkalmaz titkosítást, rendszeres frissítéseket és hozzáférés-kezelési mechanizmusokat is, hogy fokozza a védelmet [16].

Elmondható, hogy a nyílt forráskódú okosotthon-rendszerek rugalmas, költséghatékony és közösség-vezérelt alternatívát kínálnak, de a használatuk technikai hozzáértést és fokozott figyelmet igényel a biztonsági szempontokra.

Előnyök:

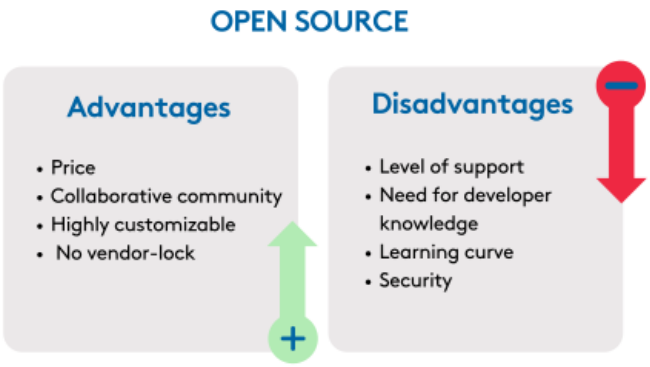
- **Energiahatékonyság**: Az intelligens termosztátok és világításvezérlő rendszerek csökkenthetik a felesleges energiafogyasztást [16].
- **Ingatlanérték-növekedés**: A beépített okosfunkciók növelhetik egy ingatlan piaci értékét [16].

- **Biztonságérzet növelése**: Az okos zárak, kamerák és mozgásérzékelők növelhetik az otthon biztonságát [16].
- **Életminőség javítása**: A személyre szabható automatizációs szabályok egyszerűsítik a mindennapokat.
- **Idő-, pénz- és energia-megtakarítás**: Az automatizált funkciók (pl. öntözőrendszer, fűtés) optimalizálják az erőforrások felhasználását [16].
- **Kényelmi funkciók lehetősége**: Távoli vezérlés, automatizáció, integráció más eszközökkel [14].

Hátrányok:

- **Magas belépési költségek**: A kezdeti eszközvásárlás és telepítés relatíve drága lehet [16].
- **Komplexitás**: A rendszerek konfigurálása technikai ismereteket igényelhet, különösen nyílt forráskódú rendszerek esetén [17].
- **Biztonsági kockázatok**: Az IoT-eszközök nyitottsága növelheti a támadási felületet (pl. hackelés, adatlopás) [14].
- **Tapasztalat hiánya**: Sok felhasználó nincs tisztában a rendszer beállításával vagy biztonságos használatával.
- **Rendszerérzékenység**: A rendszer elemei közötti kapcsolat megszakadása zavarokat okozhat a működésben [16].
- **Tanulási görbe**: A technológia elsajátítása időt és türelmet igényel, különösen az idősebb felhasználók számára [16].

A nyílt forráskódú rendszerek tehát komoly lehetőségeket kínálnak a személyre szabhatóság, közösségi támogatás és költséghatékonyság terén. Ugyanakkor a használatukhoz szükséges technikai ismeretek, a biztonsági kérdések és az esetleges komplexitás kihívást jelenthetnek a kevésbé tapasztalt felhasználók számára. A választás során ezért egyensúlyt kell teremteni az elérhető funkcionalitás és a használhatóság között.



Ábra 6: A nyílt forráskód előnyei és hátrányai.

Kommunikációs technológiák és adatátvitel az okosotthonokban

Protokollok összehasonlítása

Az IoT-architektúra több rétegből áll, amelyek egymással együttműködve biztosítják az adatgyűjtést, -feldolgozást és -továbbítást. A hardveres rétegek (pl. fizikai és adatkapcsolati réteg) felelősek az eszközök közötti kapcsolatért, míg a szoftveres rétegek (pl. alkalmazási réteg) lehetővé teszik az adatok strukturált feldolgozását és felhasználását. A különböző kommunikációs protokollok ezen architektúra eltérő rétegein működnek [17].

ZigBee

A ZigBee egy alacsony fogyasztású, vezeték nélküli protokoll, amelyet kifejezetten okosotthonokhoz és más alacsony sávszélességű IoT-alkalmazásokhoz fejlesztettek ki. Mesh topológiát használ, amely lehetővé teszi, hogy az eszközök közvetlenül vagy közvetve kommunikáljanak egymással, ezáltal nagyobb hatótávolságot biztosítva. A ZigBee protokoll támogatja az AES-128 titkosítást, és jellemzője a gyors válaszidő és nagy hálózati kapacitás [18][19][20].

MQTT (Message Queuing Telemetry Transport)

Az MQTT egy rendkívül könnyű üzenetküldési protokoll, amely a publish-subscribe modell alapján működik. Ideális szenzorokhoz és alacsony sávszélességű hálózatokhoz, mivel kis

adatcsomagokat használ. Az MQTT-t széles körben alkalmazzák felhőalapú kommunikációban, különösen olyan környezetekben, ahol megbízható és hatékony adatátvitel szükséges [21][22].

Wi-Fi

A Wi-Fi az egyik legismertebb és legelterjedtebb vezeték nélküli kommunikációs technológia. Előnye a nagy adatátviteli sebesség és a széles körű támogatás. Hátránya viszont a nagy energiafogyasztás, ami miatt kevésbé alkalmas akkumulátoros eszközökhöz. Ugyanakkor közvetlen kapcsolatot tesz lehetővé a felhővel, és gyors válaszidőt biztosít [20][23].

Bluetooth és BLE (Bluetooth Low Energy)

A Bluetooth rövid hatótávolságú, alacsony energiafogyasztású kapcsolatot biztosít, és leginkább hordozható eszközök, például okosórák és szenzorok esetében használatos. A BLE verzió kifejezetten IoT-alkalmazásokhoz készült, mivel hosszabb akkumulátor-üzemidőt és alacsonyabb energiafogyasztást kínál, miközben megőrzi a szükséges funkcionalitást [20][23].

LoRa és LoRaWAN

A LoRa egy hosszú hatótávolságú, alacsony energiafogyasztású protokoll, amely különösen alkalmas vidéki vagy nagy kiterjedésű területeken működő rendszerekhez. A LoRaWAN lehetővé teszi az eszközök több kilométeres távolságról való összeköttetését, minimális energiafelhasználással. Ez a protokoll különösen előnyös olyan környezetekben, ahol a Wi-Fi vagy a ZigBee nem elérhető [20][24].

Z-Wave

A Z-Wave egy másik alacsony fogyasztású, mesh-hálózatot használó protokoll, amely a ZigBee-hez hasonlóan elsősorban okosotthonokban terjedt el. Előnye, hogy a Wi-Fi-vel nem interferál, mivel az 800–900 MHz-es sávban működik. Bár az adatátviteli sebessége alacsonyabb, a megbízhatósága és a szabványosítása miatt sok gyártó támogatja [19][23].

CoAP és LwM2M

A CoAP (Constrained Application Protocol) egy HTTP-szerű protokoll, amelyet korlátozott erőforrású IoT-eszközökhöz terveztek. UDP-alapú, alacsony késleltetésű, és hatékony bináris adatátvitelt kínál. A LwM2M ehhez hasonlóan kis erőforrásigényű eszközök menedzselésére alkalmas, REST-alapú struktúrával és CoAP-al való kommunikációval [22].

Az egyes protokollok kiválasztása mindig az adott alkalmazási környezettől függ. Míg a ZigBee és Z-Wave ideálisak beltéri okosotthon-rendszerekhez, addig a LoRaWAN és NB-IoT nagyobb távolságú kommunikációhoz megfelelőbbek. A Wi-Fi és MQTT kiváló választás, ha magas adatátviteli sebesség vagy közvetlen felhőkapcsolat szükséges. A Bluetooth BLE verziója a kis eszközök közötti energiatakarékos kapcsolatra alkalmas.

Ábra 7: Okosotthon protokollok

Az okosotthonok egyik fő célja a működés hatékonyságának növelése, a rendszer megbízhatóságának biztosítása, valamint az adatbiztonság magas szintű fenntartása. A modern IoT-eszközök, felhőalapú rendszerek és mesterséges intelligenciával támogatott vezérlők együttesen járulnak hozzá ezekhez az alapvető célkitűzésekhez.

Üzemeltetési és karbantartási hatékonyság szempontjából az előrejelző karbantartás során az IoTeszközök és az adatelemzés lehetővé teszi a prediktív karbantartást, csökkentve az állásidőt és meghosszabbítva a berendezések élettartamát. Ehhez elengedhetetlen a szenzoradatok valós idejű elemzése és azok intelligens feldolgozása. Például a *The Edge* nevű adatvezérelt, intelligens épület hatalmas mennyiségű érzékelőadatot elemez az üzemeltetés optimalizálása és a munkakörnyezet javítása érdekében. Ezzel nemcsak az üzemidő nő, de a költségek és az energiafogyasztás is

csökkenthető. Ez az adatvezérelt megközelítés lehetővé teszi a prediktív karbantartást, növeli az épület hatékonyságát, és betekintést nyújt a helykihasználásba. [26].

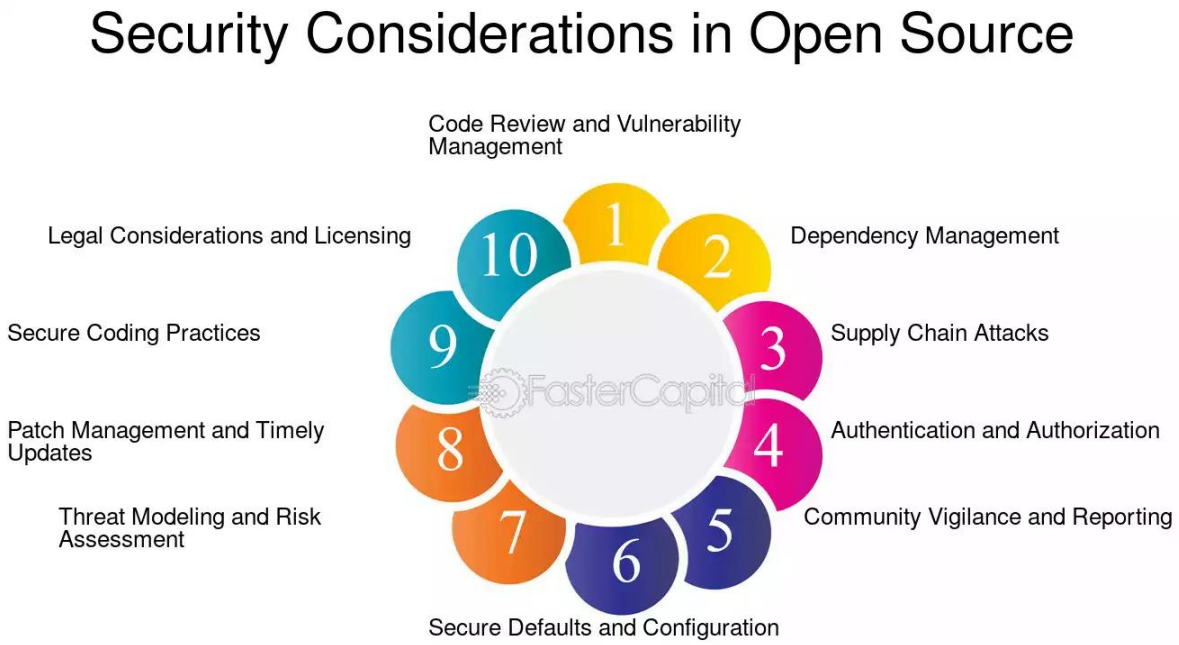
A megbízhatóság szorosan kapcsolódik a rendszer komplexitásához és annak karbantarthatóságához. A mesterséges intelligenciával vezérelt kényelmi funkciók folyamatos felügyeletet és rendszeres frissítést igényelnek, hogy a felhasználók számára zavartalan működést biztosítsanak. A felhőalapú rendszerek esetében a választott modell (nyilvános, privát, hibrid) jelentős hatással lehet a megbízhatóságra és a rugalmasságra. A nyilvános felhők skálázhatóságukról, megbízhatóságukról és hatékonyságukról ismertek, de az adatbiztonsággal és a magánélet védelmével kapcsolatos aggályokat is felvetnek, mivel az erőforrásokat több felhasználó között osztják meg. A privát felhőket kizárólag egyetlen vállalkozás vagy szervezet használja. Fizikailag elhelyezkedhetnek a szervezet helyszíni adatközpontjában, vagy egy harmadik fél szolgáltató által üzemeltetve. A privát felhők nagyobb ellenőrzést és biztonságot nyújtanak, így alkalmasak olyan szervezetek számára, amelyek szigorú szabályozási megfelelési igényekkel vagy érzékeny adatokkal rendelkeznek. A hibrid felhők egyesítik a nyilvános és a privát felhőket, amelyeket olyan technológia köt össze, amely lehetővé teszi az adatok és alkalmazások megosztását közöttük. [26].

A biztonság és adatvédelem szempontjai kiemelt fontosságúak az okosotthonok elterjedésével párhuzamosan. Az olyan technológiák, mint az AR/VR rendszerek vagy az okos zárak, új típusú támadási felületet nyitnak meg, ahol a személyes adatok (pl. biometrikus vagy helymeghatározási adatok) illetéktelen kezekbe kerülhetnek. Az okos zárak Wi-Fi-n vagy Bluetooth-on keresztül csatlakoznak, amely kommunikációs csatornák sebezhetők lehetnek, ha nem alkalmaznak megfelelő titkosítást és hitelesítést. A kiterjesztett valóság (AR) és a virtuális valóság (VR) technológiái egyre inkább integrálódnak az intelligens otthoni környezetekbe, javítva a felhasználók életterével való interakcióját. Amint azonban ezek a magával ragadó technológiák bejutnak otthonunkba, egyedi biztonsági kihívásokat és sebezhetőségeket hoznak magukkal, amelyeket gondosan kell kezelni a felhasználók magánéletének és adatbiztonságának védelme érdekében. Az AR és a VR intelligens otthonokban történő használatának egyik elsődleges biztonsági aggálya az érzékeny személyes adatok esetleges kitettsége. Ezek a technológiák gyakran nagy mennyiségű adat gyűjtését és feldolgozását teszik szükségessé a hatékony működéshez, beleértve a valós idejű helyadatokat, az AR-szemüvegekből vagy VR-fejhallgatókból készült vizuális felvételeket, valamint az élmények testreszabásához szükséges

biometrikus adatokat. Ezek az adatok rendkívül érzékenyek, és ha veszélybe kerülnek, rosszindulatú célokra, például személyazonosság-lopásra, jogosulatlan megfigyelésre vagy célzott adathalász támadásokra használhatók fel [27].

Továbbá, a rendszer integritásának megőrzése érdekében különböző technikák alkalmazása szükséges, mint például ellenőrző összegek (checksums), digitális aláírások vagy audit nyomvonalak. Az ilyen eszközök biztosítják, hogy az érzékelőktől származó adatokat ne lehessen manipulálni vagy hamisítani [26]. A gyártók egyre gyakrabban alkalmaznak Advanced Encryption Standard-titkosítást (AES-titkosítást) és kétfaktoros hitelesítést, valamint geofencing megoldásokat, amely automatikusan zárja vagy kinyitja az ajtókat a felhasználó fizikai helyzete alapján, amelyet okostelefonjuk GPS-je észlel, a fizikai és digitális hozzáférés biztonságosabbá tétele érdekében [27].

Az okosotthonok hatékonysága, megbízhatósága és biztonsága nem csupán technológiai kérdés, hanem komplex ökoszisztémát feltételez, amelynek minden elemét – a szenzoroktól kezdve a felhőkörnyezeten át a felhasználói szokásokig – holisztikus módon kell tervezni és védeni.



Ábra 8: Biztonsági megfontolások a nyílt forráskóddal kapcsolatban – Nyílt forráskódú szoftverek: Hogyan használjunk nyílt forráskódú szoftvereket és élvezzük előnyeit

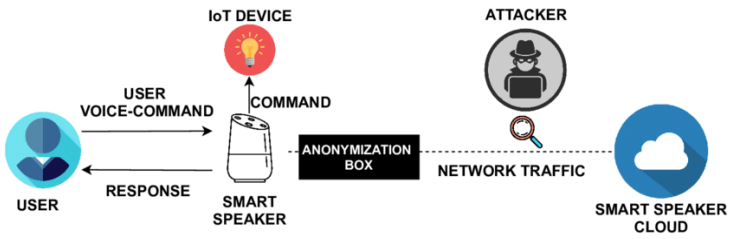
Az IoT-eszközök kommunikációs biztonsága és kihívásai

Biztonsági fenyegetések: MITM, firmware-támadások, jogosulatlan hozzáférés

Az okosotthonok és az IoT-eszközök térnyerésével egyre több biztonsági fenyegetés jelenik meg, amelyek célja az eszközök feletti illetéktelen hozzáférés megszerzése, az adatok manipulálása vagy a rendszer működésének megzavarása. Az aktív fenyegetések esetében a támadó valamilyen változtatást kísérel meg végrehajtani az IoT rendszerben vagy az általa továbbított adatokban vagy hozzáférést igyekszik szerezni ezekhez. Leggyakoribb típusai a szolgáltatásmegtagadás, közbeékelődéses támadás, parancsinjekció, brute force-támadások.

Közbeékelődéses támadások (Man-in-the-Middle – MITM)

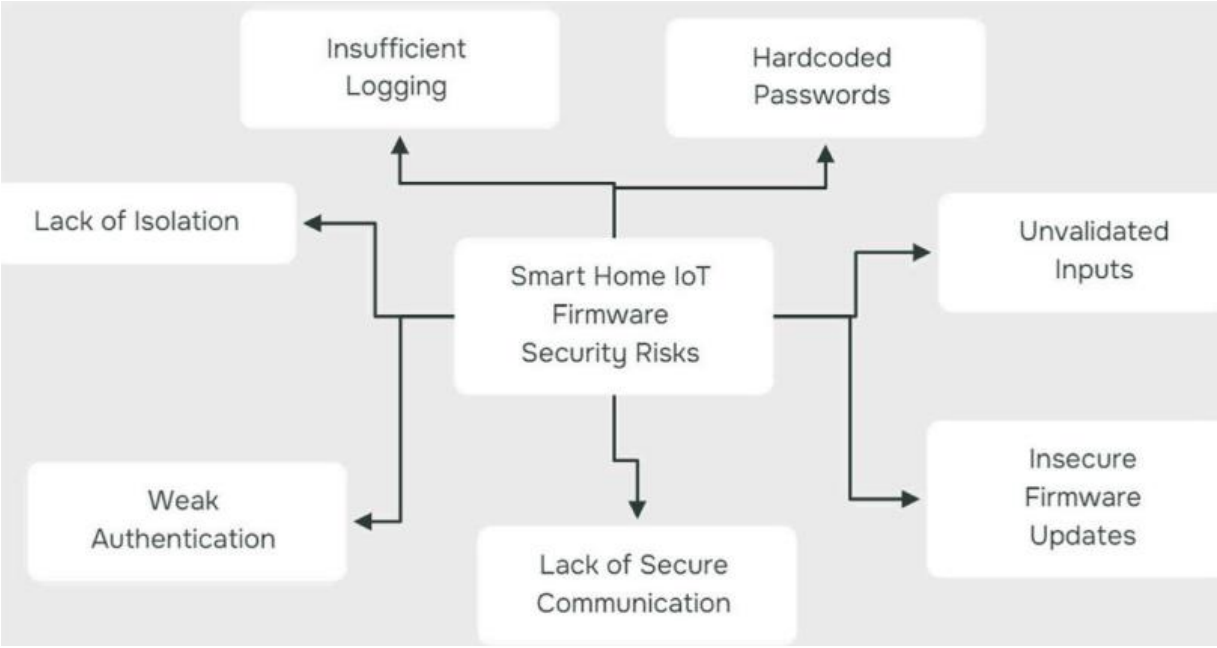
Az egyik legelterjedtebb fenyegetés az ún. közbeékelődéses támadás (Man-in-the-middle - MitM). A közbeékelődéses támadás során a támadó úgy módosítja két eszköz között a kommunikációt, hogy eltéríti az adatforgalmat, és mindkét fél számára a másik félnek adja ki magát, támadó titokban beékelődik két kommunikáló fél közé, és úgy módosítja vagy lehallgatja az adatokat, hogy egyik fél sem veszi észre a jelenlétét. Ez lehetővé teszi érzékeny információk, például jelszavak vagy vezérlőutasítások ellopását vagy rosszindulatú kód bejuttatását a rendszerbe. A MitM támadások elleni védekezés egyik legfontosabb eleme a VPN alapú titkosított kommunikáció és egy megfelelő tanúsítványkezelő rendszer használata, amely biztosítja, hogy csak hitelesített eszközök kommunikálhassanak egymással. Itt fontos szerepe van a tanúsítványok időszakos megújításának és az erős kulcskezelés szintén kulcsfontosságú a biztonság fenntartásához. [28]



Ábra 9: Az intelligens otthon ökoszisztémájának MITM fenyegetési modellje

Firmware-támadások

Az IoT-eszközök „lelke” a firmware, azaz az az alacsony szintű szoftver, amely közvetlenül irányítja az eszköz hardverét és felhasználói felületet kínál a kommunikációhoz. A firmware gyakran célpontja visszafejtéses (reverse engineering). Ez egy folyamat a bináris firmware-kód elemzésére, hogy megértsük annak működését, és ezáltal azonosítsuk a sebezhetőségeket. Ez gyakran automatizált, nem pedig manuálisan, olyan eszközök segítségével, mint az IDA Pro, a Ghidra és a Radare2. Ezek az eszközök lehetővé teszik a kutató számára, hogy visszafejtse a firmware-t, és megnézze az összeállítási kódot, amelyben könnyen napvilágra kerülhetnek kemény kódolt jelszavak, puffertúlcsordulás és egyéb biztonsággal kapcsolatos problémák. Visszafejtéssel lehetne többet megtudni az eszköz által használt kommunikációs protokollokról, és feltárni a titkosítás gyengeségeit. A második a fuzzing, ahol véletlenszerű bemeneteket táplálnak be a szoftverekbe, hogy felfedezzék a sebezhetőséget. A fuzzing automatizálható és olyan eszközök segítségével is elvégezhető, mint az AFL, a Sulley és a Peach. Ezek az eszközök nagyszámú bemenetet képesek előállítani, amelyek váratlan viselkedést váltanak ki a firmware-ben, felfedve olyan sebezhetőségeket, mint a puffertúlcsordulás, az SQL-befecskendezés és a parancsinjektálás. Ez hatékony módszernek bizonyulhat a firmware-en belüli sérülékenységek feltárásában, mivel képes feltárni olyan váratlan viselkedést, amelyet kézi teszteléssel nem lehet megtalálni. A védekezés érdekében elengedhetetlen a biztonságos firmware-frissítés, amely digitális aláírással és HTTPS/TLS protokollal történik, valamint a Secure Boot mechanizmus bevezetése, amely biztosítja, hogy csak hitelesített firmware-t lehessen futtatni az eszközön. További ajánlott megoldások: kétfaktoros hitelesítés, jelszavak egyediségének biztosítása, funkciók elkülönítése, valamint rendszeres naplózás és monitorozás a biztonsági események gyors felismerése érdekében [29].



Ábra 10: Intelligens otthoni IoT firmware-biztonsági kockázatok.

Jogosulatlan hozzáférés

A smart home eszközök, mint a kamerák, termosztátok, ajtózárak és hangasszisztensek az internetre csatlakoznak, ami kényelmet nyújt, ugyanakkor támadási felületet is biztosít a rosszindulatú szereplők számára. Jogosulatlan hozzáférés esetén a támadók:

- távolról irányíthatják az eszközöket, például kikapcsolhatják a riasztórendszert vagy kinyithatják az ajtót,
- hozzáférhetnek az eszközök által rögzített adatokhoz, például kamerafelvételekhez vagy hanganyagokhoz,
- ellophatják a felhasználók szokásaira, tartózkodási helyére vonatkozó adatokat,
- vagy szolgáltatáskiesést okozhatnak, ami hatással lehet az otthon fűtésére, világítására vagy energiaellátására [30].

Gyakori kiváltó ok a gyenge vagy alapértelmezett jelszavak használata, a titkosítás hiánya vagy nem frissített firmware, amelyen keresztül a támadók behatolhatnak a rendszerbe. A védekezéshez erős jelszavak, titkosított kommunikáció, rendszeres frissítések, és megfelelő jogosultságkezelés szükséges [31].

Védekezési lehetőségek: titkosítás, hitelesítés, rendszeres frissítés

Az adatok védelme elsődleges szempont egy intelligens otthonban. A végponttól végpontig történő titkosítás (end-to-end encryption) biztosítja, hogy az adatforgalom – például a szenzorok által gyűjtött információ vagy a felhasználói utasítások – kizárólag az arra jogosult felek számára legyen olvasható. Az olyan protokollok, mint a TLS (Transport Layer Security) vagy az HTTPS, kulcsfontosságúak az eszközök közötti kommunikáció titkosításában, megelőzve a lehallgatást és a közbeékelődéses támadásokat (MitM) [32].

Emellett fontos, hogy a felhasználók is tisztában legyenek azzal, milyen titkosítási szintet támogatnak az eszközeik, és aktiválják a legmagasabb elérhető biztonsági beállításokat [33].

Erős hitelesítés és hozzáférés-ellenőrzés

A többlépcsős hitelesítés (MFA) bevezetése jelentősen csökkenti az illetéktelen hozzáférés kockázatát. Ez kombinálja a hagyományos jelszavas védelmet biometrikus azonosítással (például ujjlenyomat, arcfelismerés) vagy eszközalapú hitelesítéssel (például telefonos jóváhagyás) [34]. A jelszavaknak egyedinek, hosszúnak (legalább 12 karakter), és speciális karaktereket is tartalmazónak kell lenniük – valamint az első használat után ajánlott megváltoztatni őket [32].

A hozzáférési jogosultságok rendszeres felülvizsgálata, valamint külön felhasználói fiókok létrehozása családtagok számára, személyre szabott jogosultságokkal, tovább növeli a biztonságot.

Rendszeres szoftverfrissítések és firmware-védelem

Az IoT-eszközök egyik legsebezhetőbb pontja a firmware, vagyis az eszközök alacsony szintű vezérlőszoftvere. A támadók gyakran ennek manipulálásán keresztül próbálnak meg bejutni a rendszerbe. Ennek elkerülésére biztonságos firmware-frissítési mechanizmusokat kell alkalmazni, mint például a digitális aláírással hitelesített firmware képfájlok, valamint titkosított kapcsolat (HTTPS) használata a frissítés során [32].

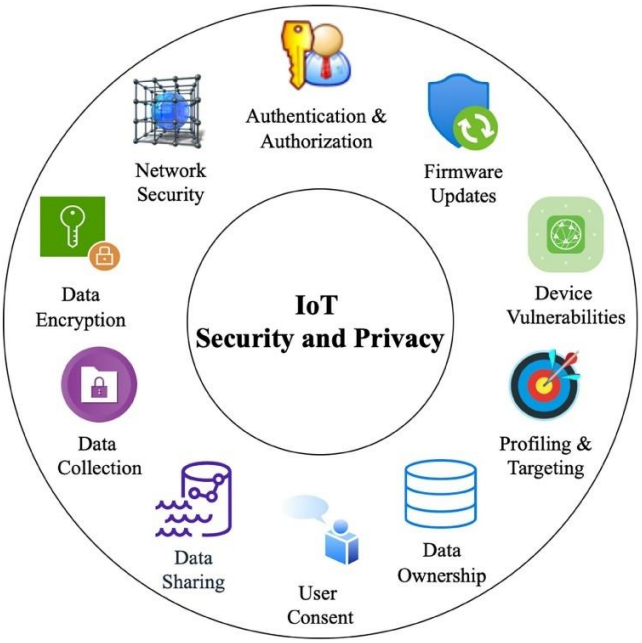
A **Secure Boot** technológia lehetővé teszi, hogy csak a gyártó által hitelesített szoftver fusson az eszközön, kizárva a manipulált firmware telepítését. Továbbá az automatikus frissítési lehetőségek biztosítása kulcsfontosságú, mivel ezáltal a gyártók gyorsan reagálhatnak az újonnan felfedezett sérülékenységekre [32].

Biztonságos hálózati architektúra

Az eszközök védelmét szolgáló intézkedések közé tartozik a Wi-Fi hálózat WPA3 titkosítással való védelme, a tűzfalak használata, valamint a router firmware-ének rendszeres frissítése is. Javasolt a vendéghálózatok bevezetése, amelyek elkülönítik a fő okosotthon-hálózatot a látogatók eszközeitől, ezáltal csökkentve a fertőzés kockázatát [33].

Biztonságos tervezés elve (Security by Design)

A legbiztonságosabb megoldások már a fejlesztési fázisban figyelembe veszik a potenciális fenyegetéseket. A Security by Design szemlélet lényege, hogy az eszközök és rendszerek eleve biztonságosan legyenek kialakítva, és ne utólag próbáljanak biztonsági rétegeket hozzáadni. Ez magába foglalja a jelszókezelést, a jogosultságok izolálását, az input validációt, valamint a naplózást és monitorozást is, amely segít a behatolási kísérletek azonosításában [32] [33].



Ábra 11: IoT biztonsági és adatvédelmi aggályok.

Blokklánc-technológia és adatintegritás

Decentralizált hitelesítés és adatvédelem

A blokklánc-technológia alapvetően alakítja át az adatintegritás és digitális hitelesítés fogalmát az okosotthonok világában is. A technológia lényege a decentralizált főkönyvi struktúra, ahol az adatok blokkokba szerveződnek, és minden blokk kriptográfiailag kapcsolódik az előzőhöz. Ez az

immutabilitás biztosítja, hogy a már rögzített adatok visszamenőleg ne legyenek módosíthatók a hálózat konszenzusa nélkül, így garantálva a megbízható és változatlan adatrekordokat [35].

A decentralizált rendszerek egyik legnagyobb előnye, hogy nincs központi szerver, ami célpontja lehetne kibertámadásoknak vagy belső visszaéléseknek. Az adatok több csomóponton tárolódnak, így egy támadás sikeressége érdekében a hálózat nagy részét kellene kompromittálni – ez pedig gyakorlatilag kivitelezhetetlen [36].

Decentralizált hitelesítési mechanizmusok (DAP)

A Decentralized Authentication Platform (DAP) olyan rendszer, amely központi hatóság igénybevétele nélkül teszi lehetővé a felhasználói azonosság ellenőrzését és hitelesítését. A hagyományos hitelesítési rendszerekkel ellentétben, amelyek központi szervereken tárolják és kezelik a felhasználói hitelesítő adatokat, a DAP-ok blokklánc-technológiát, kriptográfiai technikákat és elosztott hálózatokat használnak. Ez a decentralizált megközelítés fokozza a biztonságot, a magánélet védelmét és a személyes adatok feletti felhasználói ellenőrzést [37].

A DAP magja a nyilvános és privát kulcsú kriptográfia használata. A felhasználók létrehoznak egy pár kriptográfiai kulcsot: egy nyilvános kulcsot, amelyet megosztanak másokkal, és egy privát kulcsot, amely privát vagy titkos marad. A hitelesítés akkor valósul meg, amikor a felhasználók aláírnak egy üzenetet vagy tranzakciót a privát kulcsukkal, amely a megfelelő nyilvános kulccsal ellenőrizhető. Ez a módszer biztosítja, hogy csak a privát kulcs jogos tulajdonosa tud hitelesíteni, így nincs szükség érzékeny információk továbbítására [37].

A decentralizált hitelesítési platformok az önszuverén identitás (SSI) koncepcióját is magukban foglalják. Az SSI rendszerekben a felhasználók teljes ellenőrzést tartanak fenn személyazonossági adataik felett, helyben tárolják azokat eszközeiken vagy biztonságos, decentralizált tárolási megoldásokban. Szükség esetén szelektíven közölhetnek bizonyos információkat a szolgáltatókkal, ezzel erősítve a magánélet védelmét és csökkentve az adatszivárgás kockázatát [37].

Adatvédelem és biztonsági rétegek a blokkláncban

A blokklánc által nyújtott adatvédelem a kriptográfiai hash függvényeken, digitális aláírásokon és a nyilvános kulcsú infrastruktúrán (PKI) alapszik. Minden adatblokk időbélyeget kap, és az előző blokkokkal való kapcsolat révén nyomon követhető, megmásíthatatlan adattörténet jön létre. A

hash függvények érzékenysége biztosítja, hogy akár egyetlen bitnyi változtatás is teljesen más hash-értéket eredményezzen, azonnal észlelhetővé téve az adatmanipulációs kísérleteket [35].

A digitális aláírás lehetővé teszi, hogy csak az arra jogosult fél hozhasson létre vagy módosíthasson adatokat, míg a nyilvános kulccsal bárki ellenőrizheti az adatok eredetiségét. Ezáltal csökken a jogosulatlan hozzáférés, az adatlopás és a rendszerbe való beavatkozás esélye.

Kihívások és megoldási lehetőségek

Bár a blokklánc erős védelmet nyújt, az anonimitás és adatvédelem kérdése továbbra is kihívás. Mivel a tranzakciók minden csomópont számára láthatók, egy támadó visszafejtheti a tranzakciós minták alapján a felhasználók identitását. Erre megoldást kínál a differenciált adatvédelem (differential privacy), amely véletlenszerű zajt ad az adathoz anélkül, hogy az érdemi eredményeket torzítaná. Ezáltal a felhasználó személyazonossága rejtve marad, miközben az adatok továbbra is használhatóak elemzésre vagy tranzakcióra [36].

Ezek a modern adatvédelmi mechanizmusok lehetővé teszik, hogy a blokklánc-alapú hitelesítési rendszerek ne csak biztonságosak, de jogszabályoknak megfelelőek és felhasználóbarátok is legyenek.

Ábra 12: Decentralizált hitelesítés

Adatmanipuláció elleni védekezés

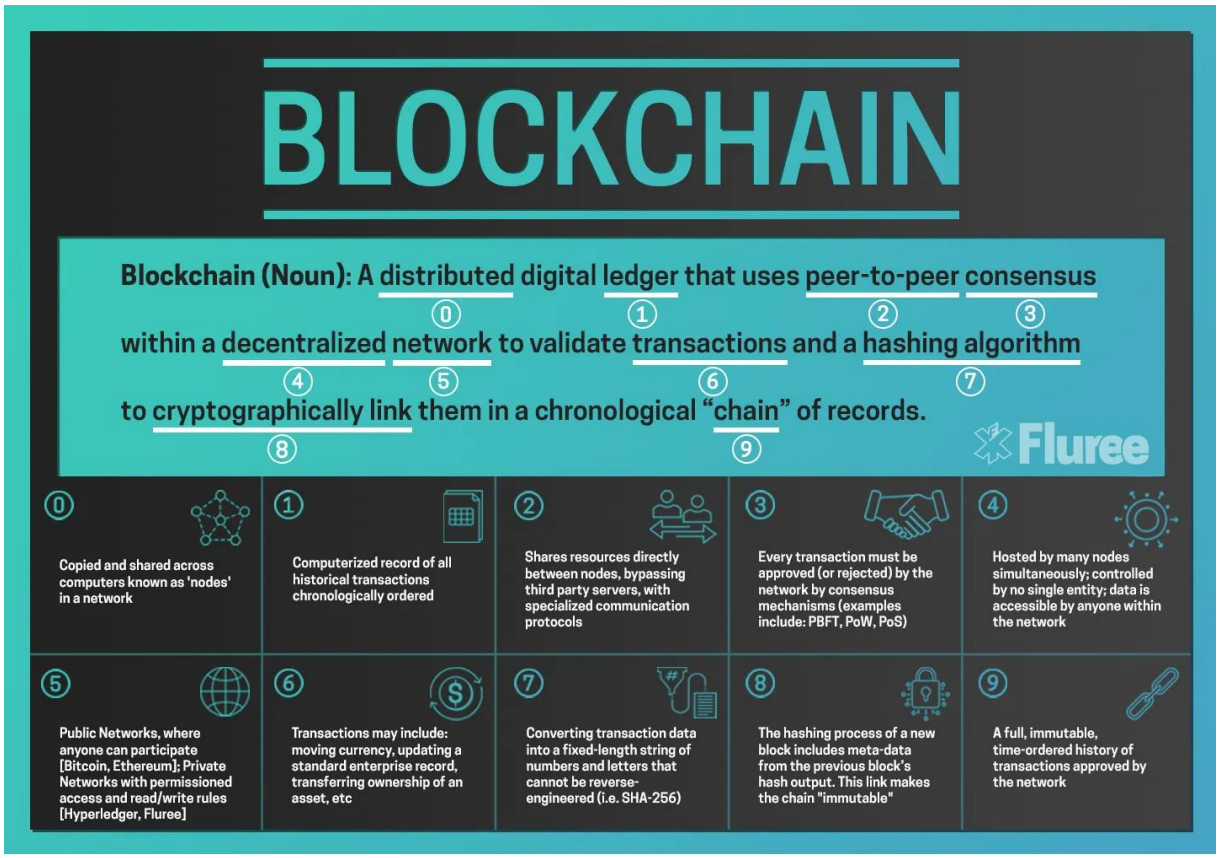
Az adatmanipuláció elleni védekezés napjaink digitális környezetében kiemelt jelentőséggel bír, különösen az okosotthonok és IoT-rendszerek esetében, ahol érzékeny információk kezelése történik. A blokklánc-technológia egyik legerősebb tulajdonsága éppen az adatok megváltoztathatatlanságában (immutabilitás) rejlik. A blokklánc egy kriptográfiailag védett, decentralizált főkönyv, amelyben minden új blokk az előző blokkok hash értékét is tartalmazza. Ez a láncolt struktúra biztosítja, hogy bármely módosítás kísérlete — akár egyetlen bit szintjén — megváltoztatja a blokk hash-ét, így a teljes lánc érvénytelenné válik, hacsak a támadó nem tudja újraszámolni az összes következő blokk hash-ét, amit a konszenzusmechanizmusok miatt szinte lehetetlen kivitelezni [38].

A blokklánc tehát nemcsak kriptográfiailag biztonságos, hanem architekturálisan is védett az adathamisítás ellen: minden résztvevő (node) azonos másolatot tárol a főkönyvről, így bármely eltérés gyorsan észlelhető és elutasítható a hálózat által [39]. Ez a decentralizált működés jelentős előnyt jelent a hagyományos, centralizált adatbázisokkal szemben, ahol az egyetlen ponton történő adatsérülés az egész rendszer integritását veszélyeztetheti.

A blokklánc alapú rendszerek emellett nyilvános auditálhatóságot is biztosítanak: minden tranzakció visszakövethető és átlátható, ami különösen előnyös lehet jogi, szabályozási vagy hibakeresési szempontból. Mivel a blokkláncra írt adatok nem törölhetők vagy módosíthatók, egy folyamatosan bővülő, hitelesített „idővonalat” hoznak létre, amely hiteles forrásként szolgálhat adatvédelmi incidensek vizsgálatakor is [40].

A decentralizált tárhelyszolgáltatások, mint például a Storj és a Sia, gyakorlati példát nyújtanak ezen elvek alkalmazására. Ezekben a rendszerekben az adatok titkosított darabokra vannak bontva, majd különböző helyeken tárolva a hálózat gépein, így még akkor sem férhető hozzá értelmezhető információ, ha az egyik tárolóegység kompromittálódik [41].

Összességében a blokklánc összetett védelmet nyújt az adatmanipuláció ellen: a kriptográfiai hash-függvények, a decentralizált adatkezelés, a konszenzusmechanizmusok és az átlátható tranzakciókezelés révén a rendszer egésze sokkal ellenállóbbá válik a belső és külső támadásokkal szemben. Ez különösen fontossá válik az olyan érzékeny környezetekben, mint az okosotthonok, ahol az adatbiztonság közvetlen hatással lehet a lakók magánéletére és fizikai biztonságára.



Ábra 13: A blokklánc működésének szemléltetése – decentralizált hálózat, konszenzus és adatintegritás

Edge Computing és lokális adatfeldolgozás az okosotthonokban

Az Edge Computing szerepe nyílt rendszerekben

A felhőalapú számítástechnika kétségtelenül forradalmasította az adatfeldolgozást, azonban nem minden esetben nyújt optimális megoldást. A központosított feldolgozási architektúra jelentős késleltetést és hálózati torlódást eredményezhet, különösen az olyan időérzékeny alkalmazások esetében, mint az egészségügy, az AR/VR, vagy a valós idejű biztonsági rendszerek [42]. Ennek kezelésére jelent meg az edge computing (peremhálózati számítástechnika), amely az adatok és szolgáltatások feldolgozását közelebb viszi az adatok keletkezési helyéhez, ezzel csökkentve a válaszidőt és javítva a hálózat teljesítményét [42].

Az edge computing decentralizált szemlélete különösen előnyös a nyílt rendszerek, például az okosotthonok esetében. A rendszer képes a peremhálózaton, például IoT-eszközökön vagy single-board számítógépeken (mint a Raspberry Pi), lokálisan végrehajtani a számításokat és adatfeldolgozást [42] [43]. Ez nem csupán csökkenti a felhőalapú kommunikáció szükségességét, hanem energiatakarékosabb is, mivel a helyi adatkezelés kevesebb adatátvitelt és így kevesebb energiafelhasználást igényel [44].

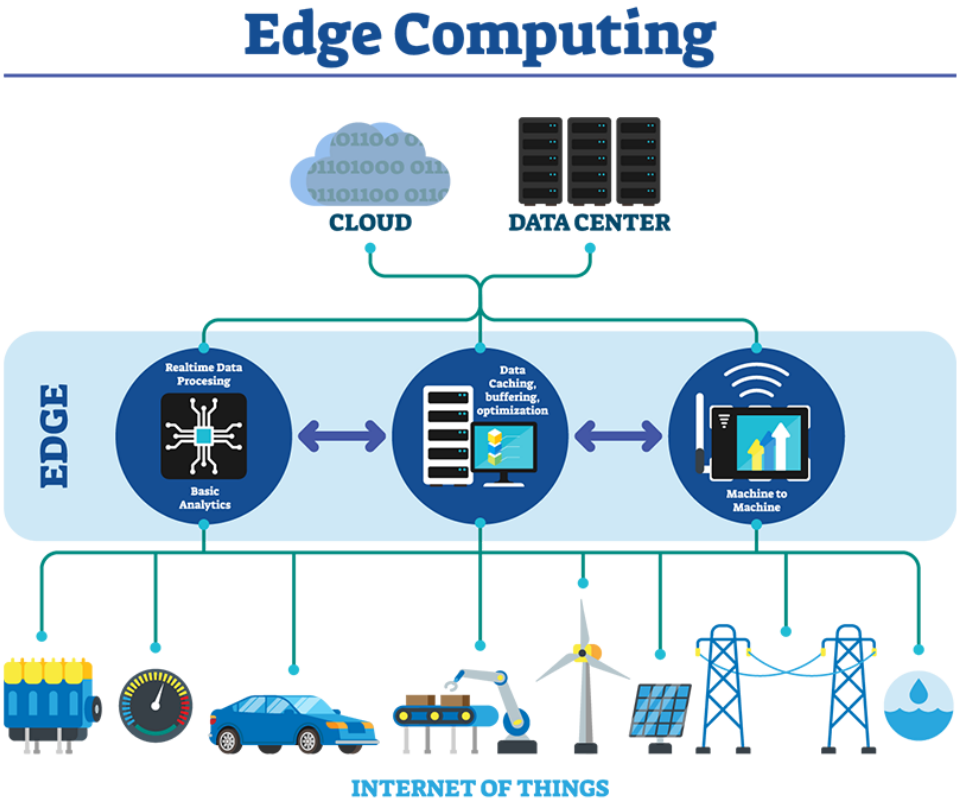
A nyílt platformokon működő edge computing rendszerek, mint a fog computing vagy a mobile edge computing (MEC), a funkcionalitás és a skálázhatóság terén is előnyösek. Lehetővé teszik az okosotthon-rendszerek egyszerű bővíthetőségét és az új eszközök zökkenőmentes integrációját. Az érzékelők és aktuátorok – például hőmérséklet- és mozgásérzékelők – adatai közvetlenül egy edge eszközre, például Raspberry Pi-re kerülnek, amely képes autonóm módon, valós időben szabályozni az otthon különféle rendszereit (pl. világítás, fűtés, légkondicionálás) [44].

Az edge computing nemcsak a késleltetés minimalizálásában játszik szerepet, hanem jelentős energiamegtakarítást is eredményez. A távoli felhőalapú feldolgozás sokszor több sávszélességet és kommunikációs csatornát igényel, míg a helyi feldolgozás rövidebb adatútvonalat és gyorsabb válaszidőt tesz lehetővé [44]. Az ilyen rendszerek tehát nemcsak biztonságosabbak, de környezetkímélőbbek és költséghatékonyabbak is.

Az érzékelőeszközök egyre gyakrabban jelennek meg otthonainkban és városainkban, valamint az aktuátorok. Az ilyen átható és heterogén tájak adatainak kezelése és összehangolása, valamint vezérlése olyan elosztott intelligenciát igényel, amely a funkcionalitás és a használhatóság befolyásolása nélkül képes növelni a vezérelt eszközök számával. Az Edge Computing létfontosságú lehet az ilyen követelmények teljesítéséhez, mivel helyi számítások és adatpufferelés/gyorsítótározás révén segít csökkenteni a valós ingerekre adott válaszidőt [42].

A számos IoT-eszközzel felszerelt intelligens otthonok az éles számítástechnika feltörekvő alkalmazási területéhez tartoznak. Az okosotthonok monitorozására és mérésére tervezett IoT-alkalmazások lehetővé teszik az előfizetők számára, hogy automatikusan és precízen leolvassák a különböző mérőket, és ennek megfelelően késedelem nélkül hozzáférjenek a számlákhoz. Ezeket az IoT-alkalmazásokat különféle közművek, például víz, villany és gáz távfelügyeletére és mérésére tervezték. Az IoT-eszközökről gyűjtött adatok a felhőbe küldés helyett egy szélső szerverre továbbíthatók feldolgozás céljából, ami valós idejű adatelemzést eredményezhet [43].

Elmondható, hogy az edge computing kulcsszerepet játszik a nyílt forráskódú IoT rendszerek működésében az Ipar 4.0 környezetben. Segítségével az okosotthonok gyorsabb, biztonságosabb és hatékonyabb adatfeldolgozást valósíthatnak meg, miközben csökkentik a felhőfüggőséget és optimalizálják az energia- és hálózati erőforrások használatát.



Ábra 14: Edge-computing-use-cases-IoT

Helyi adatfeldolgozás előnyei: gyorsaság, adatbiztonság, felhőtől való függetlenség és válaszidő-optimalizálás

A helyi adatfeldolgozás lehetővé teszi az adatok feldolgozását közvetlenül az adatforrás közelében, például egy IoT-eszközön vagy egy peremhálózati szerveren, ahelyett hogy a központi felhőbe kerülnének feldolgozásra. Ez a megközelítés jelentősen csökkenti a válaszidőt, növeli a rendszer reakcióképességét, és különösen fontos a késleltetésre érzékeny alkalmazások – mint például az ipari automatizálás, autonóm járművek, vagy az egészségügyi rendszerek – esetében [45], [46].

Az egyik legnagyobb előnye a késleltetés csökkenése: az adatok helyben történő feldolgozása révén az eszközök valós időben reagálhatnak. Például egy intelligens gyártósori érzékelő képes azonnal észlelni egy géphiba előjeleit, és automatikusan karbantartási műveletet indítani, megelőzve a gyártás leállását [45].

Emellett a lokális adatkezelés erősíti az adatbiztonságot is. Az érzékeny adatok nem kerülnek távoli szerverekre, így csökken a kibertámadások és adatlopások kockázata. A pénzügyi szektorban például a Capital One már vizsgálja az edge computing lehetőségeit csalásfelderítés céljából, hogy az ATM-ekben vagy IoT-eszközökben keletkező adatokat helyben dolgozzák fel, és így gyorsabban tudjanak reagálni biztonsági incidensekre [45].

A felhőtől való függetlenség is fontos szempont. Az edge computing lehetővé teszi, hogy az eszközök akkor is működőképesek maradjanak, ha a felhőhöz való hozzáférés átmenetileg megszűnik – például internetkapcsolat megszakadása esetén. Ez kritikus lehet a közlekedés, egészségügy vagy biztonságtechnika területén, ahol a valós idejű döntések késlekedése komoly következményekkel járhat [47].

Válaszidő-optimalizálás révén az edge computing jelentősen javítja a szolgáltatások minőségét. Egy intelligens városban például a közlekedési lámpák irányítását és forgalomfigyelést végző érzékelők lokálisan dolgozzák fel az adatokat, és így képesek valós időben módosítani a forgalomirányítást, csökkentve a torlódásokat [45].

Nem utolsó sorban, az edge computing fenntarthatósági szempontból is előnyös. A lokális adatfeldolgozás csökkenti az adatátvitel során szükséges energiafelhasználást, valamint a hálózati sávszélesség és infrastruktúra igénybevételét, ami hosszú távon kevesebb kibocsátással és energiafogyasztással jár [46].

Összességében az edge computing a gyorsaság, biztonság, fenntarthatóság és a költséghatékonyság egyensúlyát kínálja, különösen akkor, ha a felhőalapú feldolgozással kombinálva alkalmazzák. A két technológia együtt rugalmas, skálázható és megbízható adatfeldolgozási megoldást kínál a modern okosotthonok és ipari rendszerek számára [47].

Ábra 15: Az Edge Computing 5 legfontosabb előnyei

Jövőbeli trendek és kutatási irányok

Nyílt forrású AI-modulok, önfejlesztő automatizálási szabályok, energiahatékonysági törekvések

Az okosotthonok jövője egyre szorosabban kapcsolódik az olyan technológiai fejlesztésekhez, mint a nyílt forráskódú mesterséges intelligencia (AI), az adaptív automatizálási rendszerek, valamint az energiahatékonyságot célzó új megközelítések.

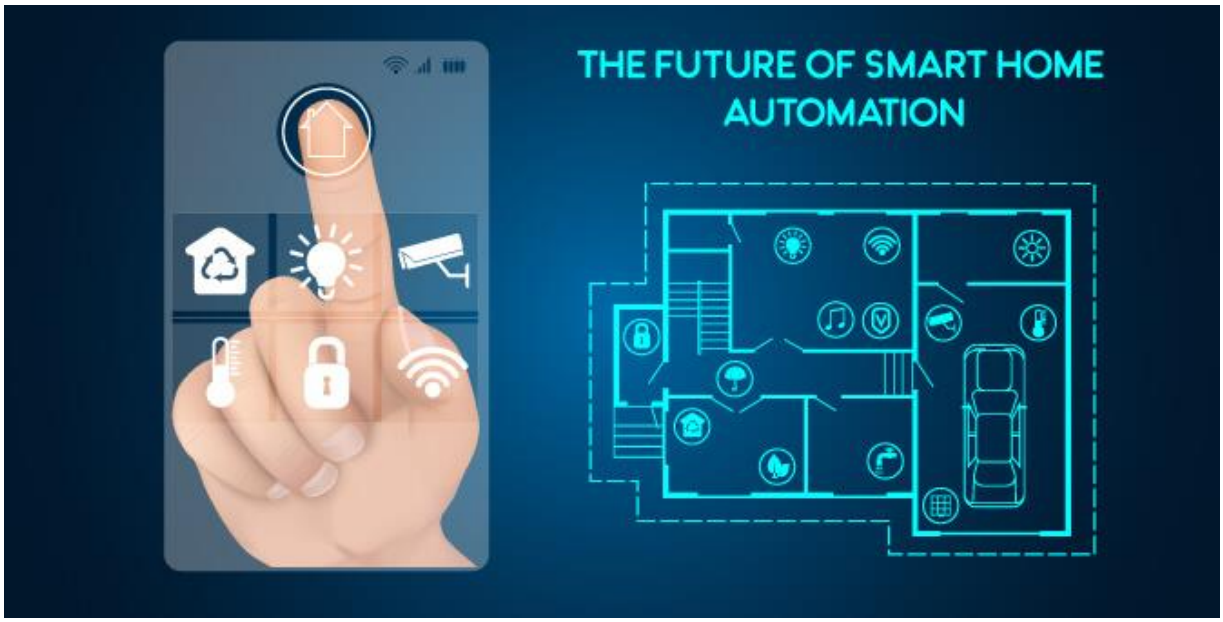
Nyílt forráskódú AI-modulok A nyílt forrású AI-közösségek rohamos fejlődése lehetővé teszi, hogy az AI-technológiákat egyre inkább demokratizáljuk és testreszabhassuk a végfelhasználók igényei szerint. A jövőben várható a nyílt forráskódú, doménspecifikus AI-modellek terjedése, a multimodális AI-képességek megerősödése, valamint a federált tanulás és decentralizált tanulási technikák térbővülése [48].

Önfejlesztő automatizálási szabályok A mesterséges intelligenciával támogatott, önfejlesztő automatizálási rendszerek lehetővé teszik, hogy az okosotthonok tanuljanak a felhasználói szokásokból, és idővel alkalmazkodjanak hozzájuk. Az ilyen rendszerstruktúrákra példa a

ThinkHome koncepció, amely szemantikus kontextus és AI kombinációjával optimalizálja az otthon energiafogyasztását és vezérlését [49].

Energiahatékonysági törekvések Az okosotthon-rendszerek fejlesztésében egyre fontosabb szempont az energiahatékonyság. Az olyan intelligens épületek, mint a ThinkHome, nemcsak az energiafogyasztást csökkentik, hanem az AI alapú vezérlésnek köszönhetően javítják az élhetőséget is. Emellett a nyílt forrású AI által inspirált fejlesztések képesek hozzájárulni a fenntarthatóbb jövő megteremtéséhez azzal, hogy minimalizálják az összes adatátvitelből fakadó energiafogyasztást [48].

Open-Source AI Governance Az AI egyre kritikusabb szerepet tölt be az iparban, a nyílt forrású AI irányítása is fejlődik. A jövő trendjei közé tartozik a decentralizált, közösségi alapú irányítási modell, az automatizált etikai ellenőrzés, az AI modellek specifikus licencelése és az AI ellátási lánc biztonságának megerősítése [50]. Ezek együttesen biztosítják, hogy a jövő AI-rendszerei ne csupán intelligensek, hanem átláthatóak, biztonságosak és etikusak is legyenek.



Ábra 16: Az intelligens otthonok automatizálásának jövője

Konklúzio

A dolgozat során áttekintettük, hogy a nyílt forráskódú IoT-rendszerek milyen fontos szerepet játszanak az okosotthonok kommunikációjában és biztonságában az Ipar 4.0 környezetében. A különböző protokollok összehasonlításától kezdve az edge computing előnyein át egészen a blokklánc-technológiáig láthattuk, hogy a decentralizált és nyílt rendszerek nem csupán technológiai alternatívák, hanem hosszú távon fenntartható és biztonságos megoldások is lehetnek. Az adatok helyi feldolgozása, a valós idejű válaszidő, az energiahatékonyság, valamint az AI-vezérelt fejlesztések mind olyan irányok, amelyek egyértelműen meghatározzák az okosotthonok jövőjét. Ahogy az innovációk terjednek, úgy válik egyre fontosabbá a biztonságos, átlátható és etikusan működtetett rendszertervezés, amelyhez a nyílt forráskódú megoldások kiváló alapot nyújtanak.

Irodalomjegyzék

[1] G. Varga, “Ipar 4.0 és kiber-fizikai rendszerek,” *International Journal of Engineering and Management Sciences*, vol. 6, no. 2, pp. 97-110, 2021. [Online]. Available: https://ojs.lib.unideb.hu/IJEMS/article/download/11056/10230

[2] Vilmate, “Cyber-Physical Systems (CPS) and Their Role in IoT,” 2023. [Online]. Available: https://vilmate.com/blog/cyber-physical-systems-cps-what-they-have-to-do-with-iot/

[3] Refaktor, “Az IoT integrációja a mindennapi életünkbe,” 2022. [Online]. Available: https://refaktor.hu/az-iot-integracioja-a-mindennapi-eletunkbe/

[4] S. Anwar, A. M. Rahmani, P. Liljeberg and H. Tenhunen, "Smart Home Sensor Systems: Advancements and Applications," *ResearchGate*, Jul. 2023. [Online]. Available: https://www.researchgate.net/publication/372947748_Smart_Home_Sensor_Systems_Advancements_and_Applications

[5] Stronghouse Project, "Manual: Smart Home Technologies," *North Sea Region Programme*, Jun. 2023. [Online]. Available: https://northsearegion.eu/media/24155/230615_stronghouse-manual.pdf

[6] Refaktor, "Felhőalapú megoldások a jövő okosotthonaiban," *refaktor.hu*, Feb. 2021. [Online]. Available: https://refaktor.hu/felhoalapu-megoldasok-a-jovo-okosotthonaiban/ [Accessed: Mar. 19, 2025].

[7] Forbes.hu, "Ilyen a magyar fejlesztésű Chameleon okosotthon-rendszer", *forbes.hu*, Oct. 2021. [Online]. Available: https://forbes.hu/uzlet/chameleon-okosotthon-otthonautomatizalas/ [Accessed: Mar. 19, 2025].

[8] Incelor, "Miért jobb a Loxone az okosotthon rendszerek között?", *incelor.com*. [Online]. Available: https://incelor.com/loxone-okosotthon-rendszer [Accessed: Mar. 19, 2025].

[9] "AI in smart home devices: The answer is open source AI," Restack.io. [Online]. Available: https://www.restack.io/p/ai-in-smart-home-devices-answer-open-source-ai-cat-ai#cm250haqh4rhjd8gg49j1k2fy. [Accessed: Mar. 20, 2025].

[10] A. El-Haggar, "Open Source Home Automation: A step towards energy-efficient smart homes," ResearchGate, Dec. 2021. [Online]. Available: https://www.researchgate.net/publication/357073943_A_Comparison_of_Open-Source_Home_Automation_Systems. [Accessed: Mar. 20, 2025].

[11] Home Assistant, "Home Assistant - Open source home automation that puts local control and privacy first," [Online]. Available: https://www.home-assistant.io. [Accessed: Mar. 20, 2025].

[12] "Explaining to OT Teams the Importance of MQTT for IT/OT Interoperability," HiveMQ. [Online] Available: https://www.hivemq.com/blog/explaining-importance-mqtt-it-ot-interoperability/. [Accessed: Mar. 20, 2025].

[13] "The best way to have Open Source Smart Home," boneIO. [Online] Available: https://boneio.eu/. [Accessed: Mar. 20, 2025].

[14] "7 Best Open Source Home Automation Tools in 2025," Eufy.com. [Online]. Available: https://www.eufy.com/blogs/home/open-source-smart-home. [Accessed: Mar. 21, 2025].

[15] J. Brockmeier, "6 open source home automation tools," Opensource.com. [Online]. Available: https://opensource.com/tools/home-automation. [Accessed: Mar. 21, 2025].

[16] D. Orosz, “Examining the Contribution of Smart Homes to the Smart Performance of Cities,” *Review of Business & Management*, vol. 17, no. Special Issue 1, pp. 23–30, 2021. [Online]. Available: https://doi.org/10.18096/TMP.2021.01.03

[17] “IoT Architecture: Layers, Components, and Importance,” Cavli Wireless. [Online]. Available: https://www.cavliwireless.com/blog/nerdiest-of-things/iot-architecture-layers-components-importance.html. [Accessed: Mar. 21, 2025].

[18] “Zigbee,” OkosotthonBlog. [Online]. Available: https://okosotthonblog.hu/wiki/okosotthon/protokollok-es-standardok/zigbee/. [Accessed: Mar. 21, 2025].

[19] “Zigbee vs Z-Wave: What's the difference?” GearBrain. [Online]. Available: https://www.gearbrain.com/difference-between-zigbee-and-zwave-2598399416.html. [Accessed: Mar. 21, 2025].

[20] “IoT Protocols: MQTT, CoAP, LwM2M, and More,” EMQX. [Online]. Available: https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m. [Accessed: Mar. 21, 2025].

[21] “Explaining the Importance of MQTT in IT-OT Interoperability,” HiveMQ Blog. [Online]. Available: http://hivemq.com/blog/explaining-importance-mqtt-it-ot-interoperability/. [Accessed: Mar. 21, 2025].

[22] “IoT Scope and Protocols,” SNDK Corp. [Online]. Available: https://www.sndkcorp.com/iot-scope-protocols#header-10. [Accessed: Mar. 21, 2025].

[23] “The technical differences between Zigbee and Z-Wave,” GearBrain. [Online]. Available: https://www.gearbrain.com/difference-between-zigbee-and-zwave-2598399416.html. [Accessed: Mar. 21, 2025].

[24] “LoRaWAN Protocol Overview,” EMQX. [Online]. Available: https://www.emqx.com/en/blog/lora-iot-technology. [Accessed: Mar. 21, 2025].

[25] CoreDNA, “Open Source vs Closed Source Software - What is the difference?,” *CoreDNA*, 2023. [Online]. Available: https://www.coredna.com/blogs/comparing-open-closed-source-software. [Accessed: Mar. 21, 2025].

[26] B. Sándor, *Az intelligens épületek digitális transzformációja: Az intelligens rendszerek és technológiák integrációja az épített környezetben*, Ph.D. disszertáció, Óbudai Egyetem, 2023. [Online]. Available: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/27419/Sandor_Barnabas_ertekezes.pdf

[27] Z. Zhang et al., "Security and Privacy Challenges of AR/VR-Enhanced Smart Homes: A Comprehensive Review," *Electronics*, vol. 13, no. 16, p. 3343, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/16/3343

[28] J. Zs. Csaba, A. Pásztor, „Kommunikációbiztonsági kihívások IoT-alapú rendszerekben", *Gradus*, vol. 10, no. 1, 2023. [Online]. Available: https://gradus.kefo.hu/archive/2023-1/2023_1_CSC_001_Johanyak.pdf

[29] *Smart Home IoT Firmware Security: Challenges and Solutions*, *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2665917424003829

[30] *The Risks of Unauthorized Access to Smart Homes*, Medium. [Online]. Available: https://medium.com/@Land2Cyber/the-risks-of-unauthorized-access-to-smart-homes-safeguarding-the-modern-dwelling-cac1ef28f412

[31] *Open Source Home Automation: The Answer to Smart Home Security Risks?*, *Restack*. [Online]. Available: https://www.restack.io/p/open-source-home-automation-answer-security-risks-cat-ai

[32] ScienceDirect: *Smart Home IoT Security Best Practices*, https://www.sciencedirect.com/science/article/pii/S2665917424003829

[33] IMSVA Blog: *Privacy and Security in Smart Homes*, https://www.imsva.com/blog/2024/august/privacy-and-security-in-smart-homes-keeping-your

[34] Thales Group: *Security by Design in Smart Homes*, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart-home/security-by-design

[35] Forbes Technology Council, "Your Essential Primer On Large Language Model Agent Tools," *Forbes*, Mar. 27, 2025. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/01/17/how-blockchain-revolutionizes-data-integrity-and-cybersecurity/

[36] N. Alsulami and M. Ababneh, “Privacy-Preserving Mechanism in Smart Home Using Blockchain,” *ResearchGate*, 2021. [Online]. Available: https://www.researchgate.net/publication/353386687_Privacy-Preserving_Mechanism_in_Smart_Home_Using_Blockchain

[37] Identity Management Institute, “Decentralized Authentication Mechanism and Platforms,” *identitymanagementinstitute.org*, 2023. [Online]. Available: https://identitymanagementinstitute.org/decentralized-authentication-mechanism-and-platforms/

[38] C-DAC, “Blockchain Explained,” *Centre for Development of Advanced Computing*, 2023. [Online]. Available: https://www.cdac.in/index.aspx?id=print_page&print=blog_blockchain_exp_CFS

[39] Y. Yuan and F.-Y. Wang, “Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance,” *ResearchGate*, 2019. [Online]. Available: https://www.researchgate.net/publication/338144930

[40] N. Alsulami and M. Ababneh, “Privacy-Preserving Mechanism in Smart Home Using Blockchain,” *ResearchGate*, 2021. [Online]. Available: https://www.researchgate.net/publication/353386687_Privacy-Preserving_Mechanism_in_Smart_Home_Using_Blockchain

[41] “Blockchain technológia és a webhosting esetleges alkalmazások,” *Hostpapi*, 2023. [Online]. Available: https://hostpapi.hu/blockchain-technologia-es-a-webhosting-esetleges-alkalmazasok/

[42] H. Shiang and M. van der Schaar, "Information-constrained resource allocation in multi-task systems," *IEEE Transactions on Signal Processing*, vol. 58, no. 7, pp. 3805–3821, Jul. 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8812214?casa_token=ZI72rPd8CnoAAAAA:ut1ONHaqjmXBKf5VFxCn6TN9FgVk2G9QVaDuIGpcr7n6ABivSuL0KaYRZu8iC5p9aDiB6rUbXXGR0A

[43] A. Yousefpour et al., "All One Needs to Know about Fog Computing and Related Edge Computing Paradigms: A Complete Survey," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8450541?casa_token=aBVXebs8TEsAAAAA:ME

vQYxbryQ-sV0sOS8pQgoOdqvrfdAQlOoyLC7ep-kfN6oE-8hb0QqLAZ-j6zJ7IzpPZyBmmdeTK4w

[44] M. Khalid, M. F. Tariq, and M. H. Aslam, "Smart Home Automation by Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 182, no. 24, pp. 32–39, 2019. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/106705858/Paper_55-Smart_Home_Automation_by_Internet_of_Things-libre.pdf?1697595818=&response-content-disposition=inline%3B+filename%3DSmart_Home_Automation_by_Internet_of_Thi.pdf&Expires=1743161430&Signature=UtytOCaO8~-h0ay31XahB6nLuIgjcVhPNfNH5KpLps65mWIB8OQn0FerGlaXRhudzg-AB1FWNle566E9HiUv0jFKfvlLs9J84PjoUVkyBFyh2b2H1j8WoYMXhlnYXJz6Z2CudU~-l2LjgCtqWSEPyHvUpbuE4wiePir3iDuk3LfodYs6cq~r9ChuO8fvfSMkq4E8cThOZZHwIe5HH6iV9g1TVdDVpxipwnJCDuKeVQ3c5C4imuoVqY4eCAQk-ZmRiVuGmAMDapH1ixE-JYyzZZGXey-OhdFTHiGVE3D9Pz5RVkBljc1lPHGF85a5z9ufSvywslpaEyP0RB5XsLROiw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[45] Silicon Valley Center, "Edge Computing: Revolutionizing Data Processing in IoT," [Online]. Available: https://siliconvalley.center/blog/edge-computing-revolutionizing-data-processing-in-iot

[46] SEEBURGER, "What is Edge Computing and Why is Edge Computing Important for Processing Real-Time Data," [Online]. Available: https://blog.seeburger.com/what-is-edge-computing-and-why-is-edge-computing-important-for-processing-real-time-data/

[47] SUSE, "The Relationship Between Edge Computing and Cloud Computing," [Online]. Available: https://www.suse.com/c/the-relationship-between-edge-computing-and-cloud-computing/

[48] K. Korir, "Open Source AI: Democratizing the Future of Artificial Intelligence," *Medium*, 2024. [Online]. Available: https://medium.com/@kiplangatkorir/open-source-ai-democratizing-the-future-of-artificial-intelligence-7deaa45bd6da

[49] M. Novakovic, H. Mahdavi, G. Provelegios, and A. Müller, "ThinkHome - Energy Efficiency in Future Smart Homes," *ResearchGate*, 2011. [Online]. Available:

https://www.researchgate.net/publication/220205714_ThinkHome_Energy_Efficiency_in_Future_Smart_Homes

[50] D. Amonoo-Neizer, "The Future of Open-Source AI Governance: Trends and Opportunities," *LinkedIn*, 2024. [Online]. Available: https://www.linkedin.com/pulse/future-open-source-ai-governance-trends-opportunities-amonoo-neizer-4b0le

Ábrajegyzék

Ábra 1: Az okosotthonok alapvető komponensei és működési elve.

- Mentés dátuma: 2025.02.11.
- https://epiteniakarok.blog.hu/2017/03/07/mitol_okos_az_okosotthon

Ábra 2: Kiberfizikai rendszerek integrálása komponens alapú megközelítésben intelligens otthonok számára.

- Mentés dátuma: 2025.02.17.
- https://www.mdpi.com/1424-8220/18/7/2156

Ábra 3: IIoT hálózati architektúra – okosszenzorok és aktuátorok kapcsolódása felhő- és edge computing rendszeren keresztül adatbázishoz.

- Mentés dátuma: 2025.02.17.
- https://www.realpars.com/blog/smart-sensors-actuators

Ábra 4: Kép egy Google Nest Hubról a Home Assistant felhasználói felülettel.

- Mentés dátuma: 2025.03.20.
- https://www.home-assistant.io/blog/2019/08/06/home-assistant-cast/

Ábra 5: Home Assistant Demo.

- Mentés dátuma: 2025.03.21.
- https://medevel.com/17-home-automation-open-source/

Ábra 6: A nyílt forráskód előnyei és hátrányai.

- Mentés dátuma: 2025.03.21.
- https://www.coredna.com/blogs/comparing-open-closed-source-software

Ábra 7: Okosotthon protokollok

- Mentés dátuma: 2025.03.24.
- https://www.simplehomelab.com/smart-home-protocols-2023/

Ábra 8: Biztonsági megfontolások a nyílt forráskóddal kapcsolatban – Nyílt forráskódú szoftverek: Hogyan használjunk nyílt forráskódú szoftvereket és élvezzük előnyeit

- Mentés dátuma: 2025.03.27.
- https://fastercapital.com/topics/considerations-for-open-source-software.html

Ábra 9: Az intelligens otthon ökoszisztémájának MITM fenyegetési modellje

- Mentés dátuma: 2025.03.27.
- https://www.researchgate.net/figure/MITM-threat-model-of-a-smart-home-ecosystem_fig1_356833189

Ábra 10: Intelligens otthoni IoT firmware-biztonsági kockázatok.

- Mentés dátuma: 2025.03.27.
- https://www.sciencedirect.com/science/article/pii/S2665917424003829

Ábra 11: IoT biztonsági és adatvédelmi aggályok.

- Mentés dátuma: 2025.03.27.
- https://onlinelibrary.wiley.com/doi/10.1002/spy2.448

Ábra 12: Decentralizált hitelesítés

- Mentés dátuma: 2025.03.27.
- https://identitymanagementinstitute.org/decentralized-authentication-mechanism-and-platforms/

Ábra 13: A blokklánc működésének szemléltetése – decentralizált hálózat, konszenzus és adatintegritás

- Mentés dátuma: 2025.03.27.
- https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1

Ábra 14: Edge-computing-use-cases-IoT

- Mentés dátuma: 2025.03.28.
- https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/

Ábra 15: Az Edge Computing 5 legfontosabb előnyei

- Mentés dátuma: 2025.03.28.
- https://www.iiot-world.com/smart-manufacturing/edge-computing-key-drivers-and-benefits-for-smart-manufacturing/

Ábra 16: Az intelligens otthonok automatizálásának jövője

- Mentés dátuma: 2025.03.28.
- https://b1hub.com.au/blog/future-smart-home-automation/

2.35. Varga Dániel,

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF COMPUTER SCIENCE

Privát 5G hálózatok

Varga Dániel, [redacted]
Mérnökinformatikus, BSc, nappali.

készítés dátuma: 2025.05.09.

Abstract

This submission explores the deployment and practical application of private 5G networks within industrial environments. The rise of Industry 4.0 has introduced a new set of technological demands, such as real-time data processing, enhanced cybersecurity, and support for a high density of connected devices.

Traditional network solutions often fall short in meeting these requirements, prompting a shift toward more robust and flexible wireless infrastructure. Private 5G networks offer a compelling answer to these challenges by enabling low-latency, high-reliability, and highly customizable communication systems tailored to specific industrial needs.

The submission outlines the key characteristics of private 5G technology, delves into the technical architecture of such networks, and examines the implementation challenges that organizations may encounter. It also highlights real-world case studies involving major industrial players, providing concrete examples of how private 5G networks are already being integrated into smart factories and automated production systems.

The objective is not only to provide a technical overview, but also to promote a deeper understanding of the strategic advantages and future potential of private 5G in the industrial sector.

Tartalom

Abstract 2
Bevezetés 4
Privát 5G hálózatok kiépítése ipari környezetben 5
A privát 5G hálózat fogalma 5
A privát 5G előnyei 5
Ipari alkalmazások 5
Privát 5G technológia alapjai 6
Az 5G alapvető technológiai jellemzői 6
A privát 5G hálózatok fogalma 7
A privát 5G hálózat fő komponensei 8
Frekvenciakezelés és spektrumhasználat 8
Frekvenciakezelés és engedélyezés privát 5G hálózatokhoz 9
Összefoglalás 10
Technikai megvalósítás ipari környezetben 10
Ipari követelmények a privát 5G hálózatokkal szemben 10
Hálózati architektúrák ipari alkalmazásokhoz 11
Esettanulmányok 13
BMW – Privát 5G alkalmazása a lipcsei gyárban 13
Huawei szerepe a privát 5G piacon 14
Hálózatbiztonság ipari privát 5G hálózatokban 14
Bosch gyártósor 5G hálózattal 16
Privát 5G összehasonlítása más ipari hálózati technológiákkal 16
Szoftveres megoldások a privát 5G hálózatokban 17
Kihívások és korlátok a privát 5G hálózatok bevezetésénél 19
Biztonsági kérdések és adatvédelem a privát 5G hálózatokban 19
Jövőbeli trendek, fejlődési irányok 20
A 6G előfutárai 20
Mesterséges intelligencia és az 5G konvergencia 21
Privát hálózatok és a digital twin összekapcsolása 21
További alkalmazási példák 21
Hazai példa 23
Összegzés és következtetések 24

Irodalomjegyzék 25

Bevezetés

Az 5G technológia nem csupán a lakossági mobilkommunikáció újabb mérföldköve, hanem egy olyan innovációs platform, amely alapjaiban formálja át az ipari működésmódokat is. Az elmúlt években az ipari termelésben megindult digitalizációs hullám – az úgynevezett Ipar 4.0 – új kihívásokat és követelményeket támasztott a kommunikációs rendszerekkel szemben. A gépek, szenzorok és rendszerek közötti valós idejű adatcsere, az autonóm vezérlés, valamint a prediktív karbantartás és minőség-ellenőrzés mind olyan alkalmazások, amelyek csak akkor működhetnek megbízhatóan, ha mögöttük egy stabil, alacsony késleltetésű, nagy sávszélességű és rendkívül biztonságos hálózat áll. [1]

Ebben a kontextusban a privát 5G hálózatok olyan kulcsfontosságú eszközzé váltak, amelyek lehetővé teszik a vállalatok számára, hogy saját igényeik szerint optimalizált, zárt és magas rendelkezésre állású hálózati infrastruktúrát építsenek ki. A privát – vagy más néven dedikált – 5G hálózatok nem osztoznak a nyilvános szolgáltatók infrastruktúráján, hanem egy adott gyár, üzemi terület vagy ipari park határain belül működnek. Ez a megközelítés nagyfokú kontrollt biztosít az adatáramlás, a sávszélesség-menedzsment, valamint a biztonsági protokollok felett. [2]

Napjainkban, amikor a gyártás rugalmassága, a költséghatékonysága és a versenyképesség megtartása minden ipari szereplő számára kulcskérdés. Különösen fontossá váltak azok a technológiai megoldások, amelyek hosszú távon is képesek növelni az üzemi hatékonyságot. A privát 5G hálózatok egyik legfőbb előnye éppen abban rejlik, hogy lehetőséget adnak a vállalatoknak arra, hogy az általuk használt kommunikációs rendszert pontosan az adott gyártási folyamatokra szabják – legyen szó autonóm járművekről, robotikáról, valós idejű minőségellenőrző rendszerekről vagy IoT-alapú adatgyűjtésről. [3]

A dolgozat célja, hogy részletesen bemutassa a privát 5G hálózatok ipari környezetben történő alkalmazását: a technológia műszaki hátterét, a megvalósítás során felmerülő kihívásokat, valamint azokat a gyakorlati példákat, amelyek már most is bizonyítják a megoldás létjogosultságát. Ezen keresztül válik érthetővé, miért tekintik a privát 5G-t az ipar jövőjének egyik legfontosabb építőkövének.

Privát 5G hálózatok kiépítése ipari környezetben

A privát 5G hálózat fogalma

A privát 5G hálózat egy olyan dedikált, nem publikus 5G hálózat, amely egy vállalat vagy cég tulajdonában van és csak az ő ipari folyamatait, tevékenységeit szolgálja ki, csak a cég irányítása alatt áll. Legnagyobb előnyei a 10 ms-nál kisebb késleltetés, a 10 Gbps sebesség, akár 1 millió eszközt is rá lehet csatlakoztatni négyzetkilométerenként, valamint a szeparált, biztonságos adatáramlás.

A privát 5G előnyei

A privát 5G hálózatok jobb biztonságot és nagyobb megbízhatóságot biztosítanak, a nyilvános hálózatokhoz képest, mivel a hálózat teljes mértékben a vállalat ellenőrzése alatt áll.[4] A privát 5G hálózatban lehetőség nyílik hálózati prioritások beállítására is, ennek segítségével optimalizálni lehet a hálózat terhelését. Ezeken kívül a fejlettebb gyárakban és logisztikai központokban egyre inkább elterjednek az önállóan mozgó eszközök, mint például a robotkarok, az önvezető szállító járművek, vagy a drónok. Ezeknek az eszközöknek stabil vezeték nélküli kommunikációra van szükségük a rendeltetésszerű működéshez, amit a privát 5G hálózat tud garantálni.

Ipari alkalmazások

A privát 5G hálózatok egyre inkább elterjednek az ipari szektorban és olyan cégeknél, mint az Audi, a Siemens és a Lufthansa, alapvető szerepet játszanak a folyamatok optimalizálásában. Az Audi Neckarsulmi gyárában a privát 5G hálózat lehetővé teszi a gyártósori adatátvitel gyorsítását és a gépek közötti valós idejű kommunikációt, amely növeli a termelési hatékonyságot és rugalmasságot.

A Siemens az ipari IoT megoldásaiban alkalmazza a privát 5G-t, amely biztosítja az adatok gyors és biztonságos áramlását a gyártási rendszerek között. Ezáltal a gépek közötti adatcsere javítja a gyártás pontosságát és csökkenti a leállásokat.

A Lufthansa szintén privát 5G hálózatokat használ a légi közlekedési és logisztikai rendszerek fejlesztésére, lehetővé téve a gyors adatcserét a repülőgépek földi kiszolgálásban és a légiforgalmi irányításban.[5] Az 5G gyors adatáviteli sebessége és alacsony késleltetés kritikus fontosságú a légi közlekedés hatékony működtetésében.

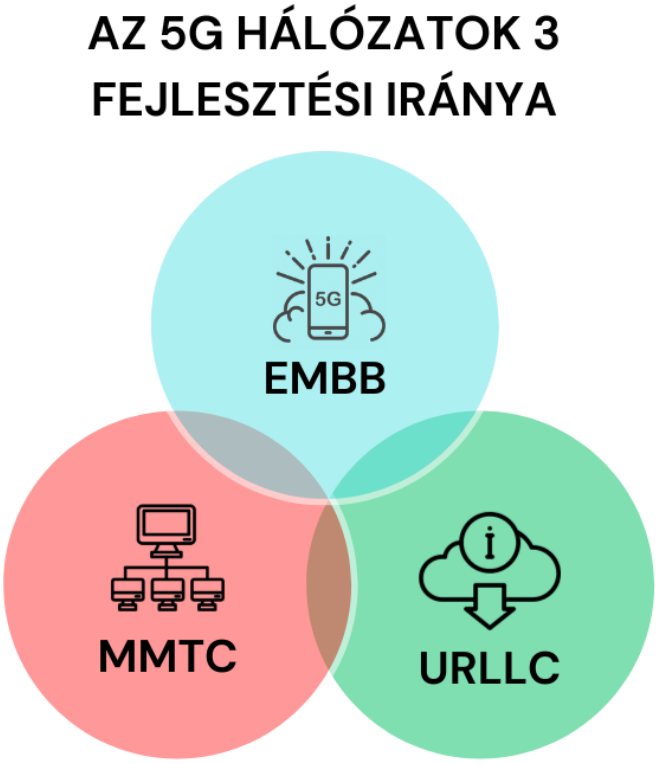
Ezek a technológiai fejlesztések jelentősen javítják a gyártási és szolgáltatási folyamatok hatékonyságát és alapot adnak az ipari szektor további fejlődéséhez.

Privát 5G technológia alapjai

Az 5G alapvető technológiai jellemzői

Az ötödik generációs mobilhálózatok, azaz az 5G, számos jelentős előrelépést hoztak a kommunikációs technológiákban. A legfontosabb újítások közé tartozik a rendkívül alacsony késleltetés (akár <1 ms), a nagy adatátviteli sebesség (elméleti maximum akár 10 Gbps), valamint a tömeges eszközkapcsolat támogatása (akár 1 millió eszköz/négyzetkilométer). [6]

Az ipari alkalmazások számára ezek a paraméterek lehetővé teszik a valós idejű vezérlést, a precíziós gyártást, illetve az önálló rendszerek – például autonóm járművek vagy robotkarok – megbízható működését. Az 5G fejlesztési irányai 3 fő területre oszlanak el. (1. ábra)



1. ábra - Az 5G hálózatok 3 fejlesztési iránya – saját szerkesztés

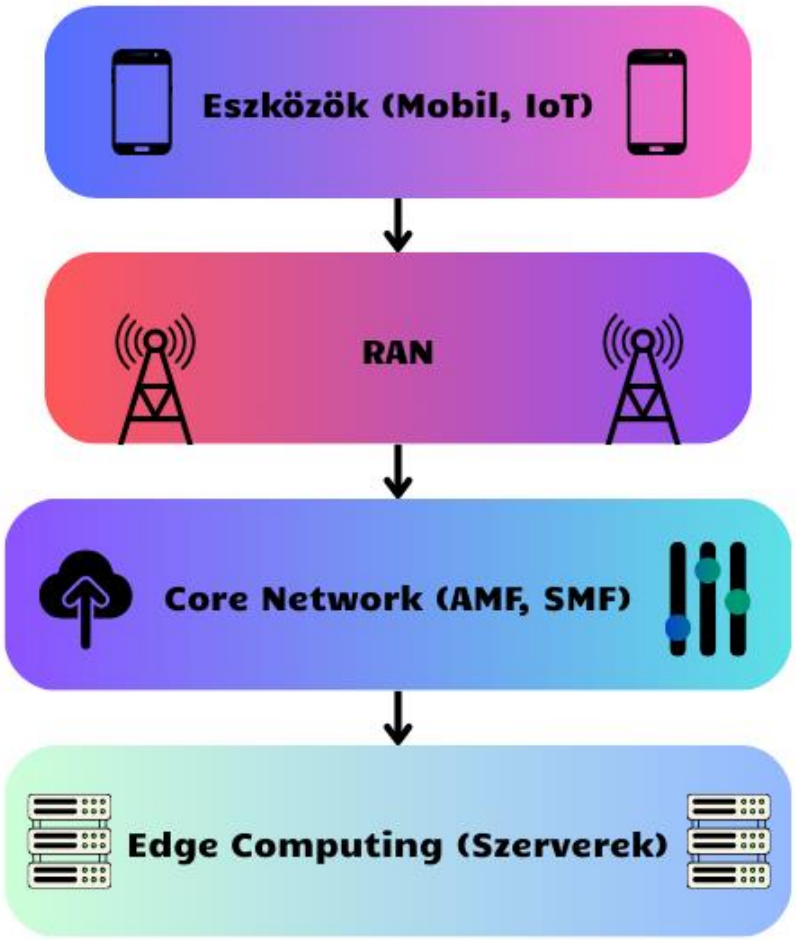
- **eMBB** (enhanced Mobile Broadband): nagy adatsebesség.
- **URLLC** (Ultra-Reliable Low-Latency Communications): ultra-alacsony késleltetés, ipari vezérléshez.
- **mMTC** (massive Machine Type Communications): nagyszámú IoT eszköz támogatása.

A privát 5G hálózatok fogalma

A privát 5G hálózat egy dedikált, helyileg telepített mobilhálózat, amelyet egy adott szervezet kizárólagosan használ, saját igényei szerint optimalizálva. A privát hálózatok lehetnek teljesen önállóak, vagy egy publikus szolgáltató infrastruktúrájára épülő, de szeparált megoldások is. A hálózati komponensek logikai elrendezését a 2. ábra szemlélteti. [7]

Fő jellemzők:

- **Teljes kontroll:** A hálózati beállításokat, biztonsági szabályokat a vállalat maga határozhatja meg.
- **Személyre szabható QoS:** Szolgáltatási minőség (Quality of Service) optimalizálható az egyes alkalmazások számára.
- **Biztonság:** A forgalom házon belül marad, nem halad át nyilvánosan interneten.



2. ábra - Ipari 5G infrastruktúra logikai modellje – saját szerkesztés

A privát 5G hálózat fő komponensei

Egy ipari privát 5G hálózat három fő technológiai rétegből áll:

- **RAN (Radio Access Network):** A bázisállamok és az eszközök közötti kommunikációt biztosítja. Ipari környezetben sokszor speciális antennákat, illetve kis cellás rendszereket alkalmaznak a beltéri lefedettség biztosítására.
- **Core Network (Maghálózat):** A maghálózat kezeli a hitelesítést, adatfeldolgozást, valamint a forgalomirányítást. Privát hálózatok esetén gyakran a helyszínen futtatják a core komponenseket, hogy minimalizálják a késleltetést.
- **Edge Computing (Mobil peremhálózati feldolgozás):** A helyi adatfeldolgozás lehetővé teszi a valós idejű alkalmazásokat anélkül, hogy az adatokat egy távoli adatközpontba kellene küldeni. [8]

Példa: Egy gyárban a robotkarok irányításához szükséges adatok feldolgozása helyben történik, ezzel garantálva a gyors válaszidőt.

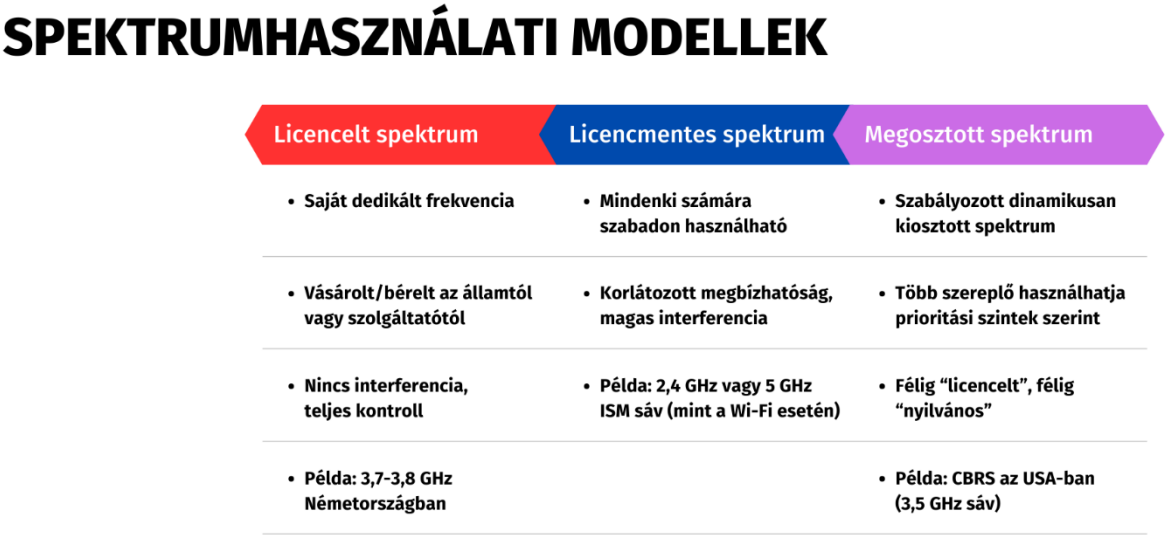
Frekvenciakezelés és spektrumhasználat

A privát 5G hálózatok számára kiemelt fontosságú a megfelelő rádiófrekvencia-használat.

Ipari környezetben a következő lehetőségek adottak:

- **Licencelt spektrum:** A vállalat saját frekvenciát vásárol vagy bérel az államtól vagy szolgáltatótól, biztosítva a zavartalan működést.
- **Licencmentes spektrum:** Szabadon hozzáférhető rádióspektrum (pl. 2,4 GHz, 5 GHz), amely nem igényel engedélyt, de nagyobb a zavarás (interferencia) kockázata, és nem garantált a stabilitás.
- **Megosztott spektrum:** Szabályozottan hozzáférhető sáv, ahol több szereplő dinamikusan osztozik a frekvencián – pl. a CBRS rendszer az Egyesült Államokban. Bizonyos szinteken engedélyezés és prioritás is érvényesül. [9]

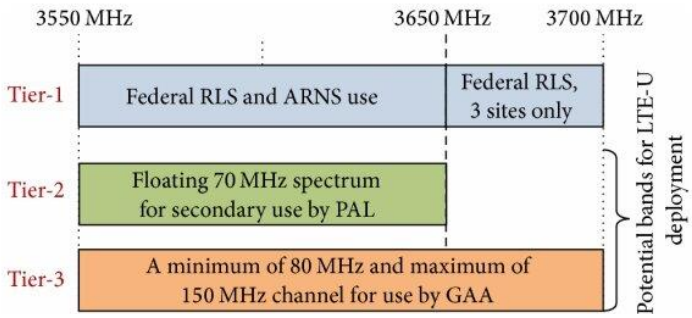
A spektrumhasználat fő típusait a 3. ábra mutatja be.



3. ábra - Spektrumhasználati modellek - saját szerkesztés

Az európai országokban, így Magyarországon is, több kezdeményezés zajlik a helyi ipari spektrumok kiosztására.

Hibrid megoldások: A licencelt és a licencmentes spektrumok kombinálása a költségoptimalizálás érdekében. A CBRS rendszer példája jól mutatja a spektrum megosztását (4. ábra).



4. ábra - CBRS spektrum három felhasználói szint között: Incumbent, Priority Access License és General Authorized Access. https://www.researchgate.net/figure/CBRS-spectrum-with-3-types-of-users_fig1_309407740

Frekvenciakezelés és engedélyezés privát 5G hálózatokhoz

A privát 5G hálózatok üzemeltetéséhez elengedhetetlen az ehhez szükséges rádióspektrum biztosítása. Az ipari felhasználásra szánt frekvenciasávokat országonként különböző szabályozó hatóságok jelölik ki és ezek használatához általában egyedi engedély szükséges.

Az Európai Unió tagállamai közül több másik – például Franciaország, Hollandia vagy Finnország – is hasonló szabályozást vezetett be. Ezek célja, hogy az ipari szereplők versenysemleges módon, a hagyományos mobilszolgáltatóktól függetlenül építhessenek saját 5G hálózatot, különösen zárt ipari környezetekben. A frekvenciakezelés kérdése tehát kulcsfontosságú, hiszen a hálózat megbízhatósága, kapacitása és interferenciamentes működése alapvetően ezen múlik.

Összefoglalás

Összefoglalva, a privát 5G hálózatok technológiai alapjai lehetővé teszik az ipari alkalmazások számára a magas szintű megbízhatóságot, biztonságot, illetve rugalmasságot. A RAN, a Core és az Edge Computing együttese biztosítja az alacsony késleltetést és a helyi adatfeldolgozás lehetőségét. A spektrumhasználat módja kritikus tényező a sikeres bevezetéshez, emiatt minden ipari szereplő számára stratégiai döntést jelent a megfelelő modell kiválasztása.

Technikai megvalósítás ipari környezetben

Ipari követelmények a privát 5G hálózatokkal szemben

Az ipari alkalmazások rendkívül specifikus követelményeket támasztanak a kommunikációs rendszerekkel szemben. Ezek közül a legfontosabbak a következők:

- Rendkívül alacsony késleltetés (URLLC támogatás), kritikus gép-gép kommunikációhoz.
- Magas megbízhatóság és hibatűrés, különösen gyártósorok vezérlésénél.
- Biztonságos adatkezelés, helyszíni adatfeldolgozás igénye.
- Skálázhatóság, az IoT-eszközök számának gyors bővüléséhez igazodva.

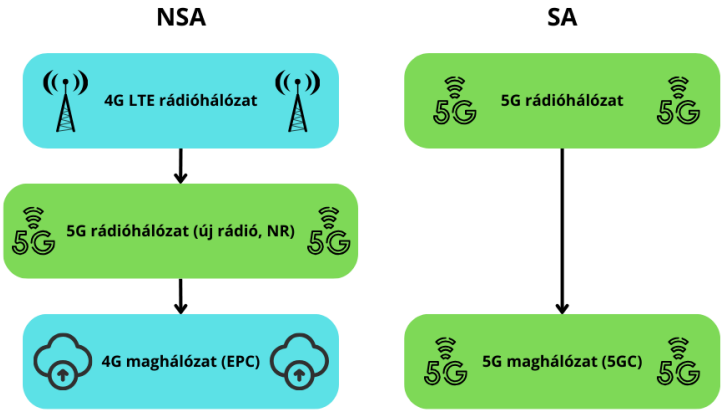
Ipari követelmények	5G megoldások
Késleltetés	Alacsony válaszidő valós idejű alkalmazásokhoz, autonóm járművekhez, ipari automatizáláshoz
Sebesség	Nagy adatátviteli sebesség biztosítja a nagy forgalmú adatkezelést, például a videóelemzéshez vagy adatszinkronizáláshoz
Skálázhatóság	Nagy számú IoT eszköz egyidejű csatlakozása, széleskörű eszközkapcsolat biztosítása az ipari környezetekben.
Biztonság	Fejlett titkosítási és adatvédelmi mechanizmusok, amelyek védelmet nyújtanak a hálózati támadásokkal szemben

Hálózati architektúrák ipari alkalmazásokhoz

Az ipari privát 5G hálózatok megvalósítása többféle architektúrában történhet, az adott alkalmazási igények függvényében. A privát 5G architektúrák közti különbséget az 5. ábra mutatja be (NSA vs SA).

Non-Standalone (NSA) vs. Standalone (SA) [10]

- NSA (nem önálló) hálózatok: A 4G/LTE infrastruktúrára építve működnek, az 5G csak kiegészítő szerepet tölt be. Előny: gyorsabb bevezetés, hátrány: nem teljes 5G képességek.
- SA (önálló) hálózatok: Teljesen független 5G infrastruktúrára épülnek. Előny: alacsony késleltetés, edge computing lehetőségek, magashatékonyság skálázhatóság



5. ábra -5G hálózati architektúrák: NSA vs SA - saját szerkesztés

Lokális Core vs. Megosztott Core

- Lokális Core: A gyárterületen helyileg telepített 5G core rendszer. Maximális adatbiztonságot és minimális késleltetést kínál.
- Megosztott Core: Egy szolgáltató által biztosított core hálózatot használnak, de dedikált szeparációval.

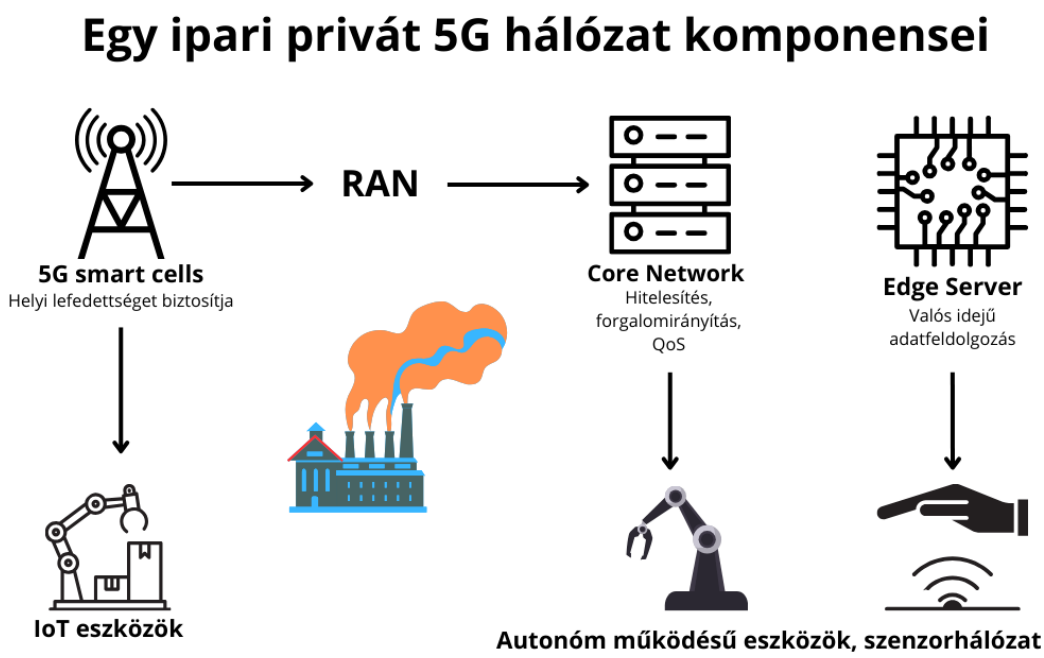
A választás függ az adatbiztonsági követelményektől, az üzemeltetési költségektől és a meglévő IT-infrastruktúrától. [11]

Eszközök és komponensek

Egy ipari privát 5G hálózat kiépítése során a következő komponensek szükségesek: [12]

- **5G kis cellák (small cells):** Biztosítják a helyi lefedettséget beltérben vagy kültéren.
- **5G RAN komponensek:** Hálózati antennák, rádióegységek (RU), elosztott egységek (DU).
- **Helyi Core szerverek:** Teljes core funkciók, például hitelesítés, forgalomirányítás helyi kezelése.
- **Edge szerverek:** Valós idejű adatfeldolgozás robotok vagy önvezető rendszerek számára.
- **IoT eszközök:** Szenzorok, robotkarok, önjáró járművek (AGV-Automated Guided Vehicles)

A főbb komponenseket a 6. ábra részletezi.



6. ábra - Egy ipari privát 5G hálózat komponensei - saját szerkesztés

Példa:
Egy autógyártó üzemben a robotkarok és az önjáró járművek (AGV-k) 5G kis cellákon keresztül kapcsolódnak a helyi core hálózathoz, miközben az Edge szerverek végzik a gépi látás feldolgozását valós időben.

Esettanulmányok

BMW – Privát 5G alkalmazása a lipcsei gyárban

A BMW a németországi Lipcsében található autógyárában indította el az egyik első privát 5G alapú hálózati projektjét, melyet a Deutsche Telekom és az Ericsson közreműködésével valósított meg. A cél egy olyan dedikált, nagy megbízhatóságú kommunikációs infrastruktúra létrehozása volt, amely képes valós időben kiszolgálni az önvezető járművek, autonóm szállítórobotok és az gyártási rendszerek adatkommunikációs igényeit. [13]

A projekt keretében a BMW egy saját 5G frekvenciát bérelt a német szövetségi hálózati hatóságtól (BNetzA), a 3,7 – 3,8 GHz közötti ipari spektrumsávban. A hálózat lefedettségét úgy alakították ki, hogy a teljes gyártócsarnokban, beleértve a raktárban és logisztikai zónákat is, biztosított legyen az alacsony terület az automatizált vezető nélküli járművek (AGV-k) flottájának irányítása lett, amely a nyersanyagok és alkatrészek belső szállításáért felel.

A projekt nem csupán technikai demonstrációként szolgált, hanem a BMW hosszú távú digitalizációs stratégiájának részét képezi. A cég a jövőben több gyárában is bevezetni tervezi a privát 5G hálózatot, mivel az jelentős előrelépést biztosít a termelés rugalmasságában, az eszközök valós idejű felügyeletében, valamint a prediktív karbantartási folyamatokban is. [14]

Huawei szerepe a privát 5G piacon

A Huawei – noha Európában az utóbbi évek geopolitikai feszültségei miatt visszafogottabban van jelen – továbbra is meghatározó szereplő a globális privát 5G piacán, különösen Ázsiában. A vállalat átfogó end-to-end megoldásokat kínál az ipari 5G rendszerekhez, amelyek hardveres (bázisállomások, antennák, edge eszközök) és szoftveres (hálózatmenedzsment, slicing, AI-alap optimalizálás) komponenseket is tartalmaznak. Kiemelt figyelmet fordítanak a hálózatok rugalmasságára, skálázhatóságára és a valós idejű adatfeldolgozás támogatására.

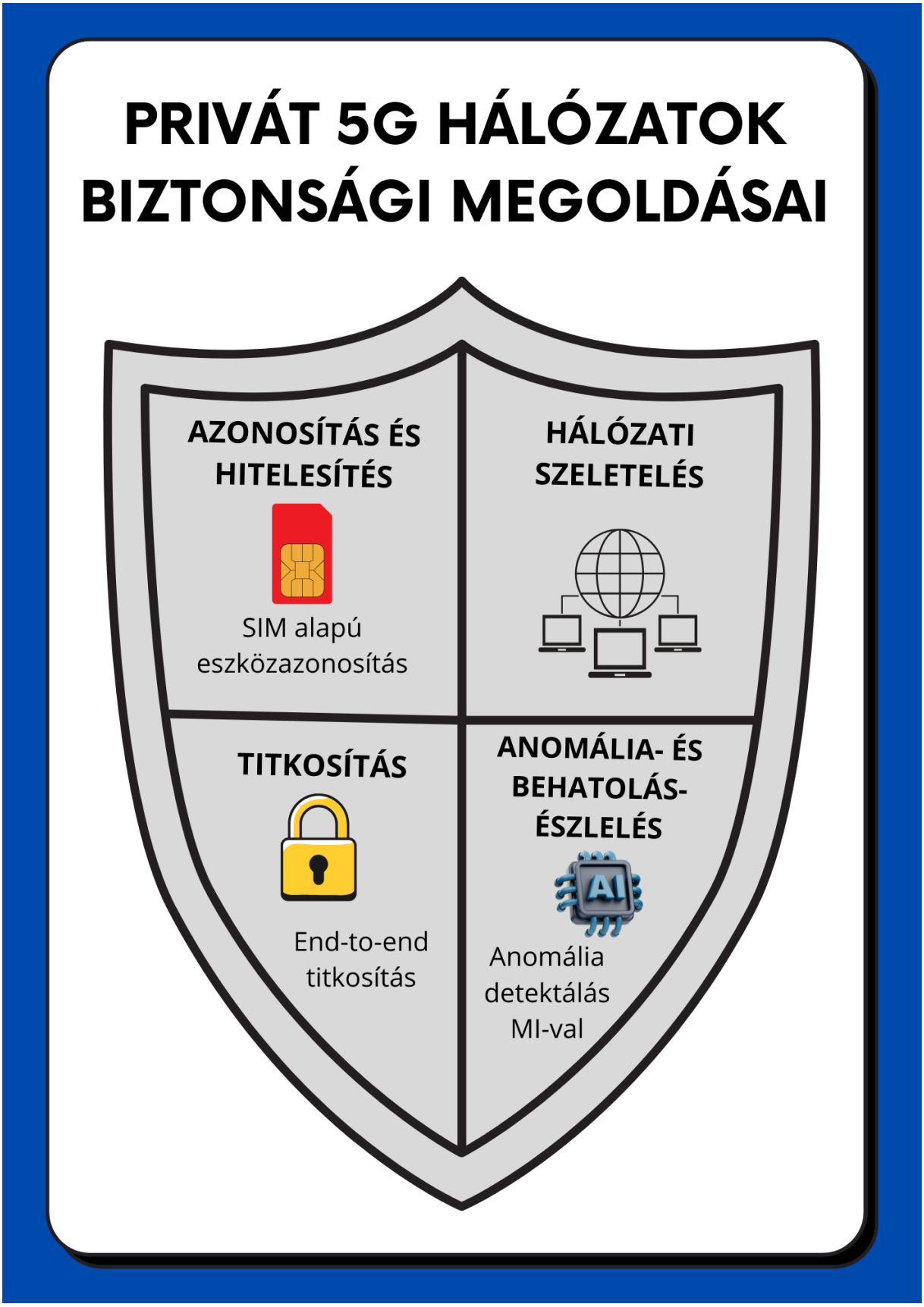
Az egyik legismertebb referencia Huawei oldalról a CHN Energy kínai energiacéghez kötődik, ahol privát 5G-t vezettek be egy szénbányában a munkafolyamatok automatizálására és a biztonsági felügyelet javítására [8]. A hálózat lehetővé teszi többek között a drónos terepfelmérést, valós idejű videóátvitelt és szenzoros adatgyűjtést nehezen megközelíthető helyeken. Hasonló projektet valósítottak meg több kínai acél- és autóipari gyárban is, például a FAW és a BAIC Group létesítményeiben, ahol a cél az automatizált szerelősorok és a minőségellenőrző rendszerek kiszolgálása volt.

Habár a Huawei privát 5G termékei leginkább a kínai és délkelet-ázsiai piacokon terjedtek el, a technológiai portfóliójuk alapján világosan látszik, hogy az ipari digitalizációs stratégiák szempontjából globális viszonylatban is versenyképes megoldásokat kínálnak.

Hálózatbiztonság ipari privát 5G hálózatokban

A privát 5G hálózatok egyik legfontosabb előnye az adatbiztonság magas szintje. Az ipari környezetekben különösen fontos a következő védelmi mechanizmusok alkalmazása: (7. ábra) [15]

- **SIM-alapú azonosítás:** Minden eszköz csak hitelesítéssel csatlakozhat.
- **End-to-end titkosítás:** Az adatok titkosítása a készüléktől egészen a feldolgozó rendszerig történik.
- **Szeparált hálózati szeletek (Network Slicing):** Külön logikai hálózatok biztosítása különböző gyártósori alkalmazások számára.
- **Folyamatos monitoring és behatolás-észlelés:** A hálózati forgalom valós idejű elemzése és anomália detektálása.



7. ábra - Privát 5G hálózatok biztonsági megoldásai - saját szerkesztés

Bosch gyártósor 5G hálózattal

A Bosch stuttgarti gyárában bevezetett privát 5G hálózat célja az volt, hogy valós idejű adatfeldolgozást és flexibilis gyártási folyamatokat tegyen lehetővé.

Főbb jellemzők:

- 5G kis cellák beltéri telepítése.
- Helyszíni 5G core infrastruktúra.
- 3 ms-os késleltetés biztosítása robotkar vezérléséhez.
- Lokális edge számítástechnika a minőségellenőrzési rendszerhez.

Az eredmények alapján a gyártósor rugalmassága 30%-kal nőtt, miközben a karbantartási idő 20%-kal csökkent. [16]

Privát 5G összehasonlítása más ipari hálózati technológiákkal

Ahhoz, hogy a privát 5G hálózatoknak a valódi előnyei jól érthetővé véljanak, érdemes összehasonlítani azokat más, ipari környezetekben is elterjedt technológiákkal, mint például a Wi-Fi vagy az LTE.

Míg a Wi-Fi széles körben elérhető és olcsó megoldás, ipari alkalmazásokban számos korlátja van. A megbízhatósága korlátozott, a késleltetés magasabb lehet és a rádiós interferencia miatt gyakran tapasztalható kapcsolatkimaradás. Az LTE hálózatok ennél megbízhatóbbak és stabilabbak, de még mindig a nyilvános infrastruktúrát használják, így nem nyújtanak olyan fokú irányítást és adatbiztonságot, mint a privát 5G.

A privát 5G rendszerek kiemelkednek a valódi alacsony késleltetésű kommunikáció, a nagy adatátviteli sebesség, valamint a hálózati szeletelés (network slicing) lehetősége révén. Utóbbi lehetővé teszi, hogy egyetlen hálózaton belül különböző szolgáltatási szinteket lehessen kialakítani, így például egyszerre lehet real-time vezérlést és nagy mennyiségű adatgyűjtést futtatni. [17]

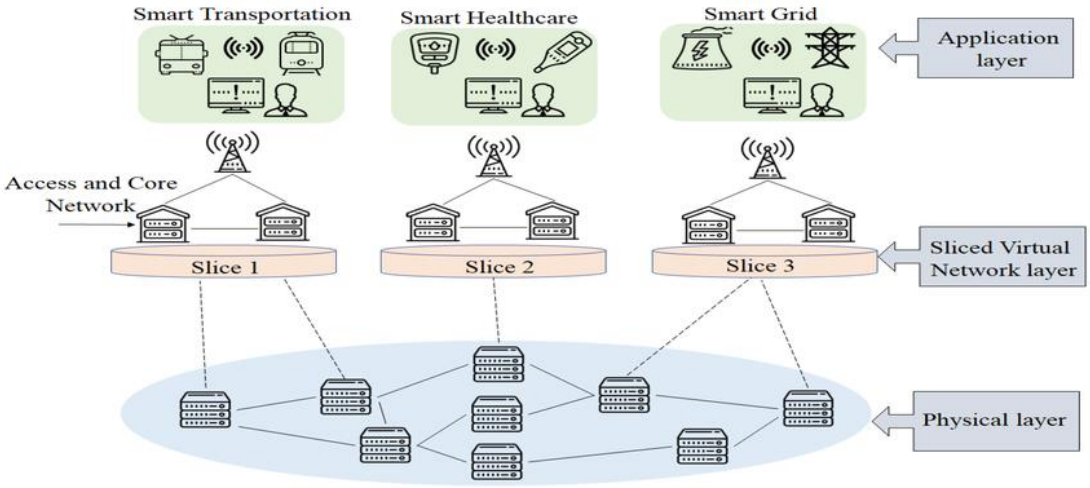
	Wi-Fi	LTE (publikus)	Privát 5G
Hozzáférés	Nyilvános, szabadon elérhető	Nyilvános, szolgáltatón keresztül	Dedikált, zárt hálózat
Késleltetés	30-100 ms	20-50 ms	<10 ms
Működési stabilitás	Interferenciára érzékeny	Stabilabb, de megosztott	Kiemelkedően stabil, kontrollált
Biztonság	Közepes, könnyen támadható	Jó, de nyilvános struktúra	Magas, zárt rendszer
Skálázhatóság	Korlátozott (kevés eszköz)	Jó	Kiváló (akár millió eszköz/km^2)
Hálózatszeletelés (slicing)	Nem támogatott	Nem jellemző	Teljes mértékben támogatott
Testreszabhatóság	Korlátozott	Szolgáltatófüggő	Teljes kontroll
Költség	Alacsony bevezetési költség	Havidíjas, szolgáltatótól függ	Magas kezdeti költség, de hosszútávon optimalizálható

Szoftveres megoldások a privát 5G hálózatokban

A privát 5G hálózatok egyik legfontosabb megkülönböztető jegye a fejlett szoftveres infrastruktúra, amely lehetővé teszi az ipari igényekhez való rugalmas, skálázható és nagyfokú testreszabhatóságot. Az ilyen hálózatokat már nem csupán a fizikai rádiós elemek és bázisállamok definiálják, hanem a mögöttes szoftveres architektúra is, amely komplex funkciókat lát el a hálózat működtetése és optimalizálása terén.

Network slicing – Az egyik kulcselem az úgynevezett szeletelés, amelynek lényege, hogy egyetlen fizikai hálózaton belül több virtuális hálózatot lehet létrehozni, különféle paraméterekkel (pl. sávszelesség, késleltetés, biztonsági prioritás). Ez lehetővé teszi, hogy például egy gyártócsarnokon belül az autonóm robotok kommunikációja egy időben, de elkülönítve fusson a minőségellenőrző kamerarendszer adatátvitelétől, garantálva mindkét funkció zavartalan működését. [18]

Az 5G hálózatszeletelés lehetővé teszi, hogy egyetlen fizikai infrastruktúrán belül több logikailag elkülönített, testreszabott hálózat működjön párhuzamosan, az eltérő ipari igények szerint. Ezt a működési elvet szemlélteti a 8. ábra, ahol a különböző szeletek (pl. URLLC, eMBB, mMTC) elkülönítve jelennek meg az architektúrában.



8. ábra - 5G hálózatszeletelés architektúrája - https://www.researchgate.net/figure/5G-Network-slicing-architecture_fig1_343413196

SDN és NFV: A szoftveresen definiált hálózat (Software Defined Networking - SDN) és a hálózati funkciók virtualizációja (Network Functions Virtualization - NFV) együttesen teszik lehetővé a fizikai infrastruktúra absztrakcióját és dinamikus irányítását. Az SDN a vezérlési és adatátviteli síkok szétválasztásán alapul, ami leegyszerűsíti a hálózat irányítását és programozhatóságát. Az NFV segítségével olyan funkciók is virtualizálhatóvá válnak, mint például a tűzfal, betöltéseloszlás vagy a mobil maghálózati komponensek, amelyek korábban fizikai eszközökhöz voltak kötve.

Orchestration és menedzsmentplatformok: Az ilyen típusú hálózatok komplexitása szükségessé teszi az automatizált hálózatmenedzsment rendszerek alkalmazását. Ezek a rendszerek képesek például az erőforrások dinamikus allokációjára, a hibakezelés automatizálására, vagy épp a szolgáltatásminőség (QoS) fenntartására különböző hálózati szeletek között. Több gyártó, például a Nokia, az Ericsson vagy a Huawei kínál saját menedzsmentmegoldásokat, amelyek kifejezetten ipari privát 5G alkalmazásokhoz készültek. [19]

Kihívások és korlátok a privát 5G hálózatok bevezetésénél

Ez a rész fontos, mivel bemutatja a privát 5G hálózatok bevezetésével járó nehézségeket, amik segítenek a dolgozat megértésében és a jövőbeli fejlesztések szempontjából is fontosak.

Magas beruházási költségek: A hálózat kiépítése és üzemeltetése jelentős befektetést igényel, különösen egyedülálló infrastruktúrák létrehozásakor. Ezt a költséget a vállalatoknak kell kigazdálkodniuk.

Technológiai komplexitás: Az 5G hálózatok fejlesztése magában foglalja az új technológiák integrálását, mint az edge computing és a kis cellás rendszerek. Ehhez megfelelő szakértelem szükséges, amit nem minden ipari szereplő rendelkezik.

Szabályozási kérdések: A privát 5G hálózatok működtetéséhez a megfelelő spektrumot kell biztosítani és gyakran szükséges állami engedélyek beszerzése is. A spektrumhasználat nem minden országban egyszerű és az ipari szereplők számára is kihívást jelenthet a megfelelő frekvenciák kiválasztása.

Szakemberhiány: Az 5G, IoT és edge computing területeken dolgozó szakemberek kereslete meghaladja a kínálatot, így a vállalatoknak komoly problémájuk lehet a megfelelő szaktudású munkavállalók toborzásával.

Biztonsági kérdések és adatvédelem a privát 5G hálózatokban

A biztonság és adatvédelem kiemelkedően fontos szempont, különösen az ipari alkalmazásokban, ahol érzékeny és üzletkritikus adatok kerülnek átvitelre. A privát 5G hálózatok egyik legnagyobb előnye éppen az, hogy lehetőséget biztosítanak a teljes adatforgalom helyben történő kezelésére, anélkül, hogy az interneten keresztül kellene adatokat küldeni vagy fogadni. Ez a fajta lokális működés jelentős mértékben csökkenti a kiberfenyegetések kockázatát.

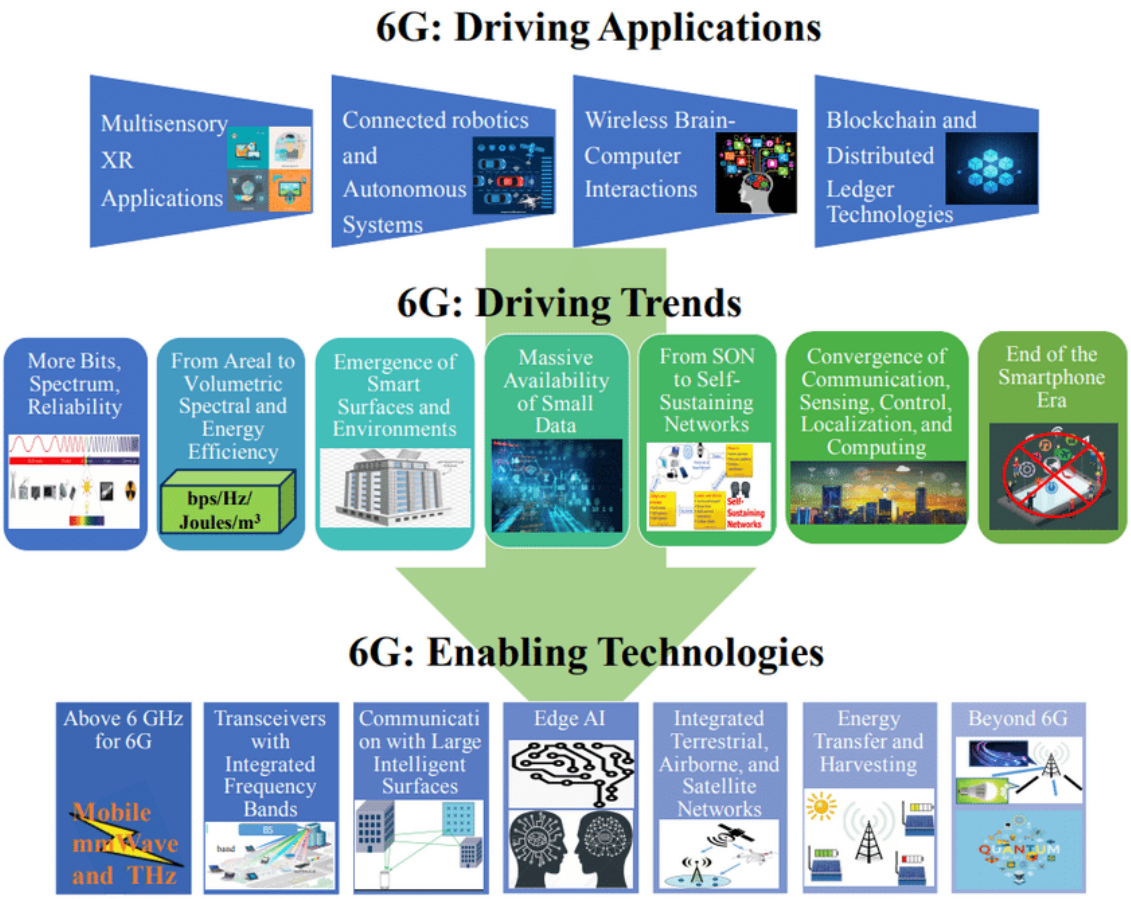
Ugyanakkor a biztonság nem garantált automatikusan. A privát hálózatok bevezetésekor új kihívások jelennek meg, például a környezet-specifikus támadások, a hálózati végpontok biztonsága, vagy a belső jogosultságkezelés megfelelő kialakítása. Mivel az edge computing rendszerek jellemzően decentralizáltak, az eszközök száma és elérhetősége is növeli a támadási felületet. Éppen ezért kulcsfontosságú a hálózati szegmentáció, a többrétegű hitelesítési mechanizmusok és az AI-alapú prediktív biztonsági megoldások alkalmazása.

A valós idejű adatelemzés, amelyre az 5G képessé teszi a rendszereket, nemcsak a termelési hatékonyság növelésére használható, hanem a fenyegetések gyors észlelésére és kezelésére is. Az automatizált, mesterséges intelligenciával támogatott kiberbiztonsági rendszerek képesek előre jelezni és blokkolni a nem kívánt hálózati viselkedést, így jelentősen növelik az általános biztonsági szintet. [20]

Jövőbeli trendek, fejlődési irányok

A 6G előfutárai

Bár az 5G technológia még csak most kezd igazán elterjedni az iparban, már folynak a 6G-vel kapcsolatos kutatások is. A 6G várhatóan nemcsak a sávszélességet növeli, hanem a hálózatok intelligenciáját is radikálisan fokozza (9. ábra). Az ipari alkalmazások szempontjából különösen fontos lehet a holografikus kommunikáció, a milliméter alatti hullámhosszok használata, valamint az érzékelés és kommunikáció összeolvadása. Ezek a fejlesztések a jövő gyáraiban akár teljesen új működési modelleket is megalapozhatnak.



9. ábra - A 6G hálózatok fő alkalmazásai, trendjei és technológiái - https://www.researchgate.net/figure/G-main-Applications-trends-and-technologies-24_fig2_339301321

Mesterséges intelligencia és az 5G konvergencia

Az MI és az 5G összekapcsolása kulcsszerepet játszhat a prediktív karbantartás, a valós idejű minőségellenőrzés vagy a gyártósorok optimalizálása terén. Az 5G biztosítja az alacsony késleltetést és a stabil adatkapcsolatot, az MI pedig képes azonnali döntések meghozatalára a beérkező adatok alapján. Az ilyen rendszerek nem csupán hatékonyabbá, hanem robosztusabbá is teszik az ipari folyamatokat, miközben emberi beavatkozásra egyre kevésbé van szükség.

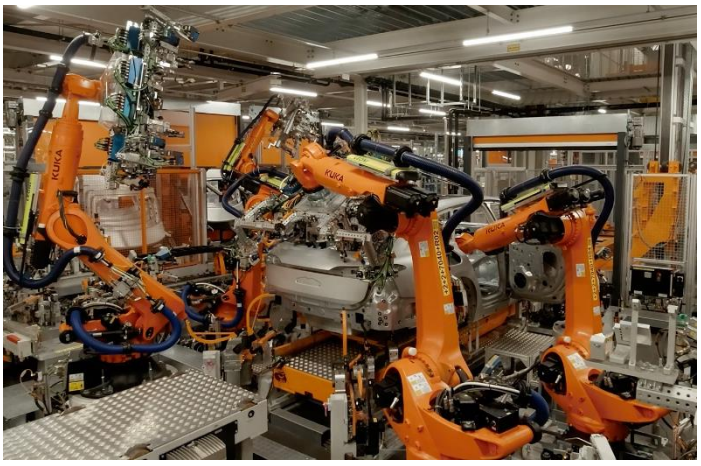
Privát hálózatok és a digital twin összekapcsolása

A digital twin technológia, amely a fizikai rendszerek digitális másolatát hozza létre, különösen jól hasznosítható, ha megbízható és valós idejű adatokkal tud dolgozni. (10. ábra) Ebben a privát 5G hálózatok kulcsszerepet játszanak, hiszen ezek teszik lehetővé az adatok gyors és biztonságos továbbítását. A digitális twin és az 5G integrációja új távlatokat nyit a szimuláció, a távoli felügyelet, vagy akár a valós idejű folyamatmódosítások területén is.

10. ábra - Adatáramlás a digital twin és a privát 5G között - https://www.researchgate.net/figure/Flow-of-digital-twin-in-5G-network_fig2_389952363

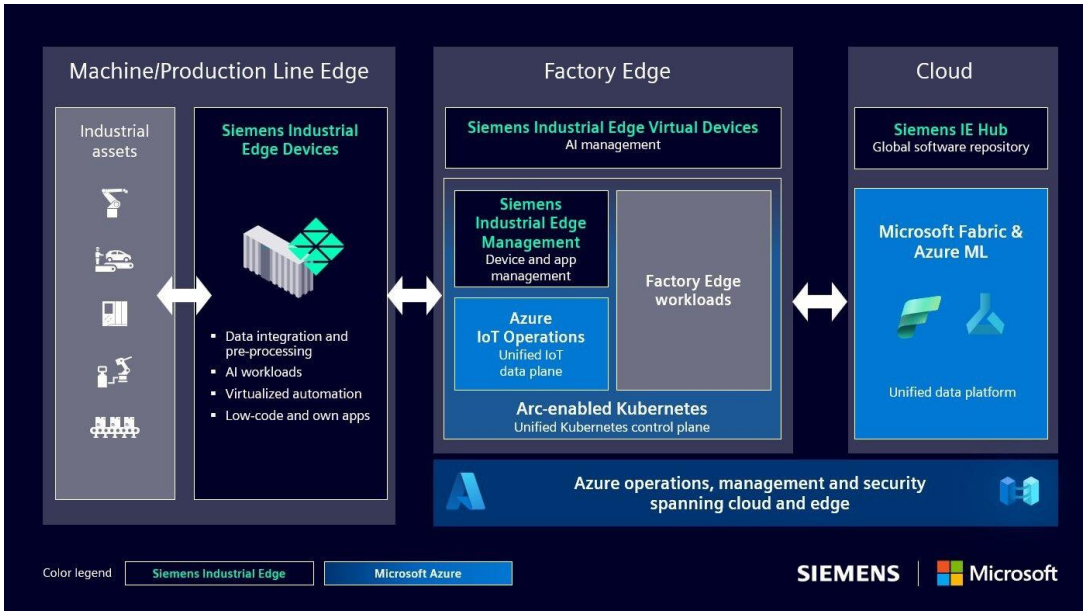
További alkalmazási példák

Audi Neckarsulm: Az Audi neckarsulmi gyárában a gyártási folyamatok hatékonyságát egy 5G-hálózatra épülő, valós idejű adatfeldolgozásra képes robotrendszer támogatja (11. ábra). A privát 5G hálózat biztosítja a gyártósorokon dolgozó autonóm eszközök közötti gyors és stabil kommunikációt, amely lehetővé teszi a hibák azonnali észlelését és a beavatkozások minimálisra csökkentését. Az élő adatkapcsolat révén a gyártás közben folyamatos visszacsatolás történik, ami a rugalmasságot és a minőségellenőrzést is magasabb szintre emeli. [21]



11. ábra - Robotkar minőségellenőrzést végez - képernyőkép innen: https://www.youtube.com/watch?v=0hSVRoScegk

Siemens: A Siemens saját ipari tesztkörnyezetében több olyan pilotprojektet is futtat, ahol a gyártósorokat edge AI és privát 5G hálózat kombinációja vezérli. Az adatokat a szenzorok azonnal továbbítják az edge-szerverek felé, ahol a mesterséges intelligencia alapú rendszerek azonnali döntéseket hoznak (12. ábra). Ez lehetővé teszi például, hogy egy gyártósor automatikusan módosítsa a gyártási paramétereket valós idejű visszajelzések alapján, ezzel növelve a hatékonyságot és csökkentve a selejtarányt.



12. ábra - Siemens Industrial Edge és a Microsoft együttműködése - https://press.siemens.com/global/en/pressrelease/siemens-xcelerator-siemens-accelerates-it-and-ot-integration-microsoft-edge-cloud-ai?

Lufthansa Technik: A Lufthansa Technik 5G-alapú karbantartási megoldásokat tesztel repülőgépek szervizelése során (13. ábra). A privát 5G hálózatot kihasználva drónokat és földi robotokat alkalmaznak a repülőgépek külső és belső állapotának felmérésére, ami korábban sokkal több időt és manuális ellenőrzést igényelt. A rendszer valós idejű képeket és adatokat továbbít, így a karbantartó csapat gyorsabban és pontosabban tud reagálni a problémákra. Ez jelentősen csökkenti az állásidőt és javítja az üzemeltetés gazdaságosságát. [22]

13. ábra - 5G alapú repülőgép karbantartás a Lufthansa-nál - https://newsroom.vodafone.de/vodafone-und-lufthansa-starte-5g-campus-netz

Ericsson és ABB: Az Ericsson és az ABB együttműködésének keretében Svédországban olyan okosgyári megoldásokat fejlesztenek, ahol az 5G-hálózatot mélyen integráltak az ipari automatizálási rendszerekbe (14. ábra). A projekt célja, hogy az ipari robotkarok, érzékelők és vezérkőrendszerek zökkenőmentesen kommunikáljanak egymással valós időben. Az 5G itt nem csupán adatkapcsolatként szolgál, hanem lehetővé teszi a vezeték nélküli vezérlést és új, rugalmasabb gyártási elrendezéseket – olyan környezetet teremtve, ahol a gyártósorok percek alatt átkonfigurálhatók. [23]

14. ábra - Ericsson 5G rádióállomás - https://totaltele.com/ericsson-wins-5g-supply-contract-with-verizon/

Hazai példa

Magyarországon is megjelentek a privát 5G technológiát alkalmazó ipari szereplők, amelyek közül az egyik legismertebb a Bosch hatvani gyára (15. ábra). A vállalat – a régió egyik legmodernebb elektronikai gyártóközpontjaként – pilot projekt keretében vezette be a privát 5G hálózatot, szorosan együttműködve a Vodafone Magyarországgal és az Ericssonnal. A cél a gyártási folyamatok optimalizálása, a valós idejű adatgyűjtés lehetővé tétele, valamint a termelési rugalmasság növelése volt.

15. ábra - A Bosch hatvani gyára - https://hatvanihirlap.hu/1tovabb-erositi-poziciojat-bosch-hatvani-gyara/

A privát 5G hálózat révén a gyárban működő gépek és szenzorok stabil, alacsony késleltetésű kapcsolaton keresztül képesek adatot küldeni és fogadni, ami lehetővé teszi a gépek állapotának valós idejű monitorozását és a gyorsabb beavatkozást meghibásodás esetén. Emellett az összegyűjtött adatok elemzésével a Bosch képes előre jelezni az esetleges problémákat és finomhangolni a gyártási paramétereket a hatékonyság növelése érdekében.

Ez a projekt jól mutatja, hogy a privát 5G nem csupán elméleti lehetőség, hanem már most is kézzel fogható előnyöket nyújt az ipari szereplők számára Magyarországon is

– különösen az olyan cégek esetében, amelyek magas szintű automatizálásra és valós idejű adatelemzésre építenek. [24]

Összegzés és következtetések

A bemutatott ipari példák alapján egyértelműen látható, hogy a privát 5G hálózatok jelentős előnyöket kínálnak a hagyományos vezetékes vagy Wi-Fi alapú megoldásokkal szemben. A BMW lipcsei gyárában kiépített rendszer révén például valós időben, nagy megbízhatósággal vezérelhetők az autonóm járművek és gyártási eszközök, ami nemcsak a hatékonyságot növeli, hanem az üzembiztonságot is. Hasonló előnyök jelentkeznek a Huawei által megvalósított ipari projektnél is, különösen ott, ahol a környezet miatt kritikus a lefedettség és az alacsony késleltetés, például bányákban vagy komplex ipari létesítményben.

A példák alapján több ajánlás is megfogalmazható a jövőbeni kiépítésekhez:

A frekvenciasáv biztosítása kulcskérdés, ahhoz, hogy egy vállalat valóban önálló és stabil hálózatot tudjon működtetni, már a tervezéskor szükséges és érdemes figyelembe venni a spektrumengedélyezés hely szabályait, különösen olyan országokban, ahol dedikált ipari sávok állnak rendelkezésre.

A szoftveres hálózatmenedzsment (pl. slicing, SDN/NFV) nem mellékes technikai részlet, hanem stratégiai eszköz: ezek teszik lehetővé, hogy egy hálózat valós igényekhez igazodva, dinamikusan és biztonságosan működjön.

Kis léptékű pilot projektek hasznosak: mind a BMW, mind a kínai példák azt mutatják, hogy érdemes egy szűkebb üzemi területen kipróbálni az új hálózatot, mielőtt kiterjesztik a teljes gyártási környezetre.

Összességében tehát a privát 5G technológia nemcsak technikai fejlődést jelent, hanem versenyelőnyt is adhat azoknak a vállalatoknak, amelyek képesek ezt célzottan, jól szabályozott környezetben bevezetni és fenntartható módon üzemeltetni.

Irodalomjegyzék

[1] 5G-ACIA – 5G Alliance for Connected Industries and Automation. *5G for Connected Industries and Automation.* https://5g-acia.org/wp-content/uploads/5G-ACIA_White-Paper_5G-for-Connected-Industries-and-Automation.pdf (elérés: 2025. május 9.)

[2] Ericsson. *Ericsson Private 5G - Private network for your industry.* https://www.ericsson.com/en/private-networks/ericsson-private-5g (elérés: 2025 május 9.)

[3] Siemens AG. *Private Industrial 5G networks – tested and proven in industry.* https://www.siemens.com/global/en/products/automation/industrial-communication/industrial-5g/private-5g-networks-infrastructure.html (elérés: 2025. május 9.)

[4] Trend Micro. *The Current Security State of Private 5G Networks.* https://www.trendmicro.com/en_us/research/23/h/private-5g-network-security.html (elérés: 2025. május 9.)

[5] SNS Telecom & IT. *Private 5G Networks: 2024 – 2030.* https://www.snstelecom.com/private5g (elérés: 2025. május 9.)

[6] Calsoft Inc. *Potential of 5G in Manufacturing and Industrial Automation.* https://www.calsoftinc.com/blogs/potential-of-5g-in-manufacturing-and-industrial-automation.html (elérés: 2025. május 9.)

[7] Infosys. *Private 5G Network Deployments (Enterprise Owned).* https://www.infosys.com/iki/techcompass/private-5g-network-deployments.html (elérés: 2025. május 9.)

[8] PMC. *Private 5G networks: a survey on enabling technologies, architecture, and deployment.* https://pmc.ncbi.nlm.nih.gov/articles/PMC9676741/ (elérés: 2025. május 9.)

[9] Cisco. *What is Private 5G Network?* https://www.cisco.com/c/en/us/solutions/private-5g-networks.html (elérés: 2025. május 9.)

[10] TechTarget. "5G NSA vs. SA: How Do the Deployment Modes Differ?" 2025. https://www.techtarget.com/searchnetworking/feature/5G-NSA-vs-SA-How-does-each-deployment-mode-differ (elérés: 2025. május 9.)

[11] GSMA, *Private 5G Industrial Networks*, GSMA, 2023. https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2023/06/GSMA-Private-5G-Industrial-Networks-Report-June-2023.pdf (elérés: 2025. május 9.)

[12] Ericsson, *Private 5G networks for Industry 4.0*, Ericsson, 2021. https://www.ericsson.com/en/reports-and-papers/white-papers/private-5g-networks-for-industrial-use (elérés: 2025. május 9.)

[13] Deutsche Telekom. "New Telekom Campus Network on air in Leipzig." 2020. https://www.telekom.com/en/media/media-information/archive/new-telekom-campus-network-on-air-in-leipzig-595050 (elérés: 2025. május 9.)

[14] The Fast Mode. "Deutsche Telekom Builds Private 5G Campus Network at BMW's Leipzig Plant with Ericsson." 2020. https://www.thefastmode.com/technology-solutions/16564-deutsche-telekom-builds-private-5g-campus-network-at-bmws-leipzig-plant-with-ericsson (elérés: 2025. május 9.)

[15] Palo Alto Networks. "What is 5G security?" https://www.paloaltonetworks.com.au/cyberpedia/what-is-5g-security (elérés: 2025. május 9.)

[16] Bosch puts first 5G campus network into operation. Bosch Media Service. https://www.bosch-presse.de/pressportal/de/en/bosch-puts-first-5g-campus-network-into-operation-221632.html (elérés: 2025. május 9.)

[17] STL Partners. "Private 5G vs Wi-Fi vs Private LTE." https://stlpartners.com/articles/private-cellular/private-5g-vs-wi-fi-vs-private-lte/ (elérés: 2025. május 9.)

[18] 5G Network Slicing Explained." Wikipedia. https://en.wikipedia.org/wiki/5G_network_slicing (elérés: 2025. május 9.)

[19] C. Smith, "5G Network Slicing: Cross-Domain Orchestration and Management," Cisco https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/network-services-orchestrator/white-paper-sp-5g-network-slicing.pdf (elérés: 2025. május 9.)

[20] Thales. Security Solutions for Private 5G Networks. https://cpl.thalesgroup.com/resources/encryption/private-5g-network-security-solutions-brief (elérés: 2025. május 9.)

[21] Intel, "Audi Industry 4.0 Manufacturing Transformation," https://www.intel.com/content/www/us/en/customer-spotlight/stories/audi-automated-factory.html (elérés: 2025. május 9.)

[22] Lufthansa Technik expands its proven 5G campus network in Hamburg, https://www.lufthansa-technik.com/en/lufthansa-technik-expands-its-proven-5g-campus-network-in-hamburg-1369d00337071944 (elérés: 2025. május 9.)

[23] 5G-SMART – a research collaboration for 5G in manufacturing, https://www.ericsson.com/en/cases/2021/5g-smart (elérés: 2025. május 9.)

[24] 5G alapú kísérleti projekten dolgozik együtt a Vodafone és a Bosch, https://ictglobal.hu/rovid-hirek/5g-alapu-kiserleti-projekten-dolgozik-egyutt-a-vodafone-es-a-bosch/ (elérés: 2025. május 9.)

2.36. Okosgyárak kibervédelmi megoldásai

Okosgyárak kibervédelmi megoldásai

Készült: 2025. május 15.

Kazi Gábor

Mérnökinformatikus BSc, kazi.gabor01@gmail.com

Az Ipar 4.0 korszakában az okosgyárakban alkalmazott M2M-kommunikáció, ipari IoT-szenzorhálózatok, felhőszolgáltatások, robotika és autonóm rendszerek magas termelékenységnövekedést hoznak, ugyanakkor rendkívül növelik a támadási felületeket. A Dragos 2024-es felmérése több, mint 1500, legalább részleges termelésleállást okozó ransomware-támadást azonosított az OT/ICS szektorban, ami 87 %-os éves növekedésnek felel meg. A dolgozat célja annak bemutatása, miként vált a kiberbiztonság kulcsfontosságúvá e modern ipari ökoszisztémákban, és milyen integrált védelmi stratégiák szükségesek a fenntartható működéshez.

Kulcsszavak: okosgyár, kiberbiztonság, zero-trust, kibertámadás, kibervédelem, szegmentálás, üzemi technológia, többrétegű védelem, anomáliadetektálás, kockázatelemzés, sebezhetőség

Tartalomjegyzék

1 Bevezetés ..... - 3 -

1.1 Az ipari digitalizáció trendje ..... - 3 -

1.2 Az okosgyárak szerepe az ipar 4.0-ban ..... - 4 -

1.3 A kiberbiztonság aktualitása és relevanciája ..... - 5 -

2 Okosgyárak technológiai háttere ..... - 8 -

2.1 IoT, M2M, SCADA, PLC, MES, ERP rendszerek ..... - 8 -

2.2 IT-OT konvergencia ..... - 9 -

2.3 Fenyegetettségi vektorok növekedése ..... - 10 -

3 Kibertámadások az iparban ..... - 11 -

3.1 Jellemző támadások ..... - 11 -

3.2 Valós példák ..... - 11 -

4 Kiberbiztonsági megoldások okosgyárakban ..... - 13 -

4.1 Hálózati szegmentálás és zónázás ..... - 13 -

4.2 Tűzfalak, IDS/IPS rendszerek ..... - 13 -

4.3 Végpontvédelem és eszközfelügyelet ..... - 14 -

4.4 ICS/SCADA – specifikus védelmi technikák ..... - 14 -

5 A Zero Trust modell az iparban ..... - 15 -

5.1 Elvek ..... - 15 -

5.2 Implementációs kihívások ..... - 16 -

6 Folyamatos monitorozás és anomáliadetektálás ..... - 18 -

6.1 SIEM és SOAR rendszerek ..... - 18 -

6.2 AI/ML alapú analitika ..... - 18 -

7 Szabványok és tanúsítványok ..... - 20 -

7.1 IEC 62443 szabványcsalád ..... - 20 -

7.2 NIST SP 800-82 (Guide to Industrial Control Systems Security) ..... - 20 -

7.3 ISO/IEC 27001 szabvány (Információbiztonság) ..... - 21 -

7.4 NIS2 irányelv (EU-s szabályozás) ..... - 21 -

8 Elemzés és javaslatok ..... - 22 -

8.1 Technikai ajánlások ..... - 22 -

8.2 Szervezeti és emberi tényezők ..... - 23 -

9 Összefoglalás és következtetések ..... - 24 -

9.1 Kritikus pontok összegzése ..... - 24 -

9.2 Jövőbeli trendek ..... - 24 -

1 BEVEZETÉS

Az ipari forradalom negyedik, azaz jelenlegi hullámában a gyárak egyre nagyobb mértékben támaszkodnak az emberi munkaerő mellett olyan összekapcsolt, szoftver-vezérelt kiber-fizikai rendszerekre (Cyber-Physical System; CPS), amelyek a termelési hatékonyság jelentős növelése mellett új típusú kockázatokat is hoznak magukkal. A CPS-ek integrációja lehetővé teszi a gépek, szenzorok és adatközpontok közötti folyamatos és automatikus információáramlást, melyek révén a gyártási folyamatok valós időben optimalizálhatóvá válnak.

A CPS-ek mellett megjelentek és elterjedtek az olyan új technológiák is, mint a felhőalapú szolgáltatások (cloud computing), robotikai rendszerek, önvezérlő járművek, valamint a dolgok internete (Internet of Things; IoT), amelyek még összetettebbé teszik a gyártási környezetet. Ezek a technológiák lehetőséget nyújtanak a gyártási láncok rugalmasabb, hatékonyabb és önállóbb működtetésére, ugyanakkor nagymértékben növelik a digitális támadási felületet, és ezzel egyenesen arányosan a kibertámadások kockázatát.

A kiberbiztonsági fenyegetések kiemelten veszélyeztetik az okosgyárak stabilitását és integritását, mivel ezek az üzemek jellemzően internetes hálózatokon keresztül működnek, kapcsolódnak egymáshoz, illetve közvetlen kapcsolatban állnak a külső partnerekkel is. Egy sikeresen végrehajtott, illetve nem megfelelően kezelt kibertámadásnak többféle következménye lehet: felléphet termelési leállás, amely jelentős pénzügyi veszteségeket okozhat, érzékeny vagy bizalmas adatok szivároghatnak ki, valamint károsodhat a vállalat valamely szellemi tulajdona. Továbbá a támadások fizikai károkat is okozhatnak, amennyiben a támadó képes beavatkozni a gyártási folyamatokba, például a gyártósorok manipulálásával vagy a robotok hibás működtetésével.

A kibertámadások által okozott károk nemcsak közvetlen gazdasági veszteséget jelentenek egy adott vállalat számára, hanem hosszútávon súlyos hatással lehetnek a vállalat hírnevére, versenyképességére, és egyes esetekben akár a nemzet- vagy rendkívüli esetben a világgazdaság egészére is. Ennek következtében elengedhetetlen a megfelelő kibervédelmi stratégiák, technológiák és szabványok alkalmazása, valamint ezek folyamatos fejlesztése és aktualizálása.

Jelen dolgozat célja annak részletes vizsgálata, hogy miként lehet hatékonyan védekezni a fent említett fenyegetések ellen, bemutatva a kibervédelmi kihívások természetét, az alkalmazható korszerű technológiákat és szabványokat, valamint néhány eset segítségével szemléltetve ezen megoldások gyakorlati jelentőségét.

1.1 Az ipari digitalizáció trendje

Az ipari digitalizáció jelentős népszerűségnek örvend a vállalatok, illetőleg a cégek körében. E trend mögött számos olyan gyakorlati ok áll, amely az ipari vállalatokat egyre inkább az automatizált és digitalizált megoldások felé tereli.

Elsősorban a gépek alkalmazása jelentős termelékenységnövekedést eredményez, hiszen képesek az embereknél gyorsabban, pontosabban és nagyobb megbízhatósággal elvégezni a feladatokat. A robotok és automatizált rendszerek folyamatos, 24 órás üzemidő mellett is fenntarthatók, jelentősen csökkentve a termelési ciklusidőket és növelve az előállított termékek mennyiségét. Az emberi munkaerővel szemben a gépek nem fáradnak el, kevésbé hajlamosak hibák elkövetésére, valamint nagyobb precizitással és következetességgel dolgoznak.

Ezen túlmenően az automatizált rendszerek fenntartási költsége általában alacsonyabb, mint az emberi munkaerőé. Bár a kezdeti beruházás jelentős lehet, hosszútávon a gépek és automatizált rendszerek használata jelentős megtakarításokat eredményez, többek között az alacsonyabb energia- és munkaerőköltségek révén. Ezek a rendszerek továbbá kevésbé érzékenyek a külső gazdasági változásokra - például a munkaerőpiaci ingadozásokra - így stabilabb működési környezetet biztosítanak a vállalatok számára.

A digitalizáció egyik kulcsfontosságú előnye a gyártási rugalmasság és agilitás növelése. Az okosgyárak képesek gyorsan és rugalmasan reagálni a változó piaci igényekre, gyorsan átállíthatják gyártósoraikat és újragondolt termékeket

állíthatnak elő hatékonyan. Ez a rugalmasság kulcsfontosságú a gyorsan változó gazdasági környezetben, különösen olyan globális kihívások során, mint a pandémia vagy egyéb válsághelyzetek voltak az elmúlt években.

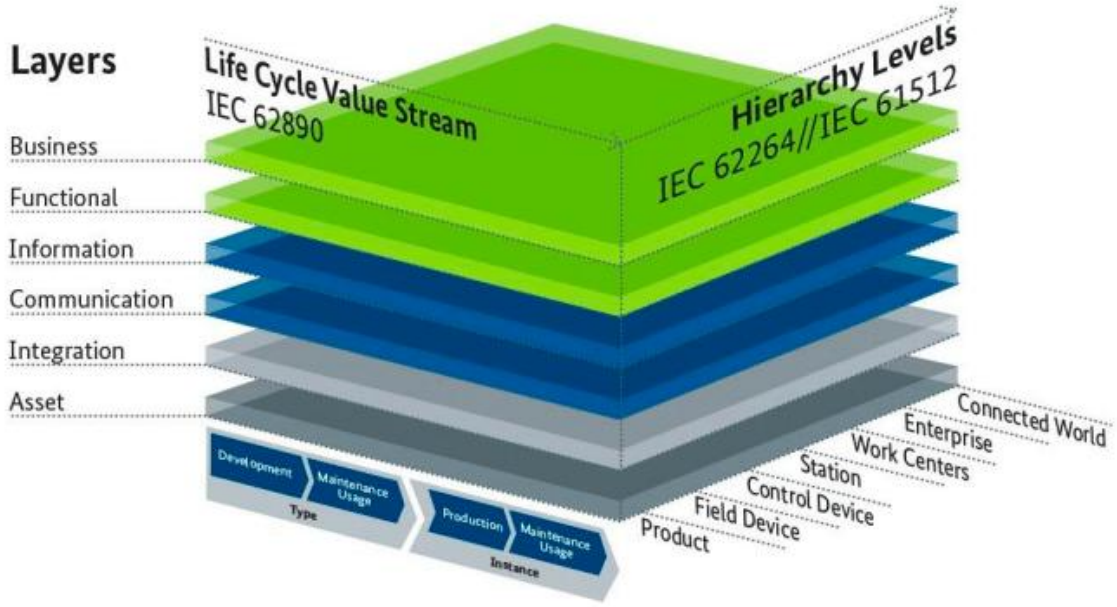
Hazai szinten, Magyarországon is felismerésre került ezen előnyök jelentősége, melynek eredményeként megalakult az Ipar 4.0 Nemzeti Technológiai Platform, támogatva a vállalatokat és kutatóintézeteket a digitalizációban. Kormányzati programok, mint például a Mintagyár projekt és a Modern Vállalkozások Programja szintén jelentősen hozzájárulnak a hazai cégek digitális fejlődéséhez.

1.2 Az okosgyárak szerepe az ipar 4.0-ban

Az okosgyár (smart factory) az Ipar 4.0 legkézzelfoghatóbb megtestesülése: olyan, teljes mértékben digitalizált termelési környezet, amely összekapcsolja a vállalat minden rétegét - a gépektől és munkaállomásoktól a vállalatirányítási rendszerig, s tovább a beszállítókig és a vevőig. Ezt a RAMI 4.0 architekturális modell háromdimenziós térképe írja le az 1. ábrán. Ez a termelési folyamatokat, a működési rétegeket és az életciklus-fázisokat egységes keretben rendezi. Az okosgyár, mint fogalom ennek a modellnek szinte implementációja, ahol a fizikai, az informatikai és az üzleti nézőpont zárt hurokba kerül. [1]

A World Economic Forum 'Lighthouse' programja alapján a vezető okosgyárak nem egyszerűen automatizált üzemcsarnokok: hanem adatvezérelt döntéshozatalt tesznek lehetővé az egész értéklánc mentén, a tervezéstől a logisztikáig. A hálózat 130-nál is több 'világítótorony' (Lighthouse) üzeme 20-30 %-os átlag termelékenység növekedést és akár 50 %-os CO_2 kibocsátás-csökkenést ért el a mesterséges intelligencia, a digitális ikerpárok és az end-to-end (E2E) integrációjával. [2]

Az okosgyárak egyik kulcsképessége a realtime (valós idejű) visszacsatolás: a szenzoradatokból, gépi látásból vagy valamely digitális ikerpárokból naplózott információk a felhő – edge párosra építve azonnal beavatkoznak a



1. ábra: RAMI 4.0 architektúra modell 3 dimenziós térképe [Publikus forrás], Plattform Industrie 4.0 and ZVEI. (https://www.researchgate.net/figure/RAMI-40-portrayed-by-Plattform-Industrie-40-and-ZVEI-2_fig1_353020204)

folyamatokba. Ez a „self-optimizing factory", azaz önmagát optimalizáló gyár koncepció egyszerre javít minőséget, csökkenti az állásidőt és a fajlagos energiafogyasztást is. [3]

A legmodernebb okosgyárakban a kiterjesztett valóság (Augmented Reality; AR) és együttműködő robotika támogatja a dolgozókat: a szerelők AR-szemüvegen keresztül kapnak utasításokat, a cobotok pedig biztonságosan dolgoznak mellettük. A kutatások szerint ez a human-machine együttműködés akár 15–25 %-kal is növelheti a folyamatok hatékonyságát és lerövidítheti a betanítási időt. [4], [5]

A digitalizált, átlátható folyamatok olyan adatvagyont termelnek, amelyre új szolgáltatások (predictive-maintenance-alapú szerviz, „gyártás-mint-szolgáltatás") építhetők. Emellett az energia-optimalizálás és a körforgásos anyagáramlás mérhetősége révén az okosgyár a vállalat fenntarthatósági céljainak első számú alkotóeleme is.

Az okosgyár nem pusztán a „digitalizált termelőcsarnok" szinonimája, hanem integrált üzleti és technológiai platform, amely egyszerre teremti meg a magas hozzáadott értéket, a gyors piaci alkalmazkodást, a fenntartható működést és a kibervédelmi kontrollok egységes érvényesítését az Ipar 4.0 korszakában.

1.3 A kiberbiztonság aktualitása és relevanciája

Az okosgyárak robbanásszerű terjedésével a kibertámadások száma és hatása is drasztikusan nőtt az OT/ICS (Operational Technology/Industrial Control System; üzemeltetési technológia/ipari irányítási rendszer) környezetekben. A Dragos 8. éves OT Cybersecurity Year in Review szerint 2024-ben 1 693 ipari zsarolóvírus-incidenst regisztráltak, ami 87 %-os növekedés 2023-hoz képest. Az esetek 75 %-a részleges, 25 %-a teljes termelésleállást eredményezett. A leginkább érintett ágazat továbbra is a gyártás (≈ 70 % az összes támadásból). [6], [7]

A Colonial Pipeline (2021) hatnapos leállása (≈ 4,4 milló USD váltságdíj, regionális üzemanyag-hiány) az egész világ figyelmét a fizikai infrastruktúrákat érintő kiberkockázatokra fordította. Hasonlóan, a Norsk Hydro alumínium-óriás 2019-es ransomware-esete 70 milló USD közvetlen kárt okozott, manuálisan kényszerültek fenntartani a termelést. [8], [9]

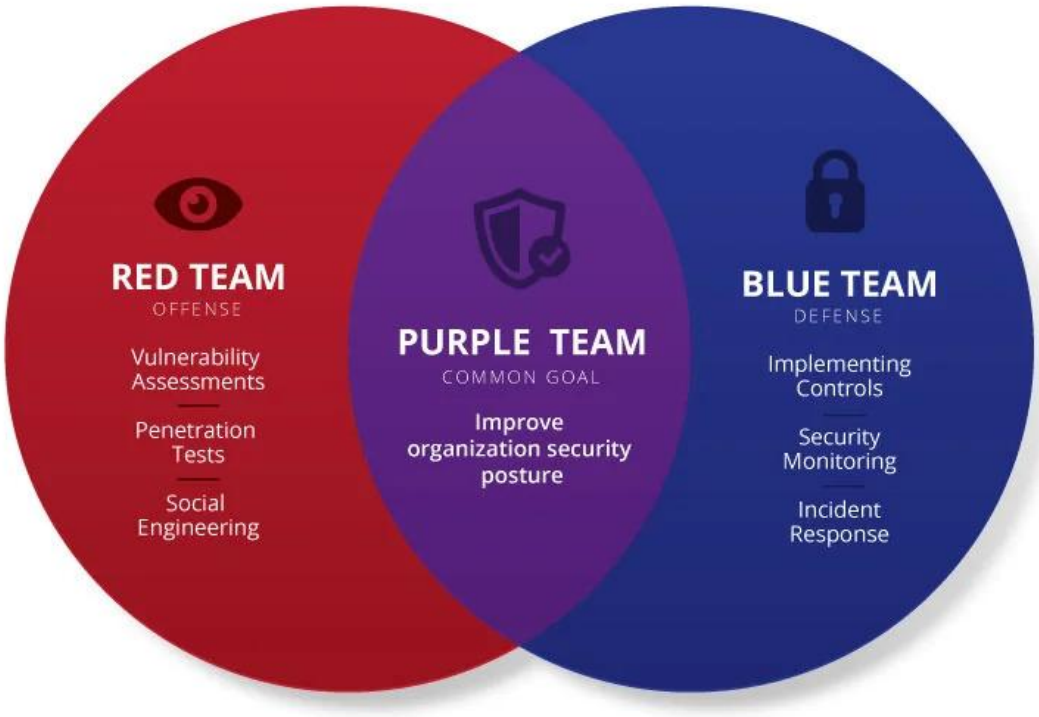
A 2024-ben kiadott nagyjából 600 OT-releváns incidens (Dragos elemzés) több, mint ötöde közvetlenül hálózaton keresztül kihasználható volt, miközben a gyártók 22 %-ban hibás kockázati besorolást adtak meg. A támadók egyre gyakrabban használják a VPN-eken (Virtual Private Network) és távelérésen keresztüli behatolási lehetőségeket. A kutatás rámutat, hogy a szigorú IT–OT szegmentációval rendelkező áldozatok gyorsabban álltak helyre, és jellemzően nem fizettek váltságdíjat. [10]

Az EU NIS2 irányelve alapján a magyar ipari szereplőknek is – különösen a jelentősebb besorolású cégeknek – IEC 62443-kompatibilis kontrollokat, incidens-jelentést és beszállítói kockázatkezelést kell bevezetniük, ellenkező esetben a forgalom 2 %-áig terjedő bírságot kockáztatnak. [11], [12]

A ransomware-ökoszisztéma növekszik: 2024-ben 80 aktív csoport célzott ipari szervezeteket, átlagosan 34 támadást indítva hetente. A motiváció a pénzügyi zsarolástól a működési szabotázsig tolódik (például hacktivisták vagy geopolitikai érdekek mentén), ami tovább erősíti a zero-trust, behatolás-észlelési (NDR/IDS) és offline mentési stratégiák szerepét.

A Dragos jelentés kiemeli az OT-biztonsági szakember-hiányt és a célzott adathalász-kampányok növekedését; a vállalatoknál az éves képzések és purple team (2. ábra) gyakorlatok bizonyultak a legköltséghatékonyabb védelmi intézkedésnek. Szemben a red vagy blue teamekkel. [10]

Az ipari digitalizáció és az okosgyár-projektek értéke csak megfelelő védelmi intézkedések mellett realizálható. A kiberbiztonság tehát nem kiegészítő, hanem alapfeltétel: nélkülözhetetlen az adatintegritás, a folytonos termelés és a szabályozói megfelelés biztosításához az Ipar 4.0 környezetében.



2. ábra: The fusion of blue and red teams into purple. [Publikus forrás], (https://whiterookcyber.com.au/wp-content/uploads/2024/08/Purple-Team-Image.webp)

2 OKOSGYÁRAK TECHNOLÓGIAI HÁTTERE

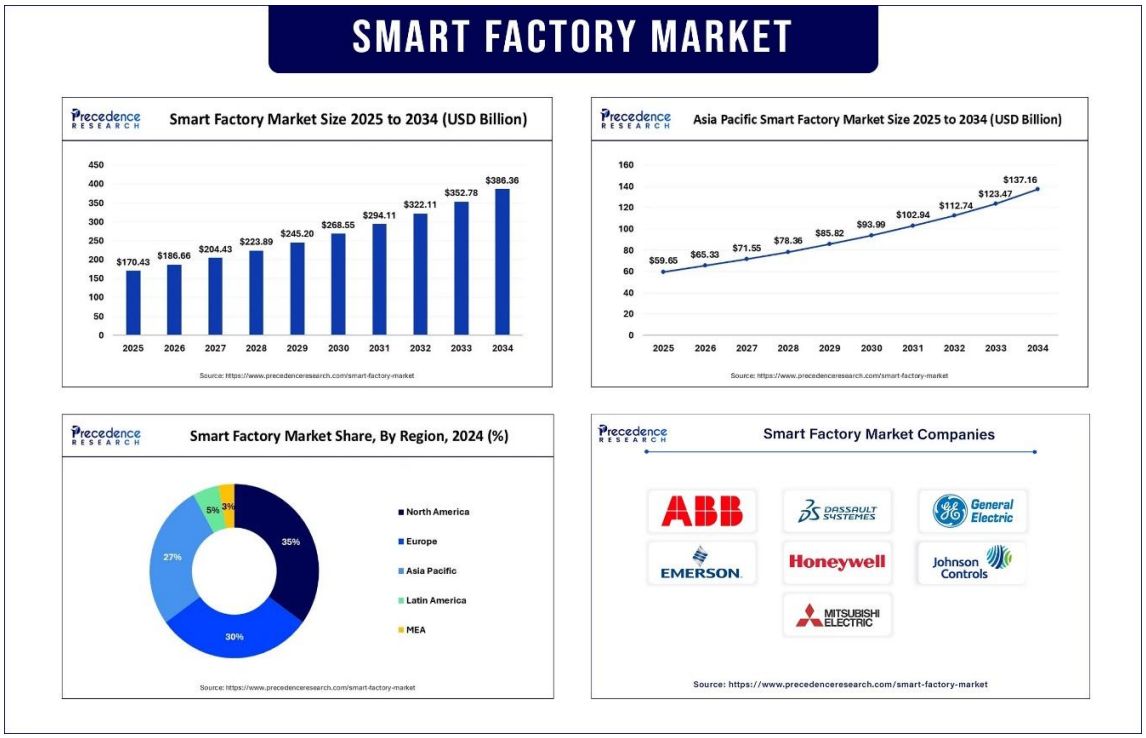
Az okosgyárak egy többrétegű (1. táblázat), egymást kiegészítő technológiák ökoszisztémáján alapuló rendszerek: az érzékelőszinttől (IoT) kezdve a valós idejű folyamatvezérlésen (SCADA/PLC) és a gyártás-végrehajtáson (MES) át egészen a vállalatirányításig (ERP). A következő alfejezetek ezeket a rétegeket, az IT- és OT-terület összefüggéseit, valamint a digitalizációval együtt növekvő fenyegetettségeket tekintik át.

2.1 IoT, M2M, SCADA, PLC, MES, ERP rendszerek

1. táblázat: Okosgyárak technológiai rétegei

Réteg	Funkció	Tech. / Protokoll	Speciális alkalmazás
Érzékelők	Fizikai állapot mérése	M2M üzenetküldés (MQTT)	Valós idejű anomáliadetektáláshoz
Vezérlő	Realtime folyamatirányítás	PLC	Hardverszintű biztonság
Felügyelet	Adatgyűjtés	SCADA	Web-alapú dashboardok
Végrehajtás	Minőségkövetés	MES	AI-vezérelt ütemező, AR-támogatás
Tervezés	Készlet, Pénzügy	ERP	Felhő-alapú mikroszervíz-architektúra

Az IIoT-szenzorok valós idejű adatfolyamot biztosítanak, ami a PLC / SCADA rétegen történő determinista szabályozás alapja. A Siemens-hez tartozó Thought-Leadership podcast alapján a gép–gép (M2M) kommunikáció MQTT-re és OPC UA PubSub-ra vált, mert ezek alacsony késleltetésű és titkosítható csatornákkal dolgoznak. A gyártósor feletti MES már nemcsak műveleti naplót vezet, hanem prediktív algoritmusokkal állítja elő az optimális sorrendet és a digitális ikerben validált paramétereket, mielőtt az információkat a PLC-k felé továbbítja. A legfelső rétegben lévő ERP/PLM szolgáltatások ma már felhő-alapú mikroszervizekké alakultak, hogy valós idejű készlet- és energiaadatokat kapjanak vissza a shop-floorról. Így zárul be a data-driven körforgás a tervezéstől a gyártásig és vissza – ez az end-to-end transzparencia az okosgyár versenyelőnyének alapja, ahogy az a 3. ábrán látható. [13]



3. ábra: Smart Factory Market Revenue Attain [Publikus forrás] precedenceresearch.com (https://www.precedenceresearch.com/insightimg/smart-factory-market-revenue.webp)

2.2 IT-OT konvergencia

Az IT (információ-technológia) rendszerek – adatközpontok, hálózatok, ERP – és az OT (üzemi technológia) rendszerek (PLC, SCADA, DCS) korábban széttagolt, eltérő életciklussal és kockázatkezeléssel működtek. Az Ipar 4.0 hatására a kettő közti határ elmosódik: a cél a közös adatmodell, közös irányítási elvek, és végső soron a vállalati szintű optimalizálás.

Üzleti előnyök:

- Valós idejű döntéstámogatás a teljes értékláncon (OEE → ERP).
- Karbantartási költség: 20–40 %-kal csökken az előrejelző modellek miatt. [13]
- Hibakeresési idő 30 % a közös láthatóság következtében secomea.com. [14]

Kihívások:

- Eltérő élettartam: a PLC több, mint 15 évig, a tűzfal 3–5 évig élhet.
- Legacy protokollok: Modbus/TCP, Profibus – hitelesítés nélküliek.
- Szervezeti változás: IT → CIA-háromszög, OT → safety & availability.

A Siemens amberg-i elektronikai gyára 2017-ről 2024-re 35-ről több, mint 400 új IT-OT integrált use-case-t aktivált: a kapacitáskihozatalt 17 %-kal, az energiaköltséget 14 %-kal csökkentette. [13]

2.3 Fenyegetettségi vektorok növekedése

1. Ransomware specializálódás: 2024-ben 87 %-kal több OT-specifikus zsarolóvírus-incidens történt, két új, kizárólag ipari rendszereket célzó csoport azonosításával. [15]
2. Internetnek kitett eszközök: Shodan/Censys lekérdezések szerint a támadók főként nyílt VPN-kapukon és más távelérési megoldásokon jutnak be; az ICS-eszköz-listázás alkalmi támadásokká fajul. [16]
3. Ellátási lánc és harmadik fél: Integrált MES és felhő-API-k sebezhetőségeinek kihasználása (pl. log4shell örökölt könyvtár a HMI-ben) új típusú „indirekt" vektort jelent.
4. „Living-off-the-Land" OT parancsok: a támadók legitim PLC-parancsokat futtatva kerülik el a klasszikus IDS-szignatúrákat; a Dragos szerint az ilyen műveletek felismeréséhez protokoll-szintű, deep-packet ML-analitika szükséges. [15]
5. Villámgyors támadási ciklus: a Secureworks 2024-es jelentésében a legrövidebb megfigyelt OT-ransomware „dwell time" kevesebb, mint 7 óra volt, ami erőteljesen lerövidíti az észlelésre és elszigetelésre rendelkezésre álló időt. [17]

A növekvő támadási felület és a gyorsuló támadások miatt „shift-left" biztonság tervezésre, szegmentált hálózati architektúrára, protokoll-szintű és AI-alapú behatolás-észlelésre van szükség már a technológiai háttér tervezésének korai fázisában. Másképp a modern támadások ellen nem lehet hatékonyan fellépni.

3 KIBERTÁMADÁSOK AZ IPARBAN

Az ipari környezeteket érő támadások mára a klasszikus vírusokból fejlődtek – ma már célzottan az üzemi technológiát (OT) veszik célba, fizikai leállást vagy akár kárt is okozva. Az alábbi két alfejezet összefoglalja a legjellemzőbb támadástípusokat és néhány, iparági mércével is emlékezetes esettanulmányt. A jellemző támadások láthatók a 2. táblázatban.

3.1 Jellemző támadások

2. táblázat: Jellemző támadási formák

Kategória	Cél / Hatás	Tipikus vektor	Megjegyzés
Ransomware	Folyamatleállás, zsarolás	VPN, RDP, email-phising	2024-ben közel 1700 incidens (dragos.com)
ICS-specifikus kártevő	Közvetlen fizikai bevatakozás (Pl. áramszünet)	PLC-protokoll-manipuláció	Stuxnet, Industroyer
Ellátási-lánc kompromittálás	Kiskapuk kihasználása üzemi szoftverekben	Frissítési csatorna, harmadik feles adatbázis	SolarWinds, log4shell-örökség
Phising	Távoli hozzáférés ellopott bejelentkezési adatokkal	Célzott spear-phish, MFA-spray	Colonial Pipelinde
„Living-off-the Land"	Lopakodó folyamat-módosítás	Legitim PLC-funkciók (write coils / force outputs)	Klasszikus IDS-szignatúrákkal nehezen érthető

[18], [19]

Az ipari rendszereket érintő leggyakoribb támadástípusok közül kiemelkedő jelentőségű a zsarolóvírusok (ransomware) terjedése, amelyek ipari hálózatokat, gyártósorokat képesek megbénítani, súlyos pénzügyi károkat okozva. 2024-ben a Dragos jelentése szerint 1693 ipari ransomware-incidens történt világszerte, ami 87%-os növekedést jelent az előző évhez képest. Ezek az incidensek többségében VPN hozzáféréseken, valamint célzott adathalász kampányokon keresztül kezdődnek, majd az IT-hálózatokról átterjedve elérik az OT-környezeteket is, így akár teljes termelési leállást okozhatnak.

Az iparban kiemelten veszélyesek a kifejezetten üzemi-környezetek ellen fejlesztett rosszindulatú programok (ICS-specifikus malware), amelyek a PLC-k, SCADA-rendszerek és egyéb vezérlőegységek manipulálására alkalmasak. Ilyen volt például a Stuxnet, amely az iráni urándúsító centrifugák működésébe avatkozott be, vagy az Industroyer, amely az ukrán energiahálózatot bénította meg IEC 104-es protokollüzenetek módosításával. [20]

Egyre nagyobb figyelmet kapnak az ellátási láncon (supply chain) keresztül végrehajtott támadások is. Itt a támadók a szoftverfrissítési folyamatok kompromittálásával, hátsó ajtókat, kiskapukat elhelyezve fertőznek meg ipari vezérlőrendszereket. Az ilyen támadások különösen nehezen észlelhetők, mivel a fertőzés közvetlenül a gyártótól származó legitimnek tűnő frissítések formájában érkezik, mint ahogy az történt a SolarWinds incidensben is. [21]

Emellett fontos megemlíteni a „Living-off-the-Land" (LotL) jellegű támadásokat is, amelyek során a támadók nem külső malware-t használnak, hanem a már meglévő, legitim ipari eszközök parancsait futtatva okoznak károkat. Az ilyen támadásokat rendkívül nehéz felismerni, mivel klasszikus IDS/IPS rendszerek nem mindig képesek detektálni a legitim műveleteket utánzó rosszindulatú parancsokat, utasításokat.

3.2 Valós példák

Az alábbi, 3. táblázatban látható néhány jelentősebb támadás az elmúlt másfél évtizedből. A fejezet további részében ezek kerülnek bemutatásra.

3. táblázat: Néhány jelentősebb támadás a múltból

Év	Esemény	Iparág	Leírás
2010	Stuxnet	Urándúsító centifugák	PLC-ket célzó worm; Több, mint 100 centrifuga tönkretétele
2016/'22	Industroyer	Ukrán áramszolgáltató	IEC 104-parancsokkal áramszünet
2017	Triton	Kőolaj-feldolgozás	SIS-vezérlő átírása → robbanásveszély
2019	Norsk Hydro	Alumínium-ipar	Leállt az automatizált termelés
2021	Colonial Pipeline	Üzemanyag-vezeték	6 napos leállás, keleti parti üzemanyaghiány
2021	JBS Foods	Élelmiszer-feldolgozás	Észak-Amerikai húsellátási problémák
2024	OT-ransomware hullám	Gyártás, energia	Közel 1700 dokumentált incidens, gyártás 70%-ban érintett.

Az ipari kibertámadások jelentőségét és súlyát jól szemléltetik a valóságban bekövetkezett nagy horderejű incidensek. Ezek közül az első kiemelkedő eset a Stuxnet (2010), amely iráni urándúsító létesítményekben lévő PLC-k vezérlését módosítva több ezer centrifugát tett működésképtelenné, ezáltal komoly geopolitikai következményeket is maga után vonva.

Hasonlóan súlyos támadás volt az Industroyer (2016 és 2022), amely az ukrán áramellátási infrastruktúrát vette célba. Ez az ICS-specifikus malware IEC 104-es protokollon keresztül küldött legitimnek látszó, de káros parancsokkal okozott regionális áramszüneteket, bizonyítva, hogy a kibertérben végrehajtott támadásoknak közvetlen fizikai következményei lehetnek.

A Triton (2017) esete szintén mérföldkő volt: elsőként vette célba közvetlenül az ipari biztonsági vezérlőrendszereket (Safety Instrumented Systems - SIS), amelyek feladata éppen az emberi élet védelme. A támadás a célzott szaúd-arábiai petrolkémiai létesítményben potenciálisan életveszélyes állapotot teremthetett volna, ha időben nem észlelik. [22]

A Norsk Hydro (2019) incidensében a LockerGoga ransomware világszerte lebénította a norvég alumíniumgyártó vállalat működését. Bár a gyárak tovább működhettek manuális üzemmódban, a támadás így is 40-52 millió USD közötti anyagi kárt okozott, nem beszélve a hosszútávú reputációs károkról. [9]

Az Amerikai Colonial Pipeline (2021) esete is emlékezetes: a DarkSide ransomware csoport egyetlen kompromittált VPN-hozzáféréssel hat napra leállította az Egyesült Államok keleti partjának egyik legfontosabb üzemanyag-vezetékét, ezzel hatalmas társadalmi és gazdasági zavart okozva, továbbá globális figyelmet irányítva az ipari infrastruktúrák kibervédelmének fontosságára. [8]

Végül a JBS Foods (2021) élelmiszeripari óriás elleni ransomware támadás is bizonyította, hogy a kibertámadások nemcsak közvetlen ipari szektorokat, hanem az ellátási lánc létfontosságú elemeit is képesek súlyosan érinteni, ebben az esetben pedig élelmiszer-ellátási problémákat okozott Észak-Amerikában.

4 KIBERBIZTONSÁGI MEGOLDÁSOK OKOSGYÁRAKBAN

Az ipari környezeteket érintő kibertámadások súlyosságának növekedése és az IT-OT rendszerek integrációjából fakadó kockázatok miatt a megfelelő biztonsági intézkédesek kialakítása és fenntartása elengedhetetlen. Az alábbi alfejezetek részletesen bemutatják azokat a technikákat, amelyek a modern okosgyárakban alapvető fontosságúak a hatékony védekezés érdekében.

4.1 Hálózati szegmentálás és zónázás

A hálózati szegmentálás és zónázás az ipari rendszerek kibervédelmének alapvető eszköze, amelynek célja a támadások során elérhető eszközök számának minimalizálása, valamint a kockázatok csökkentése a különböző üzemi területek izolációjával. A hálózati infrastruktúra zónákra osztásával elkerülhető, hogy egyetlen sérült eszköz vagy hálózati szegmens kompromittálása teljes rendszerleállást okozzon.

Az ISA/IEC 62443 szabvány javaslata alapján az ipari hálózatokat három fő rétegbe szervezik:

- Üzemi zóna (Operational Zone): Közvetlenül termelést végző eszközök (pl. PLC, RTU, szenzorok).
- Felügyeleti zóna (Supervisory Zone): SCADA rendszerek, operátori munkaállomások, MES alkalmazások.
- Vállalati zóna (Enterprise Zone): ERP rendszerek, irodai IT alkalmazások, központi adatbázisok.

Ezek a zónák fizikailag vagy logikailag elkülönített hálózati szegmensekben működnek, köztük szigorú szabályok szerint konfigurált tűzfalak végzik a kommunikáció ellenőrzését, minimalizálva a jogosulatlan adatforgalmat.

A gyakorlatban a hálózati zónázás további finomítása érdekében kisebb biztonsági domének (Security Domains) kialakítása is javasolt, amelyek szigorúan kontrollált kapcsolatokat tartanak fenn egymással. Ezáltal hatékonyan korlátozható a támadások terjedése horizontálisan (azonos zónán belül) és vertikálisan (különböző zónák között).

A hálózati szegmentálás sikeressége érdekében rendszeres auditokat kell végezni, melyek során ellenőrzik a tűzfalszabályok megfelelőségét, valamint az izoláció tényleges érvényesülését. Ezek az intézkedések jelentősen javítják a rendszer ellenálló képességét a célzott kibertámadásokkal szemben. [23]

4.2 Tűzfalak, IDS/IPS rendszerek

A tűzfalak, behatolás-észlelő (Intrusion Detection System – IDS) és behatolás-megelőző (Intrusion Prevention System; IPS) rendszerek kulcsfontosságú szerepet töltenek be az ipari hálózatok biztonságában. A hagyományos tűzfalak mellett speciális, ipari protokollokat értelmező tűzfalak (Industrial Firewalls) alkalmazása elengedhetetlen. Ezek képesek mélységi csomagelemzésre (Deep Packet Inspection; DPI), amellyel felismerhetik az ipari protokollok, például Modbus, OPC UA, Ethernet/IP szabványoktól eltérő, rosszindulatú parancsait is.

Az IDS/IPS rendszerek valós idejű hálózati forgalomelemzésen alapulnak, és képesek riasztásokat küldeni vagy blokkolni az olyan műveleteket, amelyek nem felelnek meg a normál üzemi viselkedésnek. Az ipari IDS-ek gépi tanulással támogatott anomáliaészlelést alkalmaznak, ami lehetővé teszi, hogy felismerjék az OT-környezetben szokatlan viselkedéseket, például PLC-k jogosulatlan újraprogramozását, vagy szokatlan protokollhasználatot.

A korszerű rendszerek képesek integrálódni az IT-biztonsági rendszerekkel (pl. Security Information and Event Management; SIEM), így átfogóbb képet adva az OT és IT biztonsági eseményekről. A tűzfalak és IDS/IPS megoldások megfelelő konfigurációja és folyamatos monitorozása kulcsfontosságú a hatékony ipari biztonság fenntartásához.

4.3 Végpontvédelem és eszközfelügyelet

A végpontvédelem az ipari hálózatok egyik legsérülékenyebb pontján nyújt védelmet: magán az eszközökön (PLC, HMI, PC-k). Az ipari végpontvédelem jellemzően magában foglalja az alkalmazáskontrollt, amely lehetővé teszi, hogy kizárólag engedélyezett programok és firmware verziók fussanak az eszközökön (Application Whitelisting).

Az eszközfelügyeleti (Asset Management) rendszerek automatikusan felfedezik és katalogizálják a hálózatban működő valamennyi ipari eszközt, azok konfigurációját, verzióit, szoftverállapotát. Ezek az eszközök biztosítják a teljes láthatóságot és valós idejű monitorozást, így képesek azonnal jelezni bármilyen jogosulatlan változtatást vagy csatlakoztatást, például ismeretlen USB eszköz csatlakozását vagy illetéktelen programok telepítését.

A végpontvédelem és eszközfelügyelet további fontos elemei a folyamatos frissítések és patch menedzsment, amelyek segítenek elkerülni a rendszeres biztonsági réseket okozó sebezhetőségeket.

4.4 ICS/SCADA – specifikus védelmi technikák

Az ICS/SCADA rendszerek specifikus védelmi megoldásokat igényelnek, amelyek figyelembe veszik az ipari környezet sajátosságait. Ezek közé tartoznak a következők:

- Whitelisting technológiák: Ezek lehetővé teszik, hogy kizárólag előre jóváhagyott műveletek lehessen csak végrehajthatók a vezérlőeszközökön, így blokkolva a jogosulatlan beavatkozásokat.
- Secure Remote Access (Biztonságos Távoli Hozzáférés): Távoli karbantartásokhoz speciális, erősen autentikált, titkosított kommunikációs csatornákat biztosít, valamint részletes naplózást végez minden távoli kapcsolatról.
- Adatsűrűség-alapú anomáliaészlelés: Az üzemi folyamatok megszokott viselkedésétől való eltérések automatikus felismerése, például szokatlan paraméterek vagy üzemállapotok detektálása révén.
- Digitális ikrek (Digital Twins): A fizikai berendezések pontos virtuális modelljei, amelyek lehetővé teszik a biztonsági intézkedések, konfigurációk és potenciális támadások virtuális szimulációját és ellenőrzését a valós implementáció előtt.

Emellett speciális protokollvédelmi megoldások is elérhetőek, amelyek kifejezetten ICS protokollokat, mint például Modbus, Ethernet/IP vagy OPC UA forgalmát elemzik, és képesek detektálni a protokoll szabályait megsértő parancsokat vagy manipulációkat.

Az ICS-specifikus megoldások jelentősége az, hogy képesek hatékonyan kezelni az ipari vezérlőrendszerek egyedi biztonsági kihívásait, például a PLC-k korlátozott biztonsági lehetőségeit, vagy a speciális, alacsony késleltetésű kommunikáció igényeit, így közvetlenül növelik az ipari rendszerek biztonságát és az üzembiztonságot. [24]

5 A ZERO TRUST MODELL AZ IPARBAN

A Zero Trust modell (nulla bizalom elve) egy biztonsági ajánlás, módszer, mely alapjaiban változtatja meg a kibervédelmi megközelítéseket az ipari rendszerekben. Alapvetése, hogy mindent potenciális veszélyforrásként kezel, ebből kifolyólag minden felhasználó, eszköz és hálózat folyamatos ellenőrzést igényel. Az így kialakított architektúra kiváltképp fontos az okosgyárakban, ahol a hagyományos biztonsági rendszerek és módszerek már nem elegendők.

5.1 Elvek

1. **Minden adatforrás és számítástechnikai szolgáltatás erőforrásnak minősül**:
   Egy hálózat több féle eszközosztályból is állhat. A hálózat tartalmazhat kis helyigényű eszközöket is, amelyek adatokat küldenek aggregátoroknak/tárolóknak, szoftver, mint szolgáltatás (Software as a Service; SaaS), rendszereket, amelyek utasításokat küldenek az aktuátoroknak, és egyéb funkciókat. A vállalat dönthet úgy is, hogy a személyi tulajdonú eszközöket erőforrásnak minősíti, ha azok hozzáférhetnek a vállalati tulajdonú erőforrásokhoz.
2. **Minden kommunikáció a hálózat helyétől függetlenül biztosított**:
   A hálózati hely önmagában nem jelent bizalmat. A vállalati tulajdonú hálózati infrastruktúrán (pl. egy régi hálózati peremterületen) található eszközökből érkező hozzáférési kérelmeknek ugyanolyan biztonsági követelményeknek kell megfelelniük, mint a nem vállalati tulajdonú hálózatokból érkező kérelmeknek és kommunikációnak. Más szóval, a bizalom nem adható meg automatikusan az alapján, hogy az eszköz a vállalati hálózati infrastruktúra része. Minden kommunikációnak a rendelkezésre álló legbiztonságosabb módon kell történnie, védenie kell a titkosságot és az integritást, és biztosítania kell a forrás hitelesítését.
3. **Az egyes vállalati erőforrásokhoz való hozzáférést munkamenetenként kell biztosítani**:
   A hozzáférés engedélyezése előtt ki kell értékelni a bizalmat. A hozzáférést a feladat elvégzéséhez szükséges legkevesebb jogosultsággal kell megadni. Csak az egyik erőforrás hitelesítése és engedélyezése nem biztosít automatikusan hozzáférést egy másik erőforráshoz. Minden szükséges erőforrást hitelesíteni kell. Ezen felül a munkamenet megkezdése előtt nem szabad hozzáférést biztosítani, még akkor sem, ha már korábban ez megtörtént.
4. **Az erőforrásokhoz való hozzáférést dinamikus irányelvek határozzák meg - beleértve az ügyfél identitásának, az alkalmazásnak/szolgáltatásnak és a kérelmező eszköznek a megfigyelhető állapotát, és tartalmazhatnak a egyéb viselkedési és környezeti jellemzőket is**:
   Egy szervezet úgy védi az erőforrásait, hogy meghatározza, milyen erőforrásokkal rendelkezik, kik a férnek hozzá (vagy képesek hitelesíteni a felhasználókat egy csoportban), és milyen hozzáférésre van szükségük az erőforrásokhoz ezeknek a tagoknak. Nulla bizalom esetében az ügyfél-identitás magában foglalhatja a felhasználói fiókot (vagy szolgáltatás-identitást) és a vállalat által az adott fiókhoz rendelt bármely kapcsolódó attribútumot vagy az automatizált feladatok hitelesítésére szolgáló eszközöket. A lekérdező eszköz állapota magában foglalhatja az eszköz jellemzőit, például a telepített szoftververziókat, a hálózat helyét, a lekérdezés időpontját/dátumát, a korábban megfigyelt viselkedést és a telepített hitelesítő adatokat. A viselkedési attribútumok közé tartoznak többek között, de nem kizárólagosan, az automatizált elemzések, az eszközelemzések és a megfigyelt használati mintáktól való eltérések. A házirend azon attribútumokon alapuló hozzáférési szabályok összessége, amelyeket a szervezet egy alanyhoz, adateszközhöz vagy alkalmazáshoz rendel. A környezeti attribútumok közé tartozhatnak olyan tényezők, mint az igénylő hálózat helye, az idő, a bejelentett aktív támadások, stb. Ezek a szabályok és attribútumok az üzleti folyamat igényein

és az elfogadható kockázati szinten alapulnak. Az erőforrás-hozzáférési és műveleti engedélyezési szabályok az erőforrás/adatok érzékenysége alapján változhatnak. A legkisebb jogosultság elvét alkalmazzák a láthatóság és a hozzáférhetőség korlátozására.

5. **A vállalat figyelemmel kíséri és méri a tulajdonában lévő és a kapcsolódó eszközök integritását és biztonsági helyzetét**:
   Egyetlen eszköz sem megbízható. A vállalkozás az erőforrásigény elbírálásakor értékeli az eszköz biztonsági helyzetét. A Zero Trust-ot bevezető vállalkozásnak folyamatos diagnosztikai és kárenyhítési vagy hasonló rendszert kell létrehoznia az eszközök és alkalmazások állapotának nyomon követésére, és szükség szerint a karbantartásokat kell tartania. Azokat az eszközöket, amelyekről kiderül, hogy elavultak, ismert sebezhetőségekkel rendelkeznek és/vagy nem a vállalat kezeli őket, másként kezelhetik beleértve a vállalati erőforrásokhoz való minden kapcsolat megtagadását), mint a vállalat tulajdonában lévő vagy a vállalathoz kapcsolódó eszközöket, amelyek a legbiztonságosabb állapotukban vannak. Ez vonatkozhat a kapcsolódó eszközökre is (pl. a személyes tulajdonú eszközökre), amelyek bizonyos erőforrásokhoz hozzáférhetnek, másokhoz viszont nem. Ehhez is szükség van egy megbízható felügyeleti és jelentési rendszerre, amely a vállalati erőforrások aktuális állapotáról adatokat szolgáltat.
6. **Minden erőforrás-hitelesítés és engedélyezés dinamikus, és a hozzáférés engedélyezése előtt szigorúan érvényesül**:
   Ez egy állandó körforgás: hozzáférés megszerzése, a fenyegetések feltérképezése és értékelése, alkalmazkodás, valamint a folyamatos kommunikáció során a bizalom újbóli felülvizsgálata. Egy ZTA-t (Zero Trust Architecture) bevezető vállalatnál elvárás, hogy működjön Identity, Credential and Access Management (ICAM)-, illetve eszközmenedzsment-rendszer. Ide tartozik a többtényezős hitelesítés (MFA) alkalmazása a vállalati erőforrások egy részéhez vagy egészéhez való hozzáféréskor. A felhasználói tranzakciók alatt folyamatos a monitorozás; szükség esetén újrahitelesítés és újraengedélyezés történik, amelyet a szabályzat határoz meg és érvényesít — például időalapú feltételek, új erőforrás igénylése, erőforrás-módosítás vagy rendellenes felhasználói tevékenység észlelése esetén. A cél a biztonság, a rendelkezésre állás, a használhatóság és a költséghatékonyság egyensúlyának megteremtése.
7. **A vállalat a lehető legtöbb információt gyűjti a eszközök, a hálózati infrastruktúra és a kommunikáció jelenlegi állapotáról, és ezeket felhasználja a biztonsági helyzetének javítására**:
   A vállalkozásnak adatokat kell gyűjtenie az eszközök biztonsági helyzetéről, a hálózati forgalomról és a hozzáférési kérelmekről, fel kell dolgoznia ezeket az adatokat, és a megszerzett információkat szabályzatok létrehozására és érvényesítésére, karbantartásra kell felhasználnia. Ezek az adatok arra is felhasználhatók, hogy az alanyok hozzáférési kérelmeihez kontextust biztosítsanak. [25]

5.2 Implementációs kihívások

Annak ellenére, hogy a Zero Trust alapú megközelítés komoly biztonsági előnyökhöz juttathat, implementációja számos kihívással járhat. Ugyanakkor megfelelő tervezéssel, folyamatos üzemeltetéssel hosszú távon komoly és fenntartható előnyöket biztosít. Lehetővé teszi a legkifinomultabb kibertámadások elleni sikeres védekezést:

- **Régi rendszerek kompatibilitása**: Az üzemi környezetben használt PLC-k és SCADA rendszerek, illetve más vezérlőberendezések akár több éves, évtizedes technológiákat alkalmaznak, melyek nem támogatják az elvárt, modern titkosítási és hitelesítési módszereket. Ez a probléma valamilyen köztes eszközzel, gateway-jel hidalható át.

- **Teljes eszközállomány leltározása és láthatósága a hálózaton**: Gyakran előfordul, hogy a gyártósorok, az ipari eszközök vagy érzékelők egy része nincs megfelelően dokumentálva és nem is ismerhető fel a hálózaton. Ez pedig szükséges feltétele az architektúra kialakításának. A katalogizálás és a monitorozás jelentős erőforrásokat igényelhet.
- **Üzemelteltés**: A Zero Trust megközelítés bevezetése jelentősen növeli a hálózat forgalmát, többletterhelést jelent. Ennek oka a sok komplex biztonsági szabály. Ügyelni kell a hálózat stabilitására és a késleltetés minimalizálásra az ellenőrző mechanizmusok megfelelő működése érdekében, hiszen ezek valós idejű (realtime) működést igényelnek.
- **Magas bevezetési és üzemeltetési költségek**: Egy ilyen összetett rendszer bezetése és fenntartása fejlett infrastuktúrát és stabil, megbízható hálózatot igényel. Ez óriási költségekkel járhat.

6 FOLYAMATOS MONITOROZÁS ÉS ANOMÁLIADETEKTÁLÁS

Az okosgyárak védelme nem korlátozódhat kizárólag megelőző intézkedésekre: az összetett, dinamikusan változó fenyegetések és az egyre kifinomultabb támadási módszerek miatt alapvető fontosságú a folyamatos monitorozás és az automatizált anomáliadetektálás. Ezek biztosításához speciális technológiai megoldások, például SIEM, SOAR és mesterséges intelligencia alapú analitikai rendszerekre van szükség.

6.1 SIEM és SOAR rendszerek

SIEM (Security Information and Evenet Management)

A SIEM rendszerek elsődleges célja, hogy hogy különböző forrásokból, például hálózati eszközökből, származó naplóadatokat és eseményeket egy központi platformon gyűjtsék és elemezzék. Előnyei:

- **Központi naplózás**: Egyesíti a különböző forrásokból származó logokat, majd ezek alapján logikai összefüggéseket hoz létre. Például azonosítja, ha egy operátor távoli elérése után egy PLC beállításai módosultak.
- **Automatizált eseményriasztások**: Képes a rendszer előre definiált események bekövetkezésekor azonnali riasztást küldeni. Például üzemidőn kívül történik egy bejelentkezés.

Compliance és jelentéskészítés: Az ilyen rendszerek segítenek a szabványok és jogszabályi kötelezettségek betartásában és automatikusan generál audit jelentéseket.

SOAR (Security Orchestration, Automation and Response)

A SOAR technológia a SIEM rendszerek kiegészítéseként képesek valós idejű, automatizált válaszlépéseket is végrehajtani. Előnyei:

- **Automatizált incidenskezelés**: Képesek automatizált workflow-k segítségével válaszokat adni egy-egy biztonsági eseményre. Például egy gyanús PLC-forgalom detektálása után automatikusan elkülönítheti a kérdéses eszközt, vagy blokkolhatja a hálózati kommunikációját.
- **Integráció különböző biztonsági eszközökkel**: API-kon keresztül integrálódnak különböző biztonsági eszközökkel, tűzfalakkal, IDS/IPS rendszerekkel és végpontvédelmi megoldásokkal, lehetővé téve egy egységes, gyors válaszadás automatizálását.

Visszacsatolás és tanulás: Folyamatosan elemzi a válaszlépések eredményeit, amelyek alapján a jövőbeni incidenskezelési folyamatok finomhangolhatók. [26]

6.2 AI/ML alapú analitika

Az ipari környezetekben használt mesterséges intelligencia (AI) és gépi tanulás (ML) alapú analitikai megoldások képesek automatikusan felismerni azokat a viselkedési mintákat, amelyek biztonsági incidensekre utalhatnak.

Viselkedés-alapú anomáliaészlelés: Az AI/ML alapú rendszerek folyamatosan figyelik a hálózati és eszközszintű viselkedési mintákat, majd gépi tanulási algoritmusokkal meghatározzák, hogy milyen viselkedés számít normálisnak, és mi jelent anomáliát. Példák ilyen anomáliákra:

- **PLC-parancsok szokatlan sorozata:** Egy támadó által módosított PLC-program vagy jogosulatlan beavatkozás gépi tanulás segítségével felismerhető, mivel a rendszer eltérést észlel a megszokott működéshez képest.
- **Szokatlan hálózati kommunikáció:** AI-alapú elemzés detektálhatja, ha egy eszköz – például egy HMI panel – váratlanul nagy mennyiségű adatot kezd továbbítani külső hálózatok felé.

Előrejelző biztonsági analitika: Prediktív elemzéssel a rendszer képes előre jelezni a potenciális kockázatokat és fenyegetéseket:

- **Veszélyeztetett eszközök azonosítása:** A mesterséges intelligencia folyamatosan értékeli az egyes eszközök sérülékenységét és kockázatát, lehetővé téve a proaktív biztonsági intézkedéseket.
- **Kockázat-alapú priorizálás:** Az AI-alapú analitika képes rangsorolni az incidenseket és biztonsági eseményeket azok potenciális hatása szerint, így a biztonsági csapat hatékonyabban koncentrálhat a kritikus fontosságúakra.

Az AI/ML alapú biztonsági analitika képes az OT és IT rendszerekből érkező adatokat együttesen elemezni. Az így kialakított kép lehetővé teszi, hogy pontosabban lássák az átfogó kockázati helyzetet.

7 SZABVÁNYOK ÉS TANÚSÍTVÁNYOK

Az ipari kiberbiztonság hatékony fenntartása érdekében a gyáraknak nem elegendő csupán a technikai és folyamat-alapú intézkedéseket alkalmazniuk. Fontos, hogy ezek az intézkedések összhangban legyenek olyan nemzetközileg elfogadott szabványokkal, irányelvekkel és tanúsítványokkal, amelyek keretet adnak a kiberbiztonsági tevékenységeknek. Az ipari környezetek számára ezek meghatározzák a biztonsági követelményeket, iránymutatásokat nyújtanak a megvalósításhoz és lehetővé teszik a biztonság mérését, auditálását és tanúsítását.

7.1 IEC 62443 szabványcsalád

Az IEC 62443 szabványcsalád ma a legelterjedtebb és legelismertebb ipari biztonsági keretrendszer. Főként ipari automatizálási és vezérlőrendszerek (IACS – Industrial Automation and Control Systems) biztonsági követelményeit, elveit és módszertanait rögzíti. A szabvány négy fő területet fed le:

- **Általános alapelvek (62443-1-x)**: Definiálja a biztonsági alapfogalmakat, terminológiát és módszertanokat.
- **Üzemeltetési biztonsági követelmények (62443-2-x)**: Rögzíti a biztonságos üzemeltetéshez szükséges szervezeti és folyamatszintű intézkedéseket, beleértve a kockázatkezelést, incidenskezelést és a helyreállítási folyamatokat is.
- **Rendszerbiztonsági követelmények (62443-3-x)**: Meghatározza az OT rendszerek biztonsági követelményeit, beleértve a hálózati architektúrát, biztonsági zónázást, szegmentálást, valamint a biztonsági szintek (Security Levels – SL) alkalmazását (SL 1 – SL 4).
- **Komponensek biztonsága (62443-4-x)**: A gyártók által előállított eszközökre (például PLC, SCADA, HMI) vonatkozó biztonsági követelményeket és fejlesztési folyamatokat határozza meg, beleértve a biztonságos fejlesztés (Secure Development Lifecycle – SDL) alapelveit.

Az IEC 62443 szabvány implementációja lehetővé teszi a vállalatok számára, hogy biztonsági gyakorlatukat egységesen alakítsák ki, és a tanúsítással egyértelműen igazolják kiberbiztonsági érettségüket partnereik és ügyfeleik felé. [27]

7.2 NIST SP 800-82 (Guide to Industrial Control Systems Security)

Egy átfogó, gyakorlati útmutató, amely kifejezetten az ipari vezérlőrendszerek (ICS) biztonsági kihívásaira fókuszál. Ez az amerikai szabvány részletes iránymutatást nyújt a biztonsági követelmények kialakításához, a sérülékenységek kezeléséhez, valamint a folyamatos biztonsági monitorozáshoz és eseménykezeléshez. A NIST SP 800-82 dokumentum főbb ajánlásai:

- Részletes ICS-specifikus kockázatkezelési ajánlások, beleértve a sebezhetőségek és fenyegetések értékelését.
- Hálózati architektúra kialakítására és biztonsági konfigurációkra vonatkozó javaslatok (pl. DMZ-k használata, tűzfalak konfigurálása).
- Fizikai és logikai hozzáférés-ellenőrzések, beleértve a többfaktoros autentikáció használatát.
- Incidenskezelési és helyreállítási eljárások ipari környezetben, katasztrófa utáni helyreállítási tervek kidolgozásával.
- Részletes ellenőrzőlisták és auditálási eljárások, melyek támogatják a biztonsági állapot rendszeres felülvizsgálatát.

A NIST SP 800-82 útmutató kiváltképp hasznos lehet az amerikai piacon tevékenykedő vállalatok számára, mivel megfelel az amerikai hatóságok által megkövetelt biztonsági követelményeknek is. [24]

7.3 ISO/IEC 27001 szabvány (Információbiztonság)

Az ISO/IEC 27001 szabvány nem iparspecifikus, hanem általános információbiztonsági keretrendszer, amely alkalmas arra, hogy a vállalatok ipari rendszereikhez is alkalmazzák. Az ISO 27001 segít a szervezeteknek a biztonságirányítási rendszer (Information Security Management System – ISMS) kiépítésében és működtetésében. Ez a szabvány lefedi többek között:

- Kockázatmenedzsment-folyamatok kialakítását, amely magában foglalja a fenyegetések és sérülékenységek értékelését.
- Biztonsági elvek kialakítását, beleértve a szervezeti szintű szabályzatok és folyamatok dokumentálását.
- Fizikai és logikai hozzáférés-kezelési szabályokat, hitelesítési folyamatokat, illetve adatvédelmi intézkedéseket.
- Humán tényezők kezelését (oktatás, tudatosság növelése), amely különösen releváns ipari környezetben, ahol a biztonsági kultúra kiépítése kulcsfontosságú.
- Incidenskezelést és üzletmenet-folytonossági terveket, melyek alkalmazhatók az ipari termelés folytonosságának fenntartására.

Az ISO 27001 tanúsítás nemcsak a belső folyamatok megerősítésében, hanem a partnerek és ügyfelek felé történő hitelesség növelésében is jelentős szerepet játszik. [28]

7.4 NIS2 irányelv (EU-s szabályozás)

Az Európai Unióban az ipari kiberbiztonság jogszabályi keretét a NIS2 irányelv biztosítja. Ez a jogszabály kötelezően előírja az EU tagállamok számára, hogy a kritikus infrastruktúrákat üzemeltető vállalatok – ideértve számos ipari szervezetet is – megfelelő kiberbiztonsági intézkedéseket hajtsanak végre. A NIS2 által megkövetelt fő intézkedések közé tartozik:

- Részletes kockázatelemzés és biztonsági tervek készítése.
- Incidens-bejelentési kötelezettség az illetékes hatóságok felé.
- Rendszeres biztonsági auditok és ellenőrzések végrehajtása.
- Képzési és tudatosságnövelő programok alkalmazása a dolgozók körében.
- Különös figyelem a beszállítói és ellátási láncok biztonságára.

A NIS2 irányelv betartása jogi kötelezettség az EU-s vállalatok számára, ezért ennek megfelelően kiemelt jelentőséggel bír az ipari kiberbiztonsági stratégiák kialakítása során. [29]

8 ELEMZÉS ÉS JAVASLATOK

A fejezet célja, hogy a korábban bemutatott fenyegetéskép, szabályozási keret és esettanulmány-eredmények alapján konkrét, implementálható lépéseket vázoljon fel. A javaslatok két nagy csoportra bonthatók – technikaira, illetve szervezeti és emberi tényezőkre – mivel egy okosgyár kiberbiztonsága csak technológiai és emberi kontrollok integrált kombinációjával tartható fenn.

8.1 Technikai ajánlások

Zero-Trust hálózati architektúra OT-környezetre szabva:

- **Mikroszegmentálás**: A modell zónáit további cellákra kell bontani (pl. külön VLAN), és east-west forgalmat „deny-all + explicit allow" elven ellenőrizni.
- **IdP-alapú gépi hitelesítés**: OPC UA és MQTT forgalomhoz X.509 kliens-tanúsítványokat központi identitásszolgáltató állítson ki, így a vezérlőszegmens nem bízik vakon a layer-2 MAC-címben.
- A nulla bizalom elve NIS 2 kötelezettségekkel is összecseng: az EU-irányelv 21. cikk (2) bekezdése előírja a „legalább legszigorúbb hozzáférés-vezérlést" üzemeltetőknek.

Szabványalapú biztonsági program:

- A frissített IEC 62443-2-1:2024 már kiberérettségi szinteket is definiál; az ajánlott cél legalább Security Level 2 (szándékos, de korlátozott erőforrású támadó ellen) az üzemi hálózat legtöbb elemén.
- Kötelező dokumentumok: IACS-eszközleltár, kockázatértékelés, változáskezelési eljárás, helyreállítási terv.

Többrétegű detekciós lánc: Az okosgyár védelmét érdemes „hagymamodell-szerűen" felépíteni, ahol minden réteg más és más típusú támadást fog fel, így a behatolónak minden szinten újra kell hitelesítenie magát.

- **Perem-tűzfal szint:** A vállalati és az OT-hálózat határán deep-packet-inspection képes, ip-reputációs adatbázissal frissülő tűzfal szűri a forgalmat. Itt elsősorban a külső parancs- és vezérlőcsatornák blokkolása, valamint a nem engedélyezett ipari protokollok letiltása a cél.
- **OT-IDS szint:** A belső üzemi zónákban OT-specifikus behatolás-észlelő (pl. Zeek vagy Nozomi) figyeli a Profinet, OPC UA, Modbus stb. csomagokat. Ezek a rendszerek a protokoll-szabálytalanságok és a folyamat-anomáliák (például váratlan frekvenciaváltozás) alapján jeleznek, így gyorsan kiszűrik a célzott, „low-and-slow" támadási kísérleteket.
- **Host-szintű EDR:** A vezérlőállomásokon és HMI-ken futó végpontvédelmi szoftver (EDR/XDR) rendszerhívások és viselkedésminták alapján azonosítja a kártékony kódot, majd automatizáltan izolálja a fertőzött gépet. Ez a réteg különösen fontos a „living-off-the-land" technikák ellen, amikor a támadó valódi admin-eszközökkel dolgozik.

A három szint együtt zárja a réseket: a perem blokkolja a legtöbb külső támadást, az OT-IDS korán jelzi a zónák közti gyanús mozgást, az EDR pedig gép-szinten csípi el a maradékot. Így a detekció összideje percekre csökkenthető, a hamis riasztások száma pedig kezelésben tartható.

Rugalmassági (Resilience) mérőszámok bevezetése:

Mean-Time-To-Recover (MTTR) < 2 óra, Resilience Score ≥ 0.75 (ISA-99 RT-faktor).

A mérőszámokat KPI-ként köti a NIS 2 helyreállítási követelménye.

8.2 Szervezeti és emberi tényezők

1. **Kockázat-alapú governance modell:** A frissített IEC 62443-2-1 egyértelműen az asset-owner felelősségi körébe sorolja a folyamat alapú kontrollt; javasolt a CybEx-3 (Cybersecurity Executive Committee) fórumba legalább CTO + OT-mérnök + HR-képviselet bevonása.
2. **Kompetenciakeret és képzés:** Szerepkör-alapú oktatási mátrix:
   - Shop-floor operátor: alapszintű social engineering felismerés, 6 havonta e-learning.
   - Karbantató mérnök: secure-by-design *PLC* upgrade workshop, 12 havonta.
   - OT-hálózati admin: Deep-Dive Zeek OT & YARA képzés, 12 havonta lab-vizsgával.

   A Kaspersky ICS-CERT 2024 trendjelentés szerint a phishing még mindig a sikeres gyárleállítások 18 %-át indítja el.
3. **Incident Response (IR) playbook lokalizálása:**
   - „Containment within 30 min" SLA; ha az APT-csoport által célzott rendszer biztonságkritikus (pl. OHV robot), Immediate E-Stop protokoll aktiválható.
   - Külső vészcsapat (MSSP/CSIRT) retainer szerződéssel 24/7 elérhető.
4. **Beszállítói lánc átvilágítása:**
   - SBOM-követelmények (SW Bill of Materials) minden beszállítótól.
   - Szerződésben right-to-audit clause + CVE publikáció ≤ 72 óra a gyártó részéről.
5. **Biztonságos beszerzések:** Beszerzési ellenőrzőlista: támogassa IEC 62443-4-1 certifikációt, titkosított boot, biztonsági frissítés, hard-code-olt jelszó nem megengedett.

9 ÖSSZEFOGLALÁS ÉS KÖVETKEZTETÉSEK

9.1 Kritikus pontok összegzése

Az elemzés öt olyan területet tárt fel, ahol az okosgyárak kiberbiztonsági ellenálló-képessége jelenleg a legsebezhetőbb.

1. **Hálózati architektúra:** A vezérlőrendszerek többsége még mindig csak VLAN-szinten, vagy egyáltalán nem szegmentált, így egy sikeres behatolás után a támadó gyorsan, percek alatt képes oldalirányban terjedni. A mikroszegmentálás és a „deny-all, explicit-allow" szabályrendszer bevezetése ezért elsődleges feladat.
2. **Patching és változáskezelés:** A PLC-k és HMI-k firmware-e heterogén, a frissítések gyakran manuális jegyzőkönyv alapján történnek. Ez hosszú „exploit-ablakot" hagy nyitva. Szükség van ütemezett leállási ablakokra és digitális eszközleltárra, hogy a kritikus vezérlők legkésőbb félévente biztonságos firmware-t kapjanak.
3. **Felderítés és detekció:** A jelenleg használt signature-alapú IDS-ek önmagukban már nem elég hatékonyak a célzott, ismeretlen támadásokkal szemben. A viselkedéselemzésre épülő, AI-támogatott megoldások akár harmadával javíthatják a zero-day felismerési arányt, ezért kulcsfontosságú ezek fokozatos integrálása.
4. **Humán tényező és incidenskezelés:** Az IT- és OT-csapat közötti szerepkörök sokszor nincsenek egyértelműen tisztázva, az incidens-reakciós eljárás pedig hiányos vagy elavult. Ez magas átlagos helyreállítási időt (MTTR) eredményez. Egy részletes IR-playbook, rendszeres szerepalapú tréning jelentősen csökkentené a kiesési időket.
5. **Szabályozási megfelelés:** A 2024-es NIS 2 irányelv és az IEC 62443 új kiadásai magasabb biztonsági szintet követelnek meg. Mivel a bírságok az éves forgalom több százalékát is elérhetik, a compliance-központú prioritáslista kidolgozása nemcsak jogi, hanem üzleti szempontból is elengedhetetlen.

Összességében a legnagyobb kockázatot a gyors oldalirányú mozgás, a lassú patch-ciklusok és a szervezetlen incidenskezelés jelenti; ezek célzott javítása 18–24 hónap alatt nagyságrenddel csökkentheti a kitettséget.

9.2 Jövőbeli trendek

1. **5G-Advanced és TSN konvergenciája:** Az Ultra-Reliable Low-Latency Communication (URLLC) kiterjesztés új támadási felületet nyit időszinkron-manipulációval, így a jövőben a layer-2 time-spoofing ellen is védekezni kell.
2. **SD-WAN + SASE az OT-peremen:** A Secure Access Service Edge modellek OT-gatewaybe (rugged-edge) épülhetnek; dinamikus frissítés felhőn keresztül.
3. **Generatív AI a támadók oldalán:** A Dragos 2025 Q1 jelentés (axios codebook összefoglaló) kiemeli, hogy állami APT-k már LLM-generált phishing szövegeket és malware forráskód-variánsokat osztanak meg civil hackercsoportokkal.
4. **Kvantumbiztos kriptográfia:** IEC 62443 WG-2 már vizsgálja a CRYSTALS-Dilithium és Sphincs+ beépítését OPC UA-ba (draft 0.6-Q1/25). Várhatóan 2027-től ipari szabvány lesz.
5. **Digital Twin alapú kockázat-szimuláció:** Gyártósor-twin + attack-graph modell → what-if szimulációk karbantartási ablak tervezéséhez.
6. **Kibertámadások megítélése:** A társadalom egyre inkább megismeri ezek jelentőségét, fokozott aggodalom kezd kialakulni.

Irodalomjegyzék

[1] B. Lyndon, „International Society of Automation,” [Online]. Available: https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr. [Hozzáférés dátuma: 15. május 2025.].

[2] W. E. Forum, „Global Lighthouse Netwrok: The Mindset Shifts Driving Impact and Scale in Digital Transformation,” január 2025.. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Lighthouse_Network_2025.pdf. [Hozzáférés dátuma: 15 május 2025.].

[3] Shuaiyin Ma, Wei Ding, Yang Liu, Shan Ren, Haidong Yang,, „Digital twin and big data-driven sustainable smart manufacturing based on information management systems for energy-intensive industries,” 2022.. [Online]. Available: https://doi.org/10.1016/j.apenergy.2022.119986.

[4] Michael Spiess, Thomas Eckert, „Augmented reality goes to work on the factory floor,” SAP, 2022.. [Online]. Available: https://www.sap.com/bulgaria/blogs/augmented-reality-goes-to-work-on-the-factory-floor].

[5] E. Wallace, „How Human-Machine Collaboration Fuels Consumer-Driven Manufacturing,” RTInsights, 20. január 2025.. [Online]. Available: https://www.rtinsights.com/how-human-machine-collaboration-fuels-consumer-driven-manufacturing.

[6] I. Dragos, „Dragos's 8th Annual OT Cybersecurity Year in Review,” Dragos, Inc., 25. február 2025.. [Online]. Available: https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available/.

[7] Abdulrahman H. Alamri, Lexie Mooney, „Dragos Industrial Ransomware Analysis: Q4 2024,” Dragos, Inc., 04. november 2024.. [Online]. Available: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024/.

[8] J. Easterly, „The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years,” American Cyber Defense Agency, 07. május 2023.. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[9] „Cyber-attack on Hydro,” Norsk Hydro, 15. május 2024.. [Online]. Available: https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/.

[10] A. Culafi, „Dragos: Ransomware attacks against industrial orgs up 87%,” TechTarget, 25. február 2025.. [Online]. Available: https://www.techtarget.com/searchsecurity/news/366619652/Dragos-Ransomware-attacks-against-industrial-orgs-up-87.

[11] „NIS2 Directive: new rules on cybersecurity of network and information systems,” European Commission, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[12] „NIS2 Compliance for Manufacturing and Industrial Control Systems,” Rockwell Automation, [Online]. Available: https://www.rockwellautomation.com/en-pl/capabilities/industrial-cybersecurity/nis2.html.

[13] V. Carlos, „Understanding IT/OT convergence: Benefits, challenges, and real-world insights- Ep. 1 Transcript,” Siemens, 31. július 2024.. [Online]. Available: https://blogs.sw.siemens.com/thought-leadership/2024/07/31/understanding-it-ot-convergence-benefits-challenges-and-real-world-insights-ep-1-transcript/.

[14] „The IT-OT Convergence: Benefits, Challenges, and Strategic Initiatives to Ensure Success," Secomea, 28. május 2024.. [Online]. Available: https://secomea.com/remote-access/the-it-ot-convergence-benefits-challenges-and-strategic-initiatives/.

[15] I. Dragos, „Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks," Dragos, Inc., 25. február 2025.. [Online]. Available: https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/.

[16] A. Ribeiro, „Ransomware, state actors, hacktivists exploited geopolitical tensions to target critical infrastructure in 2024," Industrial Cyber, 25. február 2025.. [Online]. Available: https://industrialcyber.co/reports/ransomware-state-actors-hacktivists-exploited-geopolitical-tensions-to-target-critical-infrastructure-in-2024/.

[17] „2024 State Of The Threat - A Year In Review," Secureworks, [Online]. Available: https://www.secureworks.com/resources/rp-state-of-the-threat-2024. [Hozzáférés dátuma: 15. május 2025.].

[18] I. Dragos, „Dragos Knowledge Pack Update: Strengthen Your Detection of Ransomware Threats," Dragos, Inc, 12. május 2025.. [Online]. Available: https://www.dragos.com/blog/dragos-knowledge-pack-update-strengthen-your-detection-of-ransomware-threats]/.

[19] Stephanie Kelly, Jessica Resnick-ault, „One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators," Reuters, 9 június 2021.. [Online]. Available: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

[20] R. Lipovsky, „Industroyer: Biggest malware threat to critical infrastructure since Stuxnet," ESET, [Online]. Available: https://www.eset.com/us/industroyer/?srsltid=AfmBOoqNNuJPpm2wpwIczjc9YzfO-BiuLpd1cQhn4CJQrUGbcRG1d3KS. [Hozzáférés dátuma: 15. május 2025.].

[21] „Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," America's Cyber Defense Agency, 15. április 2021.. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

[22] F. Intelligence, „TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," FireEye, 23. október 2018.. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/triton-attribution-russian-government-owned-lab-most-likely-built-tools/.

[23] „A Cybersecurity Framework to Protect Industrial Automation and Control Systems," CISCO, 16. augusztus 2024.. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html.

[24] M. P. C. T. T. Z. V. P. S. L. A. H. S. S. A. S. M. T. Keith Stouffer, „Guide to Operational Technology," NIST, 2023.

[25] O. B. S. M. S. C. Scott Rose, „Zero Trust Architecture," 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207.

[26] „SOAR vs. SIEM: What Is the Difference?," Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-soar-vs-siem. [Hozzáférés dátuma: 15. május 2025.].

[27] E. C. Cosman, „Structuring the ISA/IEC 62443 Standards,” ISA, [Online]. Available: https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards. [Hozzáférés dátuma: 15. május 2025.].

[28] M. Edwards, „The Ultimate Guide to ISO 27001,” isms, 19. december 2024.. [Online]. Available: https://www.isms.online/iso-27001/.

[29] „What is NIS2?,” NIS2 DIRECTIVE, [Online]. Available: https://nis2directive.eu/what-is-nis2/. [Hozzáférés dátuma: 15. május 2025.].

2.37. A mesterséges intelligencia használata a gyógyszerfejlesztésben

Ipar 4.0 beadandó

A mesterséges intelligencia használata a gyógyszerfejlesztésben

Bagó Szabolcs

Mérnök Informatikus BSc szak

2025

Tartalomjegyzék

Tartalomjegyzék

Ábrajegyzék 3
Bevezetés 4
MI-ről a gyógyszerfejlesztésben általánosan 6
Szerkezet alapú gyógyszerfejlesztés 9
Az AlphaFold egy alkalmazása a gyakorlatban 12
Virtuális szűrés 16
A virtuális szűrés szerepe a Covid–19 elleni gyógyszerkutatásban 18
Befejező gondolatok 21
Összegzés 21
Etikai kérdések 21
Személyes reflexiók és jövőbeli kilátások 22
Irodalomjegyzék 24

Ábrajegyzék

1. ábra AI metszéspontjai és kapcsolatai más mezőkkel [1] 7
2. ábra A Röntgenkrisztallográfia, az NMR spektroszkópia és a Kriogén elektronmikroszkópia (A kép a ChatGPT-vel készült, fogalommagyarázati jelleggel) 10
3. ábra A AlphaFold Protein Structure Database weboldala 12
4. ábra Az AlphaFold és az Insilico Medicine végpontok közötti, mesterséges intelligenciával működő PandaOmics és Chemistry42 gyógyszerkutatási platformok kombinálása a hepatocelluláris karcinóma gyógyszerkutatásában [4] 14
5. ábra A szerkezetalapú virtuális szűrés munkafolyamata [11] 17
6. ábra Covid Moonshot szemléltető ábra [12] 19

Bevezetés

Az emberiség régóta foglalkozik a gondolattal, hogy mesterséges úton intelligens rendszereket hozzon létre. Már az ókori mitológiákban is fellelhetünk erre való utalásokat: Héphaisztosz kovácsolt szolgái vagy a zsidó hagyományból ismert golem mind azt mutatják, hogy már akkor is megvolt a szándék arra, hogy egy értelmes, önmagától cselekvő gépet alkossanak. Az 1950-es évektől kezdve a mesterséges intelligencia (MI), mint fogalom is megjelent, majd az azt követő 75 évben hatalmas fejlődésen ment keresztül, aminek hatására a mindennapjaink szerves részévé vált. Segítséget nyújt például kutatási források kereséséhez, weboldalak teljes szövegének fordításában, hosszabb szövegek összefoglalásában, vagy akár megadott szövegek vizualizálásában is. Ezek az alkalmazások ma már nemcsak a hétköznapi élet részévé váltak, hanem képesek az emberi munkát is kiegészíteni, akár olyan érzékeny területeken is, mint az egészségügy vagy a gyógyszeripar.

A mesterséges intelligencia gyógyszerfejlesztési alkalmazása különösen figyelemre méltó, mivel olyan feladatokat képes ellátni, amelyek korábban évekbe teltek volna, jelentős pénzügyi ráfordítások mellett. A technológia nem csak felgyorsítja a gyógyszerkutatás folyamatát, hanem új típusú gyógyszerek és hatóanyagok felfedezésében is segít. A 2020-as évek elején az MI különösen a koronavírus idején bizonyította be, hogy az adatalapú, prediktív rendszerek döntő szerepet játszhatnak az emberéletek megmentésében. Azóta pedig sok kutatás vette kezdetét, aminek során a mesterséges intelligenciát megpróbálják költséghatékonyan, mégis eredményesen alkalmazni.

A dolgozatom egyik célja az volt, hogy bemutassam, hogy a mesterséges intelligencia nemcsak ipari vagy informatikai területeken számít egy hatalmas áttörésnek, hanem az egészségügy egyik legösszetettebb szegmensében, a gyógyszerkutatásban is új lehetőségekkel kecsegtet. A témaválasztó dokumentumban is hangsúlyoztam, hogy az MI nem pusztán eszköz, hanem egy hasznos segítség lehet a jövő egészségügyi fejlesztéseiben.

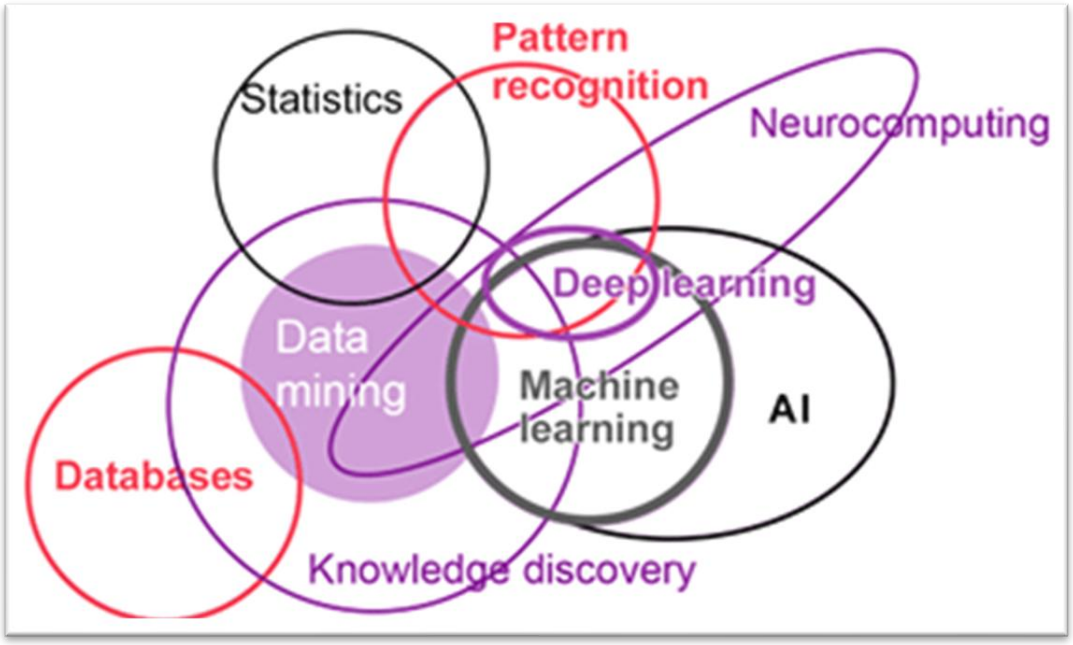
A dolgozat első részében a mesterséges intelligencia általános gyógyszeripari felhasználásáról fogok írni, majd a gyűjtött források segítségével bemutatok két kifejezetten fontos alkalmazási területet: a szerkezetalapú gyógyszerfejlesztést, azon belül fókuszálva az AlphaFold modelljére, majd a virtuális szűrést, amit a Covid-19 elleni fellépésben is

használtak. Végül a technológia etikai kérdéseiről is szót ejtek, majd kifejtem a saját nézőpontomat is a mesterséges intelligencia jövőbeli szerepéről.

MI-ről a gyógyszerfejlesztésben általánosan

Az elmúlt két évtized során a mesterséges intelligencia (MI) technológiái alapvetően átalakították a gyógyszerkutatás és -fejlesztés logikáját. A gyógyszeripar hagyományosan rendkívül idő- és költségigényes szektor, ahol a fejlesztési ciklus akár évtizedes nagyságrendű is lehet, és egyetlen új hatóanyag piacra juttatása milliárdos beruházást és rengeteg tesztelést igényel. Azonban az MI olyan lehetőséget kínál, amely egyszerre gyorsítja fel a kutatási folyamatokat és teszi azokat hatékonyabbá, adatvezéreltebbé, sőt előrejelezhetőbbé. [2] [3]

Az MI különböző formái, mint az alábbi ábrán is láthatóak, a gépi tanulás, mélytanulás, természetesnyelv-feldolgozás, a gyógyszerkutatás eltérő szakaszaiban hasznosíthatók az új hatóanyagok azonosításától kezdve a klinikai vizsgálatok modellezésén át egészen a piaci bevezetés utáni nyomon követésig. A hatóanyag-azonosítási fázisban például a mesterséges intelligencia képes több millió molekulát gyorsan és hatékonyan kiértékelni, különféle kémiai és biológiai jellemzők, illetve prediktív modellek alapján előre jelezve azok lehetséges terápiás hatásait vagy mellékhatásait. [2] [3]



1. ábra AI metszéspontjai és kapcsolatai más mezőkkel [1]

Ez nemcsak a fejlesztési ciklus lerövidítéséhez járul hozzá, hanem jelentősen csökkenti a költségeket is, mivel már a korai szakaszban kiszűrhetők a potenciálisan sikertelen vagy veszélyes vegyületek. A mesterséges intelligencia alkalmazása így lehetőséget teremt arra, hogy a gyógyszeripar elmozduljon a hagyományos, erőforrás- és időigényes próbálkozás-alapú módszerektől egy új, adatvezérelt megközelítés felé. Ez a szemléletváltás nem csupán gyorsabb és gazdaságosabb fejlesztést tesz lehetővé, hanem a humán szakértelmet is kiegészíti, illetve bizonyos területeken részben helyettesíti, különösen az előzetes adatfeldolgozás, mintázatfelismerés vagy prediktív értékelés során. Összességében tehát az MI szerepe kulcsfontosságúvá vált a gyógyszerfejlesztés innovatív és hatékonyabbá tételében. [2] [3]

A mesterséges intelligencia térnyerésével párhuzamosan egyre több tudományos publikáció és iparági jelentés is foglalkozik az MI gyógyszeripari alkalmazásainak vizsgálatával. A szakirodalom jelentős része két olyan alkalmazási terület köré csoportosul, amelyek mára meghatározóvá váltak. Az egyik a szerkezetalapú gyógyszerfejlesztés,

amelyben az MI a fehérjék térszerkezetének előrejelzésével járul hozzá a célzott gyógyszerek tervezéséhez. Ennek egyik legismertebb példája a DeepMind által fejlesztett AlphaFold modell, amely képes aminosavsorrendből pontosan rekonstruálni a fehérjék háromdimenziós szerkezetét - ez korábban csak hosszadalmas kísérleti módszerekkel volt lehetséges. [2] [3]

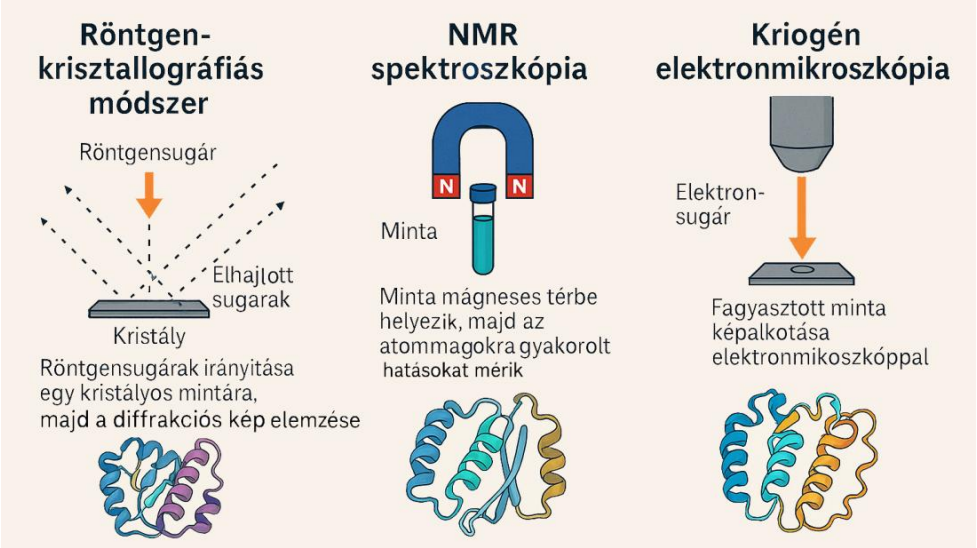
A másik jelentős terület a virtuális szűrés, amely során hatalmas molekuláris könyvtárakat elemeznek az MI-rendszerek, előre jelezve azok biológiai aktivitását egy adott célfehérjére. Ez a technika kulcsszerepet játszott a Covid-19 elleni gyógyszerkutatásban is, ahol a gyorsaság és a költséghatékonyság elsődleges szemponttá vált. A pandémia idején az MI-alapú szűrés több kutatóintézetben is alkalmazásra került a lehetséges antivirális szerek gyors azonosítására - ezt számos publikáció és esettanulmány dokumentálja. [2] [3]

A következő fejezetekben e két irányvonal, a szerkezetalapú tervezés és a virtuális szűrés, kerül részletesebb bemutatásra. E szakterületek vizsgálata nemcsak a jelenleg elérhető eredmények jobb megértéséhez, hanem a jövőbeli fejlesztési lehetőségek felismeréséhez is hozzájárul.

Szerkezet alapú gyógyszerfejlesztés

A gyógyszerkutatás hagyományos megközelítései nagymértékben támaszkodtak empirikus módszerekre, szűk molekulakönyvtárak manuális szűrésére és hosszadalmas laboratóriumi vizsgálatokra. Ezzel szemben a szerkezetalapú gyógyszerfejlesztés (Structure-Based Drug Design, SBDD) egy olyan modern stratégia, amely a célfehérjék ismert vagy előre jelzett háromdimenziós szerkezetén alapuló gyógyszerjelöltek tervezését és optimalizálását teszi lehetővé. E megközelítés célja, hogy a molekulák és a fehérjék közötti térbeli kapcsolódás, a kötődési helyek (binding sites) ismeretében nagy pontossággal lehessen előrejelezni és kialakítani a potenciálisan aktív hatóanyagokat. [5] [10]

A szerkezetalapú tervezés egyik alappillére a célfehérje szerkezetének ismerete. Ezt, ahogy azok az alább látható ábrán is szerepelnek, korábban elsősorban röntgenkrisztallográfiás módszerekkel, NMR spektroszkópiával vagy kriogén elektronmikroszkópiával határozták meg, amelyek mind idő- és költségigényesek, és nem minden fehérje esetén alkalmazhatók. Ennek következtében a gyógyszeriparban gyakran kénytelenek voltak kompromisszumokat kötni, vagy kevésbé pontos modellekre támaszkodni. [5] [10]



2. ábra A Röntgenkrisztallográfia, az NMR spektroszkópia és a Kriogén elektronmikroszkópia
(A kép a ChatGPT-vel készült, fogalommagyarázati jelleggel)

A mesterséges intelligencia térnyerésével új lehetőségek nyíltak a fehérjestruktúrák előrejelzésében. A gépi tanulási és különösen a mélytanulási modellek révén ma már lehetőség van arra, hogy egy fehérje aminosavsorrendje alapján prediktív módon rekonstruáljuk annak háromdimenziós térszerkezetét. Ezzel nemcsak jelentősen lerövidíthető a szerkezet-meghatározás ideje, hanem új, eddig ismeretlen célpontokat is azonosítani lehet. [5] [10]

A szerkezetalapú megközelítés során a gyógyszerjelöltek tervezése több lépésből áll: először a célfehérje szerkezeti jellemzőit modellezik (amennyiben nem ismert, akkor számítással előrejelzik), majd az aktív helyet (binding pocket) azonosítják. Ezután a potenciális ligandumokat vagy a gépben legenerálják, vagy nagy molekulakönyvtárakból szűrik ki azokat, amelyek nagy valószínűséggel képesek kötődni a célponthoz. A molekulák és a fehérje közötti interakciókat számítógépes módszerekkel, például dokkolással (molecular docking) vagy molekuladinamikai szimulációkkal értékelik. A legígéretesebb jelöltek további optimalizálás után lépnek a preklinikai fázisba. [5] [10]

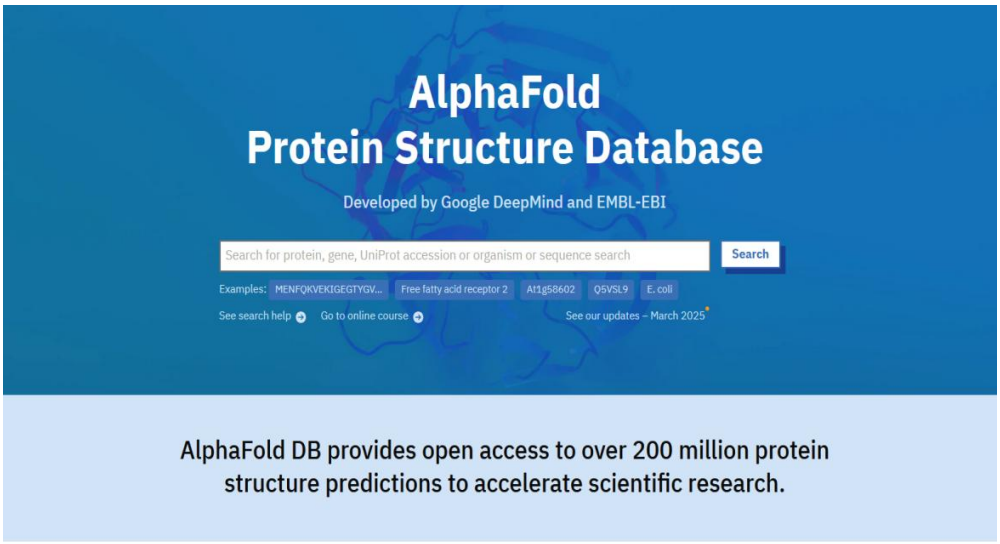
A szerkezetalapú gyógyszertervezés tehát jelentős hatékonyságnövelést eredményezhet a gyógyszerkutatásban. Ennek egyik leglátványosabb áttörését a DeepMind által kifejlesztett AlphaFold nevű mesterségesintelligencia-rendszer hozta el. [5] [10]

Az AlphaFold egy mélytanulás-alapú rendszer, amelyet kifejezetten arra fejlesztettek ki, hogy nagy pontossággal előre jelezze a fehérjék háromdimenziós szerkezetét kizárólag az aminosavsorrend alapján. A probléma, amelyre választ kínál, évtizedeken keresztül az egyik legnagyobb kihívás volt a bioinformatikában: a fehérjék folding-problémája. Az AlphaFold megoldása nemcsak tudományos áttörésnek számított, hanem gyakorlati alkalmazásai révén is forradalmasította a gyógyszerkutatási folyamatokat. [4] [5] [10]

A rendszer 2020 végén vált ismertté széles körben, amikor a CASP14 (Critical Assessment of protein Structure Prediction) versenyen a DeepMind csapata az AlphaFold 2-vel olyan pontosságot ért el, amely összevethető volt a röntgenkrisztallográfiás módszerekkel. Az AlphaFold által előrejelzett fehérjestruktúrák RMSD értéke bizonyos esetekben 1 Å-n (egy angström-ön) belül volt, ami gyakorlatilag molekuláris szintű pontosságot jelent. [4] [5] [10]

Az AlphaFold sikere abban rejlik, hogy nem csupán egy neurális hálózatot alkalmaz, hanem egy komplex architektúrát, amely többlépcsős figyelmi mechanizmusokon (attention layers) és evolúciós kapcsolatokon alapul. Az algoritmus képes az aminosavak közötti távolságmátrixok és a kontaktustérkép egyidejű predikciójára, valamint belső konzisztenciavizsgálatokkal javítja a szerkezeti becslések megbízhatóságát. [4] [5] [10]

A 2021-ben publikált, az ábrán is látható AlphaFold Protein Structure Database több mint 200 millió fehérje előrejelzett szerkezetét tette közzé nyílt hozzáféréssel, köztük számos gyógyszerfejlesztés szempontjából releváns fehérje is szerepel, amelynek korábban nem volt ismert térszerkezete. A kutatók és gyógyszeripari fejlesztők számára ez a tudástár új lehetőségeket nyit a célpontok azonosításában és a molekulák szerkezet-alapú tervezésében. [4] [5] [10]



3. ábra A AlphaFold Protein Structure Database weboldala [13]

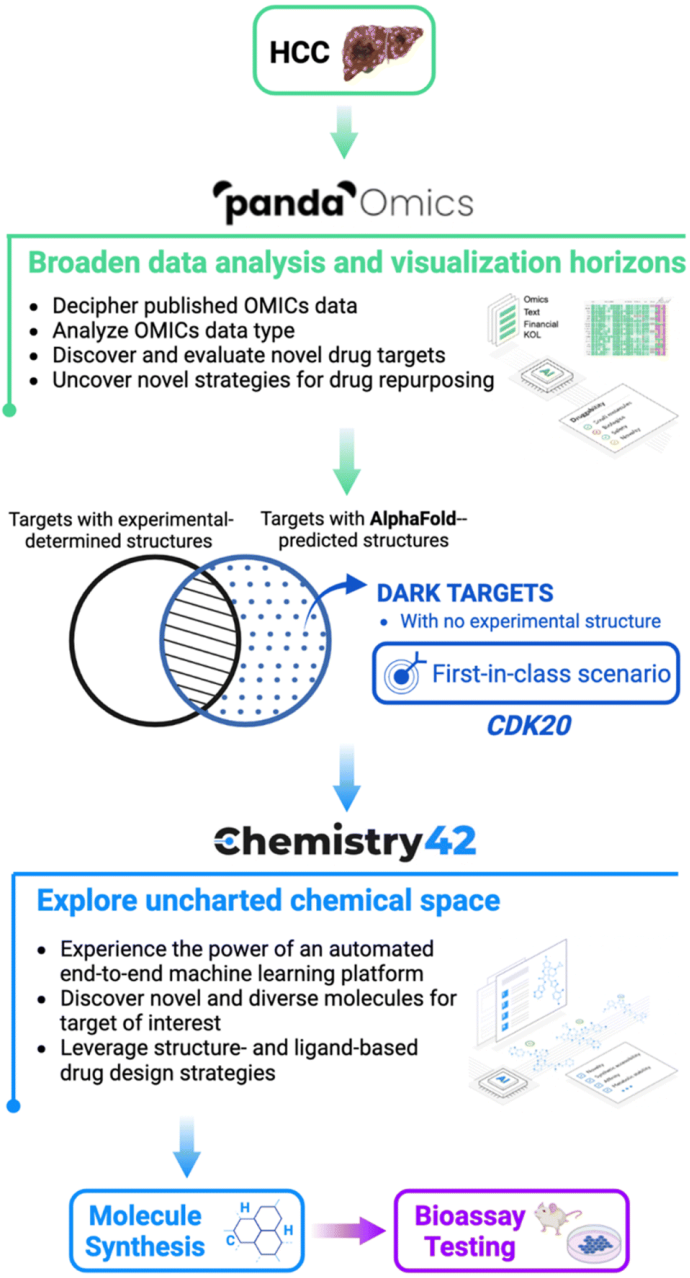
Az AlphaFold nemcsak az akadémiai kutatásban, hanem a gyógyszeripari gyakorlatban is egyre nagyobb szerepet kap. Számos biotechnológiai cég és gyógyszergyártó vállalat integrálta már modelljeit saját fejlesztési munkafolyamatába, és a platform már most is inspirált új vegyületoptimalizálási stratégiákat, többek között a fehérje-fehérje interakciókat célzó hatóanyagok fejlesztésében. [4] [5] [10]

Az AlphaFold technológia egyik első gyakorlati alkalmazása a gyógyszerfejlesztésben a ciklin-függő kináz 20 (CDK20) enzim gátlószerének felfedezéséhez kapcsolódik. A CDK20 egy kevéssé ismert célpont, amelynek korábban nem állt rendelkezésre kísérletileg meghatározott háromdimenziós szerkezete, ami jelentősen megnehezítette a hagyományos szerkezetalapú gyógyszertervezést. [4] [5] [10]

Az AlphaFold egy alkalmazása a gyakorlatban

A kutatók az AlphaFold által előrejelzett CDK20 szerkezetet használták fel kiindulási pontként egy mesterséges intelligencia által vezérelt gyógyszerfelfedezési folyamatban. A PandaOmics platform segítségével azonosították a célpontot, majd a Chemistry42 generatív

kémiai platformot alkalmazták új molekulák tervezésére. A kiválasztott vegyületeket szintetizálták és biológiai teszteknek vetették alá. [4] [5]



4. ábra Az AlphaFold és az Insilico Medicine végpontok közötti, mesterséges intelligenciával működő PandaOmics és Chemistry42 gyógyszerkutatási platformok kombinálása a hepatocelluláris karcinóma gyógyszerkutatásában [4]

Ennek a megközelítésnek köszönhetően mindössze 30 nap alatt sikerült azonosítani egy elsődleges hatóanyagot, amely 8,9 ± 1,6 μM Kd értékkel rendelkezett. Ezt követően egy második körös optimalizáció során egy még hatékonyabb vegyületet, az ISM042-2-048-at fedezték fel, amely 210 ± 42,4 nM Kd értéket mutatott. Ez a tanulmány az első példája annak, hogy az AlphaFold előrejelzéseit közvetlenül alkalmazták a gyógyszerfelfedezés korai szakaszában, emberi felügyelet alatt, különösen olyan célpontok esetében, amelyekről korábban nem állt rendelkezésre szerkezeti információ. [4] [5]

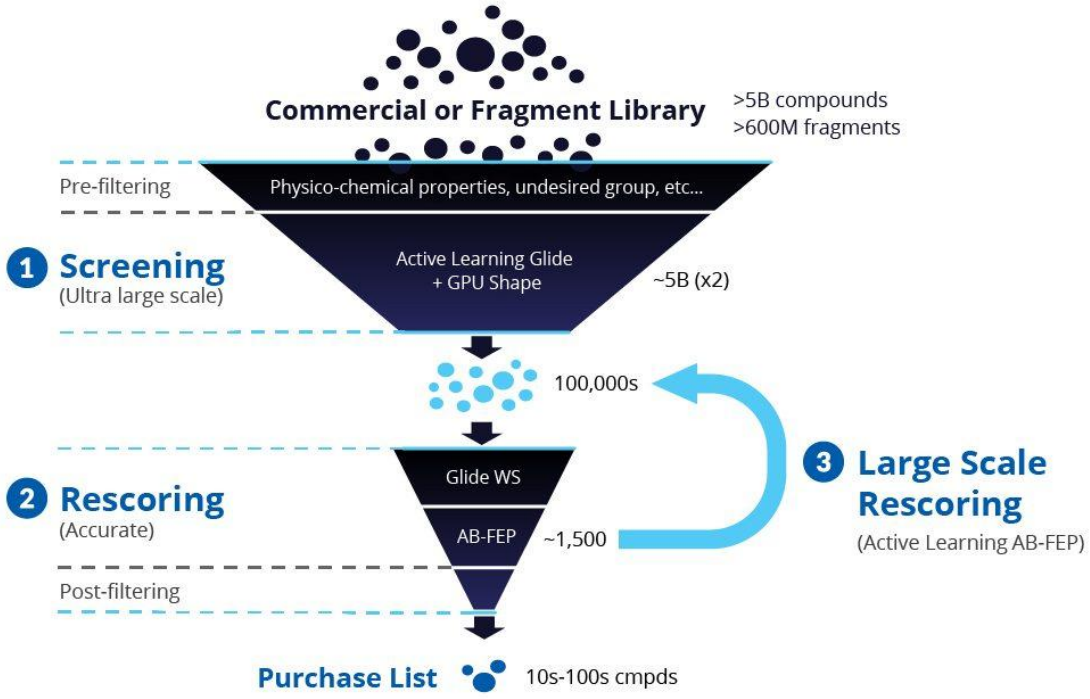
Ugyanakkor fontos megjegyezni, hogy az AlphaFold által nyújtott szerkezeti predikciók nem minden esetben teljes körűek: a flexibilis régiók, poszttranszlációs módosítások és a dinamikus konformációváltások jelenleg is kihívást jelentenek. A modell tehát nem váltja ki teljesen a laboratóriumi validációt, hanem kiegészítő eszközként funkcionál, amely a kezdeti lépéseket gyorsítja és pontosítja. [4] [5]

Összességében az AlphaFold alkalmazása új dimenziót nyitott a szerkezetalapú gyógyszerfejlesztésben, és jó példa arra, hogy a mesterséges intelligencia nem csupán a meglévő folyamatok digitalizálására képes, hanem azok átstrukturálására is. A következőkben ennek a szemléletnek egy másik gyakorlati területét vizsgálom meg: a virtuális szűrés módszertanát és alkalmazását. [4] [5]

Virtuális szűrés

A gyógyszerfejlesztés egyik legfontosabb kihívása a megfelelő hatóanyag-jelöltek azonosítása. A hagyományos laboratóriumi alapú, magas áteresztőképességű szűrés (high-throughput screening, HTS) rendkívül idő- és költségigényes folyamat, amely gyakran több százezer vagy akár több millió molekula fizikai tesztelését igényli. Ennek kiváltására vagy kiegészítésére fejlődött ki az ún. virtuális szűrés (virtual screening, VS) technológiája, amely számítógépes módszerekkel próbálja azonosítani a legígéretesebb vegyületeket nagy molekulakönyvtárakból. [7] [8]

A virtuális szűrés célja, hogy a molekulák és a célfehérjék közötti lehetséges kölcsönhatásokat in silico modellezze, és ezek alapján rangsorolja azokat a vegyületeket, amelyek a legnagyobb valószínűséggel mutatnak biológiai aktivitást az adott célpont ellen. A módszer két fő megközelítése: a ligandalapú virtuális szűrés (ligand-based virtual screening, LBVS) és az ábrán is megfigyelhető szerkezetalapú virtuális szűrés (structure-based virtual screening, SBVS). Az előbbi ismert aktív vegyületek szerkezeti jellemzőit használja ki az új jelöltek keresésére, míg az utóbbi a célfehérje háromdimenziós szerkezetét veszi alapul. [7] [8]



5. ábra A szerkezetalapú virtuális szűrés munkafolyamata [11]

A szerkezetalapú virtuális szűrés során a célfehérje kötőhelyének szerkezetét (binding site) használják fel a potenciális ligandumok molekuláris dokkolására. A molekulák energiaértékei és kötődési konformációi alapján a rendszer rangsorolja a jelölteket, gyakran többféle pontozási (scoring) algoritmus alapján. Ezek az algoritmusok figyelembe veszik a hidrogénkötéseket, hidrofób interakciókat, elektrosztatikus vonzásokat és a molekulák geometriáját. [7] [8]

A mesterséges intelligencia és a gépi tanulás integrálása a virtuális szűrésbe tovább növelte a módszer hatékonyságát. Az MI-alapú modellek képesek olyan mintázatokat azonosítani, amelyeket a klasszikus algoritmusok nem érzékelnének, és olyan prediktív erővel bírnak, amely lehetővé teszi új, korábban nem vizsgált molekulák felfedezését. Ezenkívül a kvantitatív szerkezet-aktivitás kapcsolat (QSAR) modellek révén a vegyületek várható biológiai aktivitása in silico módon megbecsülhető, ugyanakkor ezek az

előrejelzések nem helyettesítik a laboratóriumi és klinikai validációt, és nem garantálják a klinikai hatékonyságot vagy biztonságosságot. [7] [8]

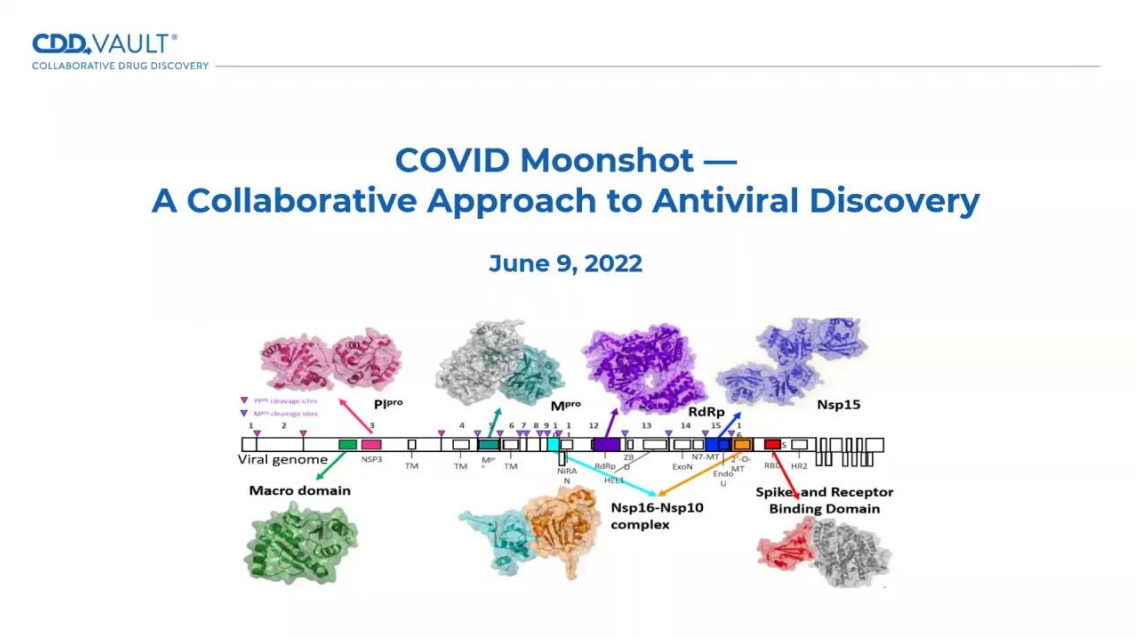
A virtuális szűrés egyik legnagyobb előnye a méretezhetőség és a költséghatékonyság. Egyetlen szuperszámítógépes vagy felhőalapú futtatás során több millió molekula szűrhető végig napok vagy akár órák alatt, ami összehasonlíthatatlan a hagyományos HTS módszerek idejével és költségeivel. A módszer ezen kívül elősegíti az újrapozicionálást (drug repurposing) is, azaz meglévő, más célra kifejlesztett gyógyszerek új terápiás alkalmazásainak felfedezését. [7] [8]

Fontos azonban hangsúlyozni, hogy a virtuális szűrés eredményei prediktív jellegűek, és nem helyettesítik a laboratóriumi validációt. A számított kötődési energia vagy a prediktált aktivitás önmagában nem garantálja a klinikai hatékonyságot vagy biztonságosságot. Ezért a VS leginkább a gyógyszerkutatás korai fázisában használható kiemelkedő hatékonysággal, ahol a cél a jelöltek gyors szűkítése a potenciálisan aktív vegyületekre. [7] [8]

A virtuális szűrés szerepe a Covid–19 elleni gyógyszerkutatásban

A 2020-ban kirobbant Covid–19 világjárvány idején a gyógyszerkutatásnak példátlan gyorsasággal kellett reagálnia az új kihívásra. Ebben a helyzetben a hagyományos laboratóriumi megközelítések nem bizonyultak elegendően gyorsnak vagy hatékonynak, ezért számos kutatóintézet és gyógyszergyártó cég a mesterséges intelligencia és a virtuális szűrés eszközeihez fordult. [9]

Az egyik legismertebb példa erre az ábrán is látható Covid Moonshot kezdeményezés volt, amely nyílt hozzáférésű molekulakönyvtárakat használt fel a SARS-CoV-2 vírus fő proteázának (Mpro) célba vételére. A kutatók az AlphaFold előrejelzéseit is felhasználva több ezer molekulát dokkoltak a célfehérje aktív helyére, majd a legígéretesebb jelölteket laboratóriumi vizsgálatoknak vetették alá. [9]



6. ábra Covid Moonshot szemléltető ábra [12]

Számos további tanulmány is igazolta, hogy a virtuális szűrés gyorsan képes repurposing céljából értékelni már ismert antivirális szereket. Így kerülhetett például klinikai figyelem középpontjába a Remdesivir, a Favipiravir vagy az Ivermectin, amelyek közül több gyógyszert a SARS-CoV-2 elleni kezelés potenciális jelöltjeként vizsgáltak. [9]

A virtuális szűrés nemcsak a kezdeti fázisokban, hanem a későbbi optimalizációs lépésekben is alkalmazható volt. A kiválasztott vegyületek módosítására, a szerkezet-hatás összefüggések finomhangolására, valamint a farmakokinetikai tulajdonságok javítására is szolgált, így jelentősen hozzájárult a hatékonyság növeléséhez és a mellékhatások csökkentéséhez. [9]

A pandémia során alkalmazott virtuális szűréses megközelítések sikeressége új lendületet adott a technológia iparági elfogadottságának. Számos nagy gyógyszercég, köztük a Pfizer, a Novartis és a Roche, integrálta a VS módszert saját kutatás-fejlesztési folyamataiba. Emellett új, kifejezetten AI-alapú gyógyszerkutató cégek (pl. Insilico

Medicine, BenevolentAI) jelentek meg, amelyek már a fejlesztés korai szakaszától teljes egészében in silico stratégiákra építenek. [9]

Összességében a virtuális szűrés nemcsak egy hatékony szűrési eszközként szolgál, hanem egy paradigmaváltás kulcseleme is a gyógyszerkutatásban. A Covid–19 járvány megmutatta, hogy sürgős globális egészségügyi krízis esetén az MI-alapú technológiák képesek valós, gyors és hatékony válaszokat adni, és hosszú távon is befolyásolhatják a gyógyszeripari innováció irányát. [9]

Befejező gondolatok

Összegzés

A dolgozat során arra törekedtem, hogy átfogó képet adjak a mesterséges intelligencia gyógyszerfejlesztési alkalmazásairól, különös tekintettel a szerkezetalapú gyógyszertervezésre és a virtuális szűrésre. A mesterséges intelligencia olyan technológiai lehetőségeket nyit meg a gyógyszeripar számára, amelyek az elmúlt évtizedek hagyományos, kísérletezésre épülő modelljeit alapvetően átalakítják. Már a gyógyszerkutatás legkorábbi szakaszától kezdve, például a célfehérjék azonosításánál vagy hatóanyag-jelöltek prediktív szűrésénél, képes időt, költséget és humán munkaerőt megtakarítani, miközben hatékonyabb és célzottabb fejlesztést tesz lehetővé.

A szerkezetalapú gyógyszerfejlesztés területén az AlphaFold által kínált fehérjestruktúra-előrejelzés forradalmi újításként jelent meg, és máris érezhető gyakorlati hatása van az ipari kutatás-fejlesztés területén. A virtuális szűrés módszertana a COVID-19 világjárvány idején nyert széleskörű figyelmet és bizonyította életképességét sürgős, valós egészségügyi kihívások kezelésében. A két technológia, bár eltérő megközelítést képvisel, közös célja, hogy a gyógyszerkutatást gyorsabbá, kiszámíthatóbbá és megbízhatóbbá tegye.

Ugyanakkor az MI-alapú gyógyszerfejlesztés nem csupán egy új eszköz, hanem egy paradigmaváltás előfutára, amely a kutatási kérdések feltevésétől kezdve a hatóanyagok piaci bevezetéséig új szemléletmódot igényel. A dolgozatban bemutatott példák jól szemléltetik, hogy a mesterséges intelligencia milyen sokrétű módon integrálódhat a gyógyszeripari folyamatokba, és mekkora potenciál rejlik benne a jövő szempontjából.

Etikai kérdések

A technológiai lehetőségek növekedésével párhuzamosan ugyanakkor egyre fontosabbá válnak az alkalmazásukhoz kapcsolódó etikai kérdések is. A mesterséges intelligencia, különösen, amikor egészségügyi adatokkal dolgozik, olyan adatvédelmi, döntési

felelősségi és átláthatósági dilemmákat vet fel, amelyek újfajta szabályozási és társadalmi válaszokat igényelnek.

Az egyik legfontosabb probléma az adatminőség és adatetika kérdése. Az MI rendszerek hatékonysága nagymértékben függ a bemeneti adatok megbízhatóságától, pontosságától és reprezentativitásától. Amennyiben a rendszerek részrehajló, hiányos vagy torz adatbázisokra épülnek, döntéseik torzak, sőt veszélyesek lehetnek. Ez különösen súlyos következményekkel járhat a gyógyszerkutatásban, ahol egy hibás predikció akár emberi életeket is érinthet.

Szintén fontos kérdés a felelősség elosztása. Ha egy MI-alapú rendszer hibázik, ki a felelős? A fejlesztő, az orvos, a gyógyszergyártó cég vagy maga az algoritmus? Az MI „feketedoboz”-jellege tovább nehezíti az átláthatóságot, különösen a mélytanulási modellek esetén, amelyek predikciói nem mindig értelmezhetők közvetlenül emberi logika szerint.

Etikai kihívás az is, hogy az MI milyen mértékben automatizálja a döntéshozatalt. A gépi modellek képesek előrejelezni hatékonyságot, toxicitást vagy mellékhatásokat, de az emberi szempontokat, például betegjogokat, társadalmi egyenlőtlenségeket, nem mindig képesek figyelembe venni. Ez különösen veszélyes lehet a globális egészségügy kontextusában, ahol az MI javaslatai hatással lehetnek arra, hogy mely gyógyszerek fejlesztése kerül előtérbe, és kik számára lesznek elérhetők.

Személyes reflexiók és jövőbeli kilátások

Úgy gondolom, hogy a mesterséges intelligencia nem csupán egy nagy technológiai fejlesztés, hanem az emberi tudás egy újfajta gyűjtőhelye, amely képes az emberi gondolkodásmódhoz hasonló mintafelismerésre, sőt sok esetekben annak túlszárnyalására is. A dolgozat készítése során lenyűgözött, hogy az olyan algoritmusok, mint az AlphaFold, képesek a biológiai komplexitás olyan szintjeit értelmezni és modellezni, amelyeket eddig kizárólag kísérletes úton, számtalan ember által végzett munkával lehetett megközelíteni.

Ugyanakkor azt is látni kell, hogy az MI nem csodaszer: nem helyettesíti a humán szakértelmet, az etikai mérlegelést vagy a társadalmi kontextus ismeretét. A jövő gyógyszerfejlesztésének legnagyobb kihívása az lesz, hogy az emberi és a mesterséges intelligenciát komplementer módon használjuk: az MI végezze az adatalapú, gyors és nagy volumenű elemzéseket, míg az ember döntsön a prioritásokról, etikai irányokról és társadalmi hatásokról.

A jövőben várhatóan egyre több gyógyszergyártó vállalat fogja beépíteni az MI-t a kutatás-fejlesztési stratégiájába. Az MI segítheti a ritka betegségek gyógyszereinek kifejlesztését, az egyedi terápiák létrehozását és az egészségügyi rendszerek fenntarthatóbb működését is, levéve a terhet az ott dolgozó emberek válláról. A mesterséges intelligencia hosszú távon nemcsak a technológiai lehetőségeket jelent, hanem hozzájárulhat egy gyorsabb és célzottabb egészségügyi ellátás megteremtéséhez is.

Dolgozatommal azt akartam bemutatni, hogy a mesterséges intelligencia nem csak egy forradalmi eszköz, hanem a gyógyszeripar jövőjének egyik nagy segítője. Bízom benne, hogy a fejlődés iránya és sebessége mellett továbbra is megmarad a hangsúly az emberi munkán, ami eddig is segítette társadalmunkat.

Irodalomjegyzék

[1] Automating E-Government Services With Artificial Intelligence - Scientific Figure, ResearchGate. Elérhető: https://www.researchgate.net/figure/AI-intersections-and-relationship-with-other-fields_fig1_336352900 [accessed 12 May 2025]

[2]Alberto Ocana, Atanasio Pandiella, Cristian Privat, Iván Bravo, Miguel Luengo-Oroz, Eitan Amir, Balazs Gyorffy, Integrating artificial intelligence in drug discovery and early drug development: a transformative approach, biomedcentral, 2025. [Online]. elérhető: https://biomarkerres.biomedcentral.com/articles/10.1186/s40364-025-00758-2

[3] Fang Bai1, Shiliang Li, Honglin Li, AI enhances drug discovery and development, researchgate, 28 November 2023. [Online]. Elérhető: https://www.researchgate.net/publication/378710510_AI_enhances_drug_discovery_and_development

[4] Feng Ren, Xiao Ding, Min Zheng, Mikhail Korzinkin, Xin Cai, Wei Zhu, Alexey Mantsyzov, Alex Aliper, Vladimir Aladinskiy, Zhongying Cao, Shanshan Kong, Xi Long, Bonnie Hei Man Liu, Yingtao Liu, Vladimir Naumov, Anastasia Shneyderman, Ivan V. Ozerov, Ju Wang, Frank W. Pun, Daniil A. Polykovskiy, Chong Sun, Michael Levitt, Alán Aspuru-Guzik, Alex Zhavoronkov, AlphaFold accelerates artificial intelligence powered drug discovery: efficient discovery of a novel CDK20 small molecule inhibitor, Royal Society of Chemistry, 10 Jan 2023. [Online]. Elérhető: https://pubs.rsc.org/en/content/articlelanding/2023/sc/d2sc05709c

[5] SciLifeLab, Artificial intelligence accelerates drug design: “astonishingly high accuracy”, SciLifeLab, August 8, 2024. [Online]. Elérhető: https://www.scilifelab.se/news/artificial-intelligence-accelerates-drug-design-astonishingly-high-accuracy/

[6] The Korea Advanced Institute of Science and Technology (KAIST), Repurposed drugs present new strategy for treating COVID-19, ScienceDaily, July 8, 2021. [Online]. Elérhető: https://www.sciencedaily.com/releases/2021/07/210708103611.htm

[7] Guangfeng Zhou, Domnita-Valeria Rusnac, Hahnbeom Park, Daniele Canzani, Hai Minh Nguyen, Lance Stewart, Matthew F. Bush, Phuong Tran Nguyen, Heike Wulff, Vladimir Yarov-Yarovoy, Ning Zheng, Frank DiMaio, An artificial intelligence accelerated virtual screening platform for drug discovery, Nature communications, 05 September 2024. [Online]. Elérhető: https://www.nature.com/articles/s41467-024-52061-7

[8] Babak Sokouti, A review on in silico virtual screening methods in COVID-19 using anticancer drugs and other natural/chemical inhibitors, Explorationpub, October 26, 2023. [Online]. Elérhető: https://www.explorationpub.com/Journals/etat/Article/1002177

[9] Victoria Rees, Using virtual screening to identify coronavirus treatments, Drug Target Review, 10 March 2020. [Online]. Elérhető: https://www.drugtargetreview.com/article/57052/using-virtual-screening-to-identify-coronavirus-treatments/

[10] Haixin Wei, J. Andrew McCammon, Structure and dynamics in drug discovery, Nature, 2024. [Online]. Elérhető: https://www.nature.com/articles/s44386-024-00001-2

[11] Schrödinger, Dramatically improving hit rates with a modern virtual screening Schrödinger, [Online]. Elérhető: https://www.schrodinger.com/life-science/learn/white-papers/dramatically-improving-hit-rates-modern-virtual-screening-workflow/

[12] collaborativedrug, Recorded Webinar: COVID Moonshot — A Collaborative Approach to Antiviral Discovery, collaborativedrug, June 10, 2022. [Online]. Elérhető: https://www.collaborativedrug.com/cdd-blog/recorded-webinar-covid-moonshot

[13] AlphaFold, AlphaFold Protein Structure Database, AlphaFold, March 2025. [Online] https://alphafold.ebi.ac.uk/

2.38. Szenzorok és alkalmazásuk az Ipar

Ipar 4.0 technológiák

GKNB_INTM087

Szenzorok és alkalmazásuk az Ipar 4.0 kiberfizikai rendszereiben

Tóth Máté

[redacted]

Mérnökinformatikus, BSc, nappali

2024/25/2

Tartalomjegyzék

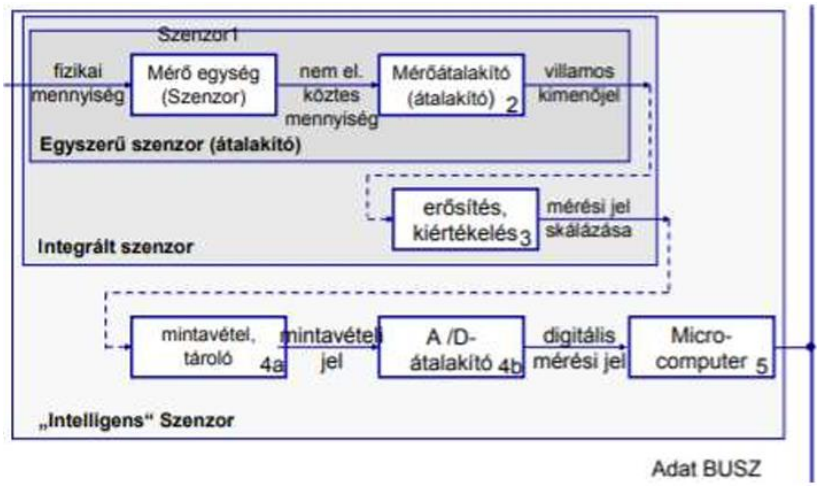
1 Bevezetés ... 3
2 Szenzor fogalma [1] [2] [3] ... 4
2.1 Szenzorok csoportosítása ... 4
2.2 Szenzorok jellemzői ... 5
Egyéb fontosabb jellemzők és hibák: ... 7
3 Szenzor fajták és jellemzésük ... 8
3.1 Közelítéskapcsolók ... 8
3.1.1 Induktív szenzorok [4][5] ... 8
3.1.2 Kapacitív szenzorok [5] ... 9
3.1.3 Pneumatikus szenzorok [5] ... 10
3.1.4 Optikai szenzorok [1][5] ... 11
3.1.5 Optoelektronikai szenzorok [1] ... 13
3.1.6 Ultrahang szenzorok [1][5] ... 14
3.2 Hall szenzorok [7] ... 16
3.3 Ellenállásos szenzorok [8] ... 16
3.4 Hőmérséklet mérő szenzorok [9] ... 17
3.4.1 Termosztát ... 17
3.4.2 Termisztor [10] ... 18
3.4.3 RTD - Ellenállásos hőmérséklet érzékelő [11] ... 18
3.4.4 PRT Platina ellenállásos hőmérő [11] ... 18
3.4.5 Termoelemek hőmérő [12] ... 19
3.4.6 Infravörös (IR) hőmérő [13] ... 20
4 Összefoglalás ... 21
5 Felhasznált irodalom ... 22

1 Bevezetés

Napjainkban a mindennapi emberi tevékenységekben használunk különféle elektronikus készüléket vagy eszközt. Az egyszerű emberben sokszor nem is tudatosul az, hogy ezekben az eszközökben szenzorok is találhatóak, igény meg van rá, ezért is nagy figyelmet fektetnek ezeknek az érzékelőknek a fejlesztésére. Ha egy szenzor gyártása megszűnik, akkor a helyére egy másik érzékelőt kell keresni. Természetesen ma már bőven van választási lehetőség, hiszen rengeteg féle létezik és folyamatosan jellenek meg új technológiák. A szenzorok lehetővé teszik sok műszaki és természettudományokkal kapcsolatos tulajdonság, mennyiség érzékelését, mint a hőmérséklet, távolság, gyorsulás. Az emberi érzékszerveket helyettesíthetjük vele, persze sokkal több mindenre képesek ezek az érzékelők. A szenzorika mint tudományág nagyon gyorsan fejlődik és még sokáig fejlődni is fog. Egy műszaki területen dolgozó embereknek, mint akár mi nekünk informatikusoknak elkerülhetetlen, hogy találkozzunk és foglalkozzunk is ezzel a tudományággal. Hiszen szenzorok vannak akár az otthoni konyhai eszközökben, videótechnikai eszközökben, telefonokban stb. Ezeknek a szenzoroknak kifejlesztéséhez, gyártásához és megfelelő alkalmazásához is tudással kell rendelkeznünk a természettudomány területein, fizikai, kémiai és műszaki ismeretekre is egyaránt szükségünk van. Ez a dolgozat a szenzorok jellemzéséről, tulajdonságairól fog szólni és azok fajtáiról, inkább felhasználási és működési szempontból.

2 Szenzor fogalma [1] [2] [3]

Akkor mi is az a szenzor? A latin „sentire” szóból ered az elnevezése, melynek jelentése észlel, érzékel. A szenzorok egyfajta jelátalakítók, amelyek mennyiséget, tulajdonságot vagy valamilyen nem villamos jelet, mechanikus, kémiai, mágneses, hőmérséklettel és optikával kapcsolatos jeleket villamos jellé alakítanak át, néha pneumatikus jellé is. Mérésérzékelőnek, detektornak, mérőváltónak, mérés jeladónak vagy energia átalakítónak is szokták nevezni. A jel maga tovább vezethető, erősíthető, szűrhető és fel is lehet dolgozni. A szenzorok lehetnek fizikai mennyiséget mérő szenzorok vagy szoftver szenzorok, melyeket figyelőknek is nevezünk. A bemeneti jeleket az információ feldolgozónak juttatják át analóg, digitális vagy hibrid formában, majd az aktuátorok meghatározzák a mért jelek alapján a kimeneti tevékenységet vagy beavatkozást. A szenzorokat többféleképpen is feloszthatjuk, osztályozhatjuk. Ilyen felosztások például a passzív vagy aktív szenzorok, abszolút vagy növekményes, esetleg analóg vagy digitális elven működő szenzorok.
Léteznek még fontos fogalmak. Ilyen a szenzorelem, mely a szenzornak az a része, amely a mért értéket megállapítja.



1. Ábra: A szenzorok felépítése
Forrás:
https://oszkdk.oszk.hu/storage/00/00/60/42/dd/1/Banlaki_Lovas_Szenzorika_es_anyagai.pdf

Az integrált szenzor az, amikor több szenzort vagy szenzorelemet együtt használva oldunk meg egy mérést. Az intelligens szenzor pedig analóg fizikai jeleket mérnek, mint a nyomás, hőmérséklet, sebesség. Ezek a szenzorok tartalmaznak az ábrán is látható analóg- digitális átalakítót, mely az analóg jelet digitálissá alakítja, hogy továbbítható legyen az aktuátor felé, ami gyakran egy mikroszámítógép.

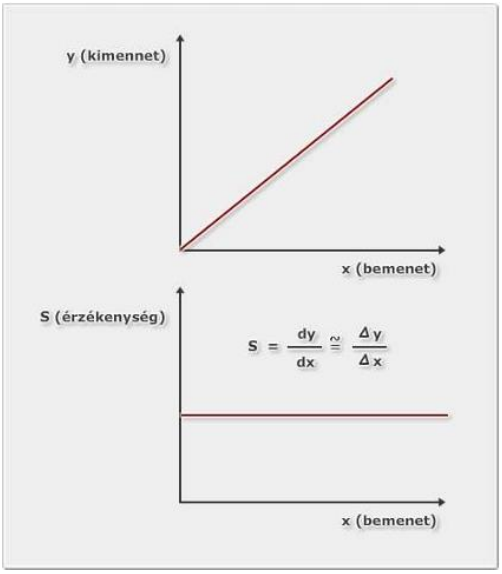
2.1 Szenzorok csoportosítása

A szenzoroknak rengeteg fajtája létezik, melyeket felosztjuk tudományágak szerint, ezek a mechanika, termodinamika, villamos, mágnes és kémiai, fizika területek. Mechanikai érzékelőkkel mérhetünk távolságot, szöget, elmozdulást, erőt, nyomást, fordulatszámot, sebességet, gyorsulást, ultrahangot és egyéb hanghullámokat, frekvenciát, tömeget, sűrűséget stb.

Vannak termikus mennyiségeket mérő szenzorok, mint a hőmérsékletet és vele kapcsolatos mennyiségeket mérnek. Elektromos és mágneses mennyiségek azok a terek, töltés, feszültség, áram, ellenállás vagy kémiai, fizikai mennyiségek, mint például a pH-érték, nedvesség, hővezetés, portartalom, különböző anyagok molekulái, optikai mennyiségek, sugárzások és még sok más mennyiség mérésére is alkalmasak. Csoportosíthatunk még jelek alapján is: Elektromos jel, kémiai jel, mágneses jel, mechanikai jel, sugárzás, termikus jel. Kölcsönhatás alapján fizikai, kémiai és bioérzékelők.
A generátor típusúak vagy aktív szenzorok nem igényelnek külön energiaforrást, mert a vizsgált közegből nyerik a működéshez szükséges energiát, vannak modulátor vagy passzív érzékelők, melyeknek külső energiaforrásra van szükség a mennyiségek megállapításához.

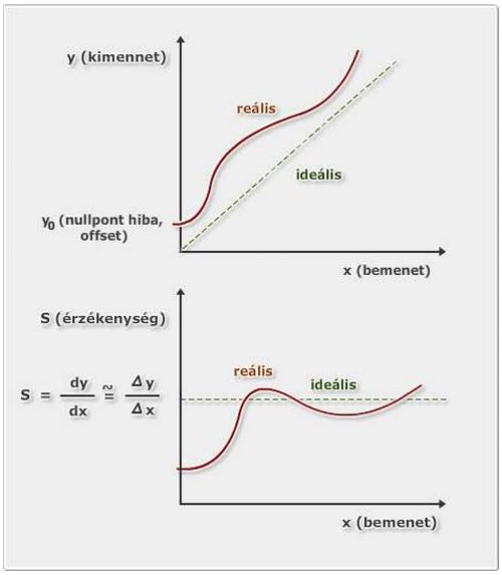
2.2 Szenzorok jellemzői

Statikus karakterisztika: A bemeneti jel és a kimeneti jel közötti függvénykapcsolatot írja le ez a jellemző. Az ideális szenzorra jellemző, hogy tökéletesen lineáris (be és kimeneti jelek között egyenes az arányosság) és zajmentes a karakterisztikája, valamint érzékenysége a bemenethez viszonyítva állandó, ahogy a következő ábrán is látható:



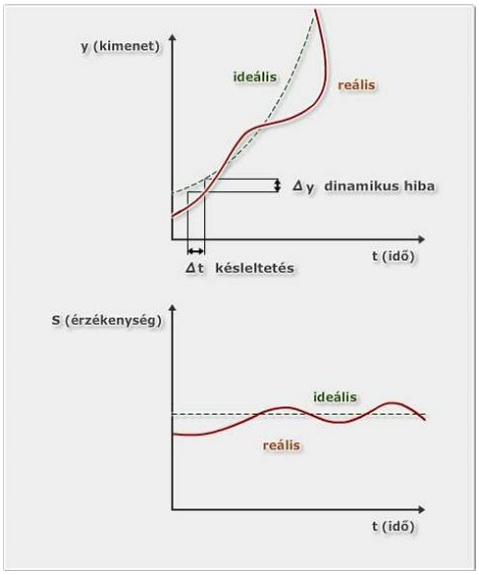
2. Ábra: A szenzor ideális karakterisztikája
Forrás: https://cserviktamas.wordpress.com/2022/09/07/szenzorok-es-meroatalakitok/

A nem ideális karakterisztika nem lineáris és gyakran nem is érinti az origót. Ez a nullpont hiba vagy offset. Az ilyen szenzoroknál az érzékenységet a görbe meredeksége határozza meg, tehát nem állandó, mint az ideális esetben.



3. Ábra: A szenzor reális karakterisztikája
Forrás: https://cserviktamas.wordpress.com/2022/09/07/szenzorok-es-meroatalakitok/

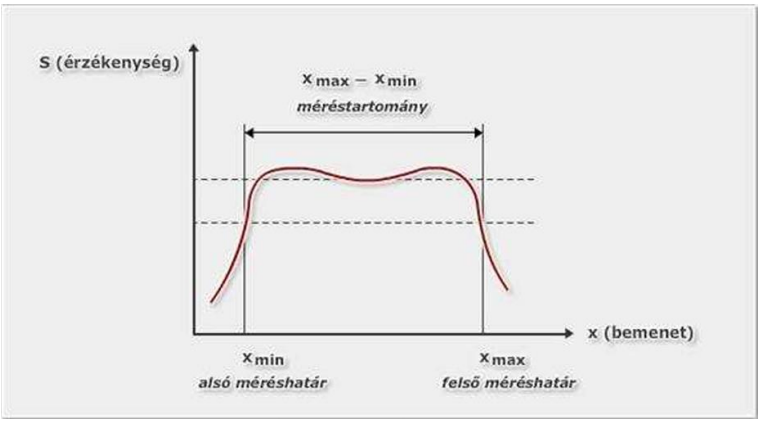
Dinamikus karakterisztika: A szenzorokat gyakran nem statikus mérésekre használjuk. Ilyenkor a kimenet nem a bemenet szerint változik, hanem az idő mértékében. Itt fontos az, hogy a szenzor mennyi idő alatt válaszol az adott eseményre. A 4. ábrán látható az ideális és a reális karakterisztikája közti különbség.



4. Ábra: A szenzor dinamikus karakterisztikája
Forrás: https://cserviktamas.wordpress.com/2022/09/07/szenzorok-es-meroatalakitok/

A reális szenzor kimenete az általában Δt késleltetéssel késik az ideálishoz képest és dinamikus hiba is léphet fel. Az is lehetséges, hogy korábban jelentkezik a jelenség. Beszélhetünk még a tranziens hibáról is, amelyre jellemző egy adott idő után eltűnik.
A feloldás a szenzor azon paramétere, mely megadja azt a legkisebb bemeneti mennyiség változást, melyre a kimenet megváltozik, ezért számunkra minél kisebb ez a mennyiség annál jobb. Tehát lesznek olyan kicsi bemeneti jelek, melyekre nem tud választ adni a szenzor és lehetnek olyan nagy jelek is, amelyre pedig alig ad változást

a kimenet. Az utóbbit nevezzük telítődésnek, mely megadja a felső méréshatárt. A szenzor mérési tartománya az alsó és felső méréshatár különbsége.



5. Ábra: A szenzor mérési tartománya
Forrás: https://cserviktamas.wordpress.com/2022/09/07/szenzorok-es-meroatalakitok/

Egyéb fontosabb jellemzők és hibák:

A szenzornak van még alsó és felső határfrekvenciája is, melyek különbsége a sávszélesség. A hiszterézis hiba a kimeneti jel maximális lehetséges eltérése egy adott tartományban növekvő vagy csökkenő paraméter változás. Okozója legtöbbször a súrlódás. Ismétlési hiba az eltérést adja meg a kimeneti jelben az ismételten elvégzett mérések között. A beállási idő az az időtartam, amely alatt a válaszjel tranziense egy adott hibahatáron belül eléri az állandósult értéket a mérendő paraméter ugrásszerű megváltozása esetén.
Egy ideális szenzorra jellemző az, hogy nincs nullponthiba, nincs felfutási idő, a sávszélesség végtelen nagy a mérési tartománya és végtelenül kicsi a feloldás. A nem ideális szenzornál fellépnek nem kívánatos jellemzők, mint a kimenet nem egyenesen arányos a bemenettel, lassan éri el a kimenet az állandósult állapotot, a működési tartomány és sávszélessége korlátozott, a kis bemenetekre nem ad választ és a kimenet megváltozhat az idő függvényében a hő hatására. Öregedés, interferencia és zajok miatt is változhat a kimenet.

3 Szenzor fajták és jellemzésük

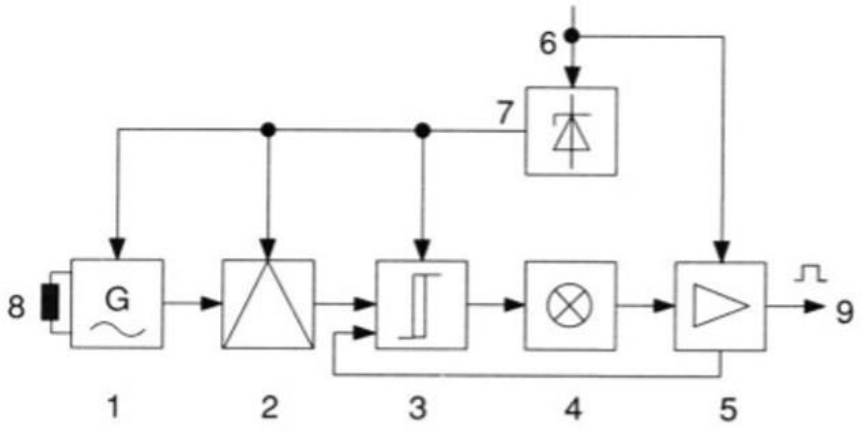
3.1 Közelítéskapcsolók

A közelítéskapcsolók bináris elven működnek, jelzik egy objektum jelenlétét, hogy az objektum az érzékelő előtt van vagy nincs. Előnyük a bemeneti és kimeneti jelek egyértelműen megadhatók. A szenzor kisméretű, ezért könnyű használni. Nem alkotnak mechanikai kapcsolatot az objektummal, ezért könnyű karbantartani. Gyorsabbak is mint mechanikus kapcsolók. Működése megfigyelhető távolból is.

3.1.1 Induktív szenzorok [4][5]

Az iparban rengeteg helyen használunk induktív szenzorokat, mint az automatizálásban. Megfelelő pneumatikus, hidraulikus munkahenger helyzetének jelzésére, munkadarabot szállító gépek helyzetének érzékelésére, valamilyen fémek számolására a futószalagon, fordulatszám mérése stb. Előnye, hogy érintésmentesen működik, ellenáll rezgésnek, pornak, nedvességnek és nagy az ismétlési pontossága. Közelítéskapcsolóknak és iniciátoroknak is szokták nevezni. Közvetlenül kapcsolható elektronikus áramkörökhöz, PLC bemenetekhez, relékhez.
Felépítése a 6. ábra alapján [5]:

1. Oszcillátor
2. Amplitúdó demodulátor
3. Trigger/komparátor
4. LED kapcsolási állapot jelzésére
5. Kimenet visszacsatolása
6. Tápfeszültség
7. Belső feszültségszabályzó
8. Tekercs
9. Kimenet



6. Ábra: Az induktív szenzor felépítése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

Az oszcillátor erősítőből, pozitív visszacsatolásból és frekvenciameghatározó elemből áll. A frekvenciameghatározó elem egy LC- rezgőkör (tekercs + kondenzátor). A

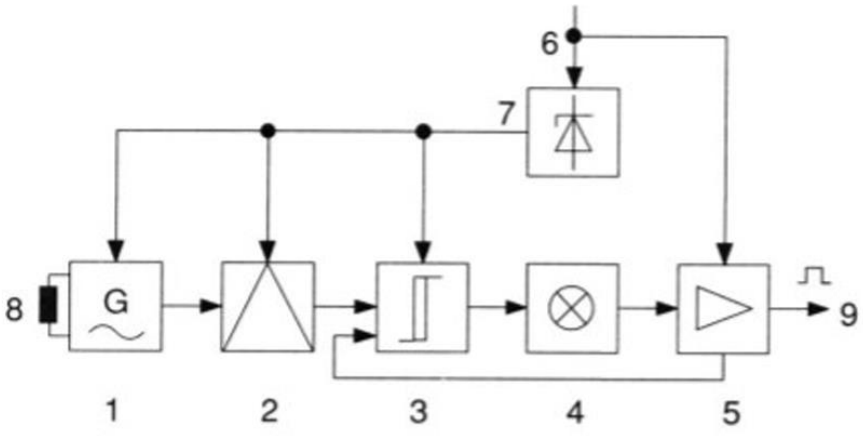
rezgőkör frekvenciája 100kHz és 1MHz között van. A rezgőkör frekvenciáját a kapacitás és az induktivitás határozza meg.
Ez kiszámítható a következő képlettel:

$$f \approx \frac{1}{2 \cdot \pi \cdot \sqrt{L \cdot C}}$$

Nagyon biztonságosak, mert nincsenek nagy zavarások. Az induktív szenzor a saját mágneses terének megváltozását érzékeli. Az LC rezgőkör nagy frekvenciával változó teret hoz létre, mely kilép az érzékelő aktív felületén levő nyíláson. Egy vezető anyag a szenzor elé érve megváltoztatja a mágneses teret, módosítja az erővonalak hosszát. A rezgésamplitúdó lecsökken. Ennek hatására a szenzor tekercsének impedanciája megváltozik. Ezt a változást az elektronika kiértékeli és ennek hatására a kimeneti jelet változtatja a szenzor. A tárgyban örvényáram jelentkezik és beszélhetünk örvényáramú veszteségről. Az érzékelési tartomány függ a tárgy anyagától. Ferromágneses anyagnál, mely lehet vas, acél, nikkel, ötvözetek stb., átmágnesezési veszteség és örvényáramú veszteség is lép fel. Az érzékelő energia felvétele kicsi, ezért nincs mágnesező hatása a fémtárgyra, nem okoz rádióvételi zavarokat és nem melegszik a fémtárgy.
Az oszcillátor szinuszos rezgését egy demodulátor egyenirányítja és a trigger értékeli ki. Az oszcillátor áramának változása erősített analóg jelként, vagy digitális jelként kerül a kimenetre. A komparátor két bementi jel összehasonlítását végzi.
Az induktív szenzorok 0,8-100 mm távolságban képesek érzékelni. Ez függ a fémtárgy anyagának elektromos vezetőképességétől, kisebb ellenállás kisebb örvényáram veszteséget okoz, tekercs átmérőjétől, minél nagyobb annál nagyobb a kapcsolási távolság.
Léteznek a fémbe szorosan szintbe építhető érzékelők és nem szintbe építhetők is. A fémbe építhetők kapcsolási távolsága kicsi, mert a mágneses erővonalak csak a felületre merőlegesen lépnek ki az árnyékolás miatt.
A szenzor kialakítása lehet hengeres, villás, gyűrűs, hasáb alakú. Készülhetnek 2,3,4 huzalos csatlakozású kivitelben. Lehetnek nyitó, záró és kizáró működésűek. Kimenetük száma lehet egy vagy kettő.

3.1.2 Kapacitív szenzorok [5]

Egy kondenzátort tartalmaz, ami az aktív elem szerepét tölti be. Ha fém vagy elektromosan szigetelőanyag kerül az érzékelési zónába, akkor kapacitásváltozással fog járni. Alkalmas még folyékony, szemcsés és porított anyagok érzékelésére is. Olyankor használják, ha az induktív érzékelő nem használható megfelelően. A kapacitív szenzornál a frekvenciameghatározó elem egy Wien-hidas RC- oszcillátor, amely akkor rezeg be, ha kapacitás megváltozik.



7. Ábra: A kapacitív szenzor felépítése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

A felépítése szinte megegyezik az induktív érzékelőkkel. Potenciométerrel állítható az érzékenység. Különbség az amplitúdómoduláció helyett frekvenciamoduláció van és mágneses tér helyett elektromos teret hasznosítja. Az oszcillátor frekvenciája:

$$f \approx \frac{1}{2 \cdot \pi \cdot R \cdot C}$$

A kapacitásváltozás függ a mért tárgy helyzetétől és távolságától, az érzékelő anyag dielektromos állandójától és a tárgy méreteitől. Ha egy nem vezető anyagot szeretnénk a szenzorral érzékelni, akkor ettől a dielektromos állandóval egyenes és a távolsággal fordított arányban változik a kapacitás. Vezető anyagnál lehet a legnagyobb a szenzor és a tárgy közti távolság. Érzékenysége ΔC kapacitásváltozással adható meg, ami a szenzor kimenetén a jel változásával következik be.
Felhasználásuk során ügyelni kell arra, hogy érzékenyek a szennyeződésekre és vízre, nedves környezetben zavar keletkezhet. Viszont 4 mm-nél kisebb falon keresztül is tud érzékelni, ha az anyagnak legalább négyszeres a dielektromos állandója a fal anyagához képest. Érzékelési távolság 50mm-ig és 100Hz a maximális frekvencia, amelyen működnek.
Vannak síkba és síkba nem építhető változatban is. Henger vagy hasáb alakúak.

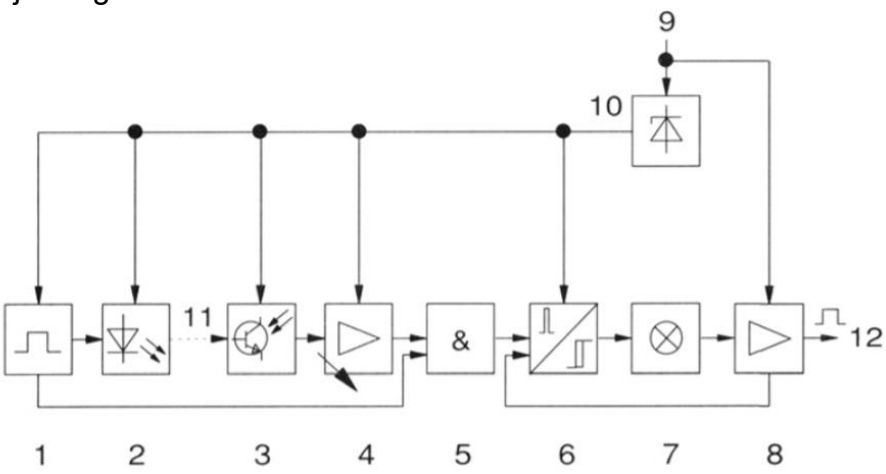
3.1.3 Pneumatikus szenzorok [5]

Az érzékelő rendelkezik egy fúvókával, a végén nyílással. A fúvókából kiáramló levegő mozgási energiáját alakítják át nyomássá. Tehát levegősugár torlónyomását használják fel pneumatikus szelepek működtetéséhez. Ezekkel olyan berendezések építhetők melyekhez nincs szükség áramra. Közvetlen fizikai kapcsolatra sincs szükség a tárgy és a szenzor között. Érzékeny felületű elemek is figyelhetőek. Nincs kopás, ezért hosszú az élettartam. Bármilyen testet képesek vagyunk érzékelni vele. Hátránya a kapcsolási idő sokkal hosszabb a többi szenzorhoz képest. Megoldásai: torlónyomás érzékelő, Gyűrűs légsugár érzékelő, légsorompó.

3.1.4 Optikai szenzorok [1][5]

Ezek a szenzorok optikai és elektronikai eszközöket használnak fel az objektumok helyzetének jelzésére. LED a fényforrás a kis méret és hosszú élettartam miatt. A fényjelet fotodióda vagy fototranzisztor érzékeli. Általában infravörös vagy vörös fényt használnak., ez azért jó, mert jól látható, kicsi a csillapítása, kisebbek a zavarások nagy fényerő és nagy távolságra alkalmas fény. Mégis a környezetből származó zavaró fényhatásokat ki kell védeni, ezért az optikai jelet modulálják. Fényszűrőket is alkalmaznak.
A kapcsolás szempontjából lehet:

- Alapból nyitott – a vevő kimenete zárt, ha a fénysugár útját nem szakítja meg semmi sem.
- Alapból zárt - a vevő kimenete zárt, ha a fénysugár útját valamilyen objektum szakítja meg.



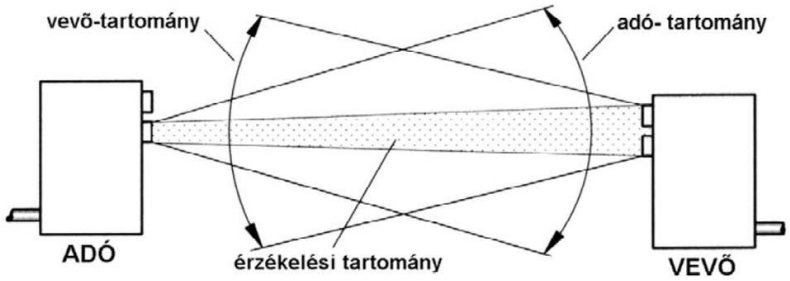
8. Ábra: Az optikai szenzor felépítése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

Felépítése a 8. ábra alapján [5]:

1. Oszcillátor
2. Fotoelektromos adó - LED
3. Fotoelektromos vevő – fotodióda vagy fototranzisztor
4. Előerősítő
5. Elektronikus csatolás
6. Impulzus/jelszint átalakító fokozat
7. LED kapcsolási állapot jelzésére
8. Kimenet visszacsatolása 9. Külső feszültségforrás
9. Feszültségstabilizátor
10. Optikai szakasz
11. Kapcsoló kimenet

Létezik egyutú fénykapus, reflexiós fénykapus és tárgyreflexiós megoldás.

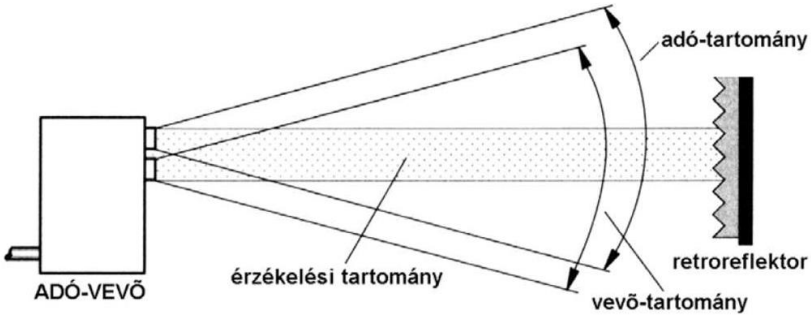
Egyutú fénykapu



9. Ábra: Az egyutó fénykapus optikai szenzor működése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

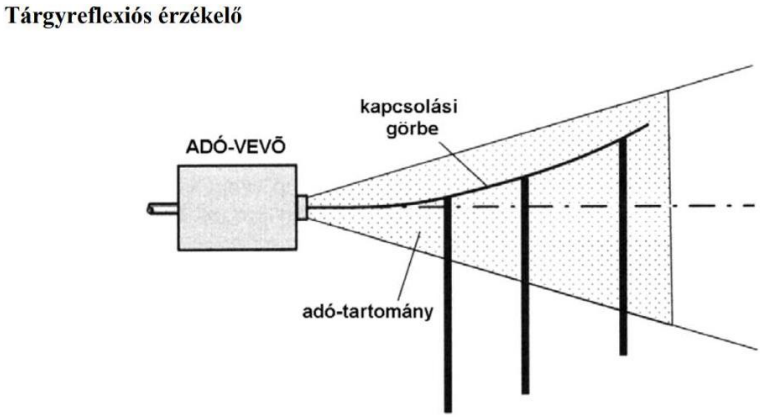
Előnye a nagyobb biztonság, nagy az ismétlési pontosság, kis méretű tárgyak nagy távolságból is érzékelhetőek, nagy pozicionálási pontosság. Hátránya az, hogy külön adóból és vevőből áll. Az adó fényjelét érzékeli a vevő és ez alapján dönti el, hogy van ott objektum vagy nincs. Az átlátszó objektumokat nem tudja jelezni.

Reflexiós fénykapu



10. Ábra: A reflexiós fénykapus optikai szenzor működése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

Előnye a nagy érzékelési biztonság, egyszerű a beállítása, az adó és vevő egybe van építve, ezért egyszerűbb és olcsóbb kialakítás. Nagyobb az érzékelési távolság a tárgyreflexiós érzékelőhez képest, de az egyutúhoz képest kisebb. A fényt szórtan visszaverő, kevésbé tükröződő és átlátszó tárgyak érzékelésére is képes. Hátránya a nagyon átlátszó és tükröződő objektumokat nem tudja jelezni. Az adó része által kibocsátott fényt egy tükörrel vagy reflektorral kell visszaverni, hogy a szenzor vevője detektálni tudja a jelet. Ezt a tükröt pontosan kell beszerelni, beállítani és karban kell tartani a fény megfelelő visszajuttatása végett a szenzorba.



11. Ábra: A tárgyreflexiós optikai szenzor működése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

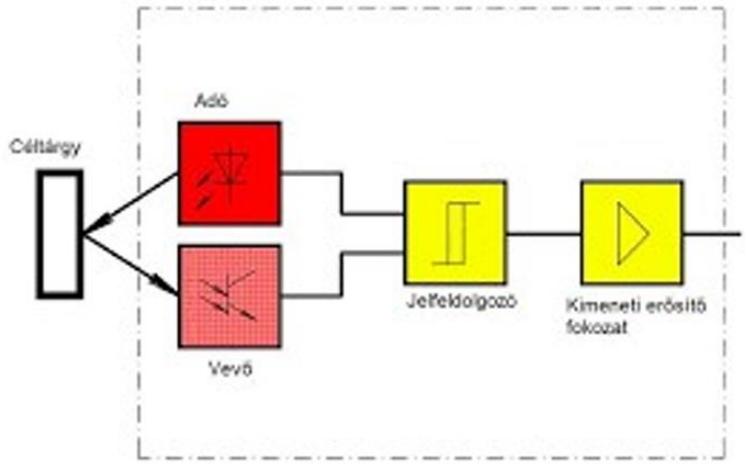
Az adó és a vevő szintén egy eszköz, sőt tükörre sincs szükség. A fényt szórtan visszaverő, kevésbé tükröződő és átlátszó tárgyak érzékelésére is képes. Bármilyen irányból jövő objektumokat képes jelezni. Hátránya a visszavert fény iránya nem egzakt, a fénykapus megoldások pontosabbak. Kicsi az érzékelési tartomány. Fényelnyelő objektumokat nem tud érzékelni. Ez a megoldás kevésbé jó megoldás a fénykapusokhoz képest, de olcsóbb a kivitelezés, hiszen csak egy adó-vevő kell hozzá.

Az optikai szenzor potenciométerrel való beállítást úgy kell végezni, hogy a tárgyakon túli tartomány kívül essen az érzékelési távolságon. Fontos figyelni a szennyeződésekre, melyek jelerősség 11 csökkenést okoznak és ez szerint kell beállítani és elhelyezni az érzékelőt. Fontos paraméter a tartalékfaktor, amely az aktuális jelerősség és a minimálisan érzékelhető jelerősség hányadosa. A távolság növekedésével csökken.
Az optikai fényérzékelőknél gyakran használnak fényvezetőket is, amikor a tárgy melyet érzékelni szeretnénk nehezen megközelíthető, segít a kisméretű objektumok érzékelésében is, valamint az érzékelési pont mozgatható. A fényvezető lehet polimer vagy üvegszál, néha több tükröt is bevetnek a fény megfelelő irányításához. A polimer jobban tűri a mechanikai hatásokat, egyszerűen méretre vágható és olcsóbb. Az üvegszál magasabb hőmérsékleten is használható, kis csillapítással és öregedéssel rendelkezik.
Az optikai szenzort használják gyártás során szerszám, valamilyen berendezés mozgásának felügyeletére, hibás elhelyezés detektálására stb.

3.1.5 Optoelektronikai szenzorok [1]

Az optoelektronikai szenzorok elektromos áramot alakítanak át fénnyé vagy fordítva. Hasonlóak a sima optikai szenzorokhoz. Ultraviola, látható fény és infravörös tartományon belül. Adónak LED-et vagy félvezető lézerdiódát alkalmaznak. LED-ek infravörös vagy vörös pulzáló fényt bocsátanak ki. A fény a tárgyról visszaverődik. Vevőnek pedig fotodiódát, foto-tranzisztort vagy pozíció érzékeny diódát alkalmaznak. A feladatuk az optikai jelet árammá alakítani. A három RGB alapszínt használják fel. Ezeket fehér fény előállítására vagy a vevő által a beeső fényt RGB színekre bontja, ebből a tárgy színe meghatározható. Fényvisszaverő és fényáteresztő tárgyak

érzékelhetők a szenzorral 100m-ig. Maximális működési frekvenciája 1,5 kHz. Szintén használható hozzá fényhullám vezető.
Előnye a hő- és nyomásváltozás nincs hatással, kis méretű tárgyak érzékelésére is alkalmas nagy távolságból.
Hátránya az érzékeny a szennyeződésekre, külső fények befolyásolják az érzékelést. Megoldásai a tárgyreflexiós érzékelő, egyutas fénysorompó, kétutas, tükörreflexiós fénysorompó. Az utóbbi kettő átlátszó anyagok esetén nem alkalmas.

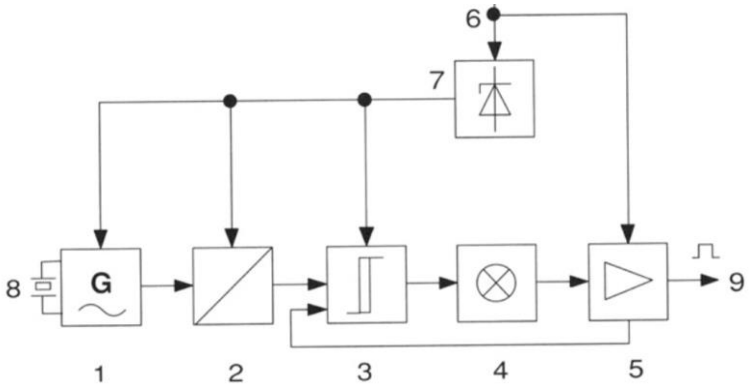


12.Ábra: Az optoelektronikai szenzor felépítése
Forrás: http://midra.uni-miskolc.hu/document/22484/16902.pdf

A szenzor jelét modulálják a zavarok csökkentése miatt. A vevőnek és az adónak szinkronban kell működniük. Tartalmaz egy jelfeldolgozó egységet, valamint kimeneti erősítőt a feldolgozott jel erősítésére, hogy a szenzorhoz csatolt mikrovezérlő áramkör megfelelő erősségű jelet kapjon.

3.1.6 Ultrahang szenzorok [1][5]

Nagyfrekvenciás hanghullámok visszaverődése és érzékelését használja fel a működéshez. Egy rövid impulzusszerű jelet küld, majd a visszavert jelet érzékeli. A használt hang frekvenciája 30-300kHz között van, az ismétlés frekvenciája pedig 1-100Hz. Szűrőkapcsolást használnak a környezetből származó zavarok kizárására. Kis tárgyak esetén figyelni kell a megfelelő beállításra. A hangot jól elnyelő anyagok detektálására nem alkalmas, ilyen például a habszivacs, szövet. A hanghullámok iránya is megtörhető, így kis, nehezen hozzáférhető objektumok jelzésére is alkalmas. A meleg levegő nagy zavarást okozhat.



13. Ábra: Az ultrahang szenzor felépítése
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

Felépítése a 13. ábra alapján [5]:

1. Oszcillátor
2. Kiértékelő egység
3. Trigger fokozat
4. LED kapcsolási állapot jelzésére
5. Kimenet visszacsatolása
6. Külső feszültségforrás
7. Feszültség stabilizátor
8. Aktív zóna
9. Kimenet

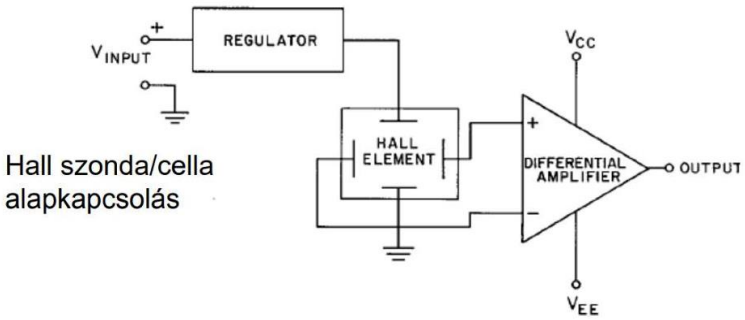
Az ultrahang előállításához piezokerámiás átalakítókat vagy elektrosztatikus átalakítókat alkalmaznak a leggyakrabban. A piezokerámiás átalakítóknál a hajlító oszcillátorra kapcsolt feszültség hatására a piezokerámia tárcsa átmérője megváltozik és elhajlik. A membrán oszcillátornál a rugalmas fém membránt a piezo rezgeti. A piezokerámia és a levegő közé épített réteggel növelik az átviteli tényezőt, hogy megfelelő hangkisugárzás legyen. Ez üreges üveggömb és műgyantából készül. Ezt a réteget úgy kell méretezni, hogy annak vastagsága a hullámhossz negyed része legyen. Ez a rezonanciafrekvenciát növeli és befolyásolja az amplitúdó erősítést. Ezeket tokozott kivitelben gyártják és jellemző a széles visszaverődési karakterisztika, alacsony frekvencia és hangszint, nagy a csillapodási idő.
A kiértékelő elektronika trigger impulzust állít elő, ezen impulzus és a visszavert hang belépése közti időt számítja ki. Az első visszavert hang megérkezése után várnia kell a szenzornak, amíg a távolabb lévő tárgyakról már nem érkezik visszhang, persze van egy adott idő ameddig maximálisan várakozik. 13 Az ultrahang szenzorokat távolságmérésre is gyakran helyezik üzembe. Ilyenkor a visszhang- terjedési időnek mérését hasznosítják. A visszhang kiértékelése ugyanott történik, ahol kibocsátották az ultrahangot. Ezt letapogató üzemmódnak is nevezik.
A későn visszajutó ultrahangok problémát okozhatnak az érzékelésben ezért azokat semlegesíteni kell. Ezért a trigger impulzusok után az idő függvényében folyamatosan növelik az erősítést. Ezért az utolsó előtt kiadott nagy távolságból érkező hangokat nem regisztrálja a szenzor.

3.2 Hall szenzorok [7]

A félvezetőben a külső mágneses térben az áramot hordó töltésekre ható erőn alapul. Ezt Lorentz erőnek is nevezik. Egy hosszú, vékony lemez eszközre merőleges irányú mágneses tér hat, mely az áramot hordozó elektronokat vagy lyukakat eltéríti, így a lemez két szélén ellentétes előjelű töltések halmozódnak fel, melyek keresztirányú Hall-feszültséget hoznak létre. Képlete:

$$U_H = K*I*B$$

I az áram, B a mágneses indukció, UH a Hall-feszültség, K érzékenységi állandó, mely geometriai és anyagi tulajdonságokat jelenti. A kimeneti jele lineáris. A Hall-generátor szilíciumból, gallium arzenidből vagy indium-antimonidból készül.



14. Ábra: A Hall-szenzor kapcsolása
Forrás: http://uni-obuda.hu/users/pap.andrea/szenzorok/2016szenzor_11.pdf

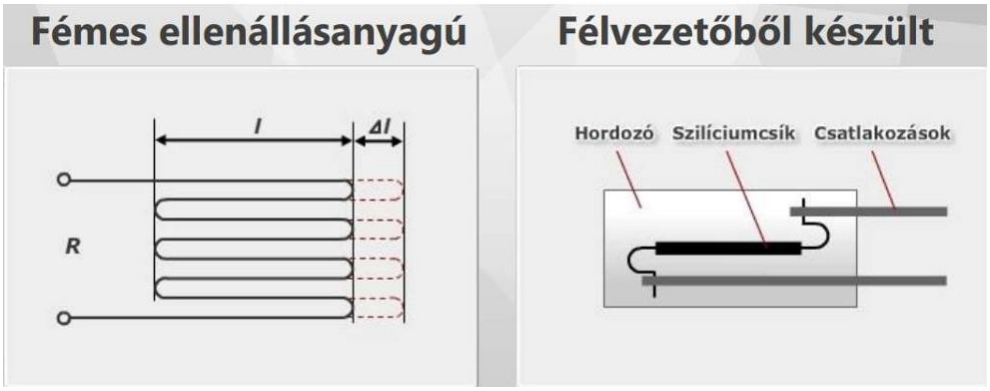
A Hall-feszültség alacsony szintű jel, ezért ezt fel kell erősíteni. Ez a differenciálerősítő feladata. Gyártják analóg és digitális kimenettel is ezeket a szenzorokat, valamint léteznek programozható Hall szenzorok is.

3.3 Ellenállásos szenzorok [8]

Sugárzások, hőmérsékletváltozás vagy mechanikai erő ellenállásváltozással jár és ez alapjáén működnek ezek a szenzorok. Érzékelő elem egy ellenállás, típusa függ a vizsgálattól, tehát lehet szilárd, cseppfolyós, gáz kivitelezésű. A szilárd anyagból készülteket mechanikai erő és hőmérséklet mérésekor használják. Fémből vagy félvezetőből gyártják.

$$R = \rho \frac{l}{S}$$

Ellenállása megváltozik, ha a képletben szereplő értékek megváltoznak, általában a hosszt és a keresztmetszetet változtatják. Ellenállásuk a hőmérséklettől is függ.
Potenciométerek is használnak, melyek állítható ellenállások. Lehet forgó (szolenoidos kivitel vagy grafit érzékelővel) vagy egyenes vonalú.
Léteznek nyúlásmérő bélyegek is. Két fajtája létezik:



15. Ábra: Nyúlásmérő bélyegek
Forrás: http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

Ha a keresztmetszet csökken akkor növekszik az ellenállás, keresztmetszet növekedés pedig ellenállás csökkenést okoz. Ezekkel lehetséges elmozdulást, erőt, nyomást, sebességet, gyorsulást mérni. Ezeket általában hidakba kötik, mint a Wheatstone-híd. A híd ágában megjelenő villamos feszültség nagysága arányos a mérendő mechanikai feszültséggel, ebből visszakövetkeztethető a megnyúlás.

3.4 Hőmérséklet mérő szenzorok [9]

A hőmérséklet mérésére is használunk szenzorokat, melyek nagyrészt fizikai paramétereiktől függenek. A hőmérsékletet több módszerrel is mérhetjük, ilyen a térfogatváltozással járó hőtágulás, elektromos jellemzők, mint az ellenállás, feszültség, kapacitás, sugárzás. Ebből adódóan rengeteg féle szenzor létezik. Ezeket két részre osztják, érintéses és nem érintéses hőmérséklet merő szenzorok. Az érintésesnél érthető, hogy fizikai kapcsolat van a mért objektummal és folyamatos hőmérsékletváltozás megfigyelése is lehetőség számunkra. Az érintés nélkülinél általában sugárzást használnak a mérésre. Ezekkel kevésbé figyelhető meg folyamatosan a hőmérsékletváltozás.
A szenzorokat besoroljuk még elektromechanikus, elektronikus és ellenállás szenzorokra. Tehát az előző fejezetekben írt ellenállásos szenzorok is alkalmasak lehetnek hőmérséklet mérésre.

3.4.1 Termosztát

Egy elektromechanikus érintéses szenzor. Két fémes anyagból gyártják, mely lehet nikkel, réz, alumínium, többnyire fémoxid keverékből is, ezért elöregednek. Általában szalag kivitelezésű. A fémeknek eltérő a hőtágulási jellemzőjük és ezt a térfogatváltozáson alapuló elhajlást használják ki. Használják elektromos kapcsolóként, termosztátos vezérlőkben, kazánokban, kemencékben, melegvíz felmelegítésére kialakított rendszerekben, autóban és házakban is a fűtésnél, egyéb háztartási eszközöknél.
A termosztát, ha hideg akkor zárt állapotban van és az áram át tud jutni a szalagon. Ha felmelegszik az érintkezés nyílt lesz és az áram nem tud átjutni a termosztáton. Tehát két állapota lehet és ezért kapcsolóként használható. Elég pontatlanok, mert az anyagok hőtágulásához szükséges hőmérséklet nagysága változó, ingadozó lehet.

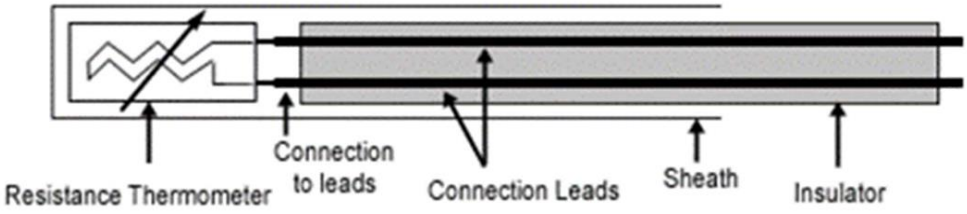
Erre kézileg korrigálható megoldást használnak, amely egy csavar, mellyel beállíthatjuk az eszközt.

3.4.2 Termisztor [10]

Nevét hőérzékeny ellenállás angol rövidítéséből kaptuk. Kerámiából készül a félvezető. Van préselt lemezes vagy golyós megoldása a félvezető anyagnak. Majd ezt hermetikusan lezárják a gyártás során. Előnye a termosztáttal szemben az érzékelési sebesség, pontosság és ismételhetőség. Gyártják NTC – negatív hőmérsékleti együtthatójú és PTC - pozitív hőmérsékleti együtthatójú megoldásban is. Az elsőnek az ellenállása csökken a hőmérséklet növekedéssel, a pozitívnak pedig nő az ellenállása a hőemelkedés során. Fontos értékeik a szobahőmérsékleten meghatározott reagálási idő a hőváltozásra és a rajtuk átfolyó áram. 1 Ω-tól 10 MΩ-ig gyártják a termisztorokat, de a legjobban a kilo nagyságrendűeket lehet hasznosítani. -50 és 250 ºC között lehet velük mérni. Gyártási technológia alapján megkülönböztethetünk gyöngy-, tárcsa-, rúd- és morzsatermisztorokat. A gyöngytermisztorok egy üvegcsőben forrasztott termisztormassza. A tárcsatermisztorok oxidpasztillák adott vastagsággal és átmérővel, amely védőréteggel van bevonva. Rúd kivitelezésű rúd alakú, a hossza és átmérője változó. A morzsatermisztorok kicsik és hasáb alakúak, integrált áramkörökbe és SMD megoldáshoz készülnek.

3.4.3 RTD - Ellenállásos hőmérséklet érzékelő [11]

Tiszta fémekből készülnek, mint a platina, réz vagy nikkel. Melyek egy vékony rétegben vannak egy kerámia hordozóra helyezve. Ezeknek a szenzoroknak a hőmérséklet növekedésével nő az ellenállásukat is és pontos hőmérséklet érzékelésre képesek. Gond a kicsi kimeneti változás (1Ω csak 1ºC változást eredményez). Áram szükséges a működéséhez. -200 és 600 ºC hőmérsékletet mérhetünk vele. Karakterisztikája lineáris.



16. Ábra: RTD fizikai felépítése
Forrás: https://www.electronics-tutorials.ws/io/io_3.html

Az RTD-t fémtokban gyártják sérülés elkerülése végett, melyből két vezetéket vezettek ki. Jó a stabilitása, ezért kedvelt hőmérséklet merő szenzor. Általában a feszültséget mérik a lábain és abból számítják ki a hőmérséklet nagyságát.

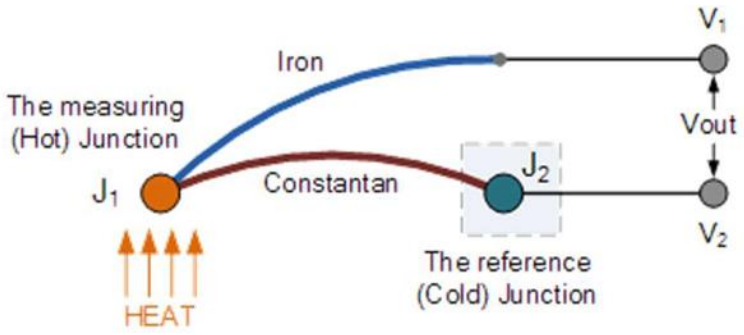
3.4.4 PRT Platina ellenállásos hőmérő [11]

Ez az RTD módosított változata. Teljesen platinából készül. Gyakrabban használják a gyakorlatban, mint a RTD-t, mert jobb jellemzőkkel rendelkezik. Alap ellenállása 0 ºC-on 100Ω és hőmérséklet növekedése megfelelőbb ellenállás változást eredményez.

Hátránya a költséges előállítás, mert a gyártáshoz használt anyagok költségesek. Áram szükséges a működéséhez és -200 - 600ºC között képes a mérésre.

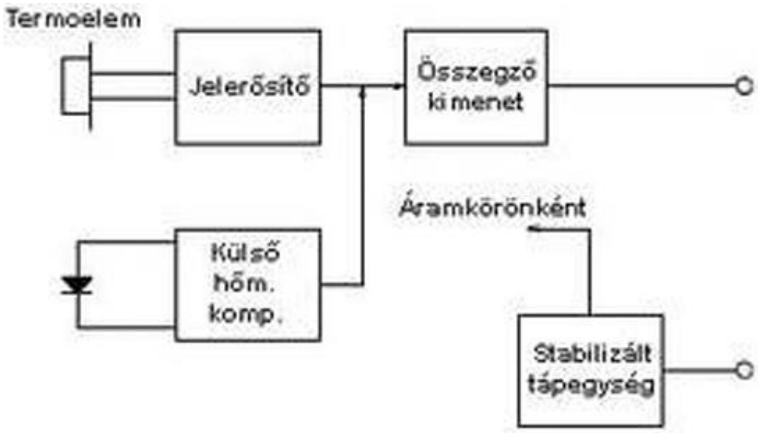
3.4.5 Termoelemek hőmérő [12]

Egyszerű használata és kis mérete miatt szeretik a gyakorlatban. Gyors érzékelés a változásokra. Ez az érzékelő is két fém kapcsolatából épül fel, melyeket egyik végüknél egybeforrasztanak. Két mérőpontja van, az egyiket állandó hőmérsékleten tartják, a másikkal pedig mérnek.



17. Ábra: Termoelem mérőpontjainak felépítése
Forrás: https://www.electronics-tutorials.ws/io/io_3.html

A két pont közti hőmérséklet különbség alapján feszültség gerjesztődik, melyet a kivezetésein megmérnek és ez alapján megkapják a hőmérsékletet. Ez a feszültség csak pár mV környékén van. 200 és 2000 ºC között képes érzékelni, de ez függ az érzékelő anyagától. Gyenge a pontosság, 0,5-5ºC eltérés is lehet. Ennek növelése végett tükröket, lencséket is beleépítenek a tokozásba.



18. Ábra: Termoelem kapcsolási blokkábra
Forrás: https://www.electronics-tutorials.ws/io/io_3.html

A hőelemekhez használnak jelerősítőket (műveleti erősítőt vagy FET tranzisztort) is, hogy könnyebben megállapítható legyen a kis hőmérsékletváltozás is, valamint egy áramkör, hogy a külső hőmérséklet által okozott zavarásokat kivédje (dióda, melynek kimeneti jele az erősítőre van kötve). Alacsony hő mérésekor ez bonyolult lehet. Működése tápegységről megy. Az összegző kimenet összegzi és továbbadja a mért adatokat. Alkalmazzák fülhőmérőkben, lakás klímaszabályozásban, mikrohullámú sütőkben, konyhai szellőztető berendezésekben, gázérzékelőkben és autóipari

területeken való felhasználása is van, mint autó klímaberendezése, vagy a kerekek, féktárcsák hőmérsékletének mérése stb.

3.4.6 Infravörös (IR) hőmérő [13]

Az infravörös (IR) hőmérők olyan eszközök, amelyek érintésmentes hőmérsékletmérést tesznek lehetővé azáltal, hogy érzékelik a tárgyak által kibocsátott infravörös sugárzást. Mivel minden test hőt sugároz ki a hőmérsékletének megfelelően, az infravörös szenzor képes ezt a sugárzást detektálni, és azt elektromos jellé alakítani, amely alapján kiszámítható a tárgy hőmérséklete.
Az IR hőmérők előnye, hogy érintés nélkül képesek mérni, így kiválóan alkalmasak olyan ipari alkalmazásokban, ahol a mért felület elérhetetlen, veszélyes, mozgásban van, vagy túl magas hőmérsékletű. Emellett gyors reakcióidővel rendelkeznek, ami lehetővé teszi a valós idejű megfigyelést és gyors beavatkozást.
Az Ipar 4.0 kontextusában az infravörös hőmérők egyre gyakrabban jelennek meg okos szenzorként, amelyek támogatják a digitális kommunikációs protokollokat, például az IO-Link-et vagy az Ethernet-alapú rendszereket. Ezek a szenzorok képesek közvetlenül adatot továbbítani felhőalapú rendszerekbe vagy edge-eszközökre, lehetővé téve az adatok elemzését, archiválását és a prediktív karbantartás alkalmazását. Az ilyen típusú szenzorok például a Balluff vagy az ifm gyártók kínálatában is megtalálhatók.
Az infravörös hőmérők tipikus ipari alkalmazási területei közé tartozik a fémmegmunkálás (pl. olvasztókemencék felügyelete), az élelmiszeripar (sütési és hűtési folyamatok ellenőrzése), illetve a gépállapot-felügyelet (csapágyak, motorok túlmelegedésének észlelése).

4 Összefoglalás

Rengeteg féle szenzor létezik a mennyiségek mérésére, tárgyak detektálására és egyéb funkciókra, ezért nem is lehet az összeset jellemezni. Kiválasztottam párat melyekkel már én is gyakran találkoztam, ezek főleg közelítéskapcsolók, valamint néhány egyéb típusú szenzorról is írtam.
A dolgozat első felében ismertetem a fontosabb fogalmakat a bevezetés után, majd a szenzorok közt megegyező tulajdonságokról és karakterisztikai jellemzőkről is írtam, mint a statikus és dinamikus karakterisztika, valamint kisebb felsorolás is van arról, hogy miféle szenzorok léteznek és ezeket mi alapján szokás felosztani, csoportosítani. Ezután a 3. fejezetben a szenzorokat jellemeztem, melyekkel gyakran találkozunk a mindennapokban, akár otthon használt eszközeinkben, járművekben vagy egyéb területeken is. Kezdtem a közelítéskapcsolókkal, melyek főleg a tárgyak helyzetének érzékelésére használunk, hogy az objektum az érzékelő előtt van vagy sem. Itt szó volt az induktív, kapacitív, pneumatikus, optikai, optoelektronikai, ultrahang szenzorokról. Ezek után pár sor van a Hall szenzorról, mert középiskolában is többször mértünk vele. Ellenállás szenzor és nyúlásmérő következett. A vége hőmérséklet mérésnél használt hő érzékelőkkel zártam, melyeket szinte minden ember használ a konyhai eszközökben és járművekben.

Tehát elmondhatjuk, hogy a szenzorok az egyik legfontosabb találmányok közé tartoznak és használatuk elengedhetetlen a mai társadalom számára és főleg az ipar megfelelő működéséhez, hiszen rengeteg területen használjuk különféle jelek, mennyiségek mérésére. Egyre jobban kezdenek elterjedni a vezeték nélküli érzékelők is, mint például a víz és áramfogyasztás mérésénél, okos házakban, egészségügyi eszközökben stb. Ezek nagy kapcsolatban állnak az IOT rendszerekkel is. Azért csak most kezdett elterjedni, mert az akkumulátorok cseréje nehézkes, de ma már napenergia és szélenergia felhasználásával nincs is szükség erre.

5 Felhasznált irodalom

[1] Miskolci Egyetem: Szenzorok. Miskolci Egyetem, http://geik.uni-miskolc.hu/intezetek/SZM/content/10/10_6.pdf

[2] Csikósné Dr. Pap Andrea Edit (2016): Szenzorok. Óbudai Egyetem, http://uni-obuda.hu/users/pap.andrea/szenzorok/2016szenzor_01.pdf

[3] Dr. Halmai Attila (2012): Szenzor- és aktuátortechnika. Digitális tankönyvtár, https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2010 0017_07_szenzor_es_aktuatortechnika/ch01s02.html

[4] Juhász Gergely: Induktív szenzor működése. cncpart.hu, https://www.cncpart.hu/induktiv-szenzor-mukodese

[5] Krámli György: Szenzorika. Nyíregyházi Főiskola, http://zeus.nyf.hu/~elat/Szenzorika_Festo.pdf

[6] Koba Máté (2016): Optikai elmozdulás érzékelő illesztése STMF4 mikrovezérlőhöz és robot helyzetérzékelése. Miskolci Egyetem, http://midra.uni-miskolc.hu/document/22484/16902.pdf

[7] Csikósné Dr. Pap Andrea Edit (2015): Szenzorok és mikroáramkörök. Óbudai Egyetem, http://uni-obuda.hu/users/pap.andrea/szenzorok/2016szenzor_11.pdf

[8] Jelenlét, pozíció, elmozdulás érzékelők. https://people.vts.su.ac.rs/~gogolak/files/SzenzAkt/HU2SEN.pdf

[9] Temperature Sensors. ElectronicsTutorials, https://www.electronics-tutorials.ws/io/io_3.html

[10] Valenta László (2013): Érzékelők, működtetők,6.1.2 fejezet: Termisztorok. Digitális tankönyvtár, https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2010 0013_erzekelok_mukodtetok/6_1_2_termisztorok.html

[11] Taking Temperature Measurements with RTDs: How-To Guide (2021-ben frissítve), Engineer Ambitiously, https://knowledge.ni.com/KnowledgeArticleDetails?id=kA03q000000x1rnCAA&l=en US#:~:text=A%20platinum%20resistance%20temperature%20detector,up%20to%20 850%20 %C2%B0C

[12] Kiss Zoltán (2018): A hőelemek és alkalmazásaik. http://www.techstorym2m.hu/a-hoelemek-es-alkalmazasaik.html

[13]**:** ifm electronic. "TW2000 – Smart Infrared Temperature Sensor." https://www.ifm.com

2.39. Alacsony energiaigényű hálózatok szerepe az okosgyárakban

Házi Feladat

Alacsony energiaigényű hálózatok szerepe az okosgyárakban

Tóth Boldizsár Hunor

Gazdasági Informatikus, Bsc

Tartalomjegyzék:

1. Bevezetés 4

2. Az Ipar 4.0 fogalma, jelentősége és digitalizáció 4

2.1 Okosgyárak digitalizációja 5

3. Az alacsony energiaigényű hálózatok szerepe az ipar digitalizációjában 5

4. Alkalmazási területek az iparban 6

4.1. Szenzorhálózatok és adatgyűjtés 6
4.2. Logisztika és eszközkövetés 6
4.3. Prediktív karbantartás 6
4.4. Energia- és környezetmenedzsment 6
5. Az LPWAN-technológiák áttekintése 6
5.1 LoRaWAN (Long Range Wide Area Network) 7
5.2 NB-IoT (Narrowband Internet of Things) 7
5.3 Sigfox 8

6. Vezeték nélküli protokollok összehasonlítása ipari alkalmazás szempontjából 8

6.1 Fő energiafogyasztási tényezők: 10
6.2 Megoldások és optimalizációk: 10

7. Biztonsági kihívások és megoldások az alacsony energiaigényű hálózatokban 10

7.1 Biztonsági kockázatok 11
7.2 Biztonsági megoldások 11

8. Okosgyárak 12

8.1 Az intelligens gyárat alkotó három fő eljárás 13
8.3 Az intelligens gyár előnyei 14
8.4 Intelligens gyári technológiák 15
8.5 Okos gyárak megvalósítása 17
8.6 Okosgyárak (Smart Factories) és az alacsony energiaigényű hálózatok szerepe 19
8.6.1 A kihívás: komplex, dinamikus ipari környezet 19
8.6.2 LPWAN előnyei az okosgyárakban 19

8.6.3 Tipikus okosgyári alkalmazások 20
8.6.4 Példa egy LPWAN-alapú okosgyári megoldásra 21
8.6.5 Jövőbeli fejlesztési irányok okosgyárakban 21
9. Fenntarthatóság és környezeti hatékonyság 22
9.1 Energiafogyasztás csökkentése 22
9.2 Hulladékcsökkentés 22
9.3 Szén-dioxid-kibocsátás mérséklése 23
9.4 Okos városok és zöld ipar 23
10. Összegzés és jövőbeli kilátások 23
Irodalomjegyzék: 25
Ábrajegyzék: 26

1. Bevezetés

Az ipari termelés napjainkban egy olyan technológiai átalakuláson megy keresztül, amelyet az Ipar 4.0 korszaka határoz meg. Ez a forradalom nem csupán új eszközök vagy rendszerek bevezetését jelenti, hanem egy teljesen új gyártási paradigma kialakulását, amelyben a digitalizáció, az automatizáció, a mesterséges intelligencia és a folyamatos adatelemzés kulcsszerepet játszik. Ebben az új környezetben kiemelten fontosak azok a technológiák, amelyek lehetővé teszik a gyártási folyamatok optimalizálását, a költségek csökkentését és a hatékonyság növelését.

Az egyik ilyen kulcstechnológia az alacsony energiaigényű hálózatok (Low-Power Networks, LPN) világa, különösen a vezeték nélküli kommunikáció területén. Az ipari környezetekben használt IoT-eszközök – szenzorok, aktuátorok, beágyazott rendszerek – működtetése gyakran hosszú távú, stabil és energiatakarékos kapcsolatokat igényel. Az LPN technológiák, mint például a LoRaWAN, az NB-IoT vagy a Sigfox, éppen erre nyújtanak megoldást.

2. Az Ipar 4.0 fogalma, jelentősége és digitalizáció

Az Ipar 4.0, vagy más néven a negyedik ipari forradalom, az információs és kommunikációs technológiák integrációját jelenti a gyártási rendszerekbe. A korábbi ipari forradalmak – a gőzgépek (I. ipari forradalom), a tömeggyártás (II.), illetve az automatizáció (III.) – után az Ipar 4.0 új szintre emeli az ipari működést.

Az Ipar 4.0 alapja a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS), amelyek az érzékelők, számítási egységek és kommunikációs modulok integrációját jelentik egy adott ipari környezetben. Ezek az eszközök képesek valós idejű adatokat gyűjteni, elemezni és döntéseket hozni vagy kommunikálni más rendszerekkel. Ezzel lehetővé válik a valós idejű gyártásirányítás, az intelligens döntéstámogatás és a prediktív karbantartás, amelyek jelentős versenyelőnyt biztosíthatnak a vállalatok számára.

Az Ipar 4.0 céljai közé tartozik:

- A termelés rugalmasságának növelése
- A működési költségek csökkentése

- A hibák korai felismerése és megelőzése
- A munkaerő hatékonyabb kihasználása
- A fenntarthatóság és környezeti felelősség előtérbe helyezése

E célok elérésében az alacsony energiafogyasztású kommunikációs megoldások kulcsszerepet játszanak, hiszen lehetővé teszik a gyártósorok és a logisztikai lánc összekapcsolását energiatakarékos módon, alacsony költségek mellett.

2.1 Okosgyárak digitalizációja

A modern okosgyárakban a szenzorok, gépek és rendszerek folyamatosan adatokat gyűjtenek a termelési folyamatokról, a gépek állapotáról és a környezeti feltételekről. Ezek az adatok alapot adnak a prediktív karbantartásnak, a termelés optimalizálásának, valamint a minőség- és energiahatékonyság növelésének.

A digitalizáció révén az okosgyárak képesek önállóan szervezni és optimalizálni folyamataikat, csökkenteni a hibákat, gyorsan reagálni a piaci változásokra, és fenntarthatóbbá tenni működésüket.

3. Az alacsony energiaigényű hálózatok szerepe az ipar digitalizációjában

A modern ipari rendszerek egyre inkább támaszkodnak az adatokra, amelyek forrását jellemzően érzékelők és egyéb IoT-eszközök jelentik. Ezek az eszközök gyakran nehezen hozzáférhető helyeken működnek, ahol nem lehet folyamatos tápellátást biztosítani. Így az energiahatékony, hosszú távon működő hálózati megoldások iránti igény egyre nő.

Az alacsony energiaigényű hálózatok előnyei:

- Hosszú akkumulátor-élettartam: akár több évig is működhetnek karbantartás nélkül
- Nagy lefedettség: LPWAN technológiák akár több kilométeres távolságban is biztosítják a kommunikációt
- Költséghatékony működés: olcsó eszközök és alacsony üzemeltetési költségek
- Skálázhatóság: könnyen bővíthető rendszerek, akár több ezer érzékelővel

A gyártási és logisztikai környezetekben ezek a technológiák lehetővé teszik az automatizált megfigyelést, a valós idejű riportálást, és a folyamatoptimalizálást úgy, hogy közben az energiafelhasználás minimalizált marad.

4. Alkalmazási területek az iparban

4.1. Szenzorhálózatok és adatgyűjtés

Az okosgyárak szíve a szenzorhálózat, amely valós idejű adatokat szolgáltat a termelési folyamatokról, a gépek állapotáról és a környezeti feltételekről. Ezek az adatok lehetővé teszik a gyors reagálást, a hibák megelőzését és a termelés optimalizálását.

4.2. Logisztika és eszközkövetés

Az alacsony energiaigényű eszközök segítségével az áruk mozgása, állapota és helyzete folyamatosan nyomon követhető, akár globális szinten is. Ez különösen fontos az ellátási lánc menedzsmentben, ahol a hatékonyság és a biztonság kulcsfontosságú.

4.3. Prediktív karbantartás

A szenzoradatok elemzése lehetővé teszi a gépek és berendezések állapotának folyamatos monitorozását, így a karbantartásokat előre lehet ütemezni, elkerülve a nem tervezett leállásokat és csökkentve a karbantartási költségeket.

4.4. Energia- és környezetmenedzsment

Az energiafelhasználás optimalizálása és a fenntarthatóság növelése érdekében az okosgyárakban kiemelt szerepet kapnak az energiahatékony hálózatok, a megújuló energiaforrások integrációja, valamint az energiafogyasztás folyamatos monitorozása és elemzése.

5. Az LPWAN-technológiák áttekintése

Az LPWAN (Low-Power Wide-Area Network) technológiák kulcsfontosságúak az Ipar 4.0 infrastruktúrájában, mivel alacsony energiafogyasztás mellett tesznek lehetővé hosszú hatótávolságú kommunikációt, amely ideális a szenzorhálózatok és más IoT-megoldások számára. Az LPWAN nem egy konkrét protokollt vagy technológiát jelöl, hanem egy olyan hálózati kategóriát, amely bizonyos közös jellemzőkkel rendelkezik: kis sávszélesség, alacsony adatátviteli sebesség, hosszú hatótávolság és hosszú akkumulátor-élettartam.

5.1 LoRaWAN (Long Range Wide Area Network)

A LoRaWAN egy nyílt szabványú LPWAN-protokoll, amely a LoRa (Long Range) rádiótechnológiára épül. Főként nem licencelt frekvenciasávokban működik (Európában például az 868 MHz-es sávban), így nem szükséges külön engedély a használatához.

Előnyei:

- Akár 15–20 km-es hatótávolság nyílt terepen
- Több éves akkumulátor-élettartam (2–10 év)
- Nyílt specifikáció és gyorsan bővülő ökoszisztéma
- Támogatja a privát hálózatok kiépítését

Hátrányai:

- Korlátozott adatátviteli sebesség (0.3 – 50 kbps)
- Nem ideális valós idejű kommunikációra
- A hálózat túlterhelődhet sűrűn telepített környezetben

LoRaWAN különösen népszerű a gyártóüzemekben, ahol az eszközök szétszórtan helyezkednek el, és csak időszakos adatküldés szükséges (pl. hőmérséklet, páratartalom, rezgésérzékelés).

5.2 NB-IoT (Narrowband Internet of Things)

Az NB-IoT egy mobilhálózati operátorok által kínált LPWAN-megoldás, amely licencelt spektrumban működik (jellemzően LTE-hálózatokon belül). Az NB-IoT az egyik legmegbízhatóbb megoldás, ha zárt terekben, például ipari csarnokokban vagy földalatti helyiségekben kell kapcsolatot biztosítani.

Előnyei:

- Magas megbízhatóság és lefedettség
- Mobilhálózatokon keresztüli működés, nincs szükség saját hálózat kiépítésére

- Támogatott a legtöbb mobilszolgáltatónál
- Integrálható már meglévő 4G/5G infrastruktúrába

Hátrányai:

- Kisebb energiahatékonyság, mint LoRaWAN esetén
- Előfizetéses modell (folyamatos költség)
- Lassabb válaszidő, nem valós idejű alkalmazásokhoz

5.3 Sigfox

A Sigfox egy alacsony költségű, kizárólagos technológiát használó LPWAN-megoldás, amely különösen alacsony adatátviteli igényű alkalmazásokra lett tervezve. A hálózat globálisan is elérhető, bár egyes régiókban korlátozottabb a lefedettsége.

Előnyei:

- Nagyon alacsony energiafogyasztás
- Egyszerű, olcsó végponti eszközök
- Hosszú hatótávolság (akár 50 km vidéken)

Hátrányai:

- Kizárólag Sigfox-hálózatra épül, nem lehet privát rendszert kiépíteni
- Erősen korlátozott üzenetméret (12 bájt/adatcsomag)
- Napi üzenetszám-korlát (általában 140/nap)

6. Vezeték nélküli protokollok összehasonlítása ipari alkalmazás szempontjából

Az ipari környezetek sajátos kihívásokat támasztanak a vezeték nélküli kommunikációval szemben: elektromágneses interferencia, fizikai akadályok, nagy távolságok és rendkívül

eltérő adatigények. Ezért fontos a különböző LPWAN-technológiák összehasonlítása az alábbi szempontok alapján:

1. táblázat Vezeték nélküli protokollok összehasonlítása-saját szerkesztés

Szempont	LoRaWAN	NB-IoT	Sigfox
Lefedettség	15–20 km (nyílt térben)	10–15 km (LTE-alapú)	10–50 km
Energiafogyasztás	Alacsony	Közepes	Nagyon alacsony
Adatátvitel	0.3–50 kbps	max. 250 kbps	max. 100 bps
Üzenet méret	max. 242 bájt	több kilobájt	12 bájt
Válaszidő	Nem valós idejű	Lassú	Lassú
Hálózattípus	Nyílt / privát	Operátor-alapú	Operátor-alapú
Alkalmazhatóság	Szenzorhálózatok, okosgyárak	Prediktív karbantartás, nyomon követés	Egyszerű állapotriportok, raktárfigyelés

Az ipari szereplők számára a választás attól függ, hogy milyen típusú adatot kell továbbítani, mekkora távolságra, és milyen energiafelhasználás engedhető meg. Például, ha egy gépsor állapotát kell figyelni napi párszor, akkor LoRaWAN vagy Sigfox ideális. Ha viszont gyakori kommunikáció és nagyobb adat szükséges, NB-IoT lehet a megoldás. 6. Energiahatékonyság és akkumulátor-élettartam kihívásai

Az ipari IoT-rendszerek legnagyobb előnye, hogy hosszú távon is képesek működni anélkül, hogy manuálisan be kellene avatkozni az eszközök karbantartásába. Azonban ennek feltétele a hatékony energiafelhasználás. Egyetlen szenzor akkumulátorának cseréje egy nehezen

hozzáférhető helyen nemcsak költséges, hanem időigényes is.

6.1 Fő energiafogyasztási tényezők:

- Kommunikációs mód: A vezeték nélküli adatküldés energiaigényesebb, mint a passzív adatgyűjtés. A hosszabb távolság nagyobb teljesítményt igényel.
- Adatküldés gyakorisága: Minél gyakrabban küld adatot a szenzor, annál rövidebb lesz az akkumulátor élettartama.
- Üresjárati fogyasztás: Fontos a „sleep mode” hatékonysága, amikor az eszköz nem aktív.
- Fizikai környezet: Magas hőmérséklet, páratartalom vagy elektromos interferencia mind befolyásolják az energiafelhasználást.

6.2 Megoldások és optimalizációk:

- Duty cycle csökkentése: Csak akkor kommunikáljon az eszköz, ha valóban szükséges.
- Adaptív adatküldési algoritmusok: Például csak akkor küldjön adatot, ha változás történt a mért értékben.
- Energiahatékony rádiómodulok alkalmazása: Például Semtech SX1276 vagy Nordic nRF sorozat.
- Helyi adatfeldolgozás: Az edge computing elv alkalmazása, amely csökkenti a szükségtelen kommunikációt.

Az LPWAN-hálózatok egyik legnagyobb előnye éppen az, hogy hosszú távon biztosítanak kapcsolatot alacsony energiafogyasztás mellett. Az ipari alkalmazásokban ez azt jelenti, hogy az eszközök akár 5–10 évig működhetnek akkumulátorcserék nélkül, jelentősen csökkentve a karbantartási költségeket.

7. Biztonsági kihívások és megoldások az alacsony energiaigényű hálózatokban

Az Ipar 4.0 világában, ahol a gépek és szenzorok folyamatosan adatokat küldenek

egymásnak és a felhőbe, a biztonság kiemelt fontosságú. Az alacsony energiaigényű hálózatok azonban számos korlátozással rendelkeznek, amelyek megnehezítik a hagyományos biztonsági mechanizmusok alkalmazását. Az eszközök erőforrásai (memória, processzor, energia) szűkösek, így a komplex titkosítás vagy hitelesítés kihívást jelent.

7.1 Biztonsági kockázatok

- Adathalászat és lehallgatás: Mivel a legtöbb LPWAN nyilvános frekvenciákon működik, fennáll az esélye annak, hogy egy támadó lehallgatja a kommunikációt.
- Adatintegritás megsértése: Ha az adatokat nem megfelelően hitelesítik, azokat meg lehet hamisítani, ami hibás döntésekhez vezethet.
- Eszközök kompromittálása: A gyenge jelszavak vagy nem megfelelő eszközazonosítás lehetőséget adhat az eszközök átprogramozására vagy meghibásítására.
- Szolgáltatásmegtagadási (DoS) támadások: Ha az eszközt folyamatos válaszadásra kényszerítik, gyorsan lemerülhet az akkumulátora.

7.2 Biztonsági megoldások

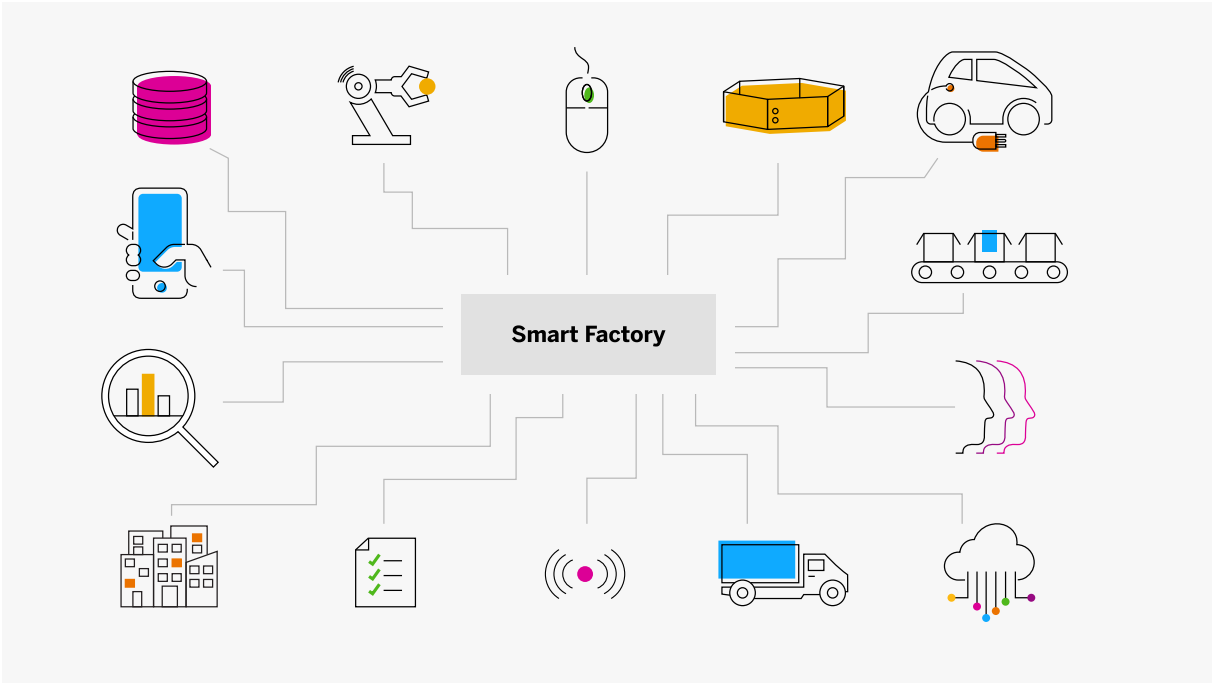
- Titkosított adatátvitel: Az LPWAN-protokollok (pl. LoRaWAN) támogatják az AES-128 titkosítást. Fontos, hogy minden eszköz egyedi kulcsot használjon.
- Hitelesítés: Az eszközök és a hálózat közötti kölcsönös hitelesítés elengedhetetlen, például a Join Accept és Join Request üzenetek esetében (LoRaWAN).
- Firmware frissítések: A biztonsági hibák javítása érdekében szükség van az eszközök távoli frissítésére. Ez kihívás, de megvalósítható LPWAN-en keresztül kis méretű csomagokban.
- Hozzáférés-szabályozás: Csak megbízható eszközök csatlakozhatnak a hálózathoz, és az eszközök hozzáférése korlátozható funkciók szerint.

A biztonság és az energiahatékonyság közötti kompromisszum kulcsfontosságú. A biztonsági mechanizmusokat úgy kell kiválasztani és konfigurálni, hogy ne csökkentsék jelentősen az akkumulátor élettartamát.

8. Okosgyárak

Az intelligens gyárak és az intelligens gyártás az Ipar 4.0 vagy a negyedik ipari forradalom néven ismert technológiai átalakulás részét képezik. Az első három ipari forradalom mindegyike egy innovatív új technológiából született, amely teljesen megváltoztatta a megmunkálás és a gyártás módját: nevezetesen a gőzmotort, a szerelősort és a számítógép teljesítményét. Ma a negyedik forradalmat a digitális átalakulás és az intelligens automatizálás vezérli.

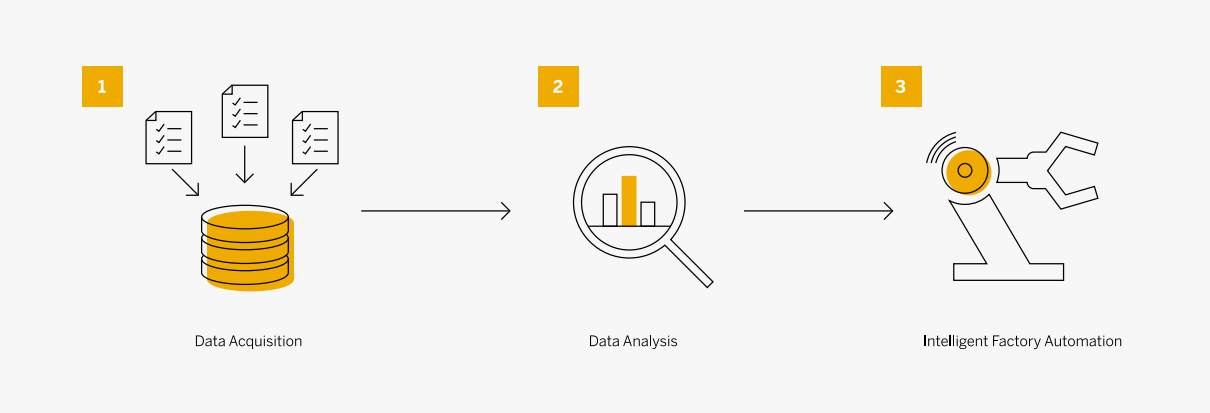
Az okosgyárak az Ipar 4.0 egyik legfontosabb megnyilvánulási formái, amit intelligens szenzorok, vezérlők, gépi tanuláson alapuló algoritmusok és hálózatba kapcsolt eszközök vezérlik. Ezen rendszerek működése az adatok valós idejű gyűjtésén, feldolgozásán és automatikus kiértékelésén alapul. Ennek a digitalizált, automatizált működésnek az alapját gyakran az alacsony energiaigényű hálózatok biztosítják.



[1]

1. ábra Okos gyár szerkezet [1]

[1] Forrás: https://www.sap.com/hungary/products/scm/what-is-a-smart-factory.html



2

2. ábra Okos Gyár 3 fő eljárása [2]

8.1 Az intelligens gyárat alkotó három fő eljárás

1. Adatgyűjtés: A mesterséges intelligencia és a modern adatbázis-technológiák lehetővé teszik a különböző hasznos adatok kezelését és beszerzését az egész vállalaton, az ellátási láncon és a világon. Érzékelők és átjárók révén az ipari dolgok internete (IIoT) lehetővé teszi a csatlakoztatott gépek számára, hogy adatokat gyűjtsenek a rendszerbe. A mesterséges intelligenciával működő rendszerek számtalan más adatportálon keresztül képesek a teljesítményhez, a piaci trendekhez, a logisztikához vagy bármely más esetlegesen releváns forráshoz kapcsolódó adatkészleteket összeállítani.

2. Adatelemzés: A gépi tanulás és az intelligens üzleti rendszerek fejlett analitikát és modern adatkezelési megoldásokat használnak az összegyűjtött különböző adatok értelmezésére. Az IIoT érzékelők figyelmeztethetnek, ha a gépeknek javításra vagy szervizelésre van szükségük. Piaci és működési adatok állíthatók össze a lehetőségek és kockázatok felismerése érdekében. A munkafolyamat hatékonysága idővel tanulmányozható a teljesítmény optimalizálása és az indoklás szerinti automatikus javítás érdekében. Valójában az összehasonlítható és elemezhető adathalmazok a kombinációk szinte végtelen lehetőségét kínálják a digitális gyároptimalizálás és az ellátási lánc előrejelzésének tájékoztatására.

[2] Forrás: https://www.sap.com/hungary/products/scm/what-is-a-smart-factory.html

3. Intelligens gyárautomatizálás: Az adatgyűjtés és -elemzés megtörténte után munkafolyamatok jönnek létre, és utasításokat küldenek a rendszeren belüli gépeknek és eszközöknek. Ezek az eszközök lehetnek a gyár négy falán belül vagy a távoli logisztikai vagy gyártási láncokban az ellátási láncban. Az intelligens munkafolyamatokat és folyamatokat folyamatosan felügyelik és optimalizálják. Ha egy hírjelentés figyelmeztet egy bizonyos termék iránti kereslet csúcsára, a 3D-s nyomtató munkafolyamatai arra utasíthatók, hogy növeljék az adott termék gyártási prioritását. Ha a nyersanyagszállítmány késedelmes, a készletpufferek rotációba helyezhetők a zavarok kiküszöbölése érdekében.

8.3 Az intelligens gyár előnyei

Sok vállalkozás foglalkozik az ellátási lánc működésével és rendszereivel, amelyek alapvetően nem változtak évtizedek óta. A fogyasztói elvárásoknak és a gazdasági bizonytalanságnak köszönhetően azonban az ellátási lánc vezetőinek olyan megoldásokra van szükségük, amelyek mérhető és jelentős előnyökkel járnak – és gyorsan hozhatnak. A Forbes magazin szerint 2017-ben a gyártóknak mindössze 43%-a indított okos gyári kezdeményezéseket. 2019-re a megkérdezettek 68%-a. A digitális átalakításba és az intelligens gyári megoldásokba beruházó vállalatok számára jelentős üzleti előnyök rejlenek, többek között:

- Termelékenység és hatékonyság: A gyártás történelme során elsősorban a reagálásról szólt – egy már megtörtént eseményt vagy trendet megvizsgálva, majd a tény után más irányba igyekezett irányítani a vállalkozást. Az intelligens gyári technológiákat úgy alakították ki, hogy csökkentsék a reaktív gyakorlatok iránti igényt, és az ellátási lánc kezelését ellenállóbb és rugalmasabb módra tereljék. A prediktív elemzések és a Big Data elemzés segítségével beazonosíthatók és bevezethetők az optimalizált folyamatok. A Just-in-time készletgazdálkodás, a pontos kereslet-előrejelzés és a jobb piaci sebesség az intelligens gyárak által nyújtott hatékonysági előnyök egy része. A digitális elemzésekkel kiegészítve az intelligens gyárakban dolgozók is ésszerűsíteni tudják erőfeszítéseiket, növelve a művelet általános termelékenységét. Az intelligens gyárakkal rendelkező gyártók 2030-ra valószínűleg meghaladják a 30%-kal magasabb nettó munkatermelékenységgel rendelkező „hagyományos” gyárakat.”

- Fenntarthatóság és biztonság: A fogyasztók egyre inkább hajlandóak egy kicsit többet költeni azokra a termékekre, amelyekről tudják, hogy társadalmi és környezeti szempontból felelős módszerekkel kell beszerezni és gyártani. A modern intelligens gyártechnológiák minden eddiginél egyszerűbbé teszik a vállalkozások számára a zöldebb, biztonságosabb és társadalmilag felelős gyártási gyakorlatok lehetőségeit. Az intelligens gyárvezetők digitális innovációkat, például blokklánc- és RFID-érzékelőket használhatnak arra, hogy megcáfolhatatlan eredetet és minőségellenőrzést biztosítsanak az összes anyagnál és ellátásnál – az ellátási lánc legtávolabbi láncszemeiből is. A Nemzetközi Automatizálási Társaság arról számol be, hogy a robotok és az automatizált eszközök segíthetnek csökkenteni vagy megszüntetni a munkahelyi sérülések öt vezető okából hármat.

- Termékminőség és ügyfélélmény: A gyerekek telefonjátékához hasonlóan a hagyományos gyártók gyakran nehezen tudtak gondoskodni arról, hogy irányelveiket pontosan fogadják és kövessék az alacsonyabb szintű beszállítók és gyártók az ellátási láncukban. Az intelligens gyárban a felhőalapú összekapcsolhatóság és az intelligens gyárak átfogó láthatósága valós idejű elemzéseket és ajánlásokat biztosít a gyártási folyamat minden szintjén. A gyors testreszabás és a változó trendekre való reagálás képessége azt jelenti, hogy a termékek szorosan naprakészek az ügyfelek kívánságaival. A rendszeradatok részletes elemzése gyorsan észreveszi a gyengeségeket vagy javítandó területeket. Ez a piac versenyképességének javulásához, a termékek jobb felülvizsgálatához és kevesebb költséges hozamhoz vagy visszahíváshoz vezet.

8.4 Intelligens gyári technológiák

Az Okos gyári technológiák rendkívül agilisak. Mivel a digitális átalakítási kezdeményezések felgyorsulnak egy vállalkozáson belül, szinte végtelen lehetőségek kínálkoznak a méretezésre, módosításra és szükség szerinti alkalmazkodásra.

- Felhőkapcsolat: Legyen az nyilvános, privát vagy hibrid, a felhő az a csatorna, amelyen keresztül minden adat és információ egy intelligens gyáron keresztül áramlik. Az üzleti és globális felhőalapú összekapcsolhatóság biztosítja, hogy az üzlet minden területe valós idejű adatokkal működjön, és azonnali rálátás legyen az összes összekapcsolt eszközre és rendszerre az ellátási láncon belül.

- Mesterséges intelligencia: Az integrált mesterséges intelligencia technológiákat használó operatív rendszerek olyan sebességgel, erővel és rugalmassággal rendelkeznek, hogy ne csak különböző adathalmazokat gyűjtsenek és elemezzenek, hanem valós idejű elemzéseket és reszponzív ajánlásokat adjanak. Az intelligens gyár automatizált folyamatait és intelligens rendszereit a mesterséges intelligencia folyamatosan optimalizálja és informálja.

- Gépi tanulás: A gépi tanulás egyik legértékesebb előnye az intelligens gyár számára a fejlett prediktív karbantartás képessége. A gyártási folyamatok felügyeletével és elemzésével riasztások küldhetők a rendszerhiba bekövetkezése előtt. A helyzettől függően automatikus karbantartás történhet, vagy szükség esetén emberi beavatkozás ajánlható.

- Big Data: A robusztus és nagy adathalmazok lehetővé teszik, hogy prediktív és fejlett elemzések történjenek egy intelligens gyárban. A vállalkozások már régóta értik a Big Data stratégiai értékét, de a közelmúltig gyakran hiányoztak a szükséges rendszerek ahhoz, hogy azt értelmesen ki lehessen használni. Az ellátási láncok és az intelligens gyárak digitális átalakulása megnyitotta a vállalkozások potenciáljának világát a Big Data elemzések segítségével történő optimalizálásban és innovációban.

- Ipari dolgok internete (IIoT): Egy intelligens gyárban, amikor az eszközöket és a gépeket egyedi azonosítókkal látják el, és képesek digitális adatok küldésére és fogadására, IIoT hálózatot alkotnak. A modern gépeknek már lehetnek digitális portáljaik, de akár több évtizedes analóg gépek is felszerelhetők IIoT gateway eszközökkel, hogy felgyorsítsák őket. Lényegében az eszköz *állapotáról* és tevékenységéről szóló jelentések, valamint az *eszközre* küldött adatok vezérlik és automatizálják a műveleteit és munkafolyamatait.

- Digitális ikrek: Egy gép vagy rendszer pontos, virtuális replikája válik digitális ikonná. Lehetővé teszi a maximális innovációt és kreativitást minimális működési kockázattal. A digitális ikrek a határig tolhatók, több virtuális módon konfigurálhatók újra, vagy tesztelhetők a kompatibilitás szempontjából egy meglévő rendszeren belül – mindezt anélkül, hogy bármilyen kockázatot vagy erőforrás-pazarlást okoznának a fizikai világban.

- Additív nyomtatás: 3D-nyomtatásként is ismert, lehetővé teszi az intelligens gyárak számára, hogy intelligens automatizálást alkalmazzanak az igény szerinti gyártáshoz. Ez különösen fontos az ellátási lánc váratlan zavarai vagy a hirtelen termékkereslet idején. A virtuális leltárak azonban még akkor is nagymértékben csökkenthetik a kockázatot és a pazarlást, ha lehetővé teszik az időben történő gyártást.

- Virtuális valóság (VR) és kiterjesztett valóság (AR): 2019-ben a Assembly Magazine úgy jellemezte az okosgyárban hordható VR eszközök egyes alkalmazásait, hogy „képesek összekapcsolni a környezeti feltételeket, a készletszinteket, a folyamat állapotát, az összeszerelési hibaadatokat, a felhasználást és az áteresztőképességi mérőszámokat kontextusfüggő módon (ahol nézel vagy sétálsz)". Ez a magával ragadó érzékszervi élmény lehetővé teszi a felhasználók számára, hogy természetes érzékeiket valós idejű adatokkal növeljék bármely helyről vagy időpontról – hogy akadálytalanul tudatosítsák a gyári állapotot.

- Blokklánc: Szerencsére az intelligens gyári technológiák fejlődésével a biztonsági megoldások is lépést tartanak velük. A blockchainnek számos alkalmazása van az ellátási láncban, a szállítókkal kötött „intelligens szerződések" létrehozásától az áruk eredetének nyomon követésén át a logisztikai lánc teljes útjának kezeléséig. Az intelligens gyárakban a blockchain különösen hasznos a csatlakoztatott eszközökhöz és gépekhez való hozzáférés kezelésében az egész vállalatban – a rendszer biztonságának és az ilyen eszközök nyilvántartási pontosságának védelme érdekében.

- Modern adatbázis: Az In-memory adatbázisok és a modern ERP rendszerek jelentik az Ipar 4.0 és az összes intelligens gyári és intelligens ellátási lánc megoldás mögött meghúzódó „agyat". A régi, lemezalapú adatbázisokat – gyakran jóval a korlátaikon túl – továbbküldik, hogy lépést tartsanak az intelligens gyárak és a modern ellátási láncok működtetéséhez szükséges komplex adatkezelési és elemzési funkciókkal.

8.5 Okos gyárak megvalósítása

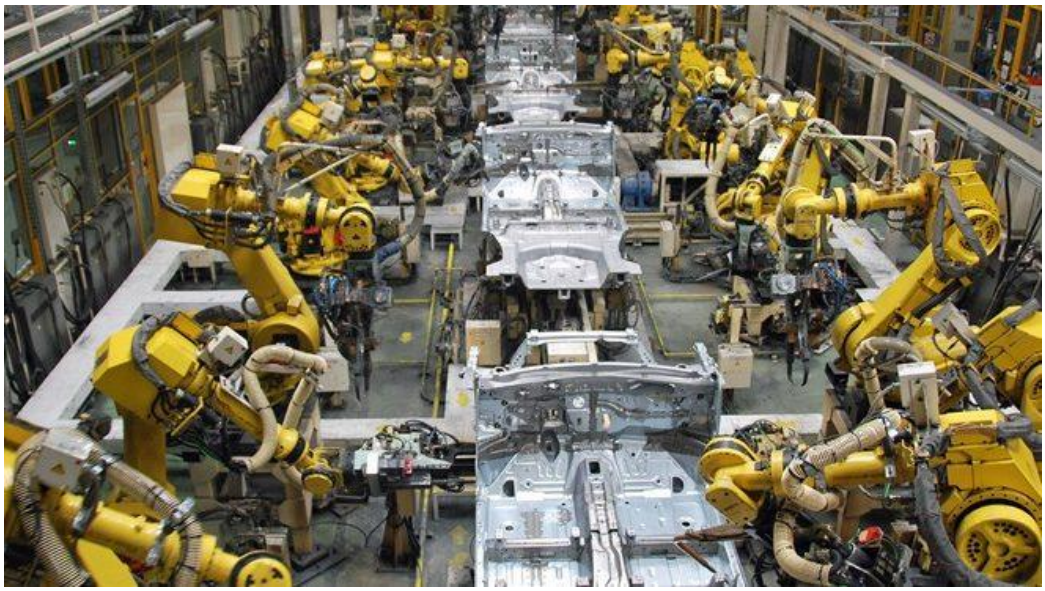
2020 hatalmas fennakadásokat és működési kockázatot jelentett a vállalkozások számára szerte a világon. A Covid19-et megelőzően a Deloitte 2019-es felmérése több mint 600 vezető gyártási ágazat vezetőjéről arról számolt be, hogy 86 %-uk úgy vélte, hogy az

elkövetkező öt évben „az intelligens gyári kezdeményezések lesznek a gyártás versenyképességének fő mozgatórugói”. Napjainkban a digitális átalakulás és az ellátási lánc modernizációja a hosszú távú célokról sürgős és azonnali prioritásokra változott az innovációra és a versenyre törekvő vállalatok számára.

Az, hogy hogyan kezdi el az intelligens gyár átalakítását, attól függ, hol van most, és mely folyamatok a legkritikusabbak a vállalkozása számára. A kezdeti rendszeraudit segít elemezni és leltározni a meglévő folyamatokat, eszközöket és üzleti rendszereket. Mielőtt elkezdi automatizálni a munkafolyamatokat és a gyártási folyamatokat, fel kell mérnie, hogyan néznek ki ma.

A digitális átalakulás útjának kezdetén fontos megjegyezni azt is, hogy az intelligens gyárban az „okos” a fejlett adatelemzési és adatkezelési kapacitásból származik. Egy intelligens gyár mögött egy modern adatbázis és egy robusztus ERP-rendszer áll. Támogatják a rendszert vezérlő speciális funkcionalitást. Az intelligens gyárátalakítás sikerének egyik fő tényezője a meglévő üzleti rendszerek képessége lesz a Big Data kezelésére és az olyan technológiák integrálására, mint a mesterséges intelligencia, a gépi tanulás és a fejlett analitika.

Végül az intelligens gyár átalakításának egyik legjobb módja, hogy a hatékonyság érdekében nem kell egyszerre megtörténnie. Nem követeli meg továbbá a meglévő üzleti tevékenységek megszakítását vagy szüneteltetését. Minden olyan kezdeményezés, amelyet a vállalkozás a digitális rendszerek modernizálására és optimalizálására tesz, egy lépéssel közelebb hozza őket egy teljesen integrált intelligens gyárhoz. Továbbá természetüknél fogva az intelligens gyári technológiák adatokat gyűjtenek és elemeznek. Ez azt jelenti, hogy az új digitális technológiák hatását és megtérülését – a telepítés pillanatától kezdve – mérni és értékelni lehet.



[3]

3. ábra Suzuki gyár [3]

8.6 Okosgyárak (Smart Factories) és az alacsony energiaigényű hálózatok szerepe

8.6.1 A kihívás: komplex, dinamikus ipari környezet

A hagyományos ipari rendszerek jellemzően vezetékes kommunikációra és manuális beavatkozásra épültek. Az okosgyár azonban:

- Rugalmas termelést követel meg (pl. testreszabott termékek gyors átállással),
- Valós idejű adatokra épít,
- Prediktív és adaptív működést igényel,
- Decentralizált vezérlést alkalmaz.

Ehhez a szenzorok, aktuátorok és gépek között megbízható, alacsony fogyasztású vezeték nélküli kapcsolat szükséges, amely könnyen skálázható.

8.6.2 LPWAN előnyei az okosgyárakban

Az alacsony energiaigényű hálózatok, különösen a LoRaWAN és NB-IoT, a következő

[3] Forrás: https://www.muszaki-magazin.hu/2018/04/02/okosgyar-lesz-az-esztergomi-suzuki/

előnyöket kínálják:

- Költséghatékony kiépítés: nincs szükség bonyolult kábelezésre, így gyorsan integrálhatók új szenzorok vagy modulok.
- Hosszú akkumulátor-élettartam: akár 5–10 év is lehet, ez különösen fontos nehezen hozzáférhető gépeknél vagy veszélyes környezetben.
- Nagy lefedettség: egy LPWAN gateway akár több ezer eszközt is kiszolgálhat nagy területen.
- Alacsony karbantartási igény: kevesebb emberi beavatkozás szükséges az eszközök életciklusa során.

8.6.3 Tipikus okosgyári alkalmazások

1. Gépmonitorozás:
    - Rezgés-, hőmérséklet- és nyomásérzékelők figyelik a gépek állapotát.
    - Ezek az adatok alapján a rendszer azonnal riaszt, ha rendellenes működést észlel, így csökkenthető a selejtarány és a leállás ideje.
2. Energiagazdálkodás:
    - A gyár különböző részein elhelyezett IoT-eszközök mérik az áramfogyasztást, segítve a túlterhelés elkerülését és a költségek optimalizálását.
    - Az LPWAN-eszközök képesek csak bizonyos időközönként adatot küldeni, így minimális energiával is fenntarthatók.
3. Környezetmonitorozás:
    - A levegő minősége, páratartalom, hőmérséklet vagy CO_2-szint monitorozása segíti a munkavállalók biztonságát, különösen zárt térben vagy vegyianyag-kezelésnél.
4. Robotok és mobil platformok nyomon követése:

- A vezeték nélküli, alacsony energiafogyasztású helymeghatározás (pl. LPWAN + GPS) segítségével nyomon követhető a mobil robotok helyzete a gyár területén belül.
- Ez javítja az anyagmozgatás hatékonyságát és elkerülhetővé teszi az ütközéseket, torlódásokat.

5. Digitális ikrek (digital twins):
    - Az LPWAN-hálózaton keresztül valós idejű adatokkal frissíthetők a gyártási eszközök digitális másolatai.
    - Ez lehetővé teszi a szimulációkat, hibakeresést és fejlesztést valós üzemi környezetben is.

8.6.4 Példa egy LPWAN-alapú okosgyári megoldásra

Tegyük fel, hogy egy autóalkatrészeket gyártó üzem szeretné csökkenteni a nem tervezett leállások számát. A gépeikre LPWAN-kompatibilis szenzorokat szerelnek, amelyek:

- Mérik a csapágyak hőmérsékletét és rezgését,
- Naponta kétszer küldenek adatot, vagy azonnal, ha küszöbértéket lépnek át,
- Az adatokat egy központi felhőalapú rendszer elemzi, és prediktív karbantartást javasol.

Az eredmény:

- 40%-kal csökkentett gépleállási idő,
- 25%-kal alacsonyabb karbantartási költség,
- 10%-kal nagyobb termelési hatékonyság.

8.6.5 Jövőbeli fejlesztési irányok okosgyárakban

- Energia-önellátó IoT-eszközök: olyan LPWAN-eszközök, amelyek a gépek rezgéséből vagy hőjéből nyerik energiájukat.

- Mesterséges intelligencia az élvonalban (edge AI): az eszközök helyben elemzik az adatokat, és csak a lényeges információkat továbbítják.
- Privát LPWAN-hálózatok: vállalatszintű, saját üzemeltetésű hálózatok nagyobb kontrollal és adatbiztonsággal.

[4]

4. ábra Robotok egy gyárban [4]

9. Fenntarthatóság és környezeti hatékonyság

Az Ipar 4.0 egyik kiemelt célja nem csupán az automatizáció, hanem a fenntartható fejlődés elősegítése is. Az alacsony energiaigényű hálózatok hozzájárulnak a környezeti hatások csökkentéséhez több szinten:

9.1 Energiafogyasztás csökkentése

A hagyományos ipari rendszerek jelentős energiát használnak fel a folyamatos adatkommunikációra. Az LPWAN-megoldások lehetővé teszik a szenzorok számára, hogy csak akkor küldjenek adatot, ha tényleg szükséges, így jelentősen csökken az energiafelhasználás.

9.2 Hulladékcsökkentés

A prediktív karbantartás segítségével az alkatrészek csak akkor kerülnek cserére, amikor

[4] Forrás: https://synerinsoft.com/hu/blog/hirek/smart-factory-mik-azok-az-okos-gyarak

valóban szükséges, ezáltal csökken a felesleges hulladék termelése.

9.3 Szén-dioxid-kibocsátás mérséklése

A hatékony logisztika és a pontos készletgazdálkodás révén elkerülhetők a felesleges szállítások és tárolások, amelyek szintén hozzájárulnak az ipar karbonlábnyomának csökkentéséhez.

9.4 Okos városok és zöld ipar

Az LPWAN-hálózatok nemcsak az iparban, hanem városi környezetben is segíthetik a környezeti célok elérését: például okos világítás, vízfelhasználás monitorozása vagy levegőminőség-figyelés területén.

10. Összegzés és jövőbeli kilátások

Az Ipar 4.0 forradalma alapvetően alakítja át az ipari termelést és a gyártási rendszereket, ahol az adatok valós idejű gyűjtése, elemzése és a gépek intelligens vezérlése központi szerepet kap. E folyamatok hatékony és gazdaságos működtetéséhez elengedhetetlenek az olyan kommunikációs technológiák, amelyek képesek hosszú távon, minimális energiafogyasztás mellett biztosítani a folyamatos adatkapcsolatot az eszközök között. Az alacsony energiaigényű hálózatok, különösen az LPWAN-megoldások (mint a LoRaWAN, NB-IoT és Sigfox), ebben a kontextusban kulcsfontosságúak.

Jövőbeli trendek és lehetőségek

Az alacsony energiaigényű hálózatok fejlődése tovább folytatódik. Az alábbi jövőbeli trendek valószínűsíthetők:

- 6G és LPWAN integrációja: A következő generációs mobilhálózatok és az alacsony energiaigényű technológiák közötti integráció még nagyobb adatátviteli sebességet és megbízhatóságot biztosíthat, miközben továbbra is fenntartja az energiatakarékosságot.

- Edge computing és mesterséges intelligencia kombinációja: A szenzoradatokat helyben feldolgozó rendszerek (edge AI) csökkentik az adatforgalmat és a reakcióidőt, ami kritikus lehet az ipari automatizációban.

- Szabványosítás és interoperabilitás: A különböző technológiák közötti együttműködés és kompatibilitás kulcsfontosságú az ipari rendszerek egységesítésében.

- Energia-önellátó szenzorok: A jövőben a szenzorok már képesek lehetnek saját maguk energiáját előállítani (pl. rezgésből, hőből), ezzel tovább növelve az autonómiát.

A fentiek alapján kijelenthető, hogy az alacsony energiaigényű hálózatok nem csupán eszközei az Ipar 4.0-nak, hanem annak egyik hajtómotorja. Az ipari digitalizáció jövője nagymértékben függ ezen hálózatok hatékony és biztonságos alkalmazásától.

Irodalomjegyzék:

[1] https://www.sap.com/hungary/products/scm/what-is-a-smart-factory.html, 2025.05.08.

[2] https://azure.microsoft.com/hu-hu/solutions/iot/iot-technology-protocols, 2025.05.06.

[3] https://chatgpt.com, 2025.05.10.

[4] https://synerinsoft.com/hu/blog/hirek/smart-factory-mik-azok-az-okos-gyarak, 2025.05.11.

[5] https://www.muszaki-magazin.hu/2018/04/02/okosgyar-lesz-az-esztergomi-suzuki/, 2025.05.12.

Ábrajegyzék:

1. ábra Okos gyár szerkezet [1] 12

2. ábra Okos Gyár 3 fő eljárása [2] 13

3. ábra Suzuki gyár [3] 19

4. ábra Robotok egy gyárban [4] 22

2.40. Az okosotthonok fejlődése és hatása a mindennapi életre, az energiamenedzsment szerepe Intelligens rendszerek az otthonokban

Az okosotthonok fejlődése és hatása a mindennapi életre, az energiamenedzsment szerepe

Intelligens rendszerek az otthonokban

Vocelka Bálint

Mérnökinformatika, vocelkab14@gmail.com

1 BEVEZETÉS

Az ipari fejlődés négy nagy szakaszát követően jelenleg az Ipar 4.0 forradalma zajlik, amely a digitális és fizikai világ összekapcsolását valósítja meg kiber-fizikai rendszerek és az IoT technológia segítségével. Ennek egyik gyakorlati példája az okosotthon, amely az otthoni rendszerek – például világítás, fűtés, biztonság – automatizált, összehangolt működését teszi lehetővé.

Az okosotthonok célja az energiahatékonyság növelése, a felhasználói szokások elemzése és az energiafogyasztás optimalizálása. Ebben kulcsszerepet játszanak az intelligens vezérlők, előrejelző rendszerek és a gépi tanulás, valamint a kommunikációs protokollok, mint a Zigbee vagy a MQTT.

A dolgozat az okosotthonok technológiai fejlődését és energiamenedzsment rendszereit vizsgálja, bemutatva a legújabb innovációkat, iparági szereplők megoldásait és ezek kapcsolatát az intelligens városi infrastruktúrával. A téma különösen aktuális, mivel hozzájárulhat egy fenntarthatóbb, energiatudatosabb jövő megteremtéséhez.

2 AZ OKOSOTTHONOK FEJLŐDÉSE ÉS TECHNOLÓGIAI

2.1 Az okosotthon-technológia történeti áttekintése

Az okosotthonok koncepciója nem új keletű, azonban a technológiai feltételek az utóbbi évtizedek során teremtődtek meg ahhoz, hogy széles körben elterjedhessenek. Az okosotthon-technikák fejlődése szorosan összefügg az információs technológia, az automatizálás, valamint a vezeték nélküli kommunikáció fejlődésével. Az alábbiakban áttekintjük a legfontosabb mérföldköveket, amelyek az okosotthonok kialakulásához vezettek.

2.1.1 Korai automatizálási törekvések (1960–1990)

Az első, okosotthonokra emlékeztető rendszerek az 1960-as és 1970-es években jelentek meg, elsősorban laboratóriumi kísérletek vagy egyedi fejlesztések formájában. Ezek célja a háztartási gépek automatizálása volt, például időzített világításvezérlés vagy egyszerű motoros redőnyrendszerek segítségével.

A 1980-as években már megjelentek az első „otthoni automatizálási" rendszerek, melyek jellemzően vezetékes hálózatokon alapultak, és többnyire fix programozással működtek. Egyik korai példa az X10 protokoll, amely a háztartási elektromos hálózatot használta kommunikációs közegként, lehetővé téve a lámpák és konnektorok vezérlését. Ugyanakkor ezek a rendszerek még nem voltak képesek adatokat gyűjteni, visszacsatolni vagy önálló döntést hozni – azaz még nem tekinthetők valódi „intelligens" rendszereknek.

2.1.2 A digitális hálózatok és számítógépes vezérlés térnyerése (1990–2010)

A 1990-es évektől kezdve a számítógépek és a mikrovezérlők elterjedése lehetővé tette a bonyolultabb háztartási vezérlőrendszerek kialakítását. Ekkoriban váltak elérhetővé a központi vezérlőegységek, amelyek képesek voltak több alrendszer összehangolt irányítására. Az első rendszerek főként luxus kategóriás ingatlanokban jelentek meg, ahol például a világítás, biztonságtechnika és klimatizálás központi rendszerből történő vezérlése már megvalósult.

A 2000-es évek elején a szélessávú internet és a Wi-Fi technológia elterjedése új lehetőségeket teremtett. Megjelentek az első távolról is vezérelhető rendszerek, amelyek internetkapcsolat segítségével okostelefonról vagy számítógépről irányíthatók voltak. Ezek már kezdetleges IoT-képességekkel is rendelkeztek, például hőmérséklet-érzékelők, mozgásérzékelők és kamerák integrációjával.

2.1.3 Az IoT technológiák megjelenése és az okosotthonok tömeges elterjedése (2010-től napjainkig)

Az okosotthon-technológia valódi forradalma a 2010-es évek elején indult meg az Internet of Things (IoT) fogalom megjelenésével. Az IoT egy új paradigmát jelentett, amely szerint az eszközök képesek egymással és központi rendszerekkel kommunikálni, adatokat cserélni és automatikus döntéseket hozni.

Ezzel párhuzamosan megjelentek a kereskedelmi forgalomban is elérhető okoseszközök:

- Intelligens termosztátok (pl. Nest Learning Thermostat), amelyek tanulják a felhasználói szokásokat
- Okos világítási rendszerek (pl. Philips Hue), amelyek szín- és fényerő szabályozással reagálnak a környezetre
- Okos zárak és biztonsági rendszerek, amelyek valós idejű értesítéseket küldenek

Energiagazdálkodási modulok, amelyek valós idejű fogyasztási adatokat szolgáltatnak és elemzéseket végeznek

A technológiai fejlődés mellett a platformszolgáltatások, mint az Amazon Alexa, Google Assistant vagy Apple HomeKit, lehetővé tették az eszközök integrált vezérlését és az egységes felhasználói élményt. Ezek az ökoszisztémák jelentősen hozzájárultak az okosotthon-technológiák gyors piaci terjedéséhez.[3]

2.1.4 A jelenlegi trendek és jövőbeli irányok

Napjainkban az okosotthon-rendszerek komplex, többkomponensű hálózatokká fejlődtek, amelyek már nem csupán eszközszintű irányítást, hanem adattudományi és gépi tanulási alapú optimalizációt is tartalmaznak. A vezérlőrendszerek

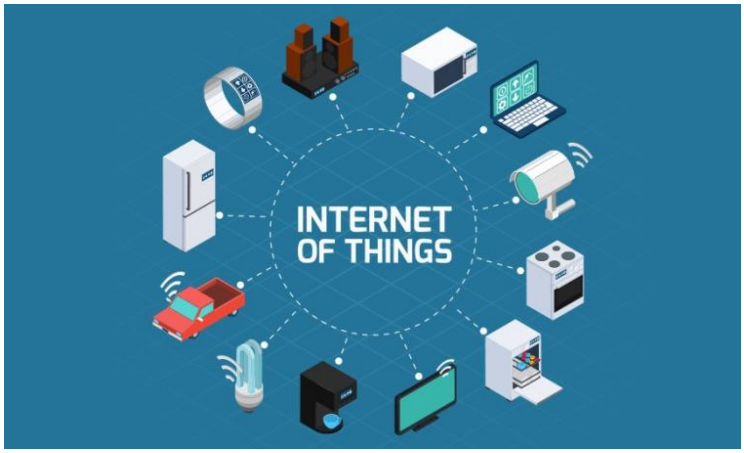
képesek energiafogyasztási mintázatokat azonosítani, előre jelezni a várható igényeket, és ezek alapján automatikusan módosítani a működést. Emellett a decentralizált vezérlés – például blockchain alapú energiaelosztási rendszerek – is egyre nagyobb figyelmet kapnak, különösen a megújuló energiaforrásokkal kombinálva.

A szabványosítás is fontos lépéseken ment keresztül: a Matter protokoll célja, hogy egységes és interoperábilis alapot nyújtson az eszközök közötti kommunikációhoz, függetlenül a gyártótól. Ez elősegíti a piaci bővülést és a felhasználói élmény javulását.

Az okosotthon-technológia fejlődése tehát egy lineáris innovációs folyamattól eljutott a hálózatos, adaptív és tanuló rendszerek szintjéig, amelyek már a jövő intelligens városainak szerves részét képezhetik.

2.2 Az IoT szerepe és elterjedése a háztartásokban

Az Internet of Things (IoT), vagyis a „dolgok internete” az Ipar 4.0 egyik alapvető pillére, amely lehetővé teszi, hogy a fizikai eszközök adatokat gyűjtsenek, dolgozzanak fel és kommunikáljanak egymással, illetve felhőalapú rendszerekkel. Az IoT technológiák térnyerése a háztartásokban forradalmasította az okosotthonok kialakítását, lehetővé téve a különböző rendszerek integrált, intelligens működtetését, amely jelentősen eltér a korábbi, szigetüzemű automatizálási megoldásoktól.



1 ábra: IoT eszközök otthoni és munkahelyi környezetekben [19]

2.2.1 Az IoT alapelvei és működési mechanizmusa

Az IoT alapvetően három fő komponensből épül fel:

Érzékelők és aktuátorok, amelyek fizikai változókat (pl. hőmérséklet, fény, mozgás, páratartalom) érzékelnek, majd ennek alapján beavatkoznak (pl. fűtés bekapcsolása).

Kommunikációs protokollok és hálózati infrastruktúra, amelyek lehetővé teszik az eszközök közötti adatcserét (pl. Zigbee, Wi-Fi, Z-Wave, MQTT).

Központi feldolgozóegységek vagy felhőalapú platformok, ahol az adatok elemzése, döntési logika és vezérlés történik.

A háztartási alkalmazások szempontjából ez azt jelenti, hogy az egyes eszközök nem csak önálló funkciót látnak el, hanem képesek komplex szabályalapú vagy prediktív viselkedésre. Egy okostermosztát például nemcsak a hőmérsékletet

méri és szabályozza, hanem képes figyelembe venni a jelenlétet, az időjárás-előrejelzést, a korábbi szokásokat és az áramtarifák változásait is.

2.2.2 IoT-eszközök kategóriái a háztartásokban

A háztartási IoT-eszközök sokfélesége gyors ütemben növekszik. A leggyakoribb kategóriák az alábbiak:

Energiagazdálkodási eszközök:

Intelligens konnektorok, világításvezérlők, termosztátok és okos mérőórák, amelyek célja az energiafogyasztás optimalizálása.

Biztonságtechnikai eszközök:

Okos zárak, kamerák, mozgásérzékelők, valamint riasztórendszerek, amelyek távolról is felügyelhetők.

Kényelemi és szórakoztató rendszerek:

Hangvezérlésű asszisztensek, multimédiás eszközök, redőnymozgatók, időjárás-szenzorok.

Háztartási gépek:

Hűtőszekrények, mosógépek, kávéfőzők és porszívók, amelyek képesek adatkommunikációra és programozott működésre.

2.2.3 A háztartási IoT-eszközök elterjedésének mozgatórugói

Az IoT-technológiák háztartási elterjedésének gyorsaságát több tényező is elősegíti:

Árcsökkenés**:** Az érzékelők, vezérlők és mikrochipek ára folyamatosan csökken, ami a tömeges piaci bevezetést ösztönzi.

Szabványosítás**:** Az új kommunikációs szabványok (pl. Matter) elősegítik az interoperabilitást a különböző gyártók termékei között.

Felhasználóbarát felületek**:** Az egyszerű mobilalkalmazások és hangvezérelt platformok révén a rendszerek könnyen kezelhetők, nem igényelnek technikai tudást.

Energiahatékonysági és biztonsági igények: A háztartások törekednek a költségek csökkentésére és a biztonság növelésére, amelyhez az IoT-rendszerek kézzelfogható segítséget nyújtanak.

Kihívások és akadályozó tényezők

Bár az IoT háztartási alkalmazása dinamikusan fejlődik, számos akadályozó tényező is jelen van:

Biztonsági kockázatok: A hálózatra kapcsolt eszközök támadhatók, így a kiberbiztonság kiemelt fontosságú (ld. 5.2. alfejezet).

Kompatibilitási problémák: A nem egységes protokollok miatt előfordulhat, hogy különböző gyártók termékei nem kommunikálnak egymással zökkenőmentesen.

Adatvédelmi aggályok**:** A személyes szokásokat rögzítő eszközök adatkezelése jogi és etikai kérdéseket is felvet.

Infrastruktúra hiányosságai**:** Bizonyos régiókban a gyenge internetkapcsolat vagy a villamos hálózat megbízhatatlansága is gátolhatja a rendszerek működését.

2.2.4 Társadalmi és gazdasági hatások

Az IoT-technológia alkalmazása nem csupán technikai jelenség, hanem társadalmi szinten is változásokat generál. A felhasználók egyre inkább elvárják az automatizált, kényelmi szolgáltatásokat, amelyek újfajta életvitelt tesznek lehetővé. A piaci szereplők pedig új üzleti modelleket építenek ki – például előfizetéses rendszerben kínált karbantartás, adatgyűjtésen alapuló szolgáltatások vagy energiaszolgáltatók által integrált IoT-eszközök formájában.

A háztartási IoT rendszerek egyre szorosabban kapcsolódnak a smart grid rendszerekhez, ahol az energiafogyasztás nemcsak optimalizálható, hanem visszacsatolható is a hálózatba – például háztartási szinten megtermelt napenergia betáplálásával.

2.3 Vezérlési és automatizálási technológiák fejlődése

Az okosotthonok működésének egyik legkritikusabb összetevője a vezérlés és az automatizálás rendszere, amely az egyes eszközök, szenzorok és alrendszerek közötti együttműködést biztosítja. E technológiák fejlődése szorosan összefügg az ipari automatizálási rendszerek fejlődésével, ugyanakkor alkalmazásuk a lakossági környezetben új kihívások és prioritások megjelenését is jelentette, például a költséghatékonyság, a felhasználóbarát kialakítás vagy az esztétikai integráció igényét.

2.3.1 A vezérlőrendszerek evolúciója

Az okosotthonok korai szakaszában a vezérlés alapvetően időzítésen vagy kézi beavatkozáson alapult. A felhasználó programozta be előre, hogy mikor kapcsoljon fel a világítás vagy mikor induljon el a fűtés. Az ilyen rendszerek nem rendelkeztek érzékelő visszacsatolással, így nem voltak képesek adaptív viselkedésre.

A következő fejlődési lépést a szabályalapú vezérlés jelentette. Ezek már képesek voltak szenzoradatokat figyelembe venni, például mozgásérzékelő vagy hőmérséklet-érzékelő jele alapján dönteni. A működés logikáját azonban a felhasználónak vagy a telepítőnek kellett előre meghatározni, nem történt gépi tanulás vagy önálló optimalizáció.

A jelenleg elérhető rendszerek a feltételes logikát és az automatizált eseményláncokat alkalmazzák, ahol „ha–akkor” típusú logikák szabályozzák a működést (pl. *ha a külső hőmérséklet 18 °C alá csökken, és a lakásban tartózkodik valaki, akkor kapcsoljon be a fűtés*). Ezeket a logikákat gyakran mobilalkalmazásban vagy felhőalapú platformon lehet konfigurálni, például az IFTTT (If This Then That) vagy gyártóspecifikus rendszerek segítségével.

2.3.2 A mesterséges intelligencia megjelenése a vezérlésben

A vezérlés legújabb szintje az intelligens**,** tanuló rendszerek megjelenése, amelyek képesek adatminták alapján saját működésüket optimalizálni. Az ilyen rendszerek:

- figyelik a felhasználói szokásokat (pl. mikor tartózkodik otthon, mikor kapcsol világítást)
- időjárás-előrejelzési adatokat dolgoznak fel
- valós idejű energiaárak alapján döntenek az eszközök működtetéséről

Ezek az MI-alapú vezérlők nem igényelnek kézi programozást, hanem automatizált döntéseket hoznak az előzetes tanulás és a környezeti változók alapján. Egy példa erre a Google által kifejlesztett Nest termosztát, amely néhány napos használat után „megtanulja” a felhasználó preferenciáit, és önállóan szabályozza a hőmérsékletet.

2.3.3 Decentralizált és lokális vezérlés

Bár sok rendszer felhőalapú, az utóbbi években megnőtt az igény a **helyi vezérlőrendszerek** iránt is, főként biztonsági és adatvédelmi okokból. A decentralizált vezérlés előnyei közé tartozik:

- a rendszer működőképessége internetkapcsolat hiányában is
- a gyorsabb reakcióidő (nincs felhő–eszköz adatforgalom)
- nagyobb adatbiztonság, mivel a személyes adatok nem hagyják el a helyi hálózatot

Az ilyen rendszerek gyakran edge computing architektúrán alapulnak, ahol az adatfeldolgozás az eszközök közelében, lokális egységekben történik.

2.3.4 Automatizálási platformok és vezérlési ökoszisztémák

A vezérlés megvalósítása gyakran különböző automatizálási platformokon keresztül történik. Ezek lehetnek gyártóspecifikusak (pl. Apple HomeKit, Samsung SmartThings, Google Home), de elérhetők nyílt forráskódú megoldások is (pl. Home Assistant, OpenHAB).

Ezek a platformok lehetővé teszik:

- az eszközök közötti integrációt
- a komplex logikák létrehozását
- a felhasználói felületen történő vizuális programozást

A vezérlés sikeressége nagymértékben függ az interoperabilitástól, vagyis attól, hogy különböző gyártók eszközei képesek-e egymással kommunikálni.

2.3.5 Vezérlés és energiahatékonyság kapcsolata

A fejlett vezérlési rendszerek nem öncélú technológiai megoldások, hanem aktívan hozzájárulnak az energiafogyasztás optimalizálásához.

A vezérlők képesek például:

- időzíteni az energiaigényes folyamatokat (pl. mosás, fűtés)
- csökkenteni a felesleges működést (pl. automatikus lekapcsolás távollét esetén)
- előnyben részesíteni az alacsony tarifájú időszakokat (pl. éjszakai áram)

Emellett a vezérlők kulcsszerepet játszanak a megújuló energiaforrások háztartási integrációjában is. Egy megfelelően konfigurált rendszer például akkor indítja el a vízmelegítést, amikor a napelemek éppen a legtöbb energiát termelik.

2.4 Felhasználói igények változása és piaci trendek

Az okosotthon-technológiák fejlődésének nem csupán technológiai, hanem társadalmi és piaci hajtóerői is vannak. A felhasználói igények az elmúlt évtizedekben jelentős változásokon mentek keresztül, részben a technológiai lehetőségek fejlődése, részben a gazdasági és környezeti tényezők hatására. Ezzel párhuzamosan a piac is reagált ezekre az elvárásokra, folyamatosan bővítve a kínálatot és új üzleti modelleket alakítva ki. [1]

2.4.1 A komfort iránti igény dominanciája az első szakaszban

Az okosotthon-technológiák korai szakaszában a felhasználói igények elsősorban a kényelmi funkciók köré összpontosultak. A világítás automatizálása, a fűtési/hűtési rendszer programozhatósága, valamint az otthoni szórakoztató rendszerek integrációja jelentették az elsődleges vonzerőt.

A cél az volt, hogy a felhasználók csökkentsék a manuális beavatkozások számát, egyszerűbbé tegyék a mindennapi életet, és technológiai újítások révén növeljék az otthoni komfortot. Ebben az időszakban még kevés figyelem irányult az energiahatékonyságra vagy a fenntarthatóságra, mivel ezek háttérbe szorultak az élményalapú használattal szemben.

2.4.2 A biztonság és adatvédelem előtérbe kerülése

A technológia elterjedésével egyre több hálózatra kapcsolt eszköz került a háztartásokba, ami új típusú igényeket generált a biztonság és adatvédelem terén. A felhasználók fokozatosan tudatosabbá váltak azzal kapcsolatban, hogy milyen adatokat gyűjtenek és továbbítanak az eszközök, és kik férhetnek hozzá ezekhez az adatokhoz.

Ez az igényváltás a gyártók részéről olyan megoldásokat kényszerített ki, mint:

- a titkosított kommunikációs csatornák használata
- a helyi adatfeldolgozás (edge computing)
- kétfaktoros hitelesítés és erős jelszókezelés bevezetése

Ezzel párhuzamosan a biztonságtechnikai rendszerek – például okos zárak, kamerák, riasztók – iránti kereslet is megnőtt, mivel ezek valós idejű értesítéseket és távfelügyeleti lehetőséget kínálnak.

2.4.3 Energiatudatosság és fenntarthatóság mint új kulcstényezők

A klímaváltozással és az energiaválságokkal kapcsolatos társadalmi diskurzus eredményeképpen az utóbbi években a fenntarthatóság és energiahatékonyság vált az egyik legfontosabb felhasználói prioritássá. A felhasználók immár nem csupán kényelmi funkciókat keresnek, hanem olyan megoldásokat, amelyek segítségével:

- csökkenthetik az energiafogyasztást
- nyomon követhetik a fogyasztási mintázataikat
- optimalizálhatják a fűtési és hűtési rendszereket
- integrálhatják a megújuló energiaforrásokat

Ez a változás jelentős hatással van az iparági fejlesztési irányokra is, mivel a gyártók olyan termékeket és platformokat kínálnak, amelyek kifejezetten az energiagazdálkodásra fókuszálnak (pl. intelligens termosztátok, energiafigyelő modulok, napelem-integrációs rendszerek).

2.4.4 Felhasználói szerepváltás: passzív használóból aktív rendszerszereplő

A felhasználók szerepe az elmúlt években passzív végfelhasználóból aktív rendszeralkotóvá változott. Az okosotthonokban alkalmazott technológiák lehetővé teszik, hogy:

- a háztartások adatokat szolgáltassanak az energiaszolgáltatóknak
- keresletoldali szabályozásban vegyenek részt (demand-side response)
- tárolt vagy termelt energiát (pl. napelemből származó) visszatápláljanak a hálózatba

Ez az ún. prosumer (producer + consumer) modell új típusú együttműködési formákat és gazdasági ösztönzőket eredményez, amelyre a szabályozóknak, energiaszolgáltatóknak és gyártóknak is reagálniuk kell.

2.4.5 Piaci trendek és üzleti modellek alakulása

A piaci szereplők az elmúlt évek során folyamatosan igazodtak a változó felhasználói igényekhez. Néhány jellemző piaci trend:

- Modularitás és skálázhatóság**:** A gyártók egyre inkább moduláris rendszereket kínálnak, amelyeket a felhasználó fokozatosan bővíthet (pl. először világításvezérlés, később fűtésautomatizálás)
- Platformalapú ökoszisztémák**:** A piacon domináns szerepet töltenek be a platformszolgáltatók (pl. Google Home, Amazon Alexa), amelyek közös felületet biztosítanak különböző gyártók eszközeihez
- Előfizetés-alapú szolgáltatások**:** Egyre gyakoribbak a szolgáltatásként nyújtott funkciók (pl. felhőalapú adatmentés, automatizálási sablonok, karbantartási támogatás)
- Nyílt forráskódú közösségi rendszerek**:** Az informatikailag képzett felhasználók számára lehetőséget adnak az egyedi konfigurációkra (pl. Home Assistant, OpenHAB)

A piac növekedése jól nyomon követhető az értékesítési adatokon is: a globális okosotthon-piac értéke 2023-ra meghaladta a 130 milliárd USD-t, és előrejelzések szerint ez 2028-ra akár 230 milliárd USD fölé is nőhet 111.

3 ENERGIATAKARÉKOSSÁG ÉS FENNTARTHATÓSÁG CÉLKITŰZÉSEI

Az energiahatékonyság és a fenntarthatóság az elmúlt évtizedekben a globális technológiai és gazdasági fejlesztések kulcsfontosságú irányelveivé váltak. A növekvő népesség, az ipari energiaigény emelkedése, valamint a fosszilis energiahordozók korlátos mennyisége és környezetszennyező hatása egyre sürgetőbbé teszik az olyan megoldások bevezetését, amelyek hozzájárulnak a környezeti terhelés csökkentéséhez. Az okosotthonok ezen törekvések lakossági szintű megvalósítását szolgálják azzal, hogy lehetővé teszik az energiafogyasztás hatékonyabb, rugalmasabb és tudatosabb szabályozását.

3.1.1 Globális energiaproblémák és a lakossági fogyasztás szerepe

A Nemzetközi Energiaügynökség (IEA) adatai szerint a világ teljes energiafelhasználásának közel 30%-áért a lakossági szektor felel 111. Ezen belül is a fűtés, hűtés, világítás és elektromos háztartási eszközök működtetése jelentik a legnagyobb energiaigényt. A hagyományos épületek jellemzően alacsony energiahatékonyságú rendszerekkel működnek, így jelentős energiaveszteség keletkezik hőszigetelési, vezérlési és kihasználtsági problémák miatt.

Az okosotthonok egyik legnagyobb előnye abban rejlik, hogy képesek valós idejű energiafelügyeletre és optimalizációra, amely révén csökkenthető a felesleges fogyasztás, illetve a megújuló energiaforrások felhasználása hatékonyabban integrálható a háztartás működésébe.

3.1.2 Fenntarthatóság, mint stratégiai cél

A fenntarthatóság az ENSZ által definiált egyik legfontosabb globális célkitűzés, amely nemcsak környezetvédelmi, hanem társadalmi és gazdasági dimenzióval is rendelkezik. Az okosotthonok ezek közül elsősorban a környezeti és gazdasági szempontokat képesek erősíteni az alábbi módokon:

Környezetterhelés csökkentése: Az energiahatékony rendszerek révén csökken az üvegházhatású gázok kibocsátása.

Erőforrás-optimalizálás: A vezérelt fogyasztás és az eszközök kihasználtsági szintjének javítása révén kevesebb nyersanyagra van szükség.

Költségcsökkentés: Az energiaárak növekedése közepette a fogyasztás csökkentése közvetlen pénzügyi előnyt jelent a háztartásoknak.

Hálózati terhelés mérséklése: Az okos vezérlők segítségével elkerülhetők a terhelési csúcsok, ami stabilabbá teszi a közüzemi energiaellátást.

3.1.3 Energiatakarékossági technológiák és lehetőségek okosotthonokban

Az okosotthonok energiatakarékossági lehetőségei széles spektrumot fednek le. A technológiailag fejlettebb rendszerek képesek proaktív módon, akár előrejelzések alapján optimalizálni a működést. Az alábbiakban bemutatunk néhány főbb területet:

Intelligens világítás**:** Automatikus fényerőszabályozás, mozgásérzékelő alapú ki-/bekapcsolás és időzítés segíti a szükségtelen energiafelhasználás elkerülését.

Fűtés/hűtés szabályozása**:** Programozható és adaptív termosztátok alkalmazása a lakók szokásaihoz és az aktuális időjáráshoz igazítja az energiafelhasználást.

Okos konnektorok és eszközfelügyelet**:** Az elektromos készülékek készenléti állapotban történő fogyasztásának automatikus megszüntetése szintén jelentős megtakarítást eredményezhet.

Energiafogyasztás monitorozása**:** Részletes, eszközszintű adatokat biztosító rendszerek elemzési lehetőségeket nyújtanak a fogyasztási szokások megváltoztatásához.

3.1.4 Energiafüggetlenség és megújuló energia integrációja

Az energiatakarékosság mellett egyre fontosabb célkitűzés a részleges vagy teljes energiafüggetlenség, amely a megújuló energiaforrások – elsősorban a napenergia – lakossági szintű alkalmazását jelenti. Az okosotthon-rendszerek képesek:

- figyelemmel kísérni a napelemes termelést
- automatikusan szabályozni a fogyasztást a megtermelt energia mennyiségéhez igazodva
- irányítani az energiatároló rendszereket (pl. akkumulátorokat) az optimális kapacitáskihasználás érdekében, akár visszatáplálni a hálózatba a felesleges energiát (ha a szabályozás lehetővé teszi).

Ez nemcsak környezetvédelmi szempontból előnyös, hanem a hálózati energiaár-ingadozásokkal szembeni védelmet is biztosíthat.

3.1.5 Szabályozási és ösztönző környezet

A fenntarthatósági célkitűzések eléréséhez szükség van a technológia mellett szabályozási ösztönzőkre is, amelyeket egyes országokban már be is vezettek:

Energiahatékonysági címkézés és követelmények**:** Szabályozott műszaki minimumok az épületgépészeti rendszerekre.

Támogatások és adókedvezmények**:** Okos eszközökre, hőszivattyúkra, napelemes rendszerekre biztosított pénzügyi ösztönzők.

Zöld hitelek és beruházási programok**:** Kifejezetten energiahatékonyságot célzó beruházások finanszírozása kedvezményes feltételekkel.

Ezek az intézkedések ösztönzik a lakosságot az energiahatékony technológiák alkalmazására, így támogatják az okosotthonok terjedését.

3.2 Kulcsfontosságú technológiák bemutatása

Az okosotthonok energiamenedzsmentjének hatékonysága nagymértékben függ az alkalmazott technológiák típusától, fejlettségétől és interoperabilitásától. Az alábbiakban bemutatásra kerülnek azok a kulcstechnológiák, amelyek meghatározó szerepet játszanak a háztartási energiafelhasználás optimalizálásában. E technológiák nemcsak az energiafogyasztás csökkentését teszik lehetővé, hanem alapot biztosítanak a prediktív vezérlés, a felhasználói viselkedés alapján történő szabályozás, valamint a megújuló energiaforrások integrációja számára.

3.2.1 Intelligens termosztátok

Az intelligens termosztátok az energiamenedzsment egyik legismertebb és legszélesebb körben használt eszközei. Működésük középpontjában az áll, hogy a fűtési és hűtési rendszereket a lehető legnagyobb hatékonysággal szabályozzák, figyelembe véve:

- a felhasználói jelenlétet (mozgásérzékelő vagy GPS-alapú jelenlétfigyelés)
- a környezeti hőmérsékletet és páratartalmat
- a szokásos napi rutinokat és preferenciákat, az időjárás-előrejelzési adatokat.

A legtöbb intelligens termosztát rendelkezik tanulási képességgel, amelynek révén néhány napos használat után optimalizálni tudja a fűtési/hűtési ciklusokat. Ezek a készülékek akár 10–20%-os energiamegtakarítást is eredményezhetnek éves szinten 111.

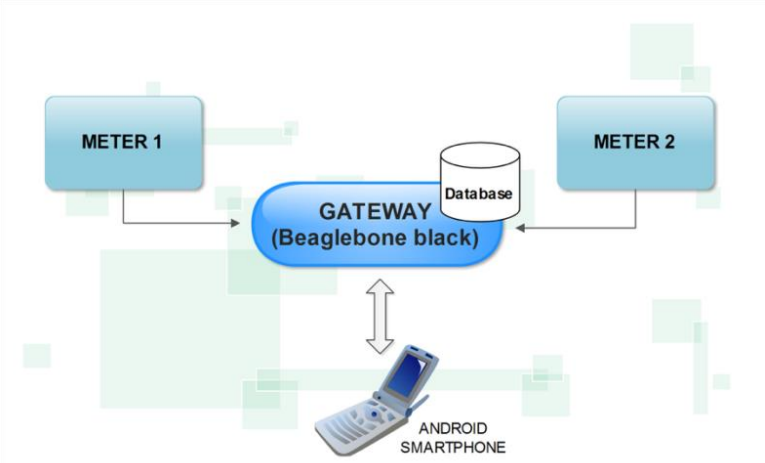
3.2.2 Okos mérőórák (Smart Meters)

Az okos mérőórák lehetővé teszik az energiafogyasztás részletes, valós idejű monitorozását.

Szemben a hagyományos mérőkkel, ezek az eszközök:

- óránkénti vagy percre lebontott fogyasztási adatokat rögzítenek
- képesek kétirányú kommunikációra az energiaszolgáltatóval
- támogatják a dinamikus árképzéshez való alkalmazkodást
- lehetővé teszik az automatizált számlázást és hálózati visszacsatolást

A fogyasztók számára az okos mérőórák haszna abban rejlik, hogy pontos képet kaphatnak energiahasználatukról, és azonosíthatják a túlzott vagy felesleges energiaigényű folyamatokat.



2. ábra: Enerdiafogyasztás monitorozásának egyszerű ábrázolása [17]

3.2.3 Okos konnektorok és fogyasztásfigyelő modulok

Az intelligens konnektorok olyan eszközök, amelyek lehetővé teszik a hozzájuk csatlakoztatott készülékek távoli ki- és bekapcsolását, valamint sok esetben azok fogyasztásának mérését is.

Az előnyeik közé tartozik:

- az eszközök készenléti üzemmódban történő automatikus lekapcsolása
- időzített működés beállítása
- integráció az okosotthon-platformokkal

Ezek a modulok egyszerűen telepíthetők és alacsony költséggel járulnak hozzá az energiafogyasztás csökkentéséhez.

3.2.4 Világításvezérlő rendszerek

Az okos világítási rendszerek – például a Philips Hue vagy LIFX – képesek fényerő, színhőmérséklet és működési idő szerinti vezérlésre.

A vezérlés történhet:

- manuálisan, mobilalkalmazáson keresztül
- automatizáltan, mozgásérzékelő vagy fényérzékelő alapján
- időzítéssel, vagy a napkelte/napnyugta idejéhez igazítva

E rendszerek alkalmazásával jelentős megtakarítás érhető el, különösen olyan nagy forgalmú helyiségekben, ahol gyakran marad égve a világítás.

3. ábra: Philips Hue okos világítási rendszere használatban [16]

3.2.5 Napelemes rendszerek és energiatárolás

A megújuló energiaforrások közül a napenergia hasznosítása vált a legelterjedtebbé a lakossági szektorban.

A napelemes rendszerek integrációja során az alábbi technológiai megoldások játszanak kulcsszerepet:

- Energiatermelés monitorozása**:** Napelemes inverterek és hozzájuk tartozó szoftverek valós időben mérik a termelést és fogyasztást
- Energiatároló rendszerek (pl. Tesla Powerwall**):** A nappal megtermelt, de fel nem használt energia eltárolása éjszakai vagy vészhelyzeti felhasználásra
- Energia-visszatáplálás**:** Bizonyos rendszerek képesek a többletenergia visszajuttatására az elektromos hálózatba, ha azt a szabályozás lehetővé teszi

E rendszerek nemcsak a környezeti lábnyom csökkentéséhez járulnak hozzá, hanem hosszú távon gazdasági megtakarítást is biztosítanak.

3.2.6 Integrált vezérlőközpontok és szoftverplatformok

A különálló technológiák működtetése önmagában kevésbé hatékony, mint az integrált rendszerhasználat. Ennek érdekében az okosotthonok egyre gyakrabban alkalmaznak központi vezérlőegységeket és platformokat, például:

Google Home, Amazon Alexa, Apple HomeKit: Egységes kezelőfelületet biztosítanak különböző gyártók eszközeihez.

Nyílt forráskódú platformok (pl. Home Assistant, OpenHAB): Testreszabható, komplex automatizálási logikákat lehetővé tevő szoftverek.

Energiagazdálkodási algoritmusok: A rendszer képes automatikusan dönteni például arról, mikor indítson el egy eszközt az aktuális energiaár vagy hálózati terhelés alapján. [14]

3.2.7 Gépi tanulás és prediktív algoritmusok

A gépi tanulás alkalmazása az energiamenedzsment területén lehetővé teszi az okosotthon-rendszerek számára, hogy a korábbi fogyasztási adatok alapján mintázatokat ismerjenek fel, és ezek segítségével előre jelezzék a jövőbeni energiaigényt. Az algoritmusok – például lineáris regresszió, döntési fák, neurális hálók – különféle inputokat használnak, mint a külső hőmérséklet, napszak, felhasználói szokások vagy az energiaárak változása. Az előrejelzések alapján a rendszer képes dinamikusan optimalizálni az eszközök működését, például időzíteni a fűtést a várható hőmérsékletcsökkenés előtt, vagy késleltetni az energiaigényes berendezések működtetését a csúcsidőszak utánra. Az ilyen adaptív szabályozás nemcsak energia- és költségmegtakarítást eredményez, hanem elősegíti az energiahálózat egyenletesebb terhelését is. A gépi tanuláson alapuló vezérlőrendszerek így kulcsszerepet játszanak a jövő önoptimalizáló okosotthonainak kialakításában

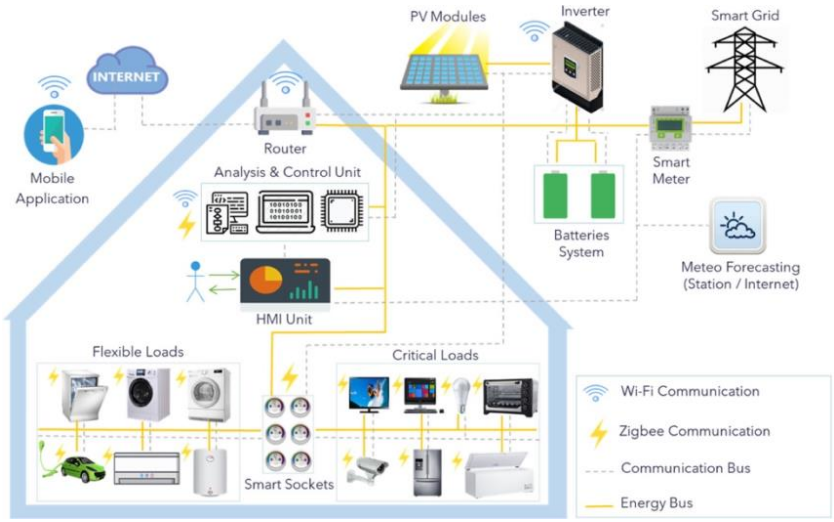
3.2.8 Adaptív vezérlőrendszerek működési logikája

Az adaptív vezérlőrendszerek lényege, hogy működésük során képesek alkalmazkodni a változó körülményekhez és a felhasználói szokásokhoz, ezáltal folyamatosan optimalizálják az energiafelhasználást. Míg a hagyományos rendszerek előre meghatározott szabályrendszer szerint működnek, az adaptív rendszerek valós idejű adatok alapján módosítják működési paramétereiket. Ez történhet például a hőmérséklet, páratartalom, jelenlétérzékelés, napszak vagy dinamikus energiaárak figyelembevételével. A vezérlő algoritmusok – gyakran gépi tanulási modellekkel kiegészítve – folyamatos visszacsatolás alapján tanulják és javítják a szabályozási stratégiákat. Ennek eredményeként nemcsak hatékonyabb energiahasználat valósítható meg, hanem a felhasználói kényelem is növelhető, hiszen a rendszer proaktívan igazodik az aktuális igényekhez. Az adaptív vezérlés különösen fontos szerepet játszik az időjárásfüggő megújuló energiák és az időalapú tarifák optimalizált kezelésében.

3.2.9 Mesterséges intelligencia szerepe

A mesterséges intelligencia (MI) az okosotthonok energiamenedzsmentjében egyre hangsúlyosabb szerepet tölt be, különösen a decentralizált és autonóm rendszerek kialakításában. Az MI-alapú rendszerek képesek nagy mennyiségű heterogén adat – például fogyasztási minták, időjárás-előrejelzések, dinamikus árak és hálózati terhelési adatok – elemzésére, majd ezen információk alapján komplex döntéseket hoznak az energiaelosztásról, -tárolásról és -

felhasználásról. Mindez lehetővé teszi, hogy a rendszer proaktívan alkalmazkodjon a környezeti és gazdasági változásokhoz, ezáltal optimalizálja a működést, csökkentse a költségeket és javítsa a rendszerstabilitást. Az MI segítségével kialakított vezérlési mechanizmusok az energiahálózattól független döntéshozatalt is támogatják, amely kulcsfontosságú a decentralizált energiatermelő egységek, például napelemes háztartások esetében. Emellett az MI hozzájárul a hibák és anomáliák korai észleléséhez is, ami növeli a rendszer megbízhatóságát és biztonságát.



4 ábra: HEMS architektúra (Home Energy Management System) [18]

3.2.10 Blockchain technológia alkalmazása energiaelosztásban

A blockchain technológia egyre nagyobb figyelmet kap az energiamenedzsment decentralizálása kapcsán, különösen a peer-to-peer (P2P) energiaelosztási modellek támogatásában. A blockchain egy elosztott főkönyvi rendszer, amely lehetővé teszi a biztonságos, átlátható és központi szereplőtől mentes adat- és tranzakciókezelést. Az okosotthonok kontextusában ez azt jelenti, hogy a háztartások – különösen a megújuló energiát termelők – közvetlenül egymással kereskedhetnek energiával, előre definiált, automatizált szabályrendszerek (ún. smart contracts) alapján. A rendszer garantálja a tranzakciók hitelességét, megváltoztathatatlanságát és nyomon követhetőségét anélkül, hogy közvetítő energiaszolgáltatóra lenne szükség.

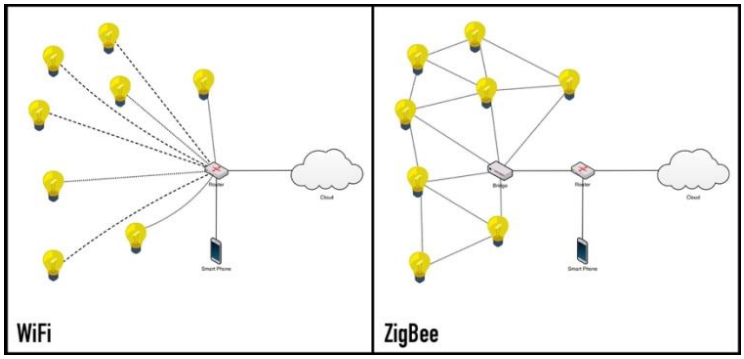
A blockchain alkalmazása emellett elősegítheti az energiaszármazás hitelesítését is (pl. zöldenergia-eredet tanúsítványok), valamint a mikrogrid rendszerek működésének automatizálását. Bár technológiai és szabályozási akadályok továbbra is fennállnak, a blockchain ígéretes eszköz a jövő decentralizált, felhasználóközpontú energiarendszereinek kialakításához. [15]

4 KOMMUNIKÁCIÓS PROTOKOLLOK ELEMZÉSE

Az okosotthonok működésének hatékonysága és megbízhatósága nagymértékben függ a használt kommunikációs protokolloktól, amelyek biztosítják az egyes eszközök közötti adatcserét, a központi vezérlés lehetőségét, valamint a távoli elérés és automatizálás funkcionalitását. A megfelelő protokoll kiválasztása kulcsfontosságú az interoperabilitás, az energiafogyasztás, a hálózati stabilitás, a biztonság és a válaszidő szempontjából egyaránt. Az okosotthonokban alkalmazott kommunikációs szabványok két fő csoportra oszthatók: vezeték nélküli és vezetékes technológiákra. A vezeték nélküli megoldások a legelterjedtebbek, mivel könnyen telepíthetők és jól skálázhatók.

4.1.1 Zigbee

A Zigbee egy alacsony energiaigényű, rövid hatótávolságú rádiófrekvenciás kommunikációs protokoll, amelyet kifejezetten M2M (machine-to-machine) kommunikációra fejlesztettek ki. A protokoll mesh hálózati topológiát alkalmaz, amely lehetővé teszi, hogy az eszközök egymáson keresztül továbbítsák az adatokat, így növelve a lefedettséget és a megbízhatóságot. A Zigbee előnyei közé tartozik az alacsony energiafogyasztás, a magas hálózati bővíthetőség, valamint a gyártófüggetlen szabványosság, ami biztosítja a kompatibilitást különböző eszközök között. Hátrányként említhető a korlátozott adatátviteli sebesség és a Wi-Fi interferencia lehetősége**,** mivel azonos frekvenciasávban működik (2,4 GHz).[4]



5. ábra: Zigbee és WiFi összehasonlítása [20]

4.1.2 Z-Wave

A Z-Wave egy másik elterjedt mesh-hálózati technológia, amely kifejezetten az okosotthon-alkalmazásokhoz lett optimalizálva. A Zigbee-től eltérően Z-Wave alacsonyabb, interferenciamentes frekvenciasávokat használ (pl. 868 MHz Európában), így jobban teljesít többrétegű falakkal rendelkező épületekben. Bár az eszközválaszték kisebb, a Z-Wave eszközök között kiemelkedően jó a kompatibilitás, mivel minden eszköznek meg kell felelnie a Z-Wave Alliance minősítési követelményeinek. Ugyanakkor a technológia zárt licenc alatt áll, ami korlátozhatja a szabad fejlesztéseket és a bővítési lehetőségeket.[5]

4.1.3 MQTT

Az MQTT (Message Queuing Telemetry Transport) egy könnyű, nyílt forráskódú üzenetküldő protokoll, amelyet elsősorban IoT-alkalmazásokhoz használnak, különösen olyan esetekben, ahol kis sávszélesség és nem megbízható hálózati kapcsolat jellemző. A protokoll publish–subscribe (közzététel–feliratkozás) modell alapján működik, és központi broker segítségével irányítja az üzenetforgalmat. Előnyei közé tartozik az alacsony hálózati terhelés, a valós idejű adatküldés lehetősége, valamint a platformfüggetlenség. Az MQTT különösen alkalmas olyan okosotthon-rendszerekhez, ahol több különböző típusú eszköz és alrendszer működik párhuzamosan, és a rendszer nyílt, rugalmas integrációt igényel.

4.1.4 Thread

A Thread egy IPv6-alapú vezeték nélküli protokoll, amelyet a Nest (ma Google Nest) fejlesztett ki, és amely mára egy nyílt ipari szabványként funkcionál. A Thread célja a biztonságos, skálázható és alacsony energiafogyasztású mesh hálózatok biztosítása, különösen az okosotthon-környezetekben. A technológia egyik előnye, hogy nativ IPv6 támogatást biztosít, így az eszközök közvetlenül csatlakozhatnak az internethez, közvetítő eszköz nélkül. A Thread egyik fontos jellemzője a „self-healing" hálózati struktúra, amely automatikusan újrarendezi a hálózati kapcsolatokat, ha egy eszköz kiesik. Ez különösen megbízható működést tesz lehetővé hosszú távon.

4.1.5 Matter

A Matter a legújabb kommunikációs szabvány, amelyet olyan iparági szereplők vezettek be, mint az Apple, Google, Amazon és a Zigbee Alliance. Célja, hogy egységes szabványt teremtsen az okosotthon-eszközök számára, amely garantálja az interoperabilitást különböző gyártók termékei között. A Matter a meglévő protokollokat (pl. Thread, Wi-Fi) használja alacsony szinten, miközben biztosítja a biztonságos hitelesítést, a könnyű párosítást és az offline működést is. A Matter várhatóan kulcsszerepet játszik majd a jövő szabványosított okosotthon-ökoszisztémáiban. [6]

4.2 Kiberbiztonság és adatvédelem kérdései

Az okosotthonok rendszerszintű működésének egyik legkritikusabb aspektusa a kiberbiztonság és az adatvédelem, mivel az összekapcsolt eszközök folyamatos adatcserét folytatnak egymással és a felhőalapú szolgáltatásokkal. E technológiai kontextusban a felhasználók személyes élettere és digitális adatai olyan kockázatoknak vannak kitéve, amelyek korábban nem jelentek meg a hagyományos, nem hálózatra kötött háztartási rendszerekben. A biztonsági kihívások és a megfelelő védelmi mechanizmusok áttekintése ezért kulcsfontosságú az energiamenedzsment-megoldások megbízhatóságának és hosszú távú működésének biztosításához.

4.2.1 Kiberbiztonsági kockázatok és támadási vektorok

A hálózatra kapcsolt otthoni eszközök potenciális célpontot jelentenek különféle kiberfenyegetések számára.

A leggyakoribb támadási formák a következők:

- Hozzáférés jogosulatlan felhasználók által: Gyenge jelszavak, hiányos hitelesítési rendszerek révén támadók átvehetik az irányítást az eszközök felett (pl. termosztát, ajtózár, kamera)

- Adatszivárgás: Az eszközök által gyűjtött adatok – például jelenlétinformációk, energiafogyasztási szokások – érzékeny személyes információk, amelyekhez való illetéktelen hozzáférés magánéleti visszaélésekhez vezethet
- Közbeékelődéses támadások (man-in-the-middle): A hálózati kommunikáció lehallgatása vagy módosítása során a támadó manipulálhatja a rendszer működését vagy bizalmas adatokat szerezhet meg
- DDoS (Distributed Denial of Service) támadások**:** A rendszer túlterhelésével egyes eszközök működésképtelenné válhatnak, ami az energiamenedzsment működését is megzavarhatja.
- Firmware-sebezhetőségek kihasználása**:** Elavult vagy nem frissített szoftverek olyan sérülékenységeket tartalmazhatnak, amelyeken keresztül a támadók bejuthatnak a rendszerbe.

4.2.2 Adatvédelem és adatkezelés problémakörei

Az okosotthon-eszközök számos személyes adatot gyűjtenek, köztük:

- energiafogyasztási mintázatok
- hőmérséklet- és mozgásadatok
- helymeghatározási információk
- felhasználói interakciók naplózása

Ezek az adatok nemcsak technikai, hanem jogi és etikai szempontból is érzékenynek számítanak. Az adatvédelmi kockázatokat súlyosbítja, hogy sok eszköz külső felhőszolgáltatókhoz kapcsolódik, így az adatok földrajzi határokat is átléphetnek, eltérő jogi szabályozás alá esve.

Az általános adatvédelmi rendelet (GDPR) az Európai Unióban szigorúan szabályozza a személyes adatok kezelését, így az okosotthon-rendszerek tervezésekor és üzemeltetésekor biztosítani kell a következő elveket:

- adatminimalizálás (csak a szükséges adatokat gyűjtik)
- transzparencia (a felhasználók tájékoztatása az adatkezelés módjáról)
- hozzáférés-szabályozás (ki férhet hozzá az adatokhoz)
- törlési jog (a felhasználó kérheti adatai törlését)

4.2.3 Biztonsági megoldások és védekezési stratégiák

A kockázatok kezelésére többféle technikai és szervezeti megoldás alkalmazható.

Az alábbiak a legfontosabbak:

- Többfaktoros hitelesítés (2FA): A felhasználók azonosításának megerősítésére szolgál, pl. jelszó + mobilalkalmazás
- Titkosított adatátvitel: A kommunikáció titkosítása (pl. TLS protokollal) megakadályozza az adatok lehallgatását és módosítását
- Automatikus firmware-frissítés: Az eszközöknek rendszeresen kell frissíteniük a szoftverüket, hogy a legújabb biztonsági hibák javítva legyenek
- Helyi adatfeldolgozás (edge computing): Minimalizálja az adatok külső szerverekre történő továbbítását, ezáltal csökkenti a kiszolgáltatottságot
- Külön hálózati szegmensek használata: A vendéghálózatokra, biztonsági zónákra osztott otthoni Wi-Fi-rendszerek növelik az elválasztást a támadható eszközök között

Emellett a gyártók részéről szükséges a biztonság alapú tervezés (security by design) megközelítés alkalmazása, amely szerint a biztonsági szempontokat már a fejlesztési folyamat legelején figyelembe kell venni.

4.2.4 Felhasználói tudatosság szerepe

A technikai megoldások mellett kiemelkedő fontosságú a felhasználói edukáció. Gyakori probléma, hogy az eszközöket alapértelmezett jelszavakkal hagyják működni, vagy nem alkalmazzák az elérhető védelmi funkciókat. A felhasználók képzése és tudatosítása a következőket foglalja magában:

- biztonságos jelszókezelés
- frissítések rendszeres telepítése
- eszközhozzáférés naplózása
- gondos eszközválasztás (megbízható gyártók termékei)

A biztonságtudatos felhasználói magatartás elengedhetetlen része a rendszer egészének védelmének, különösen egy olyan környezetben, ahol a rendszer sebezhetősége egyetlen gyenge ponton keresztül kompromittálható.

5 TECHNOLÓGIAI CÉGEK ESETTANULMÁNY-SZERŰ BEMUTATÁSA

Az okosotthonok piacán számos technológiai vállalat játszik meghatározó szerepet, különféle eszközöket, rendszereket és platformokat kínálva az energiamenedzsment, automatizálás és felhasználói élmény javítására. Az alábbi alfejezet négy jelentős piaci szereplő – Siemens, Bosch, Legrand és Somfy – tevékenységét mutatja be esettanulmány-szerűen, kiemelve az általuk kínált megoldások technológiai jellemzőit, integrációs lehetőségeit és piaci pozícióját.

5.1.1 Siemens – Komplett intelligens épületautomatizálási megoldások

A Siemens AG az egyik legnagyobb európai ipari konszern, amely vezető szerepet tölt be az épületautomatizálás és az energiahatékonysági technológiák területén. A Siemens Building Technologies divíziója olyan integrált rendszereket kínál, amelyek lehetővé teszik az okosépületek és okosotthonok teljes körű energiairányítását. [10]

Főbb megoldásaik:

- Desigo CC: egy nyílt architektúrájú épületirányítási platform, amely képes több alrendszer integrációjára (pl. HVAC, világítás, tűzjelzés, biztonság)
- Synco Living: kifejezetten lakossági célokra fejlesztett intelligens vezérlőrendszer, amely automatizálja a fűtést, szellőzést, redőnyvezérlést és világítást
- KNX-alapú kompatibilitás: a Siemens számos eszköze a KNX szabványra épül, amely az egyik legelterjedtebb vezetékes protokoll épületautomatizálásban, biztosítva az eszközök közötti kompatibilitást

A Siemens megoldásai nagy hangsúlyt fektetnek a skálázhatóságra és a teljes életciklus-kezelésre, vagyis nemcsak az eszközök üzembe helyezését, hanem azok karbantartását és optimalizálását is támogatják. Az ipari szintű megbízhatóság miatt különösen alkalmasak nagyobb, komplex rendszerekre vagy prémium okosotthon-megoldásokra. [9]

5.1.2 Bosch – Moduláris okosotthon-rendszerek lakossági fókuszban

A Bosch Smart Home divízió célja egy egyszerűen telepíthető, moduláris és felhasználóbarát okosotthon-rendszer biztosítása, amely a biztonság, a kényelem és az energiahatékonyság hármas célrendszerére épül.

Főbb jellemzők:

- Bosch Smart Home Controller: központi vezérlőegység, amely képes koordinálni az összes okoseszköz működését, helyi hálózaton vagy interneten keresztül
- Okos termosztátok és fűtésvezérlők: képesek alkalmazkodni a felhasználói jelenléthez, időjárási körülményekhez és napi rutinokhoz
- Energiatudatos szenzorok: például nyitásérzékelők, amelyek automatikusan leállítják a fűtést, ha ablakot nyitnak

A Bosch rendszerének egyik fő előnye a gyors üzembe helyezés, az egyszerű kezelőfelület és az adatvédelmi megfelelés, mivel az adatok többsége helyileg kerül tárolásra. A cég rendszeresen integrálja termékeit olyan platformokkal, mint az Amazon Alexa és a Google Assistant, így lehetővé téve a hangvezérlést és a rendszer nyitottságát. [8]

5.1.3 Legrand – Energiagazdálkodás és infrastruktúra alapú megközelítés

A Legrand francia központú multinacionális vállalat főként villamos szerelvények és épületinfrastruktúra területén vált ismertté, de az elmúlt években fokozatosan bővítette termékpalettáját az okosotthon-megoldások irányába. Fókuszában az energiagazdálkodás, a világításvezérlés és a felhasználói szokásokhoz igazodó automatizálás áll.

Kulcstechnológiák:

- Eliot program: az IoT integrációjára épülő platform, amely összeköti a Legrand eszközeit egységes vezérlési rendszerben
- Netatmo integráció: a Legrand 2018-ban felvásárolta a Netatmo-t, amely népszerű okostermosztátokat, időjárás- és jelenlétérzékelőket fejleszt
- Energiaközpontú vezérlés: okos fogyasztásmérők és lekapcsoló automatizmusok a terheléselosztás optimalizálására

A Legrand előnye a háttérrendszerekbe való beépíthetőség – például elosztószekrényekbe vagy villamos hálózatba illeszthető eszközök –, ami lehetővé teszi, hogy az okosfunkciók szervesen illeszkedjenek az épületvillamossági rendszerbe.

5.1.4 Somfy – Automatizált árnyékolás és energiatudatos kiegészítők

A Somfy specializációja az árnyékolástechnika és nyílászáró-automatizálás területe, de az elmúlt években fokozatosan épített ki komplett okosotthon-ökoszisztémát. A vállalat fő fókuszterülete az energiamegtakarítás passzív módon, a természetes fény és hő kihasználásával.

Főbb termékkategóriák:

- Okos redőnymotorok és árnyékolók, amelyek napfény- és időjárásadatok alapján automatikusan szabályozzák az árnyékolást.
- TaHoma® rendszer: központi vezérlőplatform, amely más gyártók rendszereivel (pl. Philips Hue, Sonos) is integrálható.
- Zigbee- és io-homecontrol-kompatibilitás, amelyek lehetővé teszik a stabil, alacsony energiaigényű kommunikációt.

A Somfy megoldásai különösen előnyösek olyan háztartásokban, ahol nagy az üvegfelületek aránya, és az árnyékolással jelentős fűtési és hűtési energia takarítható meg.

6 TECHNOLÓGIAI CÉGEK ILLESZKEDÉSE AZ INTELLIGENS VÁROSI INFRASTRUKTÚRÁKBA

Az intelligens városok (smart cities) célja, hogy a digitális technológiák segítségével fenntartható, hatékony és élhető környezetet biztosítsanak a lakosság számára. E cél elérése összetett rendszerszintű megközelítést kíván meg, amelyben kulcsszerepet játszanak az ipari és technológiai szolgáltatók. A 5. fejezetben részletesen bemutatott cégek nemcsak a lakossági okosotthon-megoldások területén aktívak, hanem komplex infrastruktúrákba integrálható rendszereket is fejlesztenek, amelyek illeszkednek a városi energiamenedzsment, biztonság, automatizálás és közműirányítás digitális architektúráihoz. [2]

6.1.1 Siemens – Skálázható városi energia- és infrastruktúrairányítás

A Siemens kiterjedt portfóliójának köszönhetően az egyik legismertebb szereplő az okosváros-rendszerek szintjén történő integrációban. A vállalat olyan átfogó megoldásokat kínál, amelyek az épületirányítástól kezdve a közműszolgáltatásokon át egészen a közlekedésvezérlésig terjednek.

- Desigo CC és más épületmenedzsment-platformok városi intézményekre és középületekre is skálázhatók, lehetővé téve a közszolgáltatások (iskolák, kórházak, hivatalok) energiafelügyeletét
- A Siemens részt vesz több smart grid projektben, például városi mikrohálózatok és megújuló energia integrációs megoldások fejlesztésében
- A cég IoT-platformja, a MindSphere, támogatja a városi adatgyűjtést, elemzést és optimalizálást – kulcsfontosságú eszköz a közlekedés, közvilágítás vagy hulladékgazdálkodás digitalizálásában

A Siemens technológiái közvetlenül hozzájárulnak az urbanisztikai digitalizációhoz és a fenntartható várostervezéshez.

6.1.2 Bosch – Mobilitás, biztonság és adatközpontú városfejlesztés

A Bosch a lakossági okosotthonok mellett számos intelligens városi megoldást fejleszt, amelyek adatközpontú, rugalmasan skálázható infrastruktúrát tesznek lehetővé.

- Bosch Security Systems intelligens kamerarendszerei és szenzorai a közterületi megfigyelés és városi biztonság alapjait képezik
- A Bosch saját IoT platformja (Bosch IoT Suite) lehetővé teszi az eszközök és városi rendszerek közötti kommunikációt, felhőszintű menedzsmenttel és prediktív karbantartással
- A vállalat intelligens parkolás, e-mobilitás és közlekedési szenzortechnológiák területén is aktív, így a városi mobilitási stratégiákhoz is kapcsolódik

A Bosch szerepe a smart city struktúrákban sokoldalú: az adatalapú városirányítástól a fizikai infrastruktúrákig számos rétegben jelen van.

6.1.3 Legrand – Intelligens infrastruktúra a városi létesítményekben

A Legrand elsősorban épületvillamossági rendszerei és okos hálózati infrastruktúrái révén járul hozzá az intelligens városok kialakulásához.

- A Legrand Eliot programja az IoT-kompatibilis termékek városi méretekben történő telepítését célozza: pl. intelligens világítás, fogyasztásmérés, elosztószekrény-automatizálás
- A Netatmo-szenzorok integrálhatók városi környezetfigyelő rendszerekbe is (pl. hőmérséklet, zaj, levegőminőség), így hozzájárulnak a környezeti monitoringhoz
- Intézményi szintű megoldásokat kínálnak irodaházak, iskolák és közintézmények energetikai és hálózati infrastruktúrájához – ezzel középületek intelligens hálózatba kapcsolását teszik lehetővé

A Legrand termékei tehát infrastruktúraszinten illeszkednek a városi digitális ökoszisztémákhoz. [11]

6.1.4 Somfy – Épületburkolati automatizálás városi szinten

Bár a Somfy elsődleges piaca a lakossági árnyékolástechnika, termékei egyre nagyobb szerepet kapnak a városi energiahatékonysági fejlesztésekben is.

- Intelligens árnyékolási rendszerei – például redőnymotorok és automata napellenzők – alkalmazhatók közintézményekben és irodaházakban, ahol automatikusan szabályozzák a belső hőterhelést
- Ezek a megoldások közvetlenül hozzájárulnak a fűtési és hűtési energiafogyasztás csökkentéséhez, különösen üveghomlokzatos városi épületek esetén
- A Somfy TaHoma® platformja képes más városi rendszerekkel (pl. világítás, fűtés, épületvezérlés) kommunikálni, így elősegíti a funkcionális integrációt a városi infrastruktúrákban

A Somfy technológiái passzív módon járulnak hozzá a városi szintű energiaoptimalizáláshoz és a környezetterhelés csökkentéséhez. [12]

7 ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

Az elemzés során megállapítható, hogy az okosotthon-rendszerek fejlődése az elmúlt évtizedben gyors és sokrétű volt, amiben meghatározó szerepet játszott az IoT-eszközök elterjedése, a kommunikációs protokollok fejlődése, valamint a mesterséges intelligencia alkalmazása. A fejlett vezérlési és automatizálási rendszerek lehetővé tették az energiafogyasztás valós idejű monitorozását, optimalizálását, valamint a megújuló energiaforrások háztartási szintű integrációját. Az okoseszközök kulcsszereplőkké váltak a modern háztartásokban.

A kiberbiztonsági és adatvédelmi kérdések ugyanakkor komoly kihívásokat jelentenek, különösen a hálózatra kapcsolt rendszerek esetében. A felhasználói bizalom fenntartása és a jogszabályi megfelelés elengedhetetlen ahhoz, hogy az okosotthon-technológiák széles körben elterjedhessenek.

A technológiai cégek és platformok elemzése azt mutatta, hogy a piaci kínálat sokszínű, és különböző megközelítések léteznek az egyszerű, plug-and-play megoldásoktól a komplex, nyílt forráskódú rendszerekig. Ugyanakkor a jövő szempontjából egyre nagyobb hangsúlyt kap a rendszerszintű gondolkodás, a szabványosítás és a skálázhatóság.

Következtetésként elmondható, hogy az okosotthonok energiamenedzsmentje nemcsak egy új technológia, hanem része egy nagyobb társadalmi és gazdasági változásnak is. A jövőben azok a rendszerek lesznek sikeresek, amelyek egyszerre hatékonyak, környezetbarátok, biztonságosak és könnyen használhatók. Ezeknek a rendszereknek jól kell működniük együtt, könnyen alakíthatóknak és bővíthetőknek kell lenniük. Már elindultunk ezen az úton, és az okosotthonok fontos szerepet fognak játszani a jövő energiával kapcsolatos digitális világában.

8 IRODALOMJEGYZÉK

[1] International Energy Agency (IEA), *Energy Efficiency 2023*, Paris: IEA, 2023. https://www.iea.org/reports/energy-efficiency-2023

[2] M. Moeini, R. F. Babiceanu, and K. S. Benyahia, “Smart Home Energy Management Systems

[3] Google Nest, "How the Nest Learning Thermostat Works," Google, 2023 https://support.google.com/googlenest/answer/9231673

[4] Zigbee Alliance, “Zigbee Specification,” CSA Group, 2022. https://csa-iot.org/all-solutions/zigbee/

[5] Z-Wave Alliance, “Z-Wave Technical Overview,” Z-Wave Alliance, 2023. https://z-wavealliance.org

[6] Matter (Connectivity Standards Alliance), “Matter Overview,” CSA, 2024. https://csa-iot.org/all-solutions/matter/

[7] A. Ipakchi and F. Albuyeh, “Grid of the Future,” *IEEE Power & Energy Magazine*

[8] Bosch Smart Home, “Smart Solutions for Energy Saving,” Bosch GmbH, 2023. https://www.bosch-smarthome.com

[9] Siemens AG, “Desigo CC – Integrated Building Management Platform,” Siemens, 2022 https://new.siemens.com/global/en/products/buildingtechnologies/building-management/desigo-cc.html

[10] European Commission, “Data protection in the EU,” 2023. https://commission.europa.eu/law/law-topic/data-protection_en

[11] Legrand Group, “Smart Home & Building Solutions,” Legrand, 2023. https://www.legrand.com

[12] Somfy Group, “Smart Shading & Home Automation,” Somfy, 2022. https://www.somfy.com

[13] H. Wang, Y. Lu, and X. Zhang, “Blockchain-Based Energy Management for Smart Grids,” *IEEE Internet of Things*

[14] Home Assistant, “The Open Source Home Automation Platform,” Home Assistant Foundation, 2024. https://www.home-assistant.io

[15] International Renewable Energy Agency (IRENA), *Innovation Landscape Brief: Peer-to-Peer Electricity Trading*, Abu Dhabi, 2020.

[16] https://bitrise.io/customer-stories/signify-philips-hue

[17] https://www.instructables.com/Smart-home-energy-management-system-SHEMMS/

[18] Design and implementation of an AI-based & IoT-enabled Home Energy Management System

[19]https://blog.silverpc.hu/2024/12/29/az-iot-es-a-mindennapi-elet-hogyan-alakitjak-at-az-iot-eszkozok-az-otthoni-es-munkahelyi-kornyezeteket/

[20] https://linkdhome.com/articles/what-is-zigbee-guide

2.41. A hibrid rendszerek jelentősége az Ipar

A hibrid rendszerek jelentősége az Ipar 4.0-ban

Tartalom

Bevezetés 1

2. Hibrid rendszerek alapjai 3

2.1 Definíció és jellemzők 3

2.2 Hibrid rendszerek típusai 3

2.3 A hibrid rendszerek működési elvei 4

3. A hibrid rendszerek alkalmazásai 5

3.1 Ipari alkalmazások 5

3.2 Autonóm rendszerek és robotika 6

3.3 Autonóm járművek 7

3.4 Orvosi alkalmazások 8

4. A hibrid rendszerek előnyei és kihívásai 9

4.1 Előnyök 9

4.2 Kihívások és problémák 10

5. Alkalmazott matematikai modellezés és algoritmusok 12

5.1 Hibrid automáták 12

5.2 Modellezési technikák és módszerek 13

5.3 Az algoritmusok szerepe 14

6. A hibrid rendszerek kutatásának jövőbeli irányai 15

6.1 Mesterséges intelligencia és gépi tanulás 15

6.2 Fenntarthatóság és zöld technológia 17

6.3 Elméleti alapok fejlesztése 18

7. Társadalmi és gazdasági hatások 20

7.1 Munkahelyek és automatizálás 20

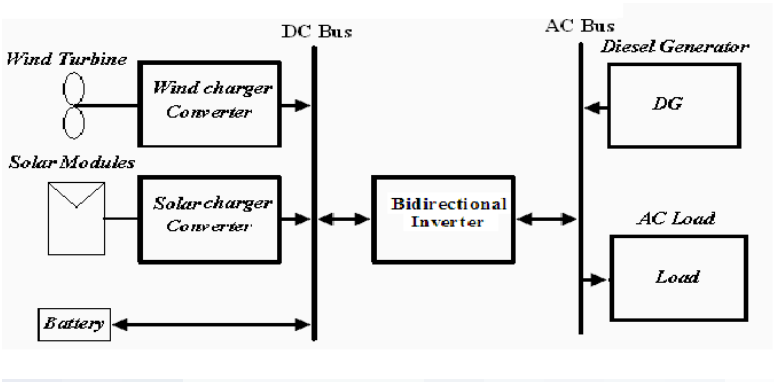
7.3 Etikai dilemmák és jogi felelősség 22

Következtetés 24

Bevezetés

Az ipari fejlődés jelenlegi szakaszát sokan a negyedik ipari forradalomként, vagyis Ipar 4.0-ként emlegetik. Ebben a forradalomban kulcsszerep jut a digitális és a fizikai rendszerek integrációjának, azaz olyan kiber-fizikai rendszereknek, amelyekben a számítógépes vezérlés (digitális, diszkrét logika) szorosan együttműködik a valós fizikai folyamatokkal (folytonos dinamika). A *hibrid rendszerek* pontosan ezt az integrációt valósítják meg: egyesítik a folytonos és a diszkrét működést egy közös keretben. Ennek köszönhetően a hibrid rendszerek képesek kezelni az ipari környezet összetett folyamatait, ahol szenzoradatok folyamatos áramlása és az azokra épülő eseményvezérelt döntések egyaránt jelen vannak.

Az Ipar 4.0-ban a gyártósorok, a robotok és az intelligens gépek mind olyan kihívásokkal szembesülnek, ahol valós időben kell reagálniuk a változó körülményekre. A hibrid rendszerek jelentősége abban rejlik, hogy valós idejű döntéshozatalra adnak lehetőséget a folyamatos folyamatok mellett. Például egy okos gyárban a gépek szenzorai folyamatosan mérik a hőmérsékletet, sebességet, nyomást stb., miközben a vezérlőegység diszkrét jelek alapján (pl. egy riasztó jelzésére) dönt beavatkozásokról. A kétféle működés kombinációja – vagyis a hibrid rendszer – biztosítja, hogy a rendszer gyorsan és adaptívan reagáljon, kihasználva mindkét megközelítés előnyeit. Ennek eredményeképpen a termelés hatékonyabb, rugalmasabb és intelligensebb lesz, ami versenyelőnyt jelenthet a vállalatok számára a modern ipari környezetben.



2. Hibrid rendszerek alapjai

2.1 Definíció és jellemzők

A hibrid rendszerek dinamikus rendszerek egy speciális osztályát alkotják, amelyekben *kétféle működési logika egyesül*: egy folytonos (continuous) és egy diszkrét komponens. Egyszerűbben

fogalmazva, a hibrid rendszer olyan rendszer, amelyben a változók időbeli alakulását folyamatos differenciálegyenletek írják le, ugyanakkor bizonyos események hatására hirtelen, ugrásszerű változások – diszkrét átmenetek – következnek be az állapotában. A folytonos viselkedés tipikusan a fizikai folyamatokat, a diszkrét viselkedés pedig az ezekhez kapcsolódó logikai döntéseket reprezentálja. A formális definíció szerint egy hibrid rendszer leírható hibrid automatával vagy hibrid dinamikai modellel.

Ezek a rendszereket elsősorban a szabályozáselmélet, a matematikai modellezés és a formális verifikáció területén tanulmányozzuk. Az ilyen rendszerek segítségével komplex, időben változó környezeteket lehet modellezni és vezérelni. Például egy önvezető jármű esetében a jármű mozgásegyenletei adják a folytonos dinamikát, míg a forgalmi lámpák, sávváltások vagy vészfékezések diszkrét eseményekként jelennek meg a modellben. A hibrid modell lehetővé teszi, hogy a jármű *viselkedését formálisan leírjuk*, beleértve minden releváns állapotot (mint pl. halad egyenes úton vagy kanyarodik), az ezeket összekötő átmeneteket (például sávot vált), és a folytonos mozgásegyenleteket (mint a haladási sebesség változása az időben).

Fontos jellemző, hogy egyszerre kezelik a folytonos és a diszkrét időfogalmat. A folytonos alrendszerben az idő valós számokkal (töretlen időskálán) telik, míg a diszkrét alrendszerben lépésenként vagy eseményenként halad előre. Ez a kettősség lehetővé teszi a valós idejű irányítási feladatok modellezését, de egyben komplexitást is ad a rendszernek, hiszen a két alrendszer összehangolt működését kell biztosítani.

2.2 Hibrid rendszerek típusai

A hibrid rendszereknek több típusa is létezik, attól függően, hogy a diszkrét és folytonos komponensek miként kapcsolódnak össze, illetve milyen szerepet töltenek be. Két gyakran említett kategória a szakirodalomban a hibrid automaták és a hibrid dinamikai rendszerek.

- Hibrid automaták: Ahogy az előző alfejezetben már utaltam rá, a hibrid automaták a hibrid rendszerek egyik legelterjedtebb modelljét jelentik. Ezek olyan formális állapotgépek, ahol minden állapothoz tartozik egy folytonos viselkedés (általában differenciálegyenlet formájában), és az állapotok között diszkrét *átmenetek* vannak definiálva. A hibrid automata modell széles körben használatos mind az elméleti kutatásban, mind pedig gyakorlati alkalmazások modellezésében. Előnye, hogy formális keretet ad a hibrid viselkedés leírására, ami jól használható *verifikációs célokra*, azaz annak ellenőrzésére, hogy a rendszer bizonyos tulajdonságoknak (például biztonsági feltételeknek) megfelel. A hibrid automaták esetében a diszkrét és a folytonos rész szorosan integrált: minden egyes állapotban egy adott folytonos dinamika érvényes, és amint egy meghatározott feltétel teljesül (pl. egy folytonos változó elér egy küszöbértéket), egy diszkrét átmenet következik, ami esetleg másik

differenciálegyenlet-rendszerre vált. Ennek köszönhetően a hibrid automata kompakt és érthető módon ragadja meg a rendszer lehetséges viselkedéseit.

- Hibrid dinamikai rendszerek: A hibrid rendszerek egy másik megközelítését jelentik azok a modellek, amelyekben a folytonos és a diszkrét részek kevésbé szorosan kapcsolódnak egyetlen állapotgép-struktúrához. Ilyen esetekben a rendszert inkább egyidejűleg működő folytonos és diszkrét komponensek halmazaként képzelhetjük el, ahol a diszkrét események és a folytonos folyamatok párhuzamosan zajlanak, és időnként kölcsönhatásba lépnek. Például egy robotika alkalmazásban a robot mozgását leíró folytonos szabályozó algoritmus mellett futhat egy magasabb szintű diszkrét tervező algoritmus, amely időnként beavatkozik (pl. új úticélt ad a robotnak). A hibrid dinamikai rendszer kifejezés sokszor egy tágabb kategóriát jelöl, ahol a rendszer viselkedése hibrid jellegű ugyan, de nem feltétlenül van egyetlen hibrid automata formájában leírva. Ide sorolhatjuk azokat a rendszereket is, amelyeknél több, lazán csatolt hibrid komponens alkot egy nagyobb rendszert. Ezek a modellek rugalmasabbak lehetnek bizonyos komplex problémák leírásában, bár a formális elemzésük nehezebb lehet, mint az egy hibrid automatával leírt rendszereké.

A fenti két típus nem egymást kizáró kategória, inkább a modellezési nézőpont különbségét tükrözi. A lényeges különbség abban áll, hogy a hibrid automata egy egységes keretbe foglal mindent (állapotok, átmenetek, differenciálegyenletek), míg a hibrid dinamikai rendszer kifejezés használata gyakran arra utal, hogy a folyamatos és diszkrét részek *külön is értelmezhetők*, és a rendszer ezek kombinációjaként szemlélhető.

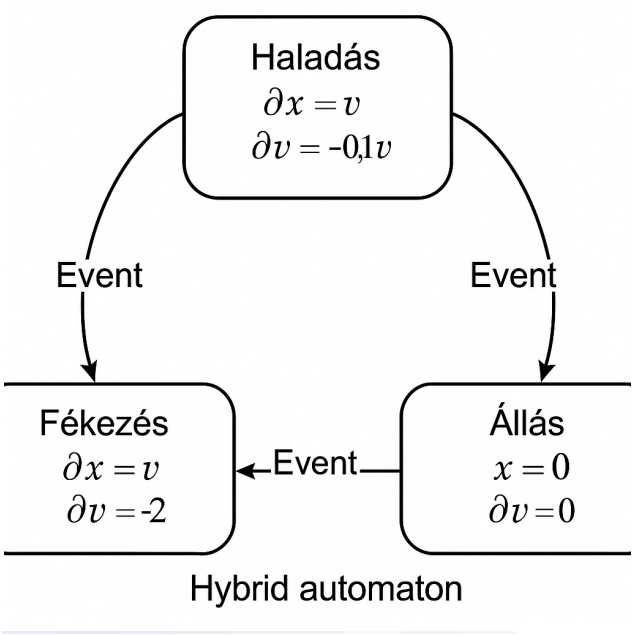
2.3 A hibrid rendszerek működési elvei

A hibrid rendszerek működésének megértéséhez tekintsük át, hogyan zajlik egy tipikus hibrid rendszer *életciklusa*, azaz miként változik az állapota az időben. A rendszer indul egy kezdeti állapotból, amely meghatározza, hogy a folytonos változók kezdetben milyen értékűek, és a diszkrét állapot (vagy módus) melyik. Ezután a rendszer folytonos dinamikája veszi át a főszerepet: a differenciálegyenletek diktálta módon a folytonos változók értékei elkezdenek változni az idő függvényében. Ezt a szakaszt nevezhetjük a rendszer *folytonos fázisának*. Ebben a fázisban a diszkrét állapot változatlan, tehát a rendszer úgymond ugyanabban a "üzemmódban" marad, miközben a paraméterei folyamatosan változnak.

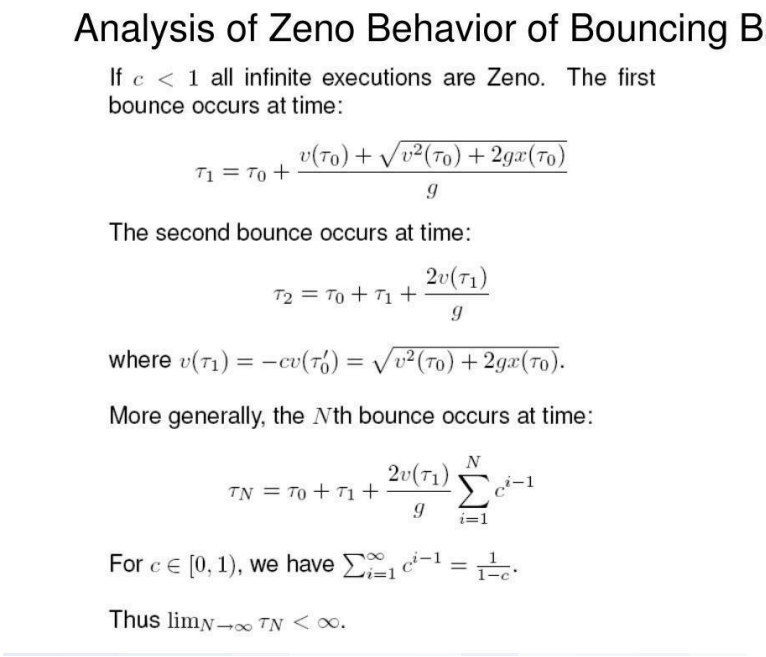
A rendszer azonban folyamatosan figyeli azokat a feltételeket, amelyek diszkrét eseményeket váltanak ki. Ezek a feltételek lehetnek a folytonos változók bizonyos küszöbértékei, külső bemenetek vagy időzítők. Amikor egy ilyen feltétel teljesül, *diszkrét esemény* következik be. Ennek hatására a rendszer egy átmenetet hajt végre: tipikusan egy *ugrás* történik a folytonos változókban (ez lehet értékük hirtelen megváltozása, vagy bizonyos változók újrainicializálása), és a rendszer diszkrét állapota

(üzemmódja) is megváltozik. Ezt nevezzük a rendszer *diszkrét fázisának*, bár ez a "fázis" többnyire nem rendelkezik időtartammal, hanem az átmenet egy pillanat alatt lezajlik.

Az átmenet után a rendszer belép egy újabb folytonos dinamikai szakaszba, immár az új diszkrét állapotnak megfelelő differenciálegyenletek mentén. Így a működés ciklikusan folytatódik: a rendszer folytonos változása újra és újra megszakadhat diszkrét eseményekkel, amelyek átstrukturálják a folytonos folyamatot (új differenciálegyenletek lépnek érvénybe, új kezdeti feltételekkel). Ezt az egész mechanizmust a hibrid automata szemléletesen ragadja meg: az állapotgép minden egyes *állapotában* más és más folytonos dinamikát ír elő, és *átmenetek* révén vált az állapotok között.



Fontos működési elv a Zénó-viselkedés lehetősége. Ez egy paradox helyzet a hibrid rendszerekben, amikor végtelen sok diszkrét esemény történik véges idő alatt. Ez a jelenség nevét Zénónak, az ókori görög filozófusnak a híres paradoxonjairól kapta. Ha egy hibrid rendszer tervezésekor nem figyelünk oda, előfordulhat, hogy bizonyos feltételek túl gyakran, akár *végtelenül gyakran* teljesülnek, így a rendszer diszkrét komponense szüntelenül váltogatná az állapotokat anélkül, hogy a folytonos rész érdemben haladna az időben. Az ilyen működés fizikailag megvalósíthatatlan, és elkerülése a tervezés során kritikus fontosságú. Egerstedt és társai (1999) munkája például foglalkozik az úgynevezett *Zénó-hibrid automaták* kérdésével, és megoldásokat kínál a probléma kezelésére. Ennek lényege, hogy korlátozzuk vagy megfelelően szabályozzuk az átmeneteket, biztosítva, hogy végtelen sok átmenet ne sűrűsödhessen egy időpillanatra. Erről a jelenségről és kezeléséről a későbbiekben – a kihívások között – még részletesen is szót ejtek.



3. A hibrid rendszerek alkalmazásai

3.1 Ipari alkalmazások

Az ipari automatizálás világa az egyik legtermékenyebb terület a hibrid rendszerek gyakorlati alkalmazására. Ebben az alfejezetben bemutatom, hogyan jelennek meg a hibrid rendszerek a modern gyárakban és üzemekben, illetve milyen konkrét előnyöket nyújtanak.

Egy tipikus modern gyártósor rendkívül összetett: gépek és robotok sora végzi a feladatokat, miközben szenzorok figyelik a folyamat minden lépését. A termelés hatékony irányítása folyamatos felügyeletet és beavatkozást igényel, hiszen a körülmények (például az alapanyag minősége, a gépek állapota vagy a termelési igény) bármikor változhatnak. Itt kerülnek képbe a *hibrid rendszerek*: a gyártósor vezérlőrendszere egyszerre dolgozik folyamatos és diszkrét módon.

A folytonos oldal például a gépek működési paramétereit szabályozza – ilyen a motorok sebessége, hőmérséklete, a szállítószalagok mozgása stb. –, mindezt differenciálegyenletekkel leírható szabályozó algoritmusok segítségével. A diszkrét oldal ezzel párhuzamosan eseményeket figyel: mikor kell egy új munkadarabot a szalagra helyezni, egy adott művelet (pl. hegesztés vagy festés) befejeződött-e, el kell-e dobni egy selejtes terméket, vagy meg kell-e állítani a gépet karbantartás miatt. Ezek az események diszkrét logikát igényelnek (pl. *ha* a szenzor szerint nincs alapanyag, *akkor* állítsd le a gépet).

Az ipari alkalmazásokban a hibrid rendszerek használata hozzájárul az üzemek hatékonyabb működéséhez. A *gyártási folyamatok optimalizálása* sokszor azon múlik, milyen gyorsan és okosan tud egy rendszer alkalmazkodni a változásokhoz. A hibrid rendszer jellegéből adódóan képes például

csökkenteni az energiaköltségeket (folyamatosan szabályozva a gépek teljesítményét a szükséges minimumra), növelni a megbízhatóságot (a diszkrét felügyelet révén hamarabb észlelhető és kezelhető egy rendellenesség), valamint támogatni a *karbantartási ciklusok előrejelzését* (a folytonos adatok elemzésével időben jelezhető, ha egy gép hamarosan meghibásodhat).

Egy konkrét példa: Képzeljünk el egy autógyár festőüzemét. A festőrobot karjának mozgása folyamatos vezérlést igényel a sima, egyenletes festékréteg felvitele érdekében – ez a folytonos rész. Ugyanakkor minden egyes karosszériát egy diszkrét folyamat keretében kell a festőállomáshoz juttatni, azonosítani, majd a festés végeztével továbbítani a szárítóba – ez a diszkrét logisztika. A hibrid rendszer gondoskodik arról, hogy a robot mozgása mindig optimális legyen *és közben* a szalag ütemezése is igazodjon a robot munkájához. Ha bárhol csúszás történik (például egy karosszéria nem érkezett meg időben), a diszkrét vezérlés késlelteti a következő folyamat indítását, míg a folytonos vezérlés a festőrobotot biztonságos állapotba hozza (pl. kiöblíti a fúvókákat, hogy ne száradjon be a festék).

3.2 Autonóm rendszerek és robotika

A robotika és az autonóm rendszerek szintén olyan terület, ahol a hibrid rendszerek alapvető fontosságúak. Egy robot vagy autonóm ügynök (például egy drón vagy önvezető jármű) *intelligens irányítása* lényegében hibrid feladat. Ennek oka, hogy a robot folyamatosan mozog és tevékenykedik a fizikai térben, ugyanakkor magas szintű döntéseket kell hoznia, amelyek diszkrét logikán alapulnak.

Vegyük példaként egy raktári logisztikai robotot, amelynek feladata árucikkek szállítása az egyik pontból a másikba. A robot folytonos része a mozgásvezérlés: kerekei folyamatosan forognak, motorjai gyorsítanak vagy lassítanak, a beépített szabályozó folyamatosan igazítja a sebességet és irányt, hogy a robot simán közlekedjen. Ugyanakkor a robotnak diszkrét döntéseket is kell hoznia: melyik útvonalon menjen, melyik polcról vegye le az árut, hogyan kerülje el az akadályokat vagy más robotokat, stb. Ezeket a döntéseket általában valamilyen logikai feltételrendszer vagy magas szintű algoritmus (például egy tervező algoritmus vagy mesterséges intelligencia) határozza meg.

A hibrid rendszer szemléletében a robot *állapotai* lehetnek például a különböző feladatok: "úton van az áruhoz", "felveszi az árut", "szállítja az árut a célhoz", "visszatér kiindulópontra". Minden ilyen állapotban a robot mozgását más és más folyamatos szabály halhatja meg (például amikor szállít, akkor a sebességére vonatkozó korlátok mások, mint üresjáratban). Az *átmenetek* pedig lehetnek az olyan események, mint "megérkezett a polchoz", "felvette az árut", "kiürült az akkumulátor 20%-ra" stb., amelyek diszkrét módon változtatják meg a robot *üzemmódját* vagy feladatát.

A robotikában a hibrid rendszerek biztosítják az alkalmazkodóképességet. Képzeljük el, hogy egy robot egyszerre több feladatot végez: szállít és közben folyamatosan szkenneli a környezetét új utasításokra. Amikor egy sürgős feladat érkezik (például *azonnal vigyen egy terméket a csomagoló állomásra*), a robot diszkrét vezérlője átállítja a prioritásokat (ez egy hirtelen esemény és

állapotváltás), míg a folytonos vezérlő rész gondoskodik arról, hogy a robot biztonságosan, de a lehető leggyorsabban új irányba induljon. Ez a zökkenőmentes váltás a feladatok között – a diszkrét logika által meghatározva, de a folytonos mozgás integritását megőrizve – a hibrid rendszer egyik legnagyobb előnye a robotikában.

3.3 Autonóm járművek

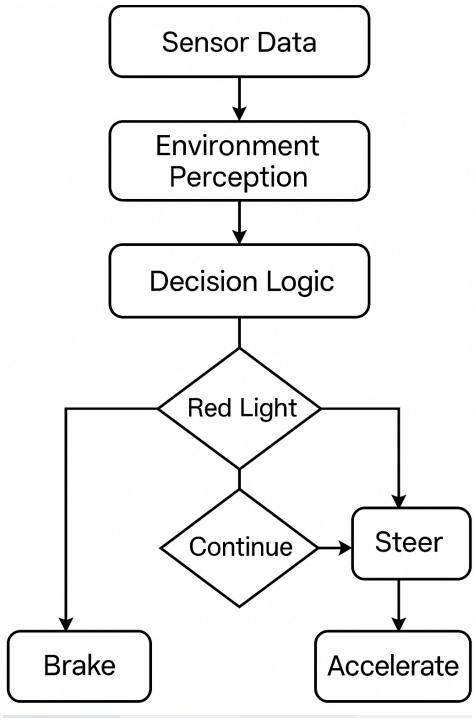
Az autonóm (önvezető) járművek a hibrid rendszerek talán legközismertebb és legizgalmasabb alkalmazási területét jelentik. Egy önvezető autóban, buszban vagy kamionban folyamatosan zajlik a környezet érzékelése és a jármű vezérlése, miközben egy sor diszkrét döntést is meg kell hozni a biztonságos közlekedés érdekében.

Az autonóm jármű folytonos alrendszere felel például a mozgásdinamikáért: a motor és a fékrendszer szabályozásáért, a kormányzás folytonos beállításáért, gyorsításért és lassításért. Mindezt összefüggő fizikai törvények írják le: differenciálegyenletek formájában modellezhető a jármű sebességének változása, a kanyarodáskor fellépő erők, vagy épp a féktávolság. Ezen a szinten a vezérlés feladata, hogy a jármű az adott pillanatban stabilan és kontrolláltan viselkedjen (ne csússzon meg, tartsa az ívet a kanyarban, maradjon a sávban stb.). A modern önvezető autókban számos érzékelő (kamerák, radarok, lidarok, GPS) ad folyamatos adatfolyamot a környezetről, melyet a jármű folyamatosan feldolgoz, hogy finomhangolja a menetstabilizáló rendszert, a sebességet és a kormányzást.

A diszkrét alrendszer ezzel párhuzamosan a magas szintű döntéshozatalért felelős. Ennek klasszikus példája a közlekedési lámpák kezelése: amikor a jármű egy lámpás kereszteződéshez közeledik, fel kell ismernie a lámpa színét és *döntést kell hoznia* (megállni vagy haladni). Maga a döntés diszkrét – hiszen az autó számára a lámpa zöld vagy piros (esetleg sárga, de az is kezelhető két állapot kombinációjaként) –, és a döntés eredménye is diszkrét: *folytatja az utat* vagy *megáll*. Ugyanakkor ennek a diszkrét döntésnek folytonos következménye van: ha meg kell állni, a fékrendszer folyamatosan növeli a fékerőt, hogy a jármű simán megálljon a vonal előtt. Itt szépen látszik a hibrid jelleg: a diszkrét esemény (piros lámpa) kivált egy állapotváltozást a vezérlési logikában (átmenet a "haladás" állapotból a "megállás" állapotba), ami új folyamatos dinamikai szabályozást aktivál (fékezés).

Az autonóm járművek hibrid rendszere rendkívül összetett, hiszen rengeteg lehetséges állapot és esemény van: útkereszteződés, előzés, akadály kikerülése, vészfékezés, parkolás stb., mind-mind külön diszkrét logikát igényel. Ehhez társul a jármű fizikai dinamikájának precíz kezelése, ami külön szakértelmet és kifinomult algoritmusokat követel. A hibrid rendszer abban segít, hogy ezt a komplexitást kezelhetőbb részekre bontsa, és garantálja, hogy a magas szintű döntések és az alacsony szintű szabályozások *összhangban legyenek*.

A valós idejű működés során a hibrid rendszer lehetővé teszi, hogy az autó minden pillanatban optimálisan cselekedjen: normál körülmények között simán haladjon az úton, de *pillanatok alatt* reagálni tudjon egy váratlan helyzetre (például egy elé ugró állatra vagy egy hirtelen fékező autóra). A diszkrét érzékelés (például az akadály észlelése) azonnal átállítja a vezérlést vészhelyzeti üzemmódba, miközben a folytonos vezérlés végrehajtja a lehető legintenzívebb még biztonságos manővert (fék+kikerülés, stb.). Az én értékelésem szerint ezek a képességek – melyeket a hibrid rendszer biztosít – jelentik az autonóm járművek biztonságos működésének alapját.



3.4 Orvosi alkalmazások

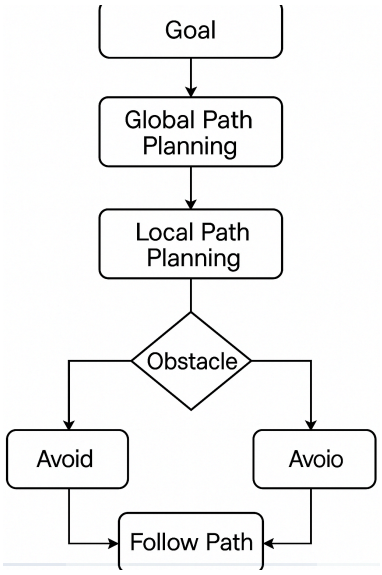
A gyógyászati és egészségügyi technológiák szintén egyre gyakrabban támaszkodnak hibrid rendszerekre. Az okos orvosi eszközök és távdiagnosztikai rendszerek területén a folytonos biológiai jelek és a diszkrét orvosi döntések kombinálása kulcsfontosságú. *Ebben az alfejezetben azt mutatom be*, miként alkalmazzák a hibrid rendszereket az egészségügyben, különösen az intelligens orvosi eszközökben és a telemedicina rendszerekben.

Intelligens orvosi eszközök: Ide tartoznak például az implantátumok, testre szerelhető szenzorok vagy terápiás eszközök (mint a pacemakerek, inzulinpumpák), amelyek folyamatosan figyelik a páciens fiziológiai adatait, és szükség esetén automatikusan beavatkoznak. Vegyük az inzulinpumpa példáját. A cukorbetegek számára kifejlesztett modern inzulinpumpák folyamatosan mérik a vércukorszintet – ez egy *folytonos adatfolyam*, melyet egy szenzor szolgáltat. Ezt az adatot a készülék minden pillanatban értékeli, ami egy folyamatosnak tekinthető szabályozási feladat: az inzulin adagolási

sebességének finomhangolása a mért glükózszint függvényében. Ugyanakkor diszkrét döntéseket is hoz a rendszer: például ha a vércukorszint túl magas, akkor egy *diszkrét esemény* aktiválódik (egy küszöbérték átlépése), és a pumpa egy adag inzulint bolus formájában bead a páciensnek. Hasonlóan, ha a vércukorszint veszélyesen alacsony, a pumpa megszakítja az adagolást.

Egy másik példa az okos pacemaker. A pacemaker folyamatosan figyeli a szív ritmusát (EKG jel) – folytonos jelenség –, és ha rendellenes ritmust észlel (például kihagy egy ütemet a szív, vagy fibrilláció kezdődik), diszkrét módon beavatkozik: egy elektromos impulzust ad le, hogy visszaállítsa a normál szívverést. Itt a hibrid rendszer lényege, hogy a készülék *folyamatosan monitoroz*, de eseményvezérelten avatkozik közbe. A pacemaker tervezőinek természetesen garantálniuk kell, hogy a készülék azonnal reagál a veszélyes ritmuszavarokra (ez diszkrét logika), ugyanakkor ne adjon le feleslegesen impulzust, amikor nincs rá szükség – ezt pedig a folytonos jel alapos elemzésével és megfelelő *küszöbértékek* megválasztásával érik el.

Távdiagnosztikai rendszerek: A modern egészségügyi ellátásban egyre fontosabb a *telemedicina*, vagyis a betegek távoli monitorozása és ellátása. Ennek tipikus példája, amikor egy beteg otthon hord egy érzékelő rendszert (vérnyomásmérő, EKG, véroxigénszint mérő stb.), és az adatok folyamatosan továbbítódnak egy központi rendszerbe. Ott egy szoftver elemzi a beérkező adatokat – a hibrid megközelítés itt is kulcsfontosságú. A szoftver folyamatosan értékeli a trendeket (például emelkedik-e folyamatosan a vérnyomás), de diszkrét riasztásokat generál, ha bizonyos értékek kritikus tartományba esnek (például *ha* a vérnyomás > 180 Hgmm, *akkor* riasztás az orvosnak). Ezen felül, sok telemedicina rendszer interaktív: ha a beteg állapotában hirtelen romlás van (diszkrét esemény), a rendszer automatikusan hívhat mentőt, vagy utasítja a pácienst egy cselekvésre (pl. vegyen be egy gyógyszert). Mindezt a *folyamatos adatelemzés* alapozza meg, hiszen a diszkrét döntések megalapozottságához folyamatos megfigyelés szükséges.



4. A hibrid rendszerek előnyei és kihívásai

4.1 Előnyök

A hibrid rendszerek alkalmazása számos kézzelfogható **előnyt** kínál a hagyományos, pusztán diszkrét vagy pusztán folytonos megoldásokkal szemben. Ezek az előnyök mind az ipari, mind a társadalmi-gazdasági területeken megmutatkoznak, és hozzájárulnak ahhoz, hogy a hibrid rendszerek egyre vonzóbbá váljanak a tervezők és döntéshozók számára. *Ebben az alfejezetben áttekintem a legfontosabb pozitívumokat*, amelyeket a hibrid rendszerek nyújtanak.

- Gyors és adaptív reagálóképesség: A hibrid rendszer egyik legnagyobb előnye a valós idejű alkalmazkodás képessége. Mivel a rendszer folyamatos komponense figyeli a környezet változásait, a diszkrét komponens pedig meghozza a szükséges döntéseket, a hibrid rendszer rendkívül gyorsan tud reagálni a váratlan eseményekre. Például egy hibrid vezérlésű autonóm drón azonnal érzékeli a szélirány változását (folytonos rész) és korrigálja a pályáját, ugyanakkor az akadályfelismerő algoritmusa észlel egy hirtelen elé kerülő madarat (diszkrét esemény) és kikerüli azt. E két szint együttes működése biztosítja, hogy a rendszer minden pillanatban a lehető legjobb választ adja a környezeti kihívásokra.

- Integrált optimalizáció: A hibrid rendszerek lehetővé teszik a folyamatok holisztikus optimalizációját. Egy ipari gyártósor esetében például nemcsak az egyes gépek működése optimalizálható (folyamatos paraméterek), hanem a teljes gyártási logisztika is (diszkrét ütemezés). A két szint összehangolásával elérhető, hogy a rendszer egészének teljesítménye jobb legyen, mintha a részeit külön-külön optimalizálnánk. Az energiahatékonyság terén is megmutatkozik ez: a hibrid rendszer folyamatosan szabályozza az energiafelhasználást, és diszkrét eseményekkel – például ideiglenes leállásokkal, készenléti módokkal – csökkenti a felesleges fogyasztást. Ennek eredményeként jelentős erőforrás-megtakarítás érhető el úgy, hogy közben a rendszer hatékonysága nem csökken, sőt javul.

- Rugalmas tervezés és bővíthetőség: A hibrid rendszerek modellt adnak a komplex rendszerek moduláris tervezéséhez. Külön lehet fejleszteni a folytonos szabályozókat (szakemberek optimalizálják a PID paramétereket, vagy a differenciálegyenlet-alapú szabályozókat), és külön a diszkrét vezérlő logikát (szoftverfejlesztők és mérnökök megírják az állapotgépet, vagy az AI modulokat). A hibrid keret integrálja e kettőt, így a végeredmény könnyebben bővíthető vagy módosítható. Ha például egy gyárban egy újabb gépet akarunk a termelésbe illeszteni, elég a hibrid rendszer diszkrét részét kibővíteni egy új állapottal/átmenettel, illetve a folytonos részhez hozzáadni az új gép modelljét. Nem kell az egész rendszert újratervezni – a hibrid architektúra lehetővé teszi a moduláris bővítést. Ez az előny nagy rendszerek esetében

különösen jelentős, hiszen a skálázhatóság kulcsfontosságú: a jövő gyárai, városai vagy hálózatai folyamatosan nőnek és változnak, így az őket vezérlő rendszereknek is könnyen alkalmazkodniuk kell.

4.2 Kihívások és problémák

Bár a hibrid rendszerek rendkívül ígéretesek és hasznosak, a megvalósításuk és alkalmazásuk során komoly kihívásokkal kell szembenézni. *Ebben az alfejezetben áttekintem a legfontosabb problématerületeket*, amelyek gátolhatják vagy nehezíthetik a hibrid rendszerek használatát, és amelyek megoldására a kutatóknak és mérnököknek különös figyelmet kell fordítaniuk.

- Rendszerkomplexitás**:** Az egyik legnyilvánvalóbb kihívás a hibrid rendszerek rendkívüli bonyolultsága. Mivel egyszerre tartalmaznak folytonos és diszkrét részeket, a lehetséges állapotkombinációk száma és a viselkedés variációi robbanásszerűen növekednek a tisztán folytonos vagy diszkrét rendszerekhez képest. Egy viszonylag egyszerű hibrid automata is sok állapot-átmenet párral rendelkezhet, a folytonos dinamikák pedig magas dimenziós differenciálegyenletekkel írhatók le. Ez a komplexitás megnehezíti a tervezést és az átláthatóságot. Gyakran előfordul, hogy emberi ésszel szinte lehetetlen minden lehetséges esetet átgondolni. A tervezőknek nagyon rendszerben kell gondolkodniuk, és még így is fennáll a veszélye, hogy egy-egy ritka eseménykombinációra nem készül fel a rendszer. Ezért kellenek fejlett tervezési módszerek és szimulációs eszközök, hogy segítsék a komplex hibrid rendszerek megértését és ellenőrzését.

- Formális verifikáció és biztonság: Ahogy növekszik egy hibrid rendszer komplexitása, úgy válik egyre fontosabbá a formális ellenőrzés. Különösen kritikus alkalmazásoknál – mint amilyen az önvezető autók, orvosi eszközök, repülőgépek vezérlése – elvárás, hogy bizonyítani tudjuk: a rendszer biztonságos és bizonyos rossz dolgok *nem történhetnek meg*. A hibrid rendszerek formális verifikációja azonban nagyon nehéz feladat. A diszkrét rendszerek ellenőrzésére kidolgozott algoritmusok (mint a modellellenőrzés) és a folytonos rendszerek stabilitási analízisei jól beváltak külön-külön, de kombinációjuk – a hibrid rendszerek verifikációja – *nagy számítási erőforrást* igényel, gyakran *nem is dönthető el* egyes általános tulajdonságokra. Az ún. *állapottér-robbanás* jelenség itt hatványozottan jelentkezik. Emiatt a kutatók sokszor csak bizonyos korlátozásokkal (például lineáris dinamikára, vagy erősen egyszerűsített diszkrét logikára) tudnak garantált eredményeket felmutatni. Ez azt jelenti, hogy egy bonyolultabb hibrid rendszernél a biztonsági garanciák kinyerése még nyitott probléma lehet. Én magam is azt tapasztaltam az irodalom áttekintése során, hogy például egy önvezető autó teljes modelljének formális bizonyítása ma még gyakorlatilag lehetetlen – a megközelítés inkább az, hogy részegységekre bontva (szenzorfúzió, követő automaták stb.) próbálnak helyes működést igazolni.

- Zénó-paradoxon: Korábban már említettem a Zénó-viselkedést mint a hibrid rendszerek egy sajátos problémáját. Ez extrém esetben a rendszer lelkét érintő kihívás: ha egy tervező figyelmetlenül definiálja a diszkrét átmenetek feltételeit, a rendszer *végtelen ciklusba* ragadhat véges idő alatt. Például képzeljünk el egy olyan szabályozót, amely minden időtartam felénél beavatkozik (diszkrét eseményként). Ha ezt naivan engedjük, akkor 1 másodperc alatt végtelen sok esemény történne: 0.5 s-nél, 0.75 s-nél, 0.875 s-nél stb. A fizikai rendszer persze nem tud végtelenszer beavatkozni, így ez elvi paradoxon.

- Implementáció és időzítés: Egy dolog egy hibrid rendszert papíron vagy számítógépen megtervezni, és egy másik dolog azt ténylegesen implementálni egy hardver-szoftver környezetben. A diszkrét vezérlő általában számítógépen futó program formájában jelenik meg, míg a folytonos vezérlés fizikai eszközökkel (pl. analóg elektronikával, vagy gyors digitális vezérlőhurkokkal) valósul meg. A kettő közötti időzítés kritikus: ha a számítógép túl lassan reagál (pl. a szoftveres döntés késik, mert mással van elfoglalva), akkor a folytonos folyamat addigra esetleg eltér a kívánt pályától. Tehát a *valósidejű rendszertervezés* egy komoly kihívás. Gondoskodni kell arról, hogy a diszkrét döntések ne csak logikailag legyenek helyesek, hanem időben is érkezzenek. Ehhez gyakran valós idejű operációs rendszereket, prioritásokat és megszakításokat kell használni, ami a szoftverfejlesztést bonyolítja. Ráadásul a szinkronizáció is probléma: ha több párhuzamos hibrid folyamat fut (pl. egy okos városban több alrendszer), akkor össze kell hangolni őket, nehogy konfliktus alakuljon ki (pl. egy közlekedési lámpa rendszere és egy önvezető autó rendszere között). Az időzítési és implementációs problémák tehát további nehézségi réteget adnak a hibrid rendszereknek.

- Emberi tényező és átláthatóság: Végül, de nem utolsósorban, a hibrid rendszerek emberi felügyelete és megértése is kihívást jelent. Egy operátor vagy mérnök számára nehéz lehet átlátni egy hibrid rendszer pillanatnyi állapotát, mert összetett (hiszen tudnia kell, épp melyik diszkrét állapotban vagyunk és hogy a folytonos paraméterek mit csinálnak). Vészhelyzetben egy ilyen rendszert manuálisan irányítani vagy beavatkozni nem egyszerű. Emellett az is kihívás, hogy a tervezők hogyan *kommunikálják* a hibrid rendszer viselkedését a nem szakértő felhasználóknak. Például egy orvos, aki használ egy hibrid rendszeren alapuló diagnosztikai eszközt, szeretné érteni, hogy a gép miért adott egy bizonyos riasztást – de a mögöttes logika lehet, hogy túl komplex, így nehéz magyarázatot adni rá. Ez az *átláthatósági probléma* a megbízhatóság szempontjából is gond, mert ha a felhasználó nem bízik a feketedoboz-szerű hibrid rendszerben, akkor vonakodhat rá bízni kritikus döntéseket.

5. Alkalmazott matematikai modellezés és algoritmusok

5.1 Hibrid automáták

A hibrid automaták modellezéséhez használt matematikai háttér alapvetően két részre oszlik: az állapotgépre és a differenciálegyenletekre. Az állapotgép diszkrét változása a rendszerben fellépő eseményeket és az ezek következményeként kialakuló állapotokat írja le. A különböző állapotok között átmenetek vannak, amelyek valamilyen diszkrét események hatására történnek. A folytonos dinamika ezen kívül leírja az egyes állapotok közötti változásokat a differenciálegyenletek segítségével. Az ilyen típusú automaták komplex viselkedése segíthet például az autonóm rendszerek irányításában, a robotikában, illetve a közlekedési irányításban.

A hibrid automata használata során felmerül a modell hűségének kérdése is: mennyire pontosan tükrözi a valós rendszer viselkedését. Ez a modellező és a mérnök szakértelmén múlik. Jó modellezési gyakorlat például, hogy a modellt ne bonyolítsuk túl (ne legyen feleslegesen sok állapot, átmenet), de a lényeges jelenségeket tartalmazza. Ebben kompromisszumot kell találni. Néha érdemes absztrahálni a folytonos részt (pl. lineárisítani a differenciálegyenleteket, ha az úgy is elég pontos), hogy a diszkrét-logikai elemzés könnyebb legyen. Máskor pedig a diszkrét rész egyszerűsítése (pl. átmenetek összevonása) segíthet.

5.2 Modellezési technikák és módszerek

A hibrid rendszerek modellezése nem merül ki abban, hogy felírunk egy hibrid automatát – sok esetben további technikákra és módszerekre van szükség, hogy a modell hasznos és kezelhető legyen. *Ebben az alfejezetben* áttekintem, milyen speciális modellezési módszerek segítik a hibrid rendszerek tervezőit és elemzőit.

- Szimuláció és szintetikus vizsgálatok: Mielőtt egy hibrid rendszert tényleges hardveren vagy valós környezetben kipróbálnánk, általában számítógépes szimulációkat végzünk. A *szintetikus modellezés* során a rendszer egyes részeit virtuálisan helyettesítjük, és megnézzük, hogyan viselkedik a modell különböző szituációkban. Például egy autonóm autó vezérlő algoritmusát először számítógépen tesztelik úgy, hogy a környezet (forgalom, gyalogosok, útviszonyok) szimulálva van. Ez a modell alapú tesztelés lehetővé teszi a rendszer viselkedésének előrejelzését és finomhangolását anélkül, hogy veszélybe sodornánk bármit is a valóságban. A hibrid rendszerek esetén a szimuláció kihívás, mert biztosítani kell a *diszkrét események pontos detektálását* a folytonos integráció közben. A legtöbb szimulációs környezetben ezt úgy oldják meg, hogy nagyon kicsi időlépésekkel (adaptív lépésközökkel) integrálnak, és ha egy őrfeltétel változtatja a jelét, akkor beavatkoznak a szimuláció menetébe (leállítják a folyamatos integrátort és végrehajtják a diszkrét lépést).

- Szimbolikus és analitikus módszerek: Bizonyos esetekben nem elegendő a numerikus szimuláció, hanem szimbolikus elemzésre van szükség. Például a *reachability analysis* során – amint említettem – azt szeretnénk tudni, hogy elérhető-e egy bizonyos rossz állapot. Erre vannak algoritmusok, amelyek megpróbálják kiszámítani az összes elérhető állapotok halmazát. Folytonos rendszernél ez tipikusan differenciálegyenletek integrálásával és matematikai transzformációkkal történik; diszkrét rendszernél gráf bejárással. Hibrid rendszereknél a kettőt ötvözni kell: olyan algoritmusok léteznek, amelyek felváltva kezelik a differenciálegyenletek megoldását és a diszkrét ugrásokat, gyakran *absztrakciókat* alkalmazva. Egy tipikus módszer a folytonos állapotterek rácshálózata vagy intervallumokra bontása, ami által végesítik a problémát (ami persze közelítéshez vezet).

- Hierarchikus és moduláris modellezés: Gyakori, hogy egy hibrid rendszer túl bonyolult egyetlen lapos modellként. Ilyenkor alkalmaznak hierarchikus modellezést, ahol a rendszer több szintre van bontva. Például lehet egy felső szintű hibrid automata, ami nagy vonalakban szabályozza a részegységek kapcsolatát, és minden egyes részegység maga is egy kisebb hibrid automata. A moduláris felépítés segít abban, hogy *lokalizáljuk* a vizsgálatot: egy modult külön is tudjunk elemezni, majd a modulok interfészeit definiálva az egész rendszert össze lehessen rakni. A moduláris modellezésnél fontos a komponensek közötti kommunikáció leírása. Gyakran használunk esemény-szinkronizációt (két modul egyszerre lép diszkrét átmenetet valamilyen jelzés hatására), vagy megosztott folytonos változókat (pl. két alrendszer ugyanazt a hőmérsékletet érzékeli). Az ilyen modellezési sémák standardizált nyelvekhez vezetnek, mint pl. a *Hybrid CSP* (Communicating Sequential Processes kiterjesztése hibridre), vagy a *Hybrid Petri-háló*, amelyek a moduláris és párhuzamos működést támogatják.

5.3 Az algoritmusok szerepe

Miután megvan a hibrid rendszer modellje – például egy hibrid automata formájában –, a következő kérdés, hogy hogyan vezéreljük vagy elemezzük a rendszert hatékonyan. Itt lépnek be a különféle algoritmusok, amelyek a hibrid modellekre épülve segítenek döntéseket hozni vagy ellenőrzéseket végezni.

- Optimális vezérlés (Optimal Control): A hibrid rendszerek vezérlésére gyakran célfüggvények minimalizálásával keresünk megoldást. Például minimalizálni akarjuk az energiafelhasználást, a végrehajtási időt, vagy a költségeket. Az *optimális vezérlés* elmélete adja meg ennek kereteit. Egy hibrid rendszer esetén ez különösen kihívásos, mert a diszkrét döntéseket is bele kell venni az optimalizálásba. Az algoritmusok gyakran a Mixed Integer Programming (MIP) területéről kerülnek ki: például a hibrid rendszer viselkedése leírható egy vegyes egészértékű lineáris programmal bizonyos közelítések mellett, és azt oldják meg integer programming algoritmusokkal. Egy másik megközelítés a *Dynamic Programming*, ami rekurzívan keresi

meg a legjobb döntéssorozatot, de ez a hibrid természet miatt könnyen robbanthat a keresési térben.

- Valós idejű döntési algoritmusok: Amikor a hibrid rendszer működik, valós időben kell futnia olyan algoritmusoknak, amelyek figyelik az eseményeket és döntenek. Ezek az algoritmusok a diszkrét vezérlő szoftver moduljai. Meg kell felelniük a valós idejű követelményeknek, azaz garantálni kell, hogy bizonyos határidőn belül választ adnak. Itt jönnek képbe az olyan algoritmikus megoldások, mint a *ütemezési algoritmusok* (scheduling), amelyek biztosítják, hogy a kritikus feladatok (pl. eseménykezelők) mindig időben lefussanak. Egy hibrid rendszer diszkrét vezérlője például lehet egy állapotgépként megírt program, ahol minden ciklusban érzékeljük a folytonos változókat és ellenőrizzük az őrfeltételeket.
- Gépi tanulás és adaptív algoritmusok: Újabban egyre nagyobb szerepet kap a gépi tanulás a hibrid rendszerekben is. Olyan algoritmusokról van szó, amelyek képesek *tanulni a folyamatos adatokból*, és ennek alapján *diszkrét döntéseket* javítani. Például egy hibrid rendszer adaptívan módosíthatja a vezérlési szabályait egy tanuló algoritmus segítségével: reinforcement learning (megerősítéses tanulás) algoritmusok megtanulhatják, hogy bizonyos állapotokban milyen diszkrét akció vezet a legjobb eredményre. A kihívás itt az, hogy a tanulás általában folyamatos paraméterekre van kitalálva, de a hibrid rendszerekben diszkrét struktúra is van, ami nem feltétlen deriválható vagy finomhangolható kicsi lépésekkel. Vannak kutatások a hibrid neurális hálózatok irányában, ahol a neurális modellt ellátják diszkrét komponensekkel, vagy ellenkezőleg, a diszkrét vezérlést "becsomagolják" egy differenciálható approximációba, hogy a gépi tanulás alkalmazható legyen. Az ilyen algoritmusok ígérete, hogy a rendszer idővel egyre jobban teljesít majd anélkül, hogy kézzel hangolnánk.
- Verifikációs algoritmusok: Az előző alfejezetben szó esett arról, hogy a hibrid rendszerek biztonságának ellenőrzése nehéz. Erre speciális algoritmusok vannak kifejlesztve, amelyek bizonyos korlátok közt mégis képesek átfogó elemzést nyújtani. Például a reachability analysis algoritmusai, amik lehetnek:
    - *Grid-based algoritmusok:* felosztják a folytonos teret kis cellákra és nyomon követik, mely cellák érhetők el. Ez explicit, de nagyon finom rács esetén robban.
    - *Flow-pipe approximation:* differenciálegyenletek megoldásakor ún. "folyamatcsövet" (flow pipe) számolnak, ami a lehetséges értékek burkát adja egy időintervallumon. Ez geometriai objektumok (pl. politope-ok, ellipszoidok) számításával jár.
    - *Monte Carlo szimulációs algoritmusok:* sok-sok random szimuláció futtatása, hogy *empirikusan* keressen hibákat. Nem ad teljes garanciát, de ha sok futásból sem látunk

hibát, növeli a bizalmat. Ezt kombinálhatják falszifikációs algoritmusokkal, amelyek kifejezetten a rossz eseteket próbálják becserkészni valamilyen heurisztika alapján.

- *SMT-solver alapú algoritmusok:* A Satisfiability Modulo Theories (SMT) eszközöket kiterjesztik hibrid logikára, ahol egy formula kiértékelhetősége egy adott hibrid rendszerben egyenértékű egy rossz rendszerpálya létezésével. Ha az SMT-solver talál megoldást, az egy ellenpéldány, ha nem, akkor bizonyította a tulajdonságot.

6. A hibrid rendszerek kutatásának jövőbeli irányai

6.1 Mesterséges intelligencia és gépi tanulás

A hibrid rendszerek és a mesterséges intelligencia (MI) konvergenciája az egyik legizgalmasabb *jövőbeli kutatási irány*. Ahogy a technológia fejlődik, egyre több rendszerbe integrálják a gépi tanulást és az MI-t, hogy azok intelligensebbé és önadaptívvá váljanak. *Ebben az alfejezetben* azt tekintem át, miként segítheti a mesterséges intelligencia a hibrid rendszerek fejlődését, és milyen kutatási kihívások merülnek fel ezen a területen.

Adaptív vezérlés gépi tanulással: Hibrid rendszerek esetében a vezérlési szabályokat (különösen a diszkrét döntéseket) hagyományosan ember tervezte logika alapján határozzák meg. A jövőben várhatóan egyre inkább bevonjuk a *gépi tanulást*, hogy maga a rendszer tanulja meg, milyen döntéseket kell hoznia adott helyzetekben. A *megerősítéses tanulás (Reinforcement Learning, RL)* ígéretes megoldás itt: a hibrid rendszer kap egy célfüggvényt (jutalomfunkciót), és próbálja kitapasztalni, mely diszkrét akciók a legjobbak hosszú távon. Például egy intelligens forgalomirányító rendszer (közlekedési lámpák hálózata) – ami tipikus hibrid rendszer – RL segítségével megtanulhatja optimalizálni a lámpák váltását a forgalmi minták alapján, csökkentve a dugókat és várakozási időket. Az ilyen integráció már jelenleg is kutatás tárgya, de a jövőben kiforrottabb lesz. Egyik nagy kihívás, hogy a RL algoritmusok sok kísérletet igényelnek (ami valós közlekedésben nem elfogadható), ezért *szimulációban* tanítják a rendszert, majd a megtanult politikát ültetik át a valóságba. Fontos kutatási kérdés, hogyan garantálható, hogy a megtanult döntéshozó modul *biztonságos* marad és extrém helyzetekben is megfelelően működik majd.

Hibrid rendszerek és neurális hálók kombinációja: Egy másik trend a *neurális háló alapú komponensek* bevonása a hibrid rendszerekbe. Például a folytonos szabályozót (vagy annak egy részét) le lehet cserélni egy neurális hálóra, amely megtanulja a kívánt vezérlési viselkedést. Ez a *neuromorf szabályozás* rugalmasságot adhat, mert a neurális háló képes bonyolult nemlineáris folytonos leképezéseket is megvalósítani, amiket hagyományos szabályozókkal nehéz lenne hangolni. Diszkrét oldalon pedig használhatunk neurális hálókat a környezet felismerésére (pl. képfeldolgozás a szenzoroktól) és az alapján kiválthatunk diszkrét eseményeket. Ilyenkor a hibrid rendszer modellje is

kibővül: a guard feltétel például lehet egy neurális háló kimenete (pl. egy kamera képe alapján a háló eldönti, van-e gyalogos az úton; ennek kimenete igaz/hamis lesz, mint guard).

Önfejlesztő hibrid rendszerek: Az MI bevonásával a hibrid rendszerek önfejlesztővé válhatnak. Képzeljünk el egy okos gyárat, ahol a vezérlőrendszer a termelési adatok alapján folyamatosan javítja önmagát: újraszervezi a logisztikát, átállít bizonyos paramétereket, vagy akár javaslatot tesz új gépek bevonására. Ehhez komplex MI-rendszerek futnak a háttérben (big data elemzés, prediktív modellek, stb.), amelyek inputja a rengeteg folytonos szenzoradat és diszkrét eseménytörténet. A hibrid rendszer itt nem zárt, hanem nyílt: kétirányú kapcsolat van a rendszer és a tanuló modul között. A jövő kutatása, hogy hogyan garantáljuk az ilyen önfejlesztő rendszerek stabilitását. Ne történhessen meg, hogy a rendszer "túltanul" valamit és emiatt egy ritka eseménynél rosszul reagál. Itt lép be az *ember a hurokban* szemlélet: valószínű, hogy a jövő hibrid rendszerei úgy fognak MI-t használni, hogy a kritikus döntéseknél az emberi felügyelő is kap egy figyelmeztetést vagy beleszólási lehetőséget.

Hibrid rendszerek tervezése MI segítségével: Nem csak a működés közben, de már a *tervezés fázisában* is segíthet az MI. Például gépi tanulást alkalmazhatunk arra, hogy a hibrid modell paramétereit azonosítsuk egy adatgyűjtési fázisban (model identification). Vagy genetikus algoritmusokat használhatunk a hibrid automata átmeneteinek optimalizálására. A jövőben elképzelhető, hogy a mérnök nagy vonalakban megadja, mit szeretne (pl. "ez egy robotika rendszer 3 állapottal: halad, kerül, megáll"), és egy MI-alapú tervezőeszköz *magától kitölti a részleteket*, megtanulja a legjobb differenciálegyenlet paramétereket és guard feltételeket példák alapján. Ez radikálisan lerövidítheti a fejlesztési ciklust. A kihívás itt is a megbízhatóság: bízhatunk-e egy automatikusan generált modellben? Ezen a téren a "machine learning for systems engineering" egy új terület, ami bizonyosan fejlődni fog.

6.2 Fenntarthatóság és zöld technológia

A fenntarthatóság és a környezettudatosság napjaink egyik legfontosabb globális célkitűzése. A technológiai fejlesztések terén is egyre nagyobb hangsúlyt kap, hogy az új rendszerek energiahatékonyak, környezetbarátok és fenntarthatóak legyenek.

Energiaoptimalizálás hibrid rendszerekkel: Számos iparágban – legyen szó gyártásról, közlekedésről vagy épületüzemeltetésről – a hibrid rendszerek alkalmazása lehetővé teszi a finomhangolt energiafelhasználást. Mint arról már esett szó, a hibrid vezérlés képes valós időben reagálni a terhelésváltozásokra, így ott és akkor használ energiát, ahol és amikor arra szükség van. A jövőbeni fejlesztésekben a cél az, hogy a hibrid rendszerek még intelligensebben integrálják a *megújuló energiaforrásokat*. Például egy okos elektromos hálózat hibrid vezérlője dönthet úgy, hogy amikor süt a nap, a napelemekről táplálja a rendszert (diszkrét döntés: átkapcsolni a forrásokat), és a folytonos szabályozó pedig finomítja, mennyi többletenergiát tároljunk akkumulátorokban. Amikor csökken a termelés, automatikusan visszaveszi a fogyasztást vagy más forráshoz nyúl. Ezzel minimalizálható a

fosszilis energiahordozók használata. A fenntarthatósági szempont tehát erősíti a hibrid rendszerek szerepét az energiamenedzsmentben. Várható, hogy a *szél- és napenergia farmok* vezérlése is egyre inkább hibrid algoritmusokra épül majd, melyek figyelembe veszik a természeti források fluktuáló jellegét (folytonos rész) és a hálózati igények diszkrét eseményeit (pl. hirtelen fogyasztói igényugrás).

Okos városok és közlekedés: A fenntartható városi környezet kulcsa az okos infrastruktúra, amely hatékonyan használja az erőforrásokat. A hibrid rendszerek már ma is jelen vannak az okos közlekedési lámpa rendszerekben és a tömegközlekedés vezérlésében. A jövőben ez tovább erősödik: egy *okos város* energiahálózata, közlekedése, vízellátása, hulladékkezelése mind hibrid rendszerekként fognak együttműködni. Például egy város vízellátó rendszere: folyamatosan figyeli a tartályok szintjét, a nyomást (folytonos változók), és diszkrét események alapján dönt, mikor kapcsoljanak be a szivattyúk vagy nyissanak/zárjanak szelepeket. Az optimalizálás célja nem csak a biztonságos ellátás, de a minimális energiapazarlás és szivárgás. Ugyanez igaz a közlekedési rendszerekre: a hibrid vezérlés segíthet csökkenteni a dugókat (és így a légszennyezést), összehangolni a tömegközlekedést az egyéni közlekedéssel, mindezt valós időben a forgalmi adatok alapján.

Ipar 4.0 és zöld gyárak: Az ipari termelésnek is fenntarthatóbbá kell válnia. A zöld gyár koncepció lényege, hogy minimális hulladékkal, újrahasznosított anyagokkal, és energiatakarékos módon termeljen. A hibrid rendszerek itt is segíthetnek: például egy gyár hibrid rendszere valós időben optimalizálhatja a gépek üzemidejét úgy, hogy a csúcsidőn kívül egyes gépek kikapcsolnak (diszkrét állapot: standby), csökkentve ezzel az energiafogyasztást. Ha a megrendelések száma csökken, a rendszer automatikusan átütemezheti a termelést úgy, hogy egy-egy gyártósor teljesen leálljon ideiglenesen (energiatakarékossági mód), míg a többin folytatódik a munka. Amint a kereslet nő, a rendszer újra aktiválja a pihenő sorokat. Ezt a diszkrét döntéshozatalt a folyamatos monitorozás támogatja, figyelve a raktárkészletet, gépek állapotát stb. Az Ipar 4.0 keretében a gyárak ilyen *önoptimalizáló* képessége a fenntarthatóság egyik alappillére lesz, és ebben a hibrid rendszerek nyújtanak megfelelő keretet.

Fenntarthatóság a kutatásban: Maga a hibrid rendszerek kutatása is reagál a fenntarthatóság témájára. Egyre több kutatás foglalkozik például *multi-objective optimalizálással*, ahol a gazdasági cél mellett környezeti cél is szerepel. Továbbá, a fenntarthatóság megköveteli a szakterületek együttműködését: a mérnököknek együtt kell dolgozniuk környezettudósokkal, közgazdászokkal, hogy a hibrid rendszerek valóban fenntarthatóak legyenek. Ez újfajta kutatási hálózatokat hoz létre, pl. okos városok kutatási programjai, ahol az informatika, a környezetvédelem és a társadalomtudomány is jelen van. A hibrid rendszerek, mint integráló keret, természetes módon illeszkednek ebbe a multidiszciplináris párbeszédbe, hiszen ők is integrálják a különböző jellegű folyamatokat.

6.3 Elméleti alapok fejlesztése

Míg a korábbi alfejezetek inkább az alkalmazási és technológiai irányokra fókuszáltak, legalább ilyen fontos a hibrid rendszerek elméleti alapjainak továbbfejlesztése. Ahhoz, hogy a gyakorlati előrelépéseket megalapozzuk és biztonságos, kiszámítható rendszereket építhessünk, az elméleti kihívások megoldása is elsőrendű feladat.

Zénó-jelenség és rendszerstabilitás: Korábban már többször említettem a Zénó-paradoxont, mint specifikus problémát. Ez a jelenség valójában a rendszer *stabilitásának és működőképességének* kérdéséhez kapcsolódik. Az elméleti kutatás célja, hogy általános kritériumokat adjon, amelyek megmondják, egy adott hibrid rendszer modellről, hogy tartalmazhat-e Zénó-viselkedést vagy sem. Ezenfelül, hogy ha tartalmazhat, milyen átalakításokkal (regularizációkkal) tehető *Zénó-mentessé*. Például olyan tételek kidolgozása folyik, amelyek bizonyos feltételek (mint a *progresszív időfeltételek* minden hurkon) mellett garantálják a Zénó elkerülését. Hasonlóképpen, a stabilitáselmélet is bővül: a klasszikus Lyapunov-stabilitás fogalma kiterjesztése hibrid rendszerekre (ún. *Lyapunov-függvények* diszkrét- és folytonos állapotváltozókkal) egy aktív kutatási terület. A jövőben várható, hogy összeáll egy egységes stabilitáselmélet, amely segít a mérnököknek már a tervezéskor eldönteni, hogy a hibrid rendszerük stabil lesz-e minden körülmények között, és nem fog "megőrülni".

Verifikációs módszerek fejlesztése: Bár a gyakorlati alkalmazások egyre többek, a *formális verifikáció* lépést tart velük: az elméleti ...fejlesztése: Bár a gyakorlati alkalmazások egyre gyarapodnak, a *formális verifikáció* terén is lépést kell tartani a komplexitással. Az elméleti kutatások célja olyan hatékony algoritmusok és eszközök fejlesztése, amelyek képesek nagyobb és összetettebb hibrid rendszerek tulajdonságait is ellenőrizni. A jövőben várható, hogy a verifikációs módszerek integrálják a gépi tanulást is (például tanulás útján szűkítik a keresési teret, vagy ismernek fel bizonyos viselkedésmintákat), illetve párhuzamosítják a számításokat a modern sokmagos vagy felhő infrastruktúrák kihasználására. Emellett a szükséges és elégséges feltételek kutatása is fontos: azaz megtalálni azokat a pontos kritériumokat, amelyek garantálják egy adott tulajdonság fennállását. Például milyen feltételek mellett invazív beavatkozás nélkül garantálható, hogy egy hibrid rendszer sosem lép tiltott állapotba? Ilyen tételek segítenék a mérnököket a biztonságkritikus rendszerek tervezésében.

Új matematikai keretrendszerek: Lehetséges, hogy a klasszikus hibrid automata formalizmus sem marad örökre változatlan. Az elméleti fejlesztés irányai közé tartozik új, kibővített modellek kidolgozása, amelyek jobban leírnak bizonyos jelenségeket. Például a *stochasztikus hibrid rendszerek* területe azt vizsgálja, hogyan lehet a véletlenszerűséget is bevonni a modellbe (pl. érzékelési zaj, vagy bizonytalan események). Ennek elméleti alapjai jelenleg is formálódnak, de a jövőben ezek az alapok szilárdabbak lesznek, és így a valós rendszerek bizonytalanságait is integrálni lehet a tervezésbe. Hasonlóan, a *hálózatba kapcsolt hibrid rendszerek* (networked hybrid systems) elmélete is fejlődik:

hogyan tudunk formális eredményeket adni olyan rendszerekre, amelyek sok hibrid alrendszer laza csatolásával jönnek létre (mint egy okos város alrendszerei). Itt olyan fogalmakra lesz szükség, mint a hierarchikus verifikáció vagy a kompozicionális modellellenőrzés, melyek lehetővé teszik, hogy a részegységek helyességéből következtessünk az egész rendszer helyességére.

Számítástudományi hatékonyság: Az elméleti alapok fejlesztéséhez tartozik a számítási bonyolultság kérdése is. Sok hibrid rendszerekkel kapcsolatos probléma elméletileg *NP-nehéz* vagy még nehezebb (például a reachability probléma általános hibrid automatára). Az elmélet feladata kategorizálni e problémákat – megmondani, mely esetek oldhatók meg hatékonyan és melyek nem. Továbbá *approximációs algoritmusok* kidolgozása, amelyek garantált (bár nem tökéletes) eredményeket adnak polinomiális időben. A jövőben tisztább képünk lesz arról, hogy a hibrid rendszerek mely aspektusait tudjuk pontosan elemezni és melyeket csak becsülni. Ez az ismeret segíti majd a tervezőket abban, hogy reális elvárásokat támasszanak – például tudni fogják, hogy egy adott mérethatár fölött már csak szimulációval vizsgálható a rendszer, formális bizonyításra nincs remény.

Közös ontológia és nyelv: Az elméleti fejlődés része az is, hogy a különböző diszciplínák közös nyelvet alakítsanak ki a hibrid rendszerekre. Jelenleg a vezérléstelméleti szakemberek, a számítástudományi formális módszeres kutatók és a gyakorlati mérnökök olykor eltérő terminológiát használnak ugyanazon jelenségre. A jövő egyik feladata, hogy egy egységes elméleti keret jöjjön létre, amely lefedi a hibrid rendszerek minden aspektusát, és amelyben egyaránt otthonosan mozog a matematikus, az informatikus és a mérnök. Ez a keret lehetővé teszi a tudás szélesebb körű átadását és az új eredmények könnyebb alkalmazását a gyakorlatban.

7. Társadalmi és gazdasági hatások

7.1 Munkahelyek és automatizálás

A hibrid rendszerek terjedése nem csak technológiai szempontból jelentős, hanem komoly társadalmi hatásokkal is jár. Az egyik legfontosabb kérdéskör, hogy miként befolyásolja a munka világát és a foglalkoztatást az automatizált, hibrid vezérlésű rendszerek megjelenése.

Az automatizálás a gazdaságtörténet során mindig is vegyes érzelmeket keltett: egyrészt növelte a termelékenységet és új iparágakat teremtett, másrészt feleslegessé tett bizonyos munkaerőt. A hibrid rendszerek által vezérelt automatizáció folytatja ezt a trendet, sőt fel is gyorsítja. Mivel a hibrid rendszerek egyre összetettebb feladatokat képesek önállóan ellátni (gondoljunk az önvezető járművekre, az intelligens gyárakra vagy a prediktív karbantartást végző rendszerekre), számos olyan területen válhat kevesebb emberi munkaerőre szükség, amelyek eddig biztos állásokat jelentettek. Például:

- A gyártósorok melletti betanított munkából sokat átvehetnek az ipari robotok és hibrid vezérlésű gépsorok.

- Az irodai adminisztrációban az ügyintézés egy részét automatizált döntéstámogató rendszerek végezhetik el.
- A közlekedési szektorban (pl. taxisofőrök, teherautó-sofőrök) az autonóm járművek megjelenése komoly munkaerő-piaci átalakulást hozhat.

E változások hatására a munkahelyek átalakulása várható. Sok hagyományos munkakör megszűnhet vagy radikálisan átalakulhat, miközben új munkakörök születnek. A történelem azt mutatja, hogy az új technológiák *hosszú távon* általában több munkahelyet teremtenek, mint amennyit megszüntetnek, de a folyamat fájdalmas lehet bizonyos csoportok számára. Fontos tehát a társadalom alkalmazkodása: megfelelő oktatási és átképzési programokkal fel kell készíteni a munkaerőt az új típusú feladatokra. Azok az emberek, akiknek a munkáját kiváltja egy hibrid rendszer, más területeken találhatnak munkát, például a rendszerek felügyeletében, karbantartásában, programozásában. Ehhez azonban új készségekre van szükségük – ilyen például az informatikai jártasság, a rendszer-szintű gondolkodás, vagy az adatelemzési képességek.

Megjelenik a digitális szakadék problémája is: nem mindenki fér hozzá egyformán az új ismeretekhez és technológiákhoz. A társadalmi egyenlőtlenségek növekedhetnek, ha az automatizálás haszna egy szűk, magas képzettségű rétegnél csapódik le, miközben sok alacsonyabb képzettségű munkavállaló egzisztenciális bizonytalanságba kerül. Ezt ellensúlyozandó, a kormányzatoknak és az oktatási intézményeknek proaktívan kell részt venniük a munkaerő átképzésében és támogatásában. Kulcsfontosságú, hogy a hibrid rendszerek által létrehozott gazdasági előnyökből (mint amilyen a termelékenységnövekedés) a társadalom minél szélesebb rétege részesüljön, és ne csupán a technológiai vállalatok profitjában jelenjen meg.

Emellett az ember-gép együttműködés új formái alakulnak ki. Nem arról van szó, hogy minden munkát gépek végeznek majd: sok területen az emberi kreativitásra, döntéshozatalra továbbra is szükség lesz, de a hibrid rendszerek segíteni fogják azt. A "kiborg-szerű" munkahely nem science fiction: például egy sebész robotasszisztenssel dolgozik (a robot kar stabilabb és precízebb, de az orvos irányítja – ez is egyfajta hibrid rendszer), vagy egy tanár AI alapú tutor szoftverrel egészíti ki a munkáját, hogy minden diákra jusson figyelem. Ezekben az esetekben a munkakörök tartalma változik: az ember inkább felügyeleti, stratégiai, kreatív szerepet tölt be, míg a repetitív, monoton vagy veszélyes részeket a gép végzi. Saját véleményem szerint ez egy pozitív irány, hiszen az emberi munka minőségét növelheti – feltéve, hogy az átmenetet jól menedzseljük.

Összességében a hibrid rendszerek automatizációja komoly társadalmi kihívást jelent a munka világában. Alkalmazkodnunk kell ahhoz, hogy a munka fogalma átalakul: bizonyos állások eltűnnek, de új lehetőségek nyílnak. A siker kulcsa a megfelelő oktatás, az élethosszig tartó tanulás támogatása és a társadalmi védőhálók megerősítése. Ha ezeket megvalósítjuk, akkor a hibrid rendszerek által hajtott automatizálás végső soron *előnyös is lehet* a társadalom számára: az emberek mentesülhetnek a

legnehezebb vagy legunalmasabb feladatok alól, és produktívabb, kreatívabb tevékenységekre koncentrálhatnak.

7.2 Gazdasági versenyelőny és hatékonyság

A hibrid rendszerek alkalmazása nem csupán technológiai ugrás, hanem gazdasági tényező is. Azok a vállalatok és nemzetek, amelyek sikeresen integrálják a hibrid rendszereket folyamataikba, komoly versenyelőnyre tehetnek szert. *Ebben az alfejezetben* azt vizsgálom, milyen gazdasági hatásai vannak a hibrid rendszerek térnyerésének, és miben nyilvánul meg a versenyelőny és hatékonyság javulása.

Először is, a hibrid rendszerek növelik a termelés hatékonyságát. Ez több szinten is igaz:

- Erőforrás-hatékonyság: Kevesebb anyag- és energiapazarlás történik, mert a rendszer finomabban szabályozza a folyamatokat (pl. optimális hőmérsékleten működteti a gépeket, minimalizálja a selejtet a gyártásban). Az ilyen megtakarítások közvetlenül csökkentik a költségeket.

- Időhatékonyság: A hibrid rendszerek valós időben reagálnak, így csökkennek a holtidők. Egy önvezető járműflotta például kisebb követési távolságokkal is biztonságosan tud közlekedni, növelve az úthálózat áteresztőképességét, ami gazdasági szinten az áruszállítás hatékonyságát javítja. Gyáraknál a gyors átállási idők (köszönhetően az automatizált beállításoknak) azt jelentik, hogy rugalmasabban lehet termelni, kisebb készletekkel, *just-in-time* rendszerben, ami szintén költségcsökkentő.

- Minőség és megbízhatóság: A hibrid rendszerek pontosabban tartják a paramétereket, így a termékek minősége egyenletesebb, kevesebb a hibás darab. A prediktív karbantartás révén ritkábban fordul elő gépleállás. Ezek mind olyan tényezők, amelyek növelik a vállalat *profitabilitását*: vagy a bevétel nő (jobb minőség -> nagyobb vevői elégedettség), vagy a kiadás csökken (kevesebb javítás, állásidő).

Mindezen keresztül a hibrid rendszerek használata versenyelőnyt jelenthet. Az a cég, amelyik ugyanazt a terméket olcsóbban vagy jobb minőségben tudja előállítani, előnybe kerül a piacon. Nem véletlen, hogy a nagy multinacionális vállalatok rengeteget fektetnek ipari automatizálásba és digitalizációba – ez ma már nem luxus, hanem a *versenyben maradás feltétele*. A *gazdasági versenyelőny* országok szintjén is megjelenik: azok az országok, amelyek ipara gyorsan adaptálja a hibrid rendszereket (pl. Németország az Ipar 4.0 programjával), megőrizhetik vagy növelhetik ipari vezető szerepüket. Ezzel szemben lemaradhatnak azok a régiók, amelyek nem tudnak beruházni ezekbe a technológiákba – így a hibrid rendszerek fejlődése hozzájárulhat a globális gazdasági egyenlőtlenségek átrendeződéséhez is.

Ugyanakkor a hibrid rendszerek *bevezetésének költsége* sem elhanyagolható. Kezdetben komoly beruházást igényel az infrastruktúra, a szoftverek és a képzés. Éppen ezért a kis- és középvállalkozások (kkv-k) számára nehéz lehet lépést tartani a nagyvállalatokkal ezen a téren. Itt az állami vagy uniós támogatások segíthetnek, például pályázatok a gyártás automatizálására, digitalizációs támogatások. A gazdaságpolitika fontos feladata, hogy ösztönözze a technológiai modernizációt a versenyszféra minden szintjén, különben a versenyelőny koncentrálódhat néhány nagy szereplő kezében.

A hatékonyságnövekedés egy másik vetülete, hogy a gazdaság egésze produktívabbá válik. Az előállított javak és szolgáltatások mennyisége nőhet anélkül, hogy több munkaórát fektetnénk be – ez a termelékenység növekedése, ami hosszabb távon akár a GDP növekedéséhez és az általános jólét emelkedéséhez vezethet. Persze ez akkor igaz, ha a felszabaduló munkaerő más területen hasznosul (ahogy az előző alfejezetben tárgyaltam). Ha az automatizáció nyomán tömeges munkanélküliség maradna, az visszavetné a gazdaságot (mert csökkenne a fogyasztás). De a történelem azt mutatja, hogy a technológiai fejlődés általában *új gazdasági tevékenységeket* hoz létre – gondoljunk a szoftveripar, telekommunikáció, e-kereskedelem felemelkedésére az utóbbi évtizedekben.

7.3 Etikai dilemmák és jogi felelősség

A hibrid rendszerek térnyerése kapcsán nem lehet elmenni a etikai és jogi kérdések mellett. Amint egyre több döntést és műveletet automatizálunk, felmerül, hogy ki a felelős ezekért a döntésekért, illetve hogyan biztosítható, hogy a gépek döntései *összhangban legyenek az emberi értékekkel és normákkal*. *Ebben az alfejezetben* azokat a dilemmákat tekintem át, amelyeket a hibrid rendszerek alkalmazása vet fel, valamint a lehetséges megoldásokat és irányelveket.

Etikai döntéshozatal gépek által: Egy klasszikus példa az önvezető autók etikai dilemmája. Mit tegyen az autonóm jármű egy elkerülhetetlen baleseti szituációban? Milyen algoritmus dönti el az „élet-halál” kérdéseket, ha mondjuk választania kell két rossz opció között (például elüti a gyalogost vagy árokba fordulva a benne ülő utasokat veszélyezteti)? Az ilyen *morális döntéseket* eddig emberek hozták, pillanatnyi reakcióik vagy neveltetésük alapján. Most viszont előre programozott logikák vagy tanult modellek döntenek – és itt komoly felelősség terheli a tervezőket. Felmerül, hogy egyáltalán jogos-e gépekre bízni ilyen döntéseket? Sokan úgy érvelnek, hogy elkerülhetetlen, mert a gép sokkal gyorsabban és potenciálisan objektívebben tud reagálni, de ennek elfogadásához társadalmi konszenzus kell. Vannak kezdeményezések *etikai irányelvek* kidolgozására az MI és automatizálás terén (például az EU etikai irányelvei a megbízható AI-ról), melyek a hibrid rendszerekre is vonatkoznak. Ezek kimondják, hogy a rendszereknek tiszteletben kell tartaniuk az emberi méltóságot, jogokat, és átlátható módon kell működniük.

Átláthatóság és felelősségre vonhatóság: Kapcsolódik az előzőhöz az a követelmény, hogy a hibrid rendszerek legyenek magyarázhatóak. Ha egy automatizált kereskedési rendszer összeomlást okoz a

tőzsdén, tudnunk kell, miért történt. Ha egy orvosi diagnosztikai hibrid rendszer tévesen nem vesz észre egy betegséget, meg kell érteni, hol hibázott a folyamat. Az átláthatóság követelménye azt sugallja, hogy még a nagyon komplex rendszereknél is szükség lehet ember által értelmezhető magyarázatokra (pl. logikai szabályok, ok-okozati láncok). Ez nem könnyű, főleg ha gépi tanulás is van a dologban (a „fekete doboz" neural network problémája). Mégis, a jog felől egyre inkább megfogalmazódik, hogy bizonyos kritikus döntéseknél *jogunk van a magyarázathoz*. Például az EU GDPR rendelete tartalmazza az automatizált döntéshozatal elleni tiltakozás jogát, és közvetve a döntés indoklásának jogát is. Tehát a jövő hibrid rendszereit úgy kell tervezni, hogy valamilyen szinten felelősségre vonhatók legyenek, vagyis visszakövethető legyen, ki (vagy mi) hibázott.

Adatvédelem és személyes adatok: A hibrid rendszerek – különösen amelyek a társadalomban működnek (okos városok, közlekedés, egészségügy) – rengeteg adatot gyűjtenek. Ezek között sok a személyes adat (helyzetünk, egészségi állapotunk, szokásaink). Az adatok kezelése újabb etikai és jogi kihívás. Egyrészt *biztosítani kell a magánszféra védelmét*, hogy a rendszer csak azt az adatot használja, ami feltétlen szükséges, és ne éljen vissza vele. Másrészt az adatok kellenek a rendszer tanulásához, fejlődéséhez (pl. közlekedési minta elemzés). Itt is a szabályozások (GDPR és társai) keretet adnak, de a gyakorlati megvalósítás bonyolult – és a hibrid rendszerek fejlesztőinek felelőssége, hogy a rendszereik *privacy-by-design* alapon készüljenek, vagyis eleve beépítsék az adatvédelmi szempontokat.

Társadalmi elfogadás: Végül etikai szempontból fontos a társadalmi diskurzus és elfogadás kérdése. Egy technológia sem működhet, ha az emberek nem bíznak benne. Ki kell érdemelni a közbizalmat, ami csak akkor sikerül, ha a hibrid rendszereket fejlesztők komolyan veszik az etikai aggályokat. Például nyilvános teszteket tartanak, bevonják a közösséget a szabályok kialakításába (gondoljunk a nagyszabású kérdőívekre, amiket önvezető autók dilemmáiról készítettek világszerte). Meggyőződésem, hogy a technológusok felelőssége párbeszédet folytatni a társadalommal: elmagyarázni, mire képes a hibrid rendszer és mire nem, milyen értékek szerint jár el, és meghallgatni a visszajelzéseket.

Összefoglalva, a hibrid rendszerek alkalmazása új etikai és jogi keretek kialakítását igényli. Ahhoz, hogy e rendszerek hasznát biztonságosan élvezhessük, szabályoznunk kell a működésüket, felelősséget kell rendelni hozzájuk, és biztosítani kell, hogy az emberi értékrend érvényesüljön bennük. Ez nem csupán technikai feladat, hanem társadalmi kihívás is – de megoldható, ha proaktívan, felelősen állunk hozzá. Az ember és gép együttélése új szintre lép a hibrid rendszerekkel, és ehhez az emberi oldalnak is fel kell nőnie normák és törvények tekintetében.

Következtetés

A dolgozat során áttekintettem a hibrid rendszerek fogalmát, típusait, gyakorlati alkalmazásait, előnyeit és kihívásait, valamint kitértem a kutatás jövőbeli irányaira és társadalmi hatásaira. Összegzésképpen elmondható, hogy a hibrid rendszerek a modern technológiai fejlődés egyik központi elemévé váltak és a jövőben is meghatározó szereplők lesznek.

A technológiai trendek mind arra mutatnak, hogy a rendszerek egyre összetettebbé és autonómabbá válnak. Legyen szó ipari gyártósorokról, autonóm járművekről, okos városokról vagy éppen orvosi eszközökről, a hibrid rendszerek *integrált, intelligens vezérlési megoldásokat* kínálnak. A folyamatos kutatás és fejlesztés eredményeként olyan rendszerek jelennek meg, amelyek képesek kezelni a dinamikus és bizonytalan környezeteket, tanulnak a tapasztalatokból, és együttműködnek más rendszerekkel hálózatba kapcsolva. Ezek a fejlesztések új ipari és szolgáltatási forradalmakat alapozhatnak meg.

A jövő technológiai kihívásai – mint amilyen a teljesen önvezető közlekedés, az ember-számítógép interakció új formái (pl. kiberrendszerek az emberi testben), vagy a globális léptékű intelligens energiaelosztás – mind arra utalnak, hogy a hibrid rendszerekre épülő megoldások kulcsfontosságúak lesznek. Az ilyen rendszerek központi szerepet fognak játszani a következő ipari forradalomban, ahol a fizikai és digitális világ határai még inkább elmosódnak. A *kiber-fizikai rendszerek* és az *Internet of Things* (a dolgok internete) térnyerése gyakorlatilag azt jelenti, hogy egyre több hibrid rendszer lesz mindenhol, és ezek egy hatalmas integrált hálózat részeként működnek majd.

Mindezek mellett nem szabad elfelejteni a biztonság és megbízhatóság kérdését. A jövő hibrid rendszereinek sikeréhez elengedhetetlen, hogy az emberek megbízzanak bennük. Ehhez olyan tervezési filozófiára van szükség, amely *beépített biztonsággal* (safety) és *védettséggel* (security) ruházza fel ezeket a rendszereket. A következő évtizedekben valószínűleg tanúi leszünk annak, hogy a hibrid rendszerek mennyire képesek megbirkózni olyan kihívásokkal, mint a kibertámadások elleni védelem, vagy a váratlan környezeti változások (pl. extrém időjárás) kezelése. Az a meggyőződésem, hogy a folyamatos innovációval ezek a kihívások leküzdhetők lesznek, és a hibrid rendszerek egyre megbízhatóbbá válnak.

A *hibrid rendszerek jövője* tehát tele van ígéretekkel. Ha a fejlődés felelős mederben halad – figyelembe véve az etikai, jogi és társadalmi szempontokat is –, akkor a hibrid rendszerek segítségével egy fenntarthatóbb, hatékonyabb és biztonságosabb világot teremthetünk. Olyan világot, ahol a technológia ténylegesen az emberi jólétet szolgálja: megkönnyíti a mindennapi életet, jobb egészségügyi ellátást nyújt, tisztább környezetet biztosít, és új lehetőségeket nyit a gazdaságban.

Irodalomjegyzék

- Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T. A., Ho, P.-H., Nicollin, X., Olivero, A., Sifakis, J., & Yovine, S. (1995). *A hibrid rendszerek algoritmikus elemzése*. Theoretical Computer Science, 138(1), 3–34. https://doi.org/10.1016/0304-3975(94)00202-T

- Farahani, S. S., Raman, V., & Murray, R. M. (2015). *Robusztus prediktív modellalapú szabályozás időlogikai követelmények teljesítéséhez*. IFAC-PapersOnLine, 48(27), 323–328. https://doi.org/10.1016/j.ifacol.2015.11.195

- Doherty, G., Massink, M., & Faconti, G. (2001). *Hibrid automaták alkalmazása emberi tényezők elemzéséhez kritikus rendszerekben*. Formal Methods in System Design, 19, 143–164. https://doi.org/10.1023/A:1011232016683

- Egerstedt, M., Johansson, K., Lygeros, J., & Sastry, S. (1999). *Viselkedésalapú robotika regulárisított hibrid automaták segítségével*. IEEE Conference on Decision and Control, 4, 3400–3405. https://doi.org/10.1109/CDC.1999.827799

- Schupp, S., Winkens, J., & Abraham, E. (2018). *Környezetfüggő elérhetőségelemzés hibrid rendszerekhez*. IEEE International Conference on Information Reuse and Integration (IRI), 518–525. https://ieeexplore.ieee.org/document/8424753

- Johansson, K. H., Egerstedt, M., Lygeros, J., & Sastry, S. (1999). *A Zénó-jellegű hibrid automaták regulárisításáról*. Systems & Control Letters, 38(3), 141–150. https://doi.org/10.1016/S0167-6911(99)00059-6

- Lee, E. A., & Seshia, S. A. (2016). *Bevezetés a beágyazott rendszerekbe: Kiber-fizikai rendszerek megközelítése* (2. kiadás). MIT Press. https://ptolemy.berkeley.edu/books/leeseshia/releases/LeeSeshia_DigitalV2_2.pdf

2.42. Labdaszállító berendezés

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

IPAR 4.0 TECHNOLÓGIÁK

Labdaszállító berendezés

Gál Bence

[redacted]

Villamosmérnöki BSc szak

Automatizálás

[2025]

Tartalomjegyzék

1. Bevezetés ***1***

2. Meglévő projekt előzetes ismertetése ***2***

2.1 Nyomógombos vezérlés 2

2.2 Szenzor 2

2.3 DC motorok és l298N H-bridge 2

2.4 Első állomás 3

2.5 Második állomás 4

2.6 Harmadik állomás 4

2.7 Negyedik állomás 5

2.7 Ötödik állomás 5

3. Továbbfejlesztett projekt ismertetése ***5***

3. 1 Szenzorok 5

3.2 Számláló 6

3.3 ESP 8266 (01s) Wi-Fi modul 6

3.4 MCP23017 6

3.5 Kód 6

4. Felhasznált eszközök bemutatása ***7***

4.1 Arduino UNO 7

4.2 LED 8

4.3 DC Motor 8

4.4 L298N H-bridge 9

4.5 Szenzor 11

4.6 LEGO 11

4.7 Tápegység 12

4.8 Kábel 12

4.9 Számláló 13

4.10 MCP23017 13
4.10.1 UART 14
4.10.2 SPI 15
4.10.3 I²C 16
4.10.4 I²C működése 17
4.11 ESP 8266 (01s) Wi-Fi modul 18

5. Építési nehézségek 19
5.1 Első állomás 19
5.2 Második állomás 19
5.3 Harmadik állomás 20
5.4 Negyedik állomás 20
5.5 Ötödik állomás 21
5.6 Szenzor 21
5.7 Számláló 22

6. Kód és kábelek bekötése 23
6.1 Nyomógomb 24
6.2 LED 24
6.2.1 Dióda 25
6.3 Első állomás 26
6.4 Második állomás 26
6.5 Harmadik állomás 27
6.6 Negyedik állomás 27
6.7 Ötödik állomás 28
6.8 Számláló 28
6.9 ESP 8266 (01S) Wi-Fi modul 28

7. Összefoglalás 29

1. Bevezetés

2024 nyarán teljesítettem a villamosmérnöki szakon előírt szakmai gyakorlatot. 1.5 hónapot töltöttem a büki Nestlé Hungária gyárban, ahol bepillantást nyerhettem az automatizálás mindennapi világába. Ez egy kihívásokkal teli terület, viszont rengeteg siker élményt biztosít és remek lehetőséget ad új emberek megismerésére.

Míg ott töltöttem az időt, sok ember alkotta találmányt megcsodáltam, ami meghatározta és a mai napig meghatározza az egész világot például: PLC, futószalag, motor, különböző típusú szenzorok, lift, konverterek, szabályozók, mikrokontrollerek és számos más dolog. A projekt ötletet is innen merítettem. Lehetőségem nyílt korszerű PLC-t programozni a TIA portálon a létradiagram struktúrában. Rájöttem, hogy egy korszerű PLC-t és ahhoz eszközöket vásárolni szimplán hobbiként csöppet sem kivitelezhető, ennek a legeslegfőbb oka, ezen eszközök költsége. Szerencsére már több mint egy éve ismerkedtem meg az Arduino termékcsaláddal. Ez idő alatt számos tapasztalatban gazdag projektet vittem végbe.

Az első ilyen egy dobókocka szimulátor volt. Lényege az volt, hogy a gomb megnyomását követően, egy kis késleltetéssel, bizonyos mennyiségű LED felvilágítson. Ehhez 7 darab 5 mm-es LED (dobókocka elrendezés miatt), 1 gyomógomb, 1 darab 10k Ohm és 7 darab 330 Ohm előtét ellenállás kellett. Mind forrasztás mentesen, azaz breadboard segítségével, mind PCB panelre ólommentes ón (Cin) segítségével ráforrasztva és faburkolatot kapva, hordozható formában is megvalósítottam.

A második egy futófény volt (batman szimbólumú elrendezéssel), aminek a felvillanási sebességét lehetett állítani egy potenciométer segítségével. Ennek megcsinálásához kellett 1 darab SN74HC95N (8 bites soros-perem párhuzamos shift regiszter), 1 darab NE555 timer, 32 darab előtét ellenállás és 32 darab LED, továbbá 1 darab ELKO kondenzátor.

A másik nagyobb volumenű alkotásom egy óra volt, ahol belehetett állítani az időt (percet és órát egyaránt). Tartalmazott 4 darab 7 szegmenses kijelzőt és 2 darab nyomógombot. Természetesen több kisebb elektronikai alkotásokat is csináltam már. Ennek a projektnek a tápforrása a hálózatból származott. A bejövő feszültséget egy transzformátorral letranszformáltam, majd egy dióda hídon keresztül, több párhuzamosan kapcsolt porcelán kondenzátoron keresztül átvezetve táplálta a projektem.

2. Meglévő projekt előzetes ismertetése

2024 nyarán kezdtem bele megvalósítani egy nagyobb projektet A tervem a következő volt: csinálok egy labdaszállító berendezést, amely valamilyen fajta emberi beavatkozás nélküli önműködő rendszer, és tükrözi a szakmai gyakorlatom során a Nestlé Hungária kft. büki gyárában látottakat. A projektem 'agyát' egy Arduino UNO mikrokontroller adja.

2.1 Nyomógombos vezérlés

Az egész eszköz vezérléséhez 2 nyomógombot használok. Egy kezdő (start) nyomógombot és egy leállító (stop) nyomógombot. A labda kiindulópontjának előzetes behelyezése után, elég csak a két gombot megnyomni a projekt működéséhez. Visszajelzésként beiktattam 3 mm-es LED-eket, vörös (hullámhossza:700 nm) és kék (hullámhossza:460 nm) színűt. Ezeket a dizájn kedvéért egymásba sorba kötve (anód-katód-anód-katód...) és előtét ellenállást elhelyezve, kirajzolódik egy "start" és egy "stop" felirat.

2.2 Szenzor

A projekt egy pontjára lézeres érzékelő szenzort helyeztem, ami a labda helyzetének pontosabb nyomon követését teszi lehetővé. A futószalag végéhez helyeztem. Amennyiben szakad a fény útja, a mikrokontrolleren „HIGH" érték jelenik meg, egyéb esetben „LOW" érték.

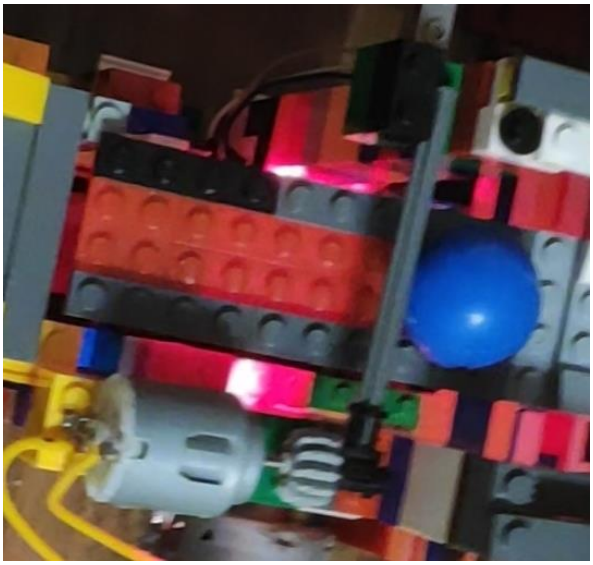
2.3 DC motorok és l298N H-bridge

Pontosan hat darab motort használtam, melynek értékei 6V és 12V volt. Céljuk a különböző típusú

feladatok ellátása. Ezen motorok vezérléséhez szükség volt motor driver-ekre is.

A következő alfejezetekben a projekt állomásait ismertetem.

2.4 Első állomás



1.ábra. Ajtó.

Az első állomás a kiindulópont (*1. ábrán* látható). Egy lejtős részen játszódik, így szükség van egy útlezáróra, ami megfogja a labdát, hogy ne guruljon tovább (ajtó). Ehhez egy 6 V-os DC motorra volt szükség.

A lejtős rész a labda elmozdulását teszi lehetővé. Ugyanis, a labdára hatnak erők. Mozgást lassító erők például a légellenás ($F_{lég}$), súrlódás (F_s). Továbbá van egy erő, ami a Földön mindenkire hatással van, ami lefelé, a Föld közepe felé mutat. Ez a gravitációs erő, melynek nagysága [1]:

$$F_g = m * g\,, \qquad (1)$$

ahol m a labda tömege, g pedig a gravitációs gyorsulás (≈9,81 m/s^2). Ezen kívül megemlíthetjük még a normálerőt (F_N), a lejtő felülete felfelé, merőlegesen (normálisan) kifejt egy erőt a labdára. Ez az erő megakadályozza, hogy a labda áthatoljon a lejtőn. Ezen erők segítségével felírhatjuk a lejtőre merőleges komponenseket, továbbá a lejtőre párhuzamos komponenseket [1]:

$$F_{||} = m * g * \sin(\theta), \quad (2)$$

ahol m a labda tömege, g pedig a gravitációs gyorsulás és θ a lejtő dőlésszöge.

2.5 Második állomás

A második állomás egy csapóajtó, amibe a labda érkezni fog, ha a lejtőről legurul. Itt két 6 V-os DC motort használtam egymással szembe fordítva és ellenkező polaritással sorba bekötve. A motorok forgó részét (armatúra) egy közös műanyag LEGO rúdra rögzítettem, amin van egy bizonyos kiterjedésű lapos LEGO felület. Mivel sorba kötöttem, ezért itt a rajtuk átfolyó áram megegyezik, de a rajtuk eső feszültség összeadódik.

2.6 Harmadik állomás

2.ábra. futószalag.

A harmadik állomás egy futószalag szerkezet, amit egy 12 V-os DC motor hajt. Ahhoz, hogy a labda ne guruljon el, oldalt korláttal körbe kellett vennem a szalagot *(2. ábra*). A csapóajtó lehajtását követően érkezik a labda a szalagra, majd a szalag a labdát belelöki egy a liftbe. A szenzor bejelez, majd lekapcsolja a szalagot és elindítja a liftet felfelé.

2.7 Negyedik állomás

A negyedik állomás a lift, amit egy 12 V-os DC motor hajt meg, vastag fonállal való rögzítéssel. Korábbi teszteléseknél még 3 darab DC 6 Volt-os motort használtam. Feladata, hogy az alsó szintről a felső szintre felszállítsa a labdát.

2.7 Ötödik állomás

Az ötödik állomás egy toló szerkezet, ami kilöki a labdát a liftből, és kezdődik a folyamat előről, azzal a különbséggel, hogy az ajtó nyitva van. Szintén egy 6 V-os DC motor valósítja meg ezt a feladatot. Amennyiben, benyomom a stop gombot, az ajtó becsukódik és leállítja az egész folyamatot.

3. Továbbfejlesztett projekt ismertetése

Ebben a fejezetben ismertetem a továbbfejlesztett projekt különbségeit, bővítéseit a régebbi fejlesztéshez képest.

3.1 Szenzorok

A legfőbb változtatás a precizitás érdekében a további szenzorok beépítése. Ennek köszönhetően a rendszer tudni fogja, hogy a labda jelenleg melyik állomásnál járhat. A jelenlegi projekt 5 darab szenzort tartalmaz.

Ezzel a módszerrel az időzítőket kiválthatom a projektből, és megbízhatóbb működést tesz lehetővé. Továbbá, a szenzorok állapotaihoz további műveleteket lehet hozzárendelni.

3.2 Számláló

Ez egy 7 szegmenses katód típusú kijelző, aminek a jelentősége az, hogy számolja a labda által megtett teljes köröket a start gomb előzetes megnyomását követően. Az értéke lenullázódik a stop gomb megnyomása után.

3.3 ESP 8266 (01s) Wi-Fi modul

Feladata, hogy képes legyen rácsatlakozni a netre router segítségével. Csináltam egy html weboldalt, ahová helyeztem két nyomógombot, amelyek benyomásával elindul vagy lekapcsolja a projektet. Így több mód van bekapcsolni és elindítani a projektet (IoT). Továbbá számlálót is elhelyeztem a weboldalra, melynek segítségével nyomon követhetjük a labda megtett köreit.

3.4 MCP23017

A további bővítéseknek ára van. Az Arduino Uno-n már nincs elegendő bemenet, ahhoz, hogy minden modult hozzá lehessen csatlakoztatni. Ennek köszönhetően választottam az MCP23017 I/O modul bővítőt. Ez a modul lehetővé teszi, hogy 2 bemenetért cserébe kapok 16 darab bemenetet. Ezzel a módszerrel a szükséges bemenetek mennyiségét megoldottam.

3.5 Kód

A több szenzornak köszönhetően, a régebbi fejlesztés kódját már nem tudtam felhasználni, mivel az túlnyomó részt az időzítőkre épült. Ennek köszönhetően kellett egy teljesen újat írnom. Továbbá, a projekt bővítésének köszönhetően megjelentek olyan elemek, mint 7 szegmenses kijelző, MCP23017 I/O modul bővítő és IoT platform. Ezekhez mind szükséges volt további kódok megírására.

4. Felhasznált eszközök bemutatása

Ebben a fejezetben bemutatom részletesen a felhasznált elemek komponenseit.

4.1 Arduino UNO

Az Arduino egy szabad szoftveres, nyílt forráskódú elektronikai fejlesztőplatform, arra tervezve, hogy a különböző projektekben az elektronikus eszközök könnyebben hozzáférhetőek, kezelhetőek legyenek. Egy speciális programnyelvet használ, leginkább a C nyelvhez lehetne hasonlítani. Az Arduino programozható része az ATMEGA328P IC. A programozásához szükséges a számítógépre letölteni az "ARDUINO IDE" nevezetű programot, ahol ki kell választani a típust (például: Arduino UNO, Arduino NANO, Arduino MEGA...). Ezt követően, ha az IC még nincs bootloader-elve, -ami előfordulhat, ha csak magát az IC-t vesszük meg-, akkor meg kell tennünk (egy másik Arduino segítségével). Amennyiben az előzőekben felsorolt feltételek adottak, rátölthetjük a kódot (de előtte a rendszer lefuttat egy ellenőrzést, hogy nincs –e hiba a megírt kódban) egy speciális kábel segítségével, ami összeköti az Arduino-t és a számítógépet.

Anyagi megfontolásból fontos, hogy az ATMEGA328P, akár a mikrokontroller nélkül is állhat önállóan, ha a következő dolgokat még beszerezzük hozzá: 2 darab 22 pF nagyságú porcelán kapacitás, egy 10k Ohm ellenállás és egy 16 MHz-es kristály (a még megbízhatóbb működés érdekében, egy ELKO kondenzátorral is elláthatjuk a bemenetet, úgy, hogy a bemenet és a föld közé kötjük).

Az Arduino UNO-nak vannak hátrányai is, ezek a bemenetek. 18 bemenettel rendelkezik, ezek közül 6 darab analóg és 12 darab digitális bemenet. Az analóg bemenetet lehet használni digitális bemenetként is. 5 darab bemenetnél szabályozhatjuk a motorok sebességét (PWM). Továbbá vannak nála jóval nagyobb órajel ciklussal dolgozó mikrokontroller-ek (ESP32).

Az Arduino UNO többféle kommunikációs protokollt támogat, amelyek lehetővé teszik az eszközök közötti adatcserét: UART, I²C, SPI, USB.

Egy hardveres UART interfészt tartalmaz a TX (D1) és RX (D0) lábakon keresztül. Ezt a protokollt használja az USB-soros kapcsolat a PC-vel történő kommunikációhoz az ATmega328P chip segítségével. A Serial könyvtárral programozható.

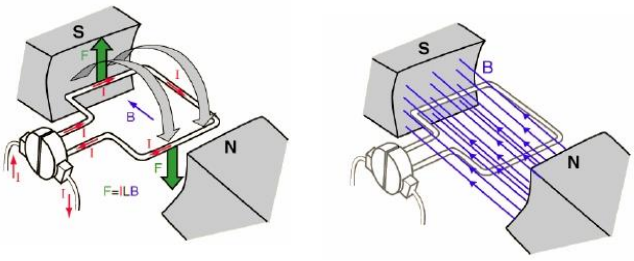
Az I²C protokoll az A4 (SDA - adatvonal) és A5 (SCL - órajel) lábakat használja. Több eszköz csatlakoztatható egyetlen buszra, ahol egy eszköz a mester (Master), a többi pedig szolga (Slave). A 'Wire' nevezetű könyvtárral használható.

Az SPI busz négy fő vonalat használ: MOSI (D11), MISO (D12), SCK (D13), SS (D10)
Nagy sebességű adatátvitelre alkalmas, például SD-kártyák, kijelzők és egyéb modulok esetében. A SPI könyvtárral használható.

4.2 LED

Méretüket tekintve a 3 mm-es LED-eket választottam kompaktságuk miatt, ami ideálissá teszi őket kis helyigényű alkalmazásokhoz. Vörös és kék színű LED-eket használtam, amelyeknek a hullámhossza 700 nm és 460 nm. Működési áramuk 20 mA. Alacsony energiafogyasztásuk miatt hosszú élettartamúak és energiatakarékosak. Széles körben használják őket kijelzőkben, jelzőfényekben és háttérvilágításban. Továbbá, a kedvező ára miatt választottam (nagy tételben még kedvezőbb). Előtét ellenállást használni hozzájuk ajánlott.

4.3 DC Motor



3. ábra. DC motor (forrás: [A1]).

A DC (egyenáramú) motorok számos alkalmazásban népszerűek, mivel egyszerű felépítésük és megbízhatóságuk miatt sokféle feladatot képesek ellátni. A DC motorok az egyenáramú elektromos energiát mechanikai energiává alakítják át. Két fő részből állnak: az állórészből (sztátor) és a forgórészből (armatúra).

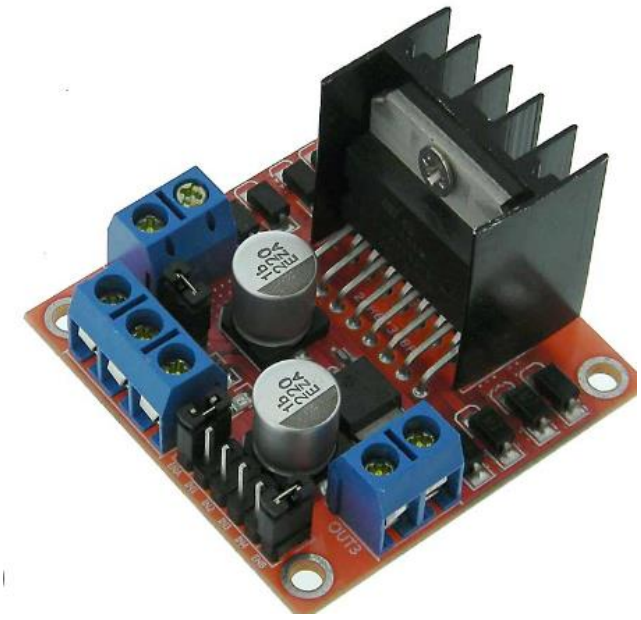
Az állandó mágnes mágneses terében van elhelyezve egy vezetőkeret (armatúra), amelyben

áram folyik. Az áram hatására a vezető körül mágneses mező alakul ki, amely merőleges lesz az állandómágnes mágneses terének vektoraira. Ez egy bizonytalan egyensúlyi helyzet, s a Lorentz-féle erőhatás miatt a forgórész elfordul. 180º-os elfordulás után stabil helyzet alakulna ki, ha a vezetőkeretben nem fordulna meg az áram iránya. Mivel a kommutátor szegmensek átcsúsznak a másik szénkefe alá, így megfordul az áramirány, s a folyamat kezdődik elölről. Az állórész állandó mágnese helyett gyakran alkalmaznak tekercset, amit egyenárammal gerjesztenek.

Az armatúraáram maga is mágneses fluxust hoz létre, amely hozzáadódik a pólusok által létesített fluxushoz. Ez a jelenség eltorzítja az indukció-eloszlást az armatúra kerülete mentén. Mint ahogy azt az ábra is mutatja, ennek az lesz a következménye, hogy a gép fluxusa csökken, és az ún. semleges vonal eltolódik. Ezért tehát ennek megfelelően el kell tolni a keféket is [2].

Viszont hátrányai is vannak. A szénkefék kopása miatt rendszeres karbantartást igényelnek. Az AC motorokhoz képest alacsonyabb hatékonyságúak lehetnek, különösen nagyobb teljesítményű alkalmazásokban. A szénkefék és a kommutátor közötti érintkezés kopást és szikrázást okozhat, ami csökkenti a motor élettartamát.

4.4 L298N H-bridge



4. ábra. L298N (forrás: [A2]).

Az Arduino-n biztonságosan 20 mA folyhat át rajta, de egyetlen egy 6 V-os DC motor is 4.8 W-ra képes, ami 0.8 A áramfelvételre van szükség, azaz 800 mA. Ez a negyvenszerese a megengedettnek. Pontosan ezért használunk motor driver-eket.

Az Arduino UNO-hoz leggyakrabban kettő féle motor driver jöhet szóba: az L293D és az L298N.

	áramterhelhetőség	feszültségtartomány	vezérlőfeszültség	hatékonyság
L293D	1.2A	4.5V-5.5V	4.5-36V	50%-90%
L298N	1.5A	4.5V-7V	5V-46V	30%-70%

1. táblázat. Két motor driver összehasonlítása

Két H-híd áramkört tartalmaz, amelyek lehetővé teszik két DC motor független vezérlését. Az áram irányának megfordításával a motor forgásirányát lehet változtatni. Van benne egy beépített 5 V-os feszültségszabályzó, amelynek kettő funkciója lehet a tápfeszültség függvényében. Amennyiben 12 V-on vagy az alatt vagyunk, akkor a szabályzót használhatjuk Arduino megtáplálásra vagy egyéb áramkörök megtáplálására. Viszont, ha 12 V felett van, akkor ki kell venni a jumper-t és az 5 V-os bemenetnél meg kell táplálni a motor driver-eket.

Egy másik igen hasznos tulajdonsága az L298N motor driver-nek a motor sebességének a szabályozása, azaz PWM (Pulse Width Modulation). Nem utolsó sorban viszonylag nagy hűtőbordával rendelkezik, ami a hőelvezetésben játszik hatalmas szerepet.

A PWM jel egy olyan téglalapjel, amelynek frekvenciája állandó, de az impulzusok kitöltési tényezője változtatható. Képlete a következő [3]:

$$D = \frac{T_{on}}{T_{on}+T_{off}} \; x \; 100\%, \tag{3}$$

ahol D a kitöltési tényező, T_{on} a magas állapot időtartama és T_{off} az alacsony állapot időtartama. Az időzítő periódikusan megszakítást generál, ahol a kimeneti jelet módosítjuk.

Bemenetek és kimenetek esetén, kapunk 2 db motor kimenetet (Output A, Output B), A Enable, B Enable, Logic Inputs, Power Ground és +12V Power. Amennyiben nem szeretnénk vezérelni a sebességet az adott motornak (a tápfeszültség határozza meg), akkor bent kell

hagyni az Enable A vagy B-nél a jumper-t. Viszont, ha szeretnénk irányítani, akkor ki kell venni a jumper-t, és be kell kötni az Arduino egyik lábába a 18 felhasználható közül vagy pedig az MCP23017-be.

Fontos, hogy az Arduino és a vezérlők földelve legyenek, de a 12 V-os táptól el kell különíteni a mikrovezérlőt, mert ez a mikrokontroller tönkremeneteléhez vezethet.

4.5 Szenzor

A projekthez KY-008 lézereket használtam, ami népszerű lézer adó modul, amelyeket gyakran használnak Arduino projekteknél. 650 nm-es hullámhosszon működik. 5 mW-os teljesítményű, aminek a működési feszültége 5 V. A KY-008 modul három darab lábbal rendelkezik. Az egyik a VCC, ahova az 5 V csatlakoztatjuk. A második a ground. A harmadik pedig a signal, amit az Arduino egyik bemenetére csatlakoztatjuk, akkor képesek vagyunk a ki-, és bekapcsolására a lézernek. Ahhoz, hogy szenzorként működjön, szükségünk van egy vevőre is.

A lézer vevők általában fotodiódák vagy fototranzisztorok, amelyek érzékelik a lézer fényét és elektromos jelet generálnak. Ugyancsak 3 lába van. Egy VCC, egy ground és egy OUT. Az OUT lábat csatlakoztatjuk az Arduino-hoz. Az „Arduino IDE” programban „Serial monitor” résznél leolvashatjuk a vevő állapotát, ha az adó eléri a vevőt, akkor az 1-es állapotot ír ki a gépünkre, viszont, ha megszakad a jel, akár csak egy kis időre is, akkor 0 értéket fogunk kapni. Ezt a programban a „Serial.println()” segítségével tudjuk megtenni.

4.6 LEGO

A LEGO egy világszerte ismert és kedvelt építőjáték, amelyet a dán LEGO Csoport gyárt. A LEGO kockák különböző méretű és színű műanyag elemek, amelyek egymásba illeszthetők. Előnye, hogy különböző dolgokat (például: ház, autó, ajtó...stb.) megtudunk valósítani kis méretben. Az utóbbi években sajnos rendkívül megemelkedett az ára.

A feladat megvalósításának a kezdetén a pálya anyaga egy nagyon fontos tényező volt. Elsősorban a faszerkezeten gondolkodtam, viszont hamar beláttam, hogy a fa megmunkálásához

nincsen meg a megfelelő felszerelésem, tudásom és szakképesítésem sem. A következő gondolatom a LEGO volt. Körülbelül kettő nap kellett, hogy felépítsem a kezdetleges vázat. Majd a projekt előrehaladtával egyre inkább kialakult a végleges forma.

4.7 Tápegység

Egy (SKU): 3240-es tápegységet használok, amibe be van építve egy állapotjelző LED (hullámhossza: ~500-565 nm), ami jelzi, hogy van –e kimeneti feszültségünk. Váltakozó áramból alakít át egyenáramot, mégpedig 12 V-ot és 6.5 A-t. 78W-os teljesítmény leadására képes. IP44 védettséggel rendelkezik. Továbbá, a tápegység rövidzárlat és túlterhelés elleni védelemmel van ellátva, stabil kimeneti feszültséget biztosít, és beépített EMI szűrővel rendelkezik. A kimeneti oldalon szabványos 2.1 x 5.5 mm-es DC apa csatlakozó található. Ehhez szükség volt még egy átalakítóra. A belső pin pozitív, a palást pin negatív polaritású.

4.8 Kábel

Kábelek esetén használtam jumper kábeleket (male-female csatlakozás), és körülbelül 5.5 m 0.5 mm^2 litze rézkábelt.

A tömör vezeték egyetlen szilárd rézhuzalból áll. Erősebb és kevésbé hajlékony, mint a Litze vezeték. Alacsonyabb ellenállású, ami kisebb veszteséget jelent az átvitele során. Felhasználást tekintve, gyakran használják épületek elektromos vezetékezésében, ahol a vezetékek rögzítettek és nem szükséges a gyakori mozgatásuk. A tömör vezetékek kevésbé érzékenyek a külső elektromágneses zajokra, mivel a szilárd szerkezetük jobban árnyékolja az áramot. Továbbá kevésbé fogékony a vibrációra és korrózióra.

A Litze vezeték egy speciálisan kialakított hajlékony és rugalmas vezeték, amit magas frekvenciájú elektromos jelek átvitelére használnak. Több rézhuzalból áll, amelyek össze vannak sodorva. Nagyobb felülettel rendelkezik a tömör vezetékhez képest, ami jobb hőleadást biztosít. Kevésbé érzékenyek a proximity-effect-re, ami csökkenti a veszteségeket. Nagyfrekvencián alacsonyabb az EMI. Továbbá, a skin depth (ahol az áram a vezeték külső felületén áramlik) miatt

nagyfrekvenciás alkalmazásokban jobb teljesítményt nyújt. Ideális felhasználási terület például robotkarokhoz.

4.9 Számláló

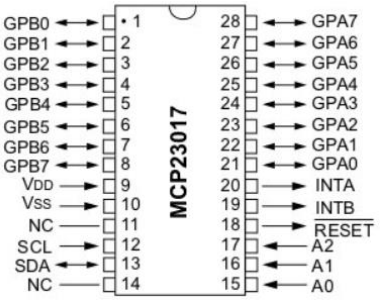
A 7 szegmenses kijelző egy gyakran használt kijelzőtípus, amelyet főként számjegyek megjelenítésére alkalmaznak. Ezeket a kijelzőket leginkább digitális órákban, számológépekben, mérőműszerekben és egyéb egyszerű elektronikus eszközökben fellelhető.

A 7 szegmenses kijelző hét külön vezérelhető LED vagy LCD szegmensből áll, amelyek megfelelő kombinációkban történő bekapcsolásával különböző számokat képezhetünk. A szegmenseket gyakran A-tól G-ig jelölik, és egy külön pontot (DP - decimal point) is tartalmazhat a tizedesértékek jelölésére. A kijelző különböző méretű lehet, én egy 5.6 mm-es változatot használtam, melynek üzemi árama 20 mA.

A hétszegmenses kijelző lehet közös katódos (Common Cathode, CC) vagy közös anódos (Common Anode, CA). CC esetén a katód (negatív pólus) közösítve van, és a szegmenseket pozitív feszültség (HIGH) alkalmazásával világítjuk meg. Míg CA esetén az anód (pozitív pólus) közösítve van, és a szegmenseket negatív feszültség (LOW) alkalmazásával világítjuk meg.

Ha a kijelző közös katódos, akkor a megfelelő kimeneteket HIGH (1) állapotba kapcsoljuk, amit az „Arduino IDE” programban meg is tudunk tenni. Például, ha szeretnénk az „A” szegmenst felvilágítani, és azt a szegmenst az Arduino D10-es lábába kötöttük, akkor „digitalWrite(10, HIGH).

4.10 MCP23017



5. ábra. MCP23017 (forrás: [A3]).

Az MCP23017 *(5. ábra.)* egy I/O modul expander. Az Arduino két lábára megfelelően rákötve, 16 további használható lábat nyerünk. I²C protokollt használ. A 3 darab hardveres címbitek (A0, A1, A2) lehetővé teszik, hogy akár 8 darab MCP23017-et csatlakoztassunk egy I²C buszra (8 × 16 = 128 GPIO).

Beépített pull-up ellenállások (100 kΩ) találhatók meg benne. Feszültségtartomány: 1.8V – 5.5V (így kompatibilis 3.3V és 5V rendszerekkel). Áramterhelés: maximum 25 mA lábanként.

A2	A1	A0	I²C cím
0	0	0	0x20
0	0	1	0x21
0	1	0	0x22
0	1	1	0x23
1	0	0	0x24
1	0	1	0x25
1	1	0	0x26
1	1	1	0x27

2. táblázat. MCP23017 címzése

4.10.1 UART

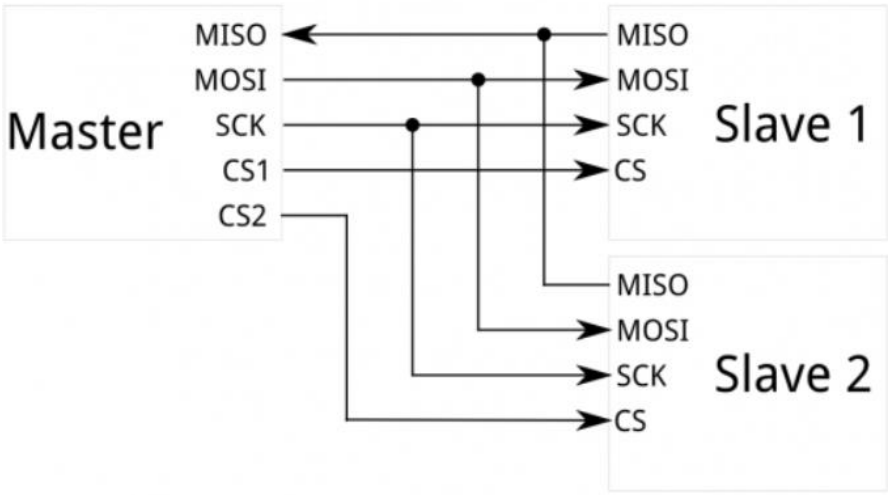
Az UART az Universal Asynchronous Receiver-Transmitter rövidítése. Ez egy soros kommunikációs protokoll, amelyben az adatok bitenként továbbítódnak egy vezetékpáron keresztül. Név szerint említve: TX (Transmit) és RX (Receive). Aszinkron kommunikáció van, -tehát nincsen órajel adatok-, az őket használó eszközöknek előre kell megállapodniuk az adatsebességről. A két készüléknek ugyanolyan sebességűnek kell lennie, ha a sebességükben túl nagy eltérés van, akkor az adatok átvitele nem 100 százalékosan garantálható.

Az aszinkron soros adatátvitel hardveres megvalósítást igényel, nehéz szoftveresen megvalósítani a pontosan és jól működő adatátvitelt. Ráadásul ezen kommunikáció sajátossága miatt

kell start, illetve stop biteket is küldeni, ez a gyakorlatban azt eredményezi, hogy minden 8 elküldött bit mellé kell még küldeni kettőt, ami a sebességet jelentősen lassítja. További hátrány, hogy csak 2 eszköz közötti kommunikáció megvalósítására tervezték.

Végül az adatsebesség is problémát jelent. A legtöbb UART eszköz csak bizonyos rögzített átviteli sebességeket támogat, és ezek közül a legmagasabbak általában 230400 bit másodpercenként [4].

4.10.2 SPI



6. ábra. SPI (forrás: [A4]).

Az SPI a Serial Peripheral Interface rövidítése. Szinkron soros kommunikációs protokoll, amelyet főként beágyazott rendszerekben használnak, hogy mikrovezérlők és perifériák, például érzékelők, memóriák vagy kijelzők között adatátvitelt biztosítsanak.

Master-Slave arcitektúrára épülő protokoll, amely 4 fővonalat használ az adatátvitelhez *(6. ábra.)*: SCLK (Serial Clock) – A mester által generált órajel, amely szinkronizálja az adatátvitelt. MOSI (Master Out, Slave In) – A mester küldi az adatokat a szolga felé. MISO (Master In, Slave Out) – A szolga küldi az adatokat a mester felé. CS (Chip Select) – A mester kiválasztja a megfelelő szolga eszközt.

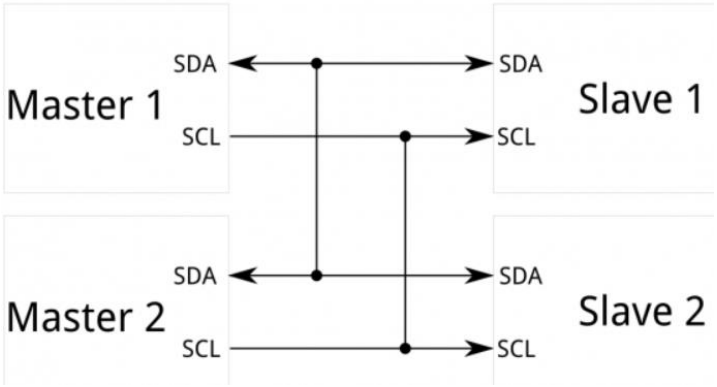
Full-duplex működésű, azaz az adatok egyszerre küldhetők és fogadhatók. Az órajelet a mester határozza meg. A chip select segítségével a master több szolgát is tud vezérelni, ahogy az a *6. ábrán*

is látható.

Az SPI legnyilvánvalóbb hátránya a szükséges vezetékek száma. Egy mester csatlakoztatása egyetlen slave-hez egy SPI buszhoz négy vezetéket igényel; minden további slave egy további lábat igényel a kiválasztáshoz. Ez nem kívánatos abban az esetben, ha sok slave eszközzel kell dolgoznunk. Továbbá, az egyes készülékek nagy számú kapcsolata megnehezítheti a nyomtatott áramkör megtervezését abban az esetben, ha kisméretű NYÁK-ot kell terveznünk. Az SPI csak egy mestert engedélyez a buszon, de támogatja a tetszőleges számú slave-et (csak a szabad IO száma korlátozza).

Az SPI jó adatátviteli sebességű, néhány eszköz esetében pedig 10MHz-es (és így 10 millió bit másodpercenkénti) órajeleket támogat, és a sebessége jól skálázható. A hardver mindkét végén általában egy szintillesztő található, amely lehetővé teszi az egyszerű szoftveres megvalósítást [4].

4.10.3 I²C



7. ábra. I²C (forrás: [A5]).

Az I²C csak két vezetéket igényel, mint például az aszinkron soros kommunikáció, de a két vezetéken több slave eszközt is csatlakoztathatunk (*7.ábra*). Az SPI-vel ellentétben az I²C többmesteres rendszert is támogathat, amely lehetővé teszi, hogy egynél több mester kommunikáljon a busz összes eszközével (bár a masterek nem tudnak egymással beszélni a buszon, és a buszvonalak használata egyidőben csak egy masternek engedélyezett).

Az adatsebesség az aszinkron soros és az SPI között van. A legtöbb I²C eszköz képes kommunikálni 100 kHz-en vagy 400 kHz-en. Az I2C-nél a küldendő adatok minden 8 bitje után meg kell küldeni egy extra bit metaadatot (az „ACK / NACK” bit). Az ATMEGA328P 400 kHz-es sebességet és bővített, 10-bites címzést engedélyez.

Minden I²C busz két jelből áll: SCL és SDA. Az SCL (SerialCLock) az órajel, és az SDA

(SerialData) az adatjel. Az órajelet mindig az aktuális mester generálja. Egyes slave eszközök le tudják húzni alacsonyra az órajelet, ezzel késleltetvén a master által küldött adatfolyamot. Ezt „órajel-nyújtásnak” nevezik.

Ellentétben az UART vagy SPI kapcsolatokkal, az I^2C meghajtók „open drain” elven működnek, azaz a megfelelő jelvezetéket alacsonyra tudják húzni, de nem képesek magasra szintet ráadni. Tehát nem fordulhat elő olyan helyzet, hogy az egyik eszköz feszültséget ad a buszra, amíg a másik éppen lehúzná a földre (zárlat). Mindegyik jelvezetékre beszerelésre kerül egy felhúzó-ellenállás, amely biztosítja a jelvezeték magas szintjét abban az esetben, ha az egyik eszköz sem húzza le alacsony szintre. Általában 4.7k Ohm szokott ez az érték lenni, ami csökkenhet, ha hosszabb vezetékeknél vagy sok buszra csatlakoztatott eszközről beszélünk [4].

A maximális feszültség különbség csak annyi lehet, ahol még a magasabb feszültségű rendszer logikai szintjének magasba billentéséhez elegendő az alacsonyabb feszültségű rendszer feszültsége. Ilyen esetben nem kell szintillesztőt használni. Ezért lehet pl. egy 5 V-os Arduino-ra csatlakoztatni egy 3,3 V-os gyorsulásmérőt. Amennyiben a feszültségkülönbség túl nagy, akkor szintillesztőt kell alkalmazni.

4.10.4 I²C működése

A címzés elküldése előtt a master az SCL lábat magasra hagyja, és az SDA-t alacsonyra húzza. Ez minden slave eszközt figyelmeztet arra, hogy az átvitel megkezdődik. Ha két master eszköz egyidejűleg kívánja elfoglalni a buszt, akkor az az eszköz, amelyik az SDA-t vonalat először húzza le alacsonyra, az lesz jogosult a kommunikációra. Lehetőség van ismételt üzenet küldésére anélkül, hogy a busz feletti rendelkezést a master átadná másik eszköznek.

Minden új kommunikációs csomagban először a címzés kerül továbbításra. 7 bites címek esetén először a címet a legfontosabb bittel (MSB) kell lezárni, amelyet egy R/W (Read/Write, Olvasás/Írás) bit követ, amely jelzi, hogy ez olvasási (1) vagy írási (0) művelet.

A cím 9. bitje a NACK/ACK (jóváhagyás, ACKnowledge) bit (ez vonatkozik a címzésre és az adatátvitelre is). Miután a címzés első 8 bitjét elküldtük (7+R/W), a fogadó eszköznek kell az

adatvonalat alacsonyra húznia, ezzel jelzi, hogy tudomásul vette, hogy vele akar a master kommunikálni és egyben azt is jelzi, hogy készen áll a kommunikációra.

A címzés elküldése után az adatok következnek. A mester egyszerűen folytatja az órajel impulzusok generálását, és az adatokat az master vagy a slave helyezi az SDA vonalra, attól függően, hogy az R/W bit olvasási vagy írási műveletet jelez-e. Az adatcsomagok száma tetszőleges, és a legtöbb slave eszköz automatikusan növeli a belső regisztert, azaz a későbbi olvasások vagy írások a sorban lévő következő regiszterből származnak.

Az összes adat elküldése után a master állítja le a kommunikációt. A leállítást az SDA vonal 0->1 (alacsonyról magasra) átmenete határozza meg, miután az SCL vonal 0->1 átmenetet mutat, és az SCL magas marad. A normál adatírás közben az SDA-érték nem változhat, ha az SCL magas, hogy elkerüljék a hamis leállási feltételeket [4].

4.11 ESP 8266 (01s) Wi-Fi modul

Ez a modul lehetővé teszi az eszközök számára, hogy vezeték nélküli hálózatokhoz csatlakozzanak, és önálló mikrovezérlőként is működhet, vagy más processzorok Wi-Fi funkcióit támogathatja. Processzora egy 32 bites Tensilica L106 RISC integrál, amely akár 160 MHz-es órajellel működik. A modul rendelkezik 160 KB RAM-mal a programok futtatásához és adatfeldolgozáshoz, valamint akár 16 MB külső flash memóriával a programkód és egyéb adatok tárolásához. Támogatja az IEEE 802.11 b/g/n szabványokat, lehetővé téve a gyors és megbízható vezeték nélküli kapcsolatokat. Számos interfészt támogat, köztük az UART-t. Több GPIO lába van, ami más eszközök csatlakozását biztosítja [5]

A projektben UART kommunikációt használok a modul és az Arduino között. Az Arduino lábai 5 V-os jelet adnak, de az ESP 8266 (01s) Wi-Fi modul 3.3 V-on működik optimálisan. Ennek köszönhetően beépítettem egy feszültségstabilizátort.

5. Építési nehézségek

A fent említett folyamat megvalósításához több tárgy által szerzett tudásra szükség volt (például: klasszikus fizika, digitális hálózatok, programozás alapjai, méréstechnika, villamosságtan, automatikai építőelemek, számítógéphálózatok...).

Az alábbi alfejezetekben szeretném részletesen kifejteni, illetve kielemezni egyes állomásokra lebontva a különböző problémákat és nehézségeket, amit a projekt megépítése során tapasztaltam.

5.1 Első állomás

Az első állomás a kiindulópont, ide kell behelyezni a labdát, ahhoz, hogy elkezdődhessen a folyamat. Mivel 5 darab szenzort használok, ezért megfelelő helyekre kellett őket elhelyeznem. Ebben az esetben, a labdához képest egy korábbi pontra. Ennek legfőbb oka, hogy a transceiver-t és receiver-t rögzítenem kell. Ehhez festőszalag volt számomra a legkézenfekvőbb megoldás.

Ennek hátránya, hogy a festőszalag egy idő után elengedhet, és elmozdulhat vagy a transceiver vagy a receiver, és hibásan fog jelezni.

5.2 Második állomás

A gondolatmenetet folytatva, az ajtó kinyílik és a labda elkezd legurulni az enyhe lejtős szakaszon és beleérkezik egy sík felületű csapóajtóba, miközben áthalad egy szenzoron. Itt számos tervet készítettem és végrehajtottam, mire találtam egy elfogadható koncepciót, mivel amit még használtam az előző fejlesztésben nem működött.

Először egy motorban gondolkodtam, hogy egy fogaskerekes áttéttel működjön a csapóajtó 9:18-hoz. Elkezdtem megvalósítani, de aztán rájöttem, hogy ez túl sok idő célszerszámok nélkül, ezért maradtam a kettő motornál. Ezek egy közös rúdon vannak (egymással szembe fordítva és ellentétes polaritással van bekötve), ami szintén LEGO-ból van, és a rúdra rá van még rögzítve egy nagy kiterjedéssel rendelkező vékony felület.

Az l298N H-bridge modul hűtőbordája gyorsan túl melegszik, ennek enyhítésére, a felhasználható bemenetek bővítésének köszönhetően PWM-et használok.

A csapóajtó rövidesen a labda megérkezése után kifog nyitni egy másik szenzornak köszönhetően, és a labda leesik a következő állomásra.

5.3 Harmadik állomás

A korábbi fejlesztésnél, ez az állomás volt a második legnehezebb része a projektemnek. Az egyik legfőbb kérdés az volt, hogy milyen anyagú legyen a szalag, például: textil, csiszolószövet vagy műbőr. Először az első kettőt próbáltam ki, de ezekre nem igazán tudtam ragasztani úgynevezett bordás felületet (aminek az anyaga LEGO), mivel, ha a motor elindul, és nincs mi megfogja, akkor a labda elmozoghat nem kedvező irányokba. Így a műbőr lett a választás.

A következő kérdés az volt, hogy a motorra ráillesztett rúdra milyen érdes felületet rakjak, hogy tudjam futtatni a szalagot. Először csiszolószövetet akartam erősíteni a rúdra ragasztóval és befőttes gumikkal. Ez nem volt jó döntés, mert elforgott. Ismét a LEGO-t hívtam segítségül, LEGO gumiabroncsokat használtam a probléma megoldására.

Amikor vásároltam a 6 V-os motorokat, úgy véltem, hogy kettő, esetleg három képes lenne meghajtani a futószalagot, de sajnos tévedtem. Be kellett fektetnem egy 12 V-os motorra, ami gond nélkül megtudja hajtani.

A korábbi megbízható fejlesztéseknek köszönhetően, nem kellett hozzá nyúlnom a szalaghoz, csak a csapóajtó és a szalag közé beillesztettem egy szenzort, ami bejelez, ha a csapóajtó nyit és leejti a labdát. A teszteléseknél nem mindig akart bejelezni a szenzor, ezért változtattam az elhelyezésén. Miután leesett a csapóajtón keresztül a labda, egy szenzoron keresztül haladva, ráesik a futószalagra. A futószalagnak a feladata, hogy szállítsa a labdát a liftbe, és mindaddig mozog a szalag míg meg nem érkezett a labda a liftbe, amit a lift aknájában található szenzor érzékel.

5.4 Negyedik állomás

Ezt az állomást módosítottam a legtöbbet. A liftakna aljába és tetejébe egyaránt be kellett építenem

1-1 szenzort, így az egészet le kellett bontanom. Javítottam a lift belső és külső struktúrájában egyaránt. Építés során leesett a motor, így újból rögzítenem kellett. Teszteléskor pedig a vastag cérna elszakadt, és ki kellett cserélni. A liftet egy 12V-os motor hajtja.

A lift kezdeti pontja fent van, majd elkezd lemenni, ha a labda elérte a csapóajtót. A csapóajtó megáll, ha elérte a liftakna alsó szenzorát. Miután a szalag bevitte a labdát a liftbe, az alsó szenzor bejelez, és lekapcsolja a szalagot és elindul a lift felfelé. Majd, ha elérte a felső lift szenzort, akkor lekapcsol, és kezdetét veheti az ötödik lépés.

5.5 Ötödik állomás

Ebben az állomásban van a kilökő szerkezet, ami egy láb kialakítású LEGO kirúgó eszköz. Ha a lift nem jön fel teljesen, akkor a toló nem tudja a labdát kirúgni, ez egy gyakori probléma volt az időzítéses megoldásnál. Az egész lift újraépítésekor át kellett helyeznem. 6V-os motor működteti.

Amennyiben optimálisan működik, a labda kilökődik és elhalad az első állomás szenzoránál, ami visszavezérli alapállapotba a toló szerkezetet, és a számláló egy értékkel megnő. Ha nem nyomtam be a stop gombot és zárja be az ajtót, akkor folytatja a folyamatot a labda (kezd mindent előről).

5.6 Szenzor

A szenzorok bővítésének idején egy komoly problémába ütköztem. A projekthez már korábban rendelkezésre állt egy lézer érzékelő és hozzá egy lézer, ehhez még szükséges volt vásárolnom mindegyikből még négy darabot. Miután megérkezett hozzám, le is teszteltem, hogy működik -e. A tesztelés során azt tapasztaltam, hogy nem működik egyik sem. Sorra vettem a hibalehetőségeket egyesével.

Az első, amit megnéztem az a kód volt. Szoftveres szinten minden rendben volt. Ezt azért is bátran magamban kijelentettem, mivel a korábbi fejlesztésnél már foglalkoztam ilyennel. Így tudtam, hogy hogyan kell megírni a kódot, ahhoz, hogy működésre bírjam.

A következő pont a hardveres rész volt. A bekötés is tökéletes volt. Több órás gondolkodás és

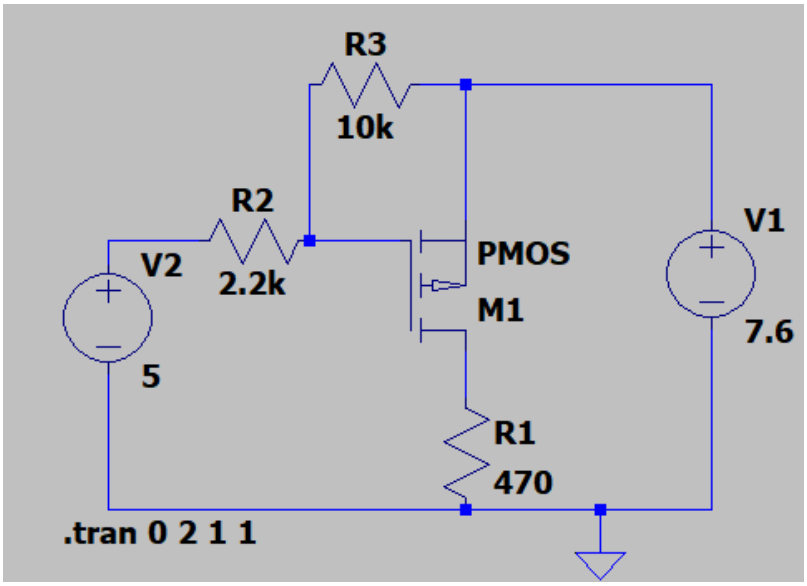
tesztelés után, megtekintettem az elmentett rendelésem, ahol megnéztem a vásárolt érzékelő és lézer adatlapját (datasheet-jét). Az érzékelő csak infravörös tartományban működik, míg a rendelt lézer vörös tartományban (650 nm) működik. Ennek köszönhetően rájöttem a problémára, és ki is cseréltem az érzékelőket, amik a 650 nm hullámhosszon operálnak.

Tesztelés időszakában, a liftakna tetején elhelyezkedő szenzor, a nem megfelelő bekötésnek vagy valamilyen érintkezésnek köszönhetően elégett a fototranzisztor, ezért cserélnem kellett.

5.7 Számláló

A datasheet alapján 20 mA és 5 V szükséges a működtetéshez, de sajnos nem működik az Arduino UNO közvetlen felhasználásával. Viszont egy külső elem alkalmazásával már működik. Ennek eredménye képpen jutottam el, ahhoz a gondolathoz, hogy ha szeretném vezérelni ezt a hét szegmenses kijelzőt, akkor szükségem lesz egy kapcsoló üzemre. Erre a célra a P-MOSFET-et választottam.

Mivel 7 darab szegmenst akarok külön-külön vezérelni, ezért 7 darab MOSFET kell erre a célra. Fontos volt, hogy teljesítmény MOSFET kell, mert az már 5V-os vezérlőjellel is nyitni tud, míg a többi MOSFET esetében ez az érték 15-20 V nagyságú.



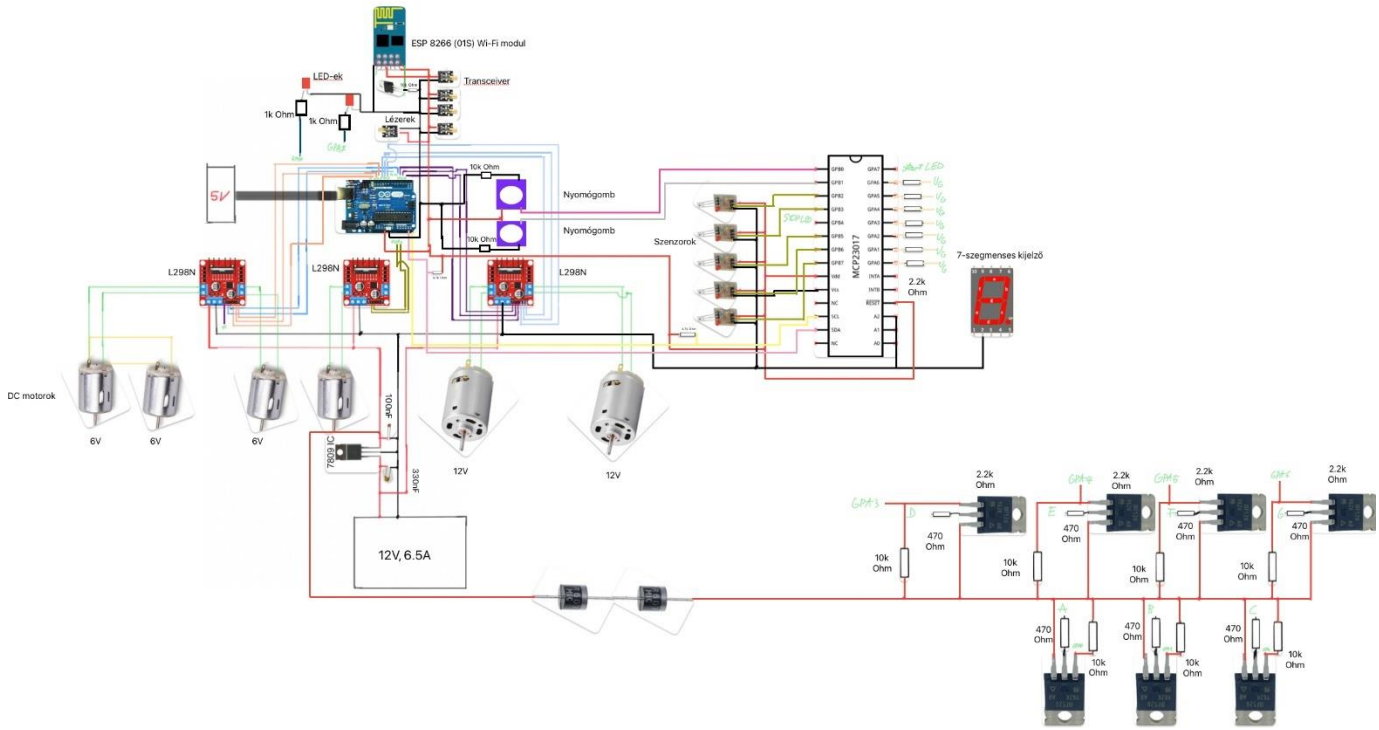
8. ábra. Kapcsolási rajz egy szegmensre.

A *8.ábra* egy kapcsolási rajzot mutat, amit az LTSPICE nevezetű programban állítottam össze. Jól

látható, hogy a V2 az Arduino UNO-t szimbolizálja, ha magas érték van a kimeneten, a 470 Ohm-os terhelés egyik lába a drain-re, a másik láb a 7 szegmens egyikére kapcsolódik. A V1 tápforrásra a Source és bázis osztással a gate csatlakozik. Amennyiben az 5 V jelet biztosít, úgy a MOSFET zár. Míg, ha az Arduino lábára LOW értéket adunk, akkor a MOSFET vezetni fog, teljesen nyitni fog (eléri a voltage treshold-ot).

Tápforrásként egy 9 V-os nem újratölthető tápforrást használtam. A hosszú üzemidőknek köszönhetően lemerült. Ennek hatására, a kívánt feszültséget a 12 V-os tápból, amit egy lineáris feszültségstabilizátorral letranszformáltam, onnan biztosítom.

6. Kód és kábelek bekötése



9. ábra. Teljes kapcsolási rajz.

.

A következőkben a kódolásról és a kábelek bekötéséről fogok beszélni ismételten állomásokra lebontva. Bemutatom, ezek nehézségeit, és hogy milyen módon oldottam meg az elém tárult problémákat.

6.1 Nyomógomb

Az egész projektet összesen kettő nyomógomb működteti. A start gomb megnyomásával kinyitja az ajtót és bekapcsolja a start LED-ket, valamint elment egy értéket. Ez az érték szükséges, ahhoz, hogy aktiválva legyenek a szenzorok. Amennyiben megnyomom a stop gombot bárhol, akkor elment egy értéket, és ha eléri a megadott szenzort, akkor kikapcsol.

Ahhoz, hogy működőképes legyen, az egyik lábát az Arduino egyik bemenetére kell kötni (A kódban szükséges a ’void setup()’ résznél ’INPUT’ néven meghivatkozni). Hardveres fronton eldönthetjük, hogy a Pull-up vagy a Pull-down megoldást válasszuk, ez egy nagyon fontos kérdés, mert nem mindegy, hogy kötjük be. A nyomógombot metódusban kell működtetni.

Ha a Pull-up opciót választjuk, akkor az egyik lábat az Arduino-ba, a szembelévőt az 5 V-ra kell bekötni, úgy, hogy beiktatunk egy 10k Ohm ellenállást, és a harmadik lábat meg földelni kell. A vezérlő alapállapotban magasnak vagy HIGH-nak vagy 1-nek fogja észlelni (ahogy tetszik), ha megnyomjuk, akkor pedig alacsonynak vagy LOW-nak vagy 0-nak észleli.

Pull-down esetén a gomb egyik lábát az Arduino-ba, a szembelévőt a ground-ba (10k Ohm ellenállást beiktatva), és a harmadik lábra az 5 V-ot. Ebben a megoldásban megfordul a beérkező érték, tehát alapállapotban 0, megnyomáskor 1-et kell, hogy kapjunk. A projektben ezt a bekötést választottam, ahogy azt a *9. ábra* is mutatja. A kódban sajnos nagyon nem mindegy, melyiket választjuk, mert akkor úgy kell megírni az adott feltételeket.

A bekapcsolást és kikapcsolást digitális úton is megvalósítottam. Készítettem egy weboldalt, ahol két nyomógomb szerepel, melynek megnyomásával ugyanazt az eredményt érem el, mint analóg verzióban. Ezt ebben a fejezetben az ESP 8266 Wi-Fi modul résznél kifejtem bővebben.

6.2 LED

Egy 3 mm-es lednek és bármely más lednek ugyanaz a működése (fénykibocsátó dióda). A LED két kivezetéssel rendelkezik: anód (pozitív) és katód (negatív). Ahhoz, hogy a LED világítson, megfelelő polaritással kell csatlakoztatni. Az anód a hosszabb láb, amit a pozitív pólusához kell bekötni. A másik

lábat, a katódot a tápfeszültség negatív pólusához kell kötni. Ha ezt megtettük, és megfelelő nagyságú soros előtét ellenállást kötöttünk hozzá, akkor a LED világítani fog, de ha ellentétesen kötöttük be, akkor nem fog világítani a dióda, csak egy irányban engedi az áramot átfolyni. Amennyiben elfelejtünk előtét ellenállást bekötni, és úgy kapcsoljuk rá a tápra, akkor a LED el is durranhat.

6.2.1 Dióda

A korábban említett órás projektemnél egy kis méretű transzformátort használtam, aminek a kimenete is váltóáram volt (AC-AC konverter). A transzformátor az elektromágneses indukción alapul. Az elektromágneses indukció képlete a következő: [6]

$$U = -N\frac{d\Phi}{dt}, \tag{4}$$

ahol, U az indukált feszültség (V), N a tekercs menetszáma, Φ a mágneses fluxus (Wb, weber), és dΦ/dt a mágneses fluxus időbeli változása. A mínuszjel a Lenz-törvényből ered, amely kimondja, hogy az indukált áram mindig olyan irányban folyik, hogy akadályozza a mágneses tér változását, amely létrehozta.

A fent említett váltakozó áram kimenetet át kellett alakítanom egyenárammá, amit egy dióda híddal és két ELKO kondenzátorral oldottam meg.

A diódák olyan félvezető eszközök, amelyek elsősorban egyenirányításra, jelalakításra és védelemre szolgálnak. Néhány dióda típus: egyenirányító dióda, zéner-dióda, schottky-dióda.

Egyenirányító dióda esetében nagy áram- és feszültségtűrés, alacsony feszültségesés (pl. 0,7 V a szilícium, 0,3 V a germánium esetében). AC áram egyenirányítására használják. Ezt a dióda típust használtam én is (1N4007).

Zéner-dióda esetében feszültségstabilizálásra és túlfeszültség-védelemre használják. Ilyen például az 1N4733A.

A schottky-diódát nagy sebességű kapcsolásra használják. Alacsony feszültségesés jellemzi (0.2 V-0.4 V). Ilyen például az 1N5819.

6.3 Első állomás

Már korábban leírtam, hogy egy motort nem jó ötlet közvetlenül egy Arduino-hoz kötni, és ezért van szükség motor driver-re. A H-hídnak hála polaritást tudunk változtatni, amit kód formájában meg is tudunk tenni. Például: Ha az ’A’ kimeneten van a motor, akkor az Arduino-ba be kell kötni az ’A’ logic input egyet és kettőt (*8. ábra*). LI1=HIGH és LI2=LOW vagy LI1=LOW és LI2=HIGH. Ezeket úgynevezett ’digitalWrite()’-ba kell beleírni. Mivel az L298N még a motor sebességének állítását is lehetővé teszi, ezért, ha az Enable ’A’-t bekötjük, és még a kódba beírjuk, hogy ’analogWrite()’, akkor tudjuk módosítani 0-255 kitöltési tényező között. A 0 azt jelenti, hogy a jel mindig ki van kapcsolva (0% kitöltési tényező, tehát nincs feszültség a kimeneten). A 255 azt jelenti, hogy a jel mindig be van kapcsolva (100% kitöltési tényező, tehát maximális feszültség van a kimeneten). A 127 körülbelül 50%-os kitöltési tényező.

Sajnos nem mindegyik állomáson tudom változtatni a sebességet a motoroknak, mivel ezek plusz bemenetet vesznek el, ezért ennél az állomásnál sem használtam (közvetlen van rákötve a tápforrásra, így maximális sebességgel forog). Néhány tesztelés után, megfelelően betudtam állítani a ’delay()’ értékeket (ezeket ms-ban értendők). Rögzítést tekintve egy LEGO alkatrészre ragasztottam pillanatragasztóval. Próbáltam a ragasztószalagot is, de az sajnos nem volt tartós, megbízható megoldás.

6.4 Második állomás

A korábbi fejlesztési állapotban a késleltetések kulcsszerepet játszottak, mivel nem volt a projektemben egy szenzoron kívül több. Ezen állomáson is nagy befolyásoló ereje volt, de ugyanakkor nem is volt megbízható. Mivel voltak olyan szituációk, amikor korábban hajtódott le a csapóajtó.

A jelenlegi fejlesztésemben ezt egy szenzorral orvoslom, amivel az előbb említett incidenst kiküszöbölőm. Miután ráérkezik a labda, egy kicsi idő ráhagyással a csapóajtó leenged, majd visszaáll az eredeti pozíciójába, ha a labda elérte a következő szenzort, ami majd a harmadik állomást (szalag) indítani fogja. Bekötés szempontból fontos, hogy itt 2 motort kötök sorba és egymással szemben, ellentétes polaritással, amit a *8. ábra* is mutat. Továbbá, közös PWM-et használok a terhelésnek

köszönhetően kialakult hő csökkentése érdekében.

6.5 Harmadik állomás

A korábbi fejlesztési állapotban, az Arduino kevés bemenetére és az egyre magasabb költségekre hivatkozva csak egy szenzort tudtam használni, aminek megvoltak a következményei.

Ilyen volt, hogy a szalag a labdát minél lassabban vigye át (PWM), mert előfordulhat, hogy a szenzor nem fogja érzékelni. Ez a sok “delay()”-nek köszönhető az Arduino programban, mivel itt a sorokat, egymás után futtatja le. Mivel egy “while” ciklust használok, a start gomb egyszeri benyomása után történő örökké való labdát szállító ciklus jön létre. Viszont a “while” cikluson belül, ahhoz, hogy a következő feltételre lépjen, be kell a szenzornak jeleznie.

A jelenlegi fejlesztésemben a több szenzor használatát jelöltem ki célul, viszont ehhez több bemenetre volt szükségem. Már akkor elkezdtem kidolgozni a lehetőségeket, hogy ezt milyen metódussal valósítsam meg. Számításba vettem az Arduino Mega és az ESP32 mikrokontrollert is, de végül egy még kedvezőbb megoldást választottam, ami egy I/O modul expander volt. Név szerint az MCP23017. Ennek köszönhetően kettő bemenetért cserébe, kaptam 16 plusz bemenetet, amivel új lehetőségeket eszközölhettem. Ilyen például a több szenzor és a 7 szegmenses kijelző, amit egy számlálóként használok.

Így a szalag nem késleltetésre indul, hanem egy szenzor szól neki, és állítja is majd le.

6.6 Negyedik állomás

A korábbi fejlesztésben, Itt is időzítővel dolgoztam. Viszont, jelenleg a liftakna mindkét pontjában beépített szenzorok segítségével ezt megoldottam.

A kódban egy bizonyos ideig emelkedő értéket valósítottam meg ’for ciklus’ segítségével, amivel a sebességet tudom befolyásolni a PWM-nek köszönhetően. Ez a lift simább mozgását teszi lehetővé, és ezzel kisebb kilengés is jár.

A start gomb megnyomása után, az egyik szenzor szól a liftnek, hogy a labda egy bizonyos ponton van, ezért a lift lemegy a liftakna alsó részébe. Ebben a pontban várja a labdát, hogy beérkezzen. Ha a szenzor jelzett, hogy beérkezett a liftbe a labda, akkor a lift elindul felfelé, egészen addig, míg a felső szenzor nem fog jelezni.

6.7 Ötödik állomás

Ebben az esetben is fontos a PWM használata, mivel a motor által kifejtett erő határozza meg, milyen erővel lökődik ki a labda a liftből. Több tesztelés után, megtaláltam az ideális sebességet.

Akkor lép működésbe, ha a felső szenzor bejelez, mikor a lift megérkezett. Az eredeti pozíciójába, akkor megy, ha a labda, elérte a kiindulás előtti szenzort.

Az egész folyamat kezdődik előről, mindaddig, míg meg nem nyomjuk a stop gombot.

6.8 Számláló

Ha a start benyomása után elhaladt a labda a kiindulás előtti szenzoron, akkor a számláló értéke nulláról egyre módosul, majd kettőre, háromra…a legvégén kilencre. A programban a könnyű kezelés céljából elneveztem a 7 darab bemenetet, és 'if' feltételekkel pedig a LED-ek megfelelő sorrendben való felvilágítással (HIGH) számjegyeket ír ki.

Ha a stop gombot megnyomjuk, akkor lenullázódik az érték. Amennyiben újra elszeretnénk indítani a folyamatot, akkor nincs más teendőnk, csak benyomjuk újra a start gombot, és újra elkezd majd a számláló a feltételeknek megfelelően számolni felfelé.

6.9 ESP 8266 (01S) Wi-Fi modul

Az Arduino-val létrehoztam egy szoftveres soros kommunikációs csatornát. Az Arduino 9600 baud rate-en működik, míg a Wi-Fi modul 19200 baud rate-en. A zavartalan működés érdekében közös baud rate-re hoztam (9600).

A kódban „AT" parancsokat használok, köztük az IP-cím lekérdezését (AT+CIFSR), majd beállítom STA módba. Rácsatlakozok a Wi-Fi hálózatra, többkapcsolatos módot engedélyezek, majd elindítok egy webszervert a 80-as porton. Ez a kezdeti beállítás.

Ha érkezik soros adat, azt egy karakterláncba beolvassa (req). Ahhoz, hogy ezt nyomon

kövessem, a serial monitorra kiiratom. A létrehozott weboldalon lévő start és stop nyomógombhoz hozzárendeltem az ESP-nek kiosztott IP-címet és a soros adatot, amit elküld, ha megnyomom. Ha a kérés „GET/START=ON”, bekapcsol a projekt. Stop esetén „GET/START=OFF”, kikapcsol a projekt. Egyéb esetben törli a Buffer-ből a soros adatokat. Továbbá, ha az ESP megkapta a soros adatot, és teljesítette, akkor küld egy HTTP választ a weboldalnak, ami a gombok színének megváltozását eredményezi. Nem utolsó sorban. a weboldalon található egy számláló, ami a számláló értékeit tölti fel.

A weboldalt a „Visual Studio Code” nevezetű programban csináltam. Kezdetben nem reagált az ESP az elküldött soros adatokra. Egy rövid utánajárást követően rájöttem, hogy csak, akkor látja az ESP, ha live szerveren vagyok. Kommunikáció során nem azonnal reagál, ennek oka a programban lévő időzítők lehetnek.

7. Összefoglalás

Sok időmet igénybe vette ez a projekt, jóval többet, mint amit gondoltam, de ennek köszönhetően sokkal több dologban tájékozottabb lettem.

Jövőbeli fejlesztés terén, mivel nekem egy Arduino UNO mikrokontrollerem van, amiből az ATMEGA328P IC-t el lehet könnyedén távolítani, ezért olcsóbb megoldás lenne, ha külön működtetném (16 MHz kristály, 10k Ohm és 2 darab 22 pF kapacitás szükséges hozzá), mivel egy eredeti UNO körülbelül 12000 forint körül mozog, míg az IC 2400 forint darabja.

Az egyik legfontosabb fejlesztés hardveres fronton lenne. Jobb kábel management alkalmazása és 3D nyomtatott alkatrészek, melyek LEGO alkatrészekkel kompatibilisek.

Továbbá a kommunikáció nem azonnali átvitelét vélhetően a „delay()” késleltetések okozzák a kódban. Ennek megoldására a „millis()” tenné lehetővé, melynek segítségével párhuzamosan lehet futtathatni más funkciót, anélkül, hogy megállítanánk.

Irodalomjegyzék

[1] Berta Miklós, Farzan Ruszlán, Giczi Ferenc, Horváth András*:* *Fizika mérnököknek* (UNIVERSITAS KHT, Győr, 2006), p. 796.

[2] Oláh Ferenc, Rózsa Gábor: *Automatikai építőelemek* Győr-UNIVERSITAS Kht., Győr (2008), p. 374.

[3] Puklus Zoltán: *Teljesítményelektronika* (UNIVERSITAS KHT, Győr, 2007), p. 235.

[4] I2C kommunikáció `https://electro.blog.hu/2020/04/26/i2c_kommunikacio`, 2020

[5] ESP 8266 Wi-Fi Modules `https://www.espressif.com/en/products/modules/esp8266/?`, 2025

[6] Standeisky István: *Elektrodinamika* (UNIVERSITAS KHT, Győr, 2007), p. 363.

Ábrajegyzék

[A1] https://univgyor.hu/978-96398-193-2-0-automatikai-epitoelemek-1

(utolsó látogatás időpontja: 2025. február 3.)

[A2] https://www.emag.hu/oem-motor-meghajto-modul-l298n-ai0016-s190/pd/DJYQ1GMBM/?cmpid=105273&utm_source=google&utm_medium=cpc&utm_campaign=(HU:_Without_Whoop!)_Shopping_Ads_-_3P_No_sales_-_Toys_-__J%C3%A1t%C3%A9kok&utm_content=110383287524&gad_source=1&gclid=Cj0KCQjwna6_BhCbARIsALId2Z3VqiFvwj3meiWaZvrlP1CTCq55KeP2R5Tiz08DdsZ4Mf-oN6lTHFMaAjYNEALw_wcB

(utolsó látogatás időpontja: 2024. október 10.)

[A3] https://tronixstuff.com/2011/08/26/arduino-mcp23017-tutorial/

(utolsó látogatás időpontja: 2025. február 4.)

[A4] https://electro.blog.hu/2020/04/26/i2c_kommunikacio

(utolsó látogatás időpontja: 2025. február 4.)

[A5] https://electro.blog.hu/2020/04/26/i2c_kommunikacio

(utolsó látogatás időpontja: 2025. február 4.)

Mellékletek

1. melléklet

A videó, kód és a weboldal a Google Drive linken keresztül elérhető: https://drive.google.com/drive/folders/1tYnMQGDdrkukyeStoX3bYa3NKIV5Wh8j?usp=sharing

2.43. Kiberbiztonság az okosotthonokban – Honnan tudjuk, hogy tényleg biztonságban leszünk?

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

IPAR 4.0 TECHNOLÓGIÁK

Kiberbiztonság az okosotthonokban – Honnan tudjuk, hogy tényleg biztonságban leszünk?

Csanda Norbert
[redacted]

(GKNB_INTM087)

2024/25/2

Abstract

Az okosotthon egy olyan lakókörnyezet, amelyben az eszközök és rendszerek, például a világítás, fűtés, biztonsági kamerák és háztartási gépek automatizáltan és távolról vezérelhetők internetkapcsolaton keresztül. Az IoT (Internet of Things) technológia lehetővé teszi, hogy ezek az eszközök kommunikáljanak egymással és a felhasználóval, növelve a kényelmet, az energiahatékonyságot és a biztonságot. Mivel az okosotthonok eszközei az internethez csatlakoznak, sebezhetők a kiberfenyegetésekkel szemben, például adatszivárgás, hacker támadások vagy zsarolóvírusok révén. A védekezés érdekében erős jelszavakat és kétlépcsős hitelesítést kell alkalmazni, rendszeresen frissíteni kell a szoftvereket és firmware-t, elkülönített Wi-Fi hálózatot kell használni az IoT-eszközök számára, valamint biztonságos, titkosított kommunikációt kell alkalmazni. Az okosotthonok fejlődése az elmúlt évtizedekben jelentős volt: a 2000-es években megjelentek az első automatizált rendszerek, például a programozható termosztátok, majd a 2010-es években az IoT térnyerésével az eszközök összekapcsolódtak a Wi-Fi és mobilalkalmazások segítségével. A 2020-as évektől kezdve a mesterséges intelligencia-alapú asszisztensek, mint az Alexa és a Google Assistant, fejlett döntéshozatali és predikciós képességekkel bővítik az okosotthonokat. A jövőben nagyobb adatvédelem, 6G hálózatok, fejlettebb automatizáció és önállóan tanuló rendszerek várhatók, amelyek tovább növelik az okosotthonok intelligenciáját és biztonságát.

Az okosotthonok elterjedése jelentősen növelte a felhasználói kényelmet és az automatizáció lehetőségeit, azonban ezzel párhuzamosan új kiberbiztonsági kihívások is megjelentek. Az IoT-eszközök sérülékenységei számos támadási lehetőséget kínálnak, amelyek révén rosszindulatú szereplők illetéktelen hozzáférést szerezhetnek az otthoni hálózatokhoz, személyes adatokhoz, vagy akár fizikailag is veszélyeztethetik az ingatlan, okosotthon biztonságát.

A dolgozat célja, hogy technológiai szemszögből feltárja az okosotthonok leggyakoribb biztonsági kockázatait, beleértve a gyenge hitelesítést, az adatvédelmi problémákat, a hálózati sebezhetőségeket és az IoT-specifikus támadásokat, például a túlterheléses (DDoS) támadásokat és a botnetek térnyerését. Továbbá bemutatja azokat a védelmi stratégiákat, amelyekkel minimalizálhatók ezek a kockázatok, ideértve az erős autentikációs rendszereket, a titkosítási eljárásokat, a behatolásészlelő és anomáliadetektáló megoldásokat, valamint a Zero Trust megközelítés alkalmazását.

A beadandóban kitérek az iparági szabványokra és a jogszabályi megfelelőségre, például a GDPR által támasztott adatvédelmi követelményekre, valamint megvizsgálja az intelligens otthonok biztonságos fenntartásához szükséges kompetenciákat és eszközöket. Összességében egy átfogó elemzést nyújt az okosotthonok kiberbiztonsági helyzetéről, feltárja a lehetséges fenyegetéseket és ismerteti a modern védelmi technológiákat annak érdekében, hogy a felhasználók megbízható és biztonságos otthoni környezetet alakíthassanak ki.

Tartalomjegyzék

Abstract 2
Bevezetés 5
Kiberbeiztonsági problémák a mai okosotthonokban 6
Gyenge hitelesítés és jelszókezelési problémák 6
Elavult szoftverek és firmware-ek 7
Nem biztonságos kommunikációs protokollok 7
Adatszivárgás és adatvédelmi kockázatok 9
Személyes adatok gyűjtése és tárolása 9
Nem megfelelő adatátvitel és tárolás 9
Hálózati sebezhetőségek 9
GDPR és adatvédelmi előírások az okosotthonokban 11
Az okosotthonokban kezelt személyes adatok 11
A legnagyobb adatvédelmi kockázatok az okosotthonokban 11
Védekezési lehetőségek és ajánlások 11
Ipari szabványok az okosotthonok biztonságában 12
ISO/IEC 27001 és IoT-biztonság 12
ETSI EN 303 645 12
NIST Cybersecurity Framework 12
Biztonsági ajánlások az okosotthonok számára 12
Erős hitelesítési és hozzáférés-kezelési eljárások 12
Titkosítás és biztonságos kommunikáció 12
Hálózati védelem és szegmentáció 13
Rendszeres frissítések és patch management 13
Adatvédelem és megfelelés 13
Hálózati architektúrák és csatlakozási módok 14
Hálózati architektúrák 14
Központosított architektúra 14
Decentralizált vagy mesh architektúra 14
Hibrid architektúra 15
Csatlakozási módok 15
WiFi 15
Bluetooth 15
Zigbee és Z-Wave 15
Ethernet 17
Hálózati szegmentáció 18

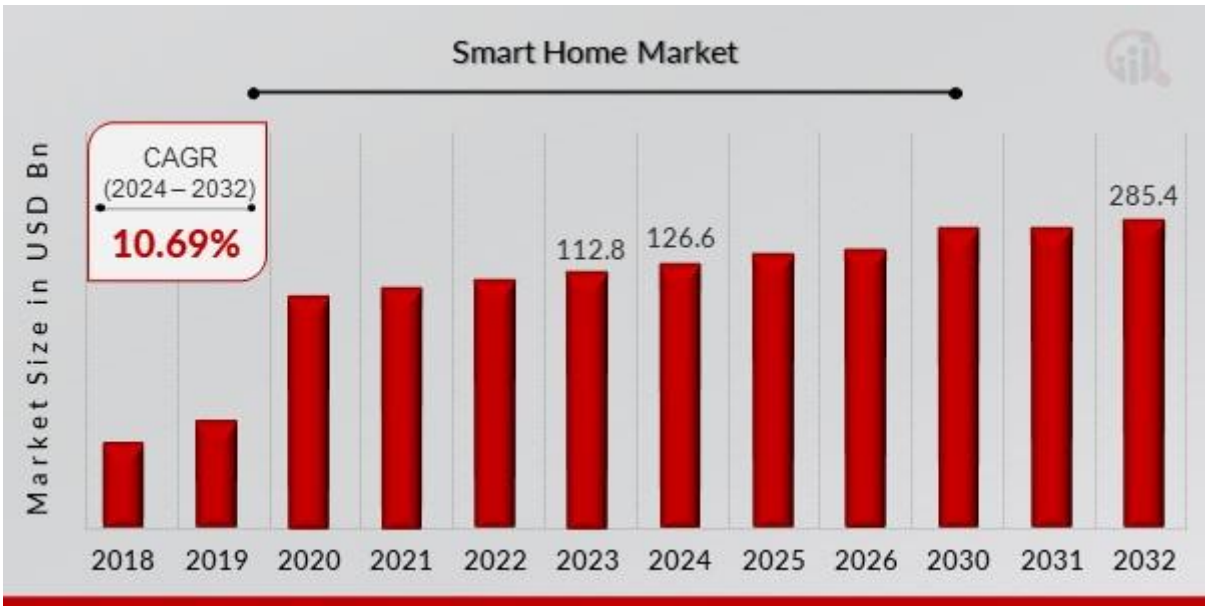
Hálózati szegmentáció jelentősége 18
Behatolásérzékelő és anomáliadetektáló rendszerek 20
Behatolásérzékelő rendszerek (IDS) az okosotthonokban 20
Anomáliadetektáló rendszerek az IoT-eszközök biztonságában 20
Gyakori fenyegetések, amelyeket az IDS és ADS felismerhet 21
IDS és ADS rendszerek telepítése okosotthonokban 21
Tűzfalak az okosotthonokban 23
Milyen fenyegetéseket képes szűrni a tűzfal? 23
Tűzfalak típusai 23
Port Forwarding és UPnP kockázatai az okosotthonokban 25
Port Forwarding (Porttovábbítás) kockázatai 25
Támadási felület növekedése 25
Gyenge hitelesítés és brute-force támadások 25
Man-in-the-Middle (MitM) támadások és adatlopás 25
Botnetekbe való bevonás 26
Universal Plug and Play (UPnP) kockázatai 26
Automatikus portmegnyitás és kontrollálhatatlan hozzáférés 26
Külső támadók kihasználhatják az UPnP sérülékenységeit 26
IoT-eszközök és rosszindulatú szoftverek 26
Hogyan csökkenthetők ezek a kockázatok? 26
Port Forwarding helyett biztonságos alternatívák használata 26
Az UPnP letiltása, ha nincs rá szükség 27
Zero Trust megközelítés alkalmazása okosotthon-hálózatokban 28
Túlterheléses támadások (DDoS) és botnetek 29
Túlterheléses támadások 29
Botnetek 30
Energetikai rendszerek veszélyeztetése 31
Milyen eszközök kompetenciák kellenek egy okosotthon biztonságos fenntartásához? 32
Szükséges eszközök 32
Szükséges kompetenciák 32
Szubjektív vélemény összegzésként 34
Források 35

Bevezetés

Az okosotthonok térnyerése forradalmasította a mindennapi életünket, kényelmesebbé és hatékonyabbá téve otthonainkat. Az intelligens eszközök – legyen szó okoszárakról, kamerákról, termosztátokról vagy hangvezérelt asszisztensekről – mind összekapcsolódnak az interneten keresztül, és a felhasználók számára eddig elképzelhetetlen vezérlési lehetőségeket biztosítanak. Azonban ez a digitalizált környezet új kihívásokat is szül, különösen a kiberbiztonság területén.

Egy nemrégiben végzett kutatás szerint az okosotthonokban használt IoT eszközök több mint 98%-a legalább egy kritikus biztonsági rést tartalmaz, amelyet egy rosszindulatú támadó kihasználhat. Ez azt jelenti, hogy egy nem megfelelően védett intelligens otthon nemcsak a tulajdonosok személyes adatait és privát szféráját veszélyeztetheti, hanem akár fizikailag is fenyegetést jelenthet – például egy feltört okoszár révén a támadók akadálytalanul bejuthatnak az otthonba.[1]

Ettől függetlenül az okosotthonok piaca várhatóan 2024-es 126,67 milliárd USD-ról 2032-re 285,4 milliárd USD-ra növekszik, éves átlagos növekedési rátája 10,69% lesz az előrejelzési időszakban (2024–2032). Emellett az okosotthon-piac mérete 2023-ban 112,8 milliárd USD volt. Az energiahatékonyság és az alacsony szén-dioxid-kibocsátás a piac növekedését elősegítő legfontosabb hajtóerők.[2]



1. ábra- Okosotthon piac mérete és várható mérete (USD Milliárdban) - https://www.marketresearchfuture.com/reports/smart-home-market-974

Kiberbeiztonsági problémák a mai okosotthonokban

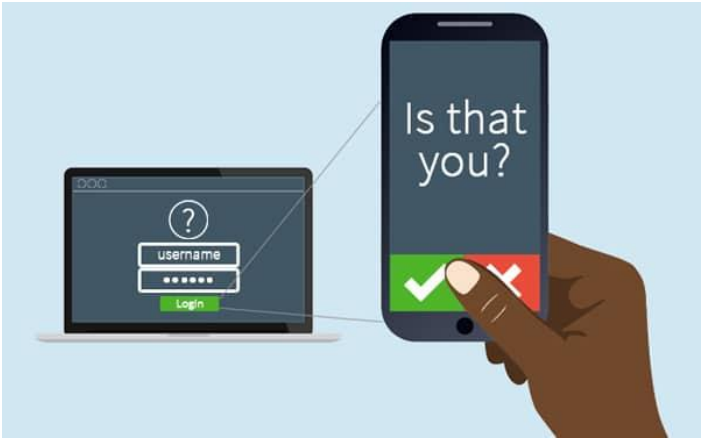
A lakosság nagy része, aki már okosotthonban él, még most sincs tisztában azzal milyen biztonsági fenyegetéseknek vannak kitéve az otthonukban lévő internethez kapcsolódó okoseszközök miatt. Ezek az eszközök alapvetően remek kényelmet és hatékonyságot biztosítanak, de emellett sajnos számos kiberbiztonsági kihívást is felvetnek.

Gyenge hitelesítés és jelszókezelési problémák

Az emberek hatalmas része ugyanazon jelszót használja rengeteg eszközhöz, fiókhoz vagy alkalmazáshoz, ami ráadásul sok esetben nem is túl nehezen kitalálható. Hozzátartozók neveit, születési dátumokat tartalmaznak speciális karakterek nélkül.

Túlnyomó többségben viszont az okoseszközöket, amiket megvásárol a végfelhasználó egy alapértelmezett jelszó véd, aminek nem szentelnek időt vagy jelentőséget, hogy megváltoztassák. A támadók ebben az esetben nagyon könnyen hozzá tudnak férni az adott eszközhöz és az azon átfutó vagy tárolt adatokhoz. Lehetőséget adva a támadóknak arra, hogy nyomon kövessék az eszközök használati szokásait, például mikor nincs otthon a tulajdonos.[3] [4]

Két faktoros hitelesítést sem gyakran alkalmaznak az okoseszközöknél. A nagyobb gyártók, mint például Google Nest, Amazon Alexa vagy Apple Homekit kínálnak lehetőséget a két faktoros hitelesítésre, de a felhasználók nem élnek ezzel sok esetben. Ha a gyártó a 2FA kötelezővé tenné, akkor sokkal biztonságosabb lenne a mai okosotthonok nagy része. Ezzel szemben a helyi hálózaton keresztül működő IoT-eszközök (pl. okosizzók, szenzorok) általában nem támogatják a 2FA-t, mivel a vezérlésükhöz nincs szükség felhőalapú bejelentkezésre.



2. ábra – Két faktoros hitelesítés -https://netgaincloud.com/what-is-two-factor-and-multi-factor-authentication-and-why-do-i-need-it/

Elavult szoftverek és firmware-ek

A rendszeres frissítések hiánya miatt az eszközök sebezhetőek maradnak az ismert biztonsági rések ellen. A felhasználók gyakran nem telepítik a legújabb frissítéseket, így az eszközök védtelenek maradnak.

Egy lengyelországi élményfürdőt üzemeltető cég figyelmeztetésben részesült az adatvédelmi hatóság által, mivel elavult informatikai eszközöket és szoftvereket használtak, ami adatvédelmi problémához vezetett. Az elavult szoftverek használata miatt bekövetkező incidensek gyakran elkerülhetők lennének, ha az adatkezelők megfelelő figyelmet fordítanának a naprakész verziók használatára. [5]

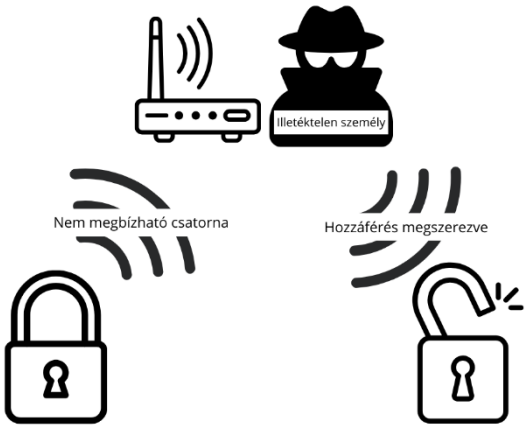
A megelőző intézkedések közé tartozik, hogy az eszközök szoftverét és firmware-ét rendszeresen frissíteni kell, mivel ez alapvető a biztonsági rések bezárása érdekében. Az automatikus frissítések engedélyezése szintén hasznos lehet, mivel így biztosítható, hogy az eszközök mindig a legújabb biztonsági javításokkal rendelkezzenek. Továbbá, a felhasználóknak és rendszergazdáknak folyamatosan figyelemmel kell kísérniük a biztonsági híreket és értesítéseket, hogy időben értesüljenek az újonnan felfedezett sebezhetőségekről és a hozzájuk tartozó frissítésekről**.**Az elavult szoftverek és firmware-ek használatának elkerülése, valamint a rendszeres frissítések alkalmazása kulcsfontosságú az okosotthonok biztonságának fenntartásában. [6]

Nem biztonságos kommunikációs protokollok

A kiberbiztonság szempontjából az okosotthonok esetében is a nem biztonságos kommunikációs protokollok használata jelentős kockázatot jelent. Ezek a protokollok, mint például a HTTP (Hypertext Transfer Protocol), az FTP (File Transfer Protocol) vagy a Telnet, titkosítatlan adatátvitelt tesznek lehetővé, ami azt jelenti, hogy a hálózati forgalmat figyelő illetéktelen személyek könnyen hozzáférhetnek a szenzitív adatokhoz. Az MQTT (Message Queuing Telemetry Transport) egy gyakran alkalmazott protokoll az IoT-eszközök esetében, de ha a felhasználók nem állítanak be megfelelő hitelesítést, a támadók könnyen hozzáférhetnek az eszközök által továbbított adatokhoz. 2023-ban egy kutatócsoport több ezer nyilvános MQTT-brókert azonosított, amelyek jelszó nélkül elérhetőek voltak, így bárki hozzáférhetett a privát okosotthon-eszközök adataihoz.[7]

A biztonságosabb alternatívák, mint a HTTPS (Hypertext Transfer Protocol Secure) vagy az SFTP (SSH File Transfer Protocol), titkosítást alkalmaznak, ami megvédi az adatokat a lehallgatástól. Az okosotthonok gyártóinak és felhasználóinak is kiemelt figyelmet kell fordítaniuk a biztonságos kommunikációs protokollok használatára, valamint az eszközök rendszeres frissítésére, hogy minimalizálják a biztonsági kockázatokat.

Az okoszárak esetében a sérülékeny kommunikáció jelenti az egyik fő problémát. Ha az eszköz Wi-Fi-n vagy Bluetooth-on keresztül kommunikál, a nem megfelelően titkosított kapcsolat lehetővé teszi a támadók számára, hogy lehallgassák vagy manipulálják a jeleket, ezáltal távolról feloldva a zárat vagy megváltoztatva annak beállításait. Emellett az okoszárak szoftverei, mint minden szoftver, tartalmazhatnak biztonsági réseket, amelyeket a hackerek kihasználhatnak a hozzáférés megszerzésére. A felhőalapú szolgáltatások használata további kockázatot jelent, mivel a felhőszolgáltatás biztonságának sérülése esetén a támadók hozzáférhetnek a felhasználók adataihoz, beleértve a zárak állapotát és a hozzáférési naplókat. Végül, a gyenge vagy alapértelmezett jelszavak használata jelentősen megkönnyíti a hackerek dolgát. [8] [9]



3. ábra – Okoszár feltörése – Saját szerkesztés

A hőmérséklet-szabályozók esetében az adatgyűjtés és a magánélet védelme kerül előtérbe. Az okostermosztátok, például a Nest, képesek tanulni a felhasználók napi rutinját és ennek alapján optimalizálni a fűtési és hűtési rendszert. Egy támadó számára ez az információ rendkívül értékes, mivel egy adatszivárgás esetén kiderülhet, hogy mikor nincs otthon senki, ami betörési kockázatot jelent. A hálózati sebezhetőségek szintén problémát jelentenek, mivel a hőmérséklet-szabályozók az otthoni hálózathoz kapcsolódnak, így a hackerek ezen keresztül is bejuthatnak a rendszerbe, és akár más okosotthon-eszközöket is vezérelhetnek. Ezenkívül az okos hőmérséklet-szabályozók részt vehetnek elosztott szolgáltatásmegtagadási (DDoS) támadásokban. [10]

Adatszivárgás és adatvédelmi kockázatok

A mai IoT eszközökön az adatok áramlása korántsem biztonságos, hiszen egy 2019-es tanulmány szerint a hálózati forgalmuknak az 90%-a titkosítatlanul halad át az interneten, ami a támadók számára tálcán kínálja a lehetőséget, hogy megszerezzenek érzékeny vagy személyes adatokat. [11]

Személyes adatok gyűjtése és tárolása

Az okosotthonokban használt IoT eszközök számos adatvédelmi és adatszivárgási kockázatot rejtenek magukban, hiszen különböző típusú adatokat rögzítenek és tárolnak. Az egyik ilyen adattípus például a biometrikus adatok. Ezek olyan adatok, amelyek lehetővé teszik egy személy azonosítását. Az ujjlenyomatok, arcfelismerési minták vagy az írisz-szkennelés mind ide tartozik, amit akár mobiltelefonok is használnak.

Az okoshangszórók (Amazon Echo, Google Nest) folyamatosan figyelik a környezetüket, hogy reagáljanak a felhasználó által adott parancsokra. 2019-ben kiderült, hogy az Amazon alkalmazottjai manuálisan is meghallgatták a felhasználók által folytatott beszélgetéseket, a rendszer fejlesztése érdekében, anélkül, hogy a tulajdonosok, felhasználók tudtak volna róla. [12]

Több népszerű okosotthon-eszköz, például okos kamerák és mozgásérzékelők, titokban megosztották a felhasználók földrajzi helyzetét a gyártókkal és harmadik felekkel. Ezeket az esetek egy átlag felhasználó sok esetben nem veszi komolyan, pedig, ha ez rossz kezekbe kerül, akkor az egy lehetséges bűncselekmény előszele lehet. [13]

Nem megfelelő adatátvitel és tárolás

Az egyik legnagyobb veszélyt a korábban is említett adatok titkosítatlan vagy gyenge titkosítással történő továbbítása és tárolása jelenti. Ha egy okosotthon-eszköz nem használ biztonságos adatátviteli protokollokat, akkor az adatok könnyen lehallgathatók és módosíthatók lehetnek. Továbbá az eszközök gyakran kapcsolódnak harmadik fél szolgáltatásokhoz, például hangasszisztensekhez vagy felhőalapú tárolókhoz, amelyek szintén adatvédelmi kockázatot hordoznak. Az ilyen szolgáltatások gyakran nem egyértelműek abban a tekintetben, hogy pontosan hogyan kezelik a felhasználói adatokat, és milyen módon biztosítják azok védelmét.

Hálózati sebezhetőségek

A hálózati sebezhetőségek szintén gyakori problémát jelentenek az okosotthonokban. A legtöbb okosotthon-eszköz az adatokat nem helyben tárolja, hanem külső szervereken. A nem megfelelően védett Wi-Fi hálózatok, a gyenge jelszavak és a helytelen hálózati konfigurációk mind-mind növelik a

kockázatot. A wifi kapcsolatot a WPA2-es titkosítási szabvány segítségével teszik biztonságosabbá a gyártók. Már 2017-ben kiderült, hogy ez a szabvány nem annyira biztonságos, hiszen brute force támadásokkal feltörhető. Egy biztonsági konferencián demonstrálták, hogy egy megfelelő eszközzel mindössze 10 perc alatt feltörhető egy gyenge jelszóval védett WPA2 hálózat. Ha egy támadó bejut a helyi hálózatba, könnyen hozzáférhet az eszközökhöz, és akár érzékeny adatokat is megszerezhet. Ezen kívül a felhasználói tudatosság hiánya is nagyban hozzájárul az adatszivárgásokhoz. Sokan nincsenek tisztában azzal, hogy milyen adatokat gyűjtenek róluk az eszközök, és nem fordítanak kellő figyelmet az adatvédelmi beállítások megfelelő konfigurálására. Példa lehet egy lehetséges adatszivárgásra, hogy egy okoscsengő, ami képet is rögzít az a felhasználók által már használt csengők videófelvételeit nyilvánosságra hozza.[14]

GDPR és adatvédelmi előírások az okosotthonokban

Az okosotthonok egyre több adatot gyűjtenek és dolgoznak fel a felhasználókról, ami komoly adatvédelmi kihívásokat vet fel. Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) határozza meg azokat az adatvédelmi követelményeket, amelyeket az okosotthonokban használt IoT-eszközök gyártóinak, szolgáltatóinak és a felhasználóknak is figyelembe kell venniük.

Az okosotthonokban kezelt személyes adatok

Az okosotthonok által gyűjtött adatok közé tartoznak például a felhasználói adatok, mint név, e-mail cím, telefonszám, bejelentkezési adatok, eszközhasználati adatok, például világítási szokások, hőmérsékleti beállítások, biztonsági kamerák felvételei, helymeghatározási adatok, mint GPS-adatok és Wi-Fi kapcsolódási pontok, valamint hang- és videófelvételek, például a hangvezérelt asszisztensek által rögzített beszélgetések. Mivel ezek az adatok személyes vagy akár különleges kategóriájú adatok is lehetnek (például biometrikus adatok), a GDPR előírásainak megfelelő védelmi intézkedésekre van szükség. [15]

A legnagyobb adatvédelmi kockázatok az okosotthonokban

A GDPR előírásai alapján az okosotthonokat üzemeltető vállalatoknak biztosítaniuk kell az adatminimalizálást, ami azt jelenti, hogy csak a szükséges adatokat lehet gyűjteni és tárolni. Az adatkezelés során az átláthatóság és a tájékoztatás elengedhetetlen, a felhasználóknak egyértelműen tájékoztatást kell kapniuk arról, hogy milyen adatokat gyűjtenek, és mire használják fel azokat. Emellett az adatkezeléshez egyértelmű és aktív hozzájárulás szükséges, amelyet a felhasználók bármikor visszavonhatnak. A felhasználók jogait is biztosítani kell, például kérhetik adataik más rendszerbe történő átvitelét, valamint bármikor hozzáférhetnek saját adataikhoz.[15]

Védekezési lehetőségek és ajánlások

Az adatbiztonság érdekében elengedhetetlen a megfelelő titkosítás alkalmazása, az adatok tárolása és továbbítása során végpontok közötti titkosítással. Emellett fontos a hálózati biztonság növelése is, például a hálózati szegmentációval és tűzfalak alkalmazásával az eszközök közötti biztonságos kapcsolat fenntartásához. Az adatkezelési beállításokat rendszeresen felül kell vizsgálni, és a felhasználóknak ellenőrizniük kell, hogy mely alkalmazások és szolgáltatások férnek hozzá az adataikhoz. Az IoT-eszközöket rendszeresen frissíteni kell, hogy védelmet nyújtsanak az újonnan felfedezett biztonsági résekkel szemben.[16]

Ipari szabványok az okosotthonok biztonságában

ISO/IEC 27001 és IoT-biztonság

Az ISO/IEC 27001 az egyik legszélesebb körben alkalmazott információbiztonsági szabvány, amely meghatározza az információvédelmi irányítási rendszerek (ISMS) kereteit. Az okosotthonok esetében ez a szabvány segít a kockázatelemzésben, az adatvédelem biztosításában és az illetéktelen hozzáférések elleni védelemben.[17]

ETSI EN 303 645

Az Európai Távközlési Szabványügyi Intézet (ETSI) által kidolgozott ETSI EN 303 645 szabvány az IoT-eszközök minimális biztonsági követelményeit határozza meg. Tartalmazza például az alapértelmezett jelszavak tiltását, a szoftverfrissítések biztosítását és a biztonságos adatkezelést. Ez különösen fontos az okosotthonok számára, hiszen az IoT-eszközök gyakran válnak kibertámadások célpontjává.[18]

NIST Cybersecurity Framework

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) kidolgozta a Cybersecurity Framework-et, amely iránymutatásokat nyújt az IoT-biztonság kezelésére. Ez a keretrendszer öt alapvető pillérre épül: azonosítás, védelem, észlelés, válaszadás és helyreállítás. Az okosotthonok esetében ez a megközelítés segít az eszközök és a hálózatok védelmében.[19]

Biztonsági ajánlások az okosotthonok számára

Erős hitelesítési és hozzáférés-kezelési eljárások

Az ipari ajánlások szerint az IoT-eszközök esetében erős hitelesítési mechanizmusokat kell alkalmazni. Az egyedi és erős jelszavak, a kéttényezős hitelesítés (2FA), valamint a biometrikus azonosítás segíthet csökkenteni a jogosulatlan hozzáférések kockázatát.[20]

Titkosítás és biztonságos kommunikáció

A TLS (Transport Layer Security) és az AES (Advanced Encryption Standard) titkosítási protokollok alkalmazása elengedhetetlen az adatok védelméhez. Az okosotthonokban az eszközök közötti kommunikáció titkosítása minimalizálja az adatszivárgás lehetőségét.[21]

Hálózati védelem és szegmentáció

A hálózati szegmentáció olyan gyakorlat, amely elkülöníti az IoT-eszközöket az otthoni hálózat többi részétől. Például az IoT-eszközöket egy külön Wi-Fi hálózatra helyezve csökkenthető a támadási felület. A tűzfalak és behatolásészlelő rendszerek (IDS/IPS) használata szintén javasolt.[20]

Rendszeres frissítések és patch management

Az ipari ajánlások kiemelik a szoftverek és firmware-ek rendszeres frissítésének fontosságát. A sebezhetőségek időben történő javítása jelentősen csökkentheti a támadások kockázatát.[20]

Adatvédelem és megfelelés

Az okosotthonok esetében különös figyelmet kell fordítani a felhasználói adatok védelmére. A GDPR előírja az átlátható adatkezelést és a felhasználói jogok biztosítását. A gyártóknak be kell építeniük az adatvédelem alapelveit (privacy by design) az okosotthon-rendszerekbe.[22]

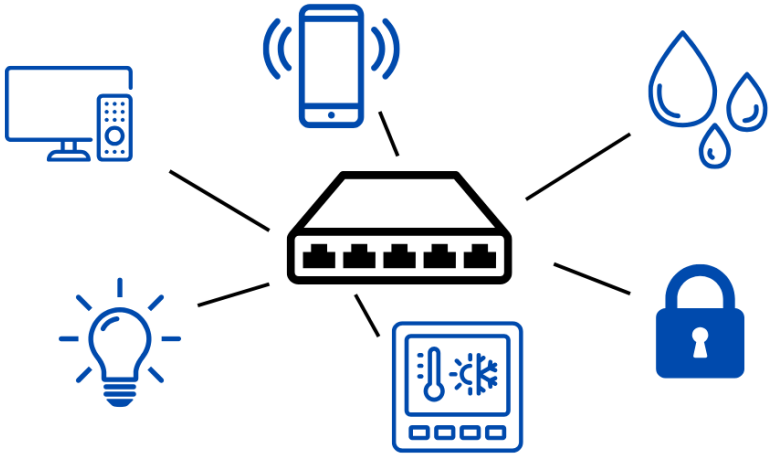
Hálózati architektúrák és csatlakozási módok

Hálózati architektúrák

Az okosotthonok világában a hálózati architektúra kulcsfontosságú szerepet játszik a rendszer hatékony és megbízható működésében. A hálózat felépítése alapvetően meghatározza, hogy az eszközök hogyan kommunikálnak egymással, és milyen mértékben képesek együttműködni.

Központosított architektúra

A központosított architektúra egy olyan modell, ahol egyetlen központi egység, például egy hub vagy gateway irányítja az összes okosotthon-eszköz közötti kommunikációt. Ez a megközelítés egyszerűsíti a hálózat kezelését, mivel minden eszköz a központi egységhez csatlakozik, és azon keresztül kommunikál. Ugyanakkor ez a megoldás egyetlen meghibásodási pontot is jelent, mivel a központi egység kiesése az egész rendszer működését befolyásolja.[23]



4. ábra – Központosított hálózati architektúra – Saját szerkesztés

Decentralizált vagy mesh architektúra

Ezzel szemben a decentralizált, vagy mesh architektúra esetében az eszközök közvetlenül egymással kommunikálnak, hálót alkotva. Ez a megközelítés növeli a hálózat megbízhatóságát, mivel az adatforgalom több útvonalon is áramolhat. Ha egy eszköz meghibásodik, a többi eszköz továbbra is képes kommunikálni egymással. A Zigbee és a Z-Wave protokollok gyakran használják ezt az architektúrát, mivel ideálisak az alacsony energiafogyasztású, nagy számú eszközt kezelő okosotthonokhoz.[23]

Hibrid architektúra

A hibrid architektúra a központosított és decentralizált megoldások előnyeit ötvözi. Ebben a modellben bizonyos eszközök a központi egységhez csatlakoznak, míg mások közvetlenül egymással kommunikálnak. Ez a megközelítés rugalmasságot és megbízhatóságot biztosít, lehetővé téve a felhasználók számára, hogy a legmegfelelőbb megoldást válasszák az adott igényeikhez.[23]

Csatlakozási módok

A megfelelő csatlakozási mód kiválasztása kulcsfontosságú a rendszer hatékony és megbízható működéséhez.

WiFi

A Wi-Fi a legelterjedtebb vezeték nélküli technológia, amely nagy sávszélességet biztosít, így ideális az olyan eszközök számára, amelyek nagy mennyiségű adatot továbbítanak, például kamerák vagy okos TV-k. A Wi-Fi hálózatok biztonsága a korábban említett megfelelő titkosítás beállításával növelhető, ami elengedhetetlen a személyes adatok védelme érdekében.[23]

Bluetooth

A Bluetooth egy rövid hatótávolságú vezeték nélküli technológia, amely alacsony energiafogyasztású, így ideális az olyan eszközök számára, amelyek kis mennyiségű adatot továbbítanak, például okos zárak vagy hőmérséklet-szabályozók. A Bluetooth technológia előnye, hogy egyszerűen beállítható és használható, de a hatótávolsága korlátozott.[23]

Zigbee és Z-Wave

A Zigbee és a Z-Wave alacsony energiafogyasztású mesh hálózati protokollok, amelyeket kifejezetten okosotthonokhoz terveztek. Ezek a protokollok megbízható és biztonságos kommunikációt biztosítanak, és képesek nagy számú eszközt kezelni. A mesh hálózatok előnye, hogy az eszközök közvetlenül egymással kommunikálnak, így a hálózat megbízhatósága növekszik.

A Zigbee eszközök nagyon kevés energiát használnak, ezáltal az akkumulátorral működő eszközök akár több évig is működnek egyetlen töltéssel. A Zigbee eszközök a mesh hálózatnak köszönhetően képesek egymás jeleit továbbítani. Ha esetleg egy eszköz meghibásodik, akkor a hálózaton egyből új útvonalat keresnek, annak érdekében, hogy fenn tudják tartani a kommunikációt egymás közt. Többféle márka is képes kommunikálni egymással (pl.: Philips, Samsung). A Zigbee eszközök 128 bites AES titkosítást használnak, ami a lehallgatás ellen nagyon erős védelem. Hátrányai közé tartozik a kis adatátviteli sebesség, tehát nagy mennyiségű adat áramlása esetén nem optimális. A Zigbee a 2,4GHz-es frekvenciát használja, amit a WiFi vagy a Bluetooth is, ezért hajlamos lehet a jeleket zavarni. Hatótávolsága megközelítőleg 10-20 méter.

A Z-Wave a Zigbee-vel szemben a 800-900 MHz-es tartományt használja, így kevésbe áll fenn az interferencia esélye. A 30 méteres hatótáv, amire ezek az eszközök képesek, több mint a Zigbee esetén. Ugyanakkor a Z-Wave is rendkívül alacsony energiát fogyaszt. Kevesebb kompabilitási probléma áll fenn ezt a technológiát használó eszközök esetén, mert szigorúan szabályozott szabványt használ. Egy Z-Wave hálózat maximum 232 eszközt képes kezelni, ami egy egyszerű okosotthonban jelen pillanatban kevés esetben okoz problémát. A legnagyobb hátránya a Z-Wave-nek, hogy még alacsonyabb az adatátviteli képessége, mint a Zigbee-nek. [24] [25]

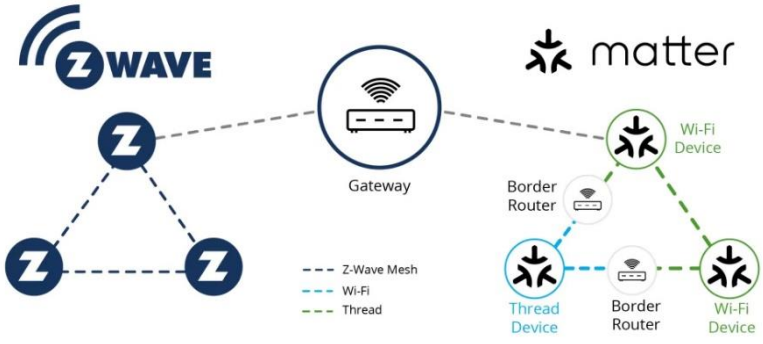
Matter

A Zigbee és a Z-Wave mellett egyre nagyobb szerepet kap a Matter, amely egy új generációs, nyílt forráskódú, IP-alapú kommunikációs protokoll, és célja, hogy egységesítse az okosotthon-ökoszisztémák közötti kapcsolatokat. A protokoll fejlesztését a Connectivity Standards Alliance (CSA) koordinálja, több nagyvállalat – köztük az Apple, Google, Amazon és Samsung – együttműködésével.

A Matter legnagyobb előnye az interoperabilitás, vagyis az, hogy a különböző gyártók eszközei zökkenőmentesen képesek kommunikálni egymással, függetlenül attól, hogy melyik okosotthon-platformot (pl. Apple HomeKit, Google Home, Alexa) használják. A Matter protokoll IP-alapú működése révén könnyen integrálható a meglévő Wi-Fi, Ethernet és Thread hálózatokba. A Thread egy különösen fontos alacsony energiafogyasztású mesh hálózati technológia, amely megbízható, skálázható és biztonságos kapcsolódást biztosít a Matter-kompatibilis eszközök számára.

A Matter emellett end-to-end titkosítást, hitelesített eszközcsatlakozást és biztonságos adatkezelést kínál, továbbá támogatja a helyi (felhőfüggetlen) vezérlést, ami nagyobb adatvédelmet és gyorsabb válaszidőt biztosít.

Első hivatalos verziója (Matter 1.0) 2022 októberében jelent meg, és már több száz tanúsított eszköz érhető el a piacon, a világ vezető gyártóitól.[26] [27]



5. ábra – Z-Wave és Matter az okosotthonban - https://okosotthonblog.hu/hirek/a-z-wave-es-a-matter-betekintes-a-z-wave-szovetseg-terveibe/

Ethernet

Az Ethernet egy vezetékes kapcsolat, amely a legstabilabb és leggyorsabb adatátvitelt biztosítja. Ez a csatlakozási mód olyan eszközök esetén alkalmazható, ahol a sebesség és stabilitás kulcsfontosságú, például hálózati tárolók vagy nagy teljesítményű számítógépek esetén.

A hálózati architektúra kiválasztása és a csatlakozási módok kiválasztásakor figyelembe kell venni az okosotthon eszközeinek típusát, az elvárt teljesítményt, a hatótávolságot és a biztonsági követelményeket. A megfelelő csatlakozási mód biztosítja, hogy az eszközök zökkenőmentesen működjenek együtt, és az okosotthon hatékonyan szolgálja a felhasználók igényeit.[23]

Az okosvilágítás, például az okosizzók és okoslámpák, leggyakrabban Wi-Fi-n vagy Zigbee/Z-Wave-en keresztül csatlakoznak, és applikációval vezérelhetők. Az okos termosztátok, Wi-Fi-n keresztül kapcsolódnak, lehetővé téve a távoli vezérlést és a kommunikációt más eszközökkel. Az okos biztonsági rendszerek, beleértve az okoskamerákat és mozgásérzékelőket, Wi-Fi-n vagy Etherneten keresztül csatlakoznak, értesítéseket küldve és távoli megfigyelést biztosítva. Az okos háztartási gépek, mint a hűtőszekrények és mosógépek, Wi-Fi-n vagy Bluetooth-on keresztül csatlakoznak, értesítéseket küldve és távolról is vezérelhetők. Az okos zárak Bluetooth-on, Wi-Fi-n vagy Zigbee/Z-Wave-en keresztül kommunikálnak, lehetővé téve a kulcs nélküli belépést és a belépési események naplózását. Például egy okosizzó Wi-Fi-n csatlakozik, és applikációval vezérelhető, egy okos termosztát Wi-Fi-n automatikusan szabályozza a hőmérsékletet, egy okos kamera Wi-Fi-n távoli videó streamelést biztosít, és egy okos zár Bluetooth-on kulcs nélküli nyitást tesz lehetővé. [25]

Hálózati szegmentáció

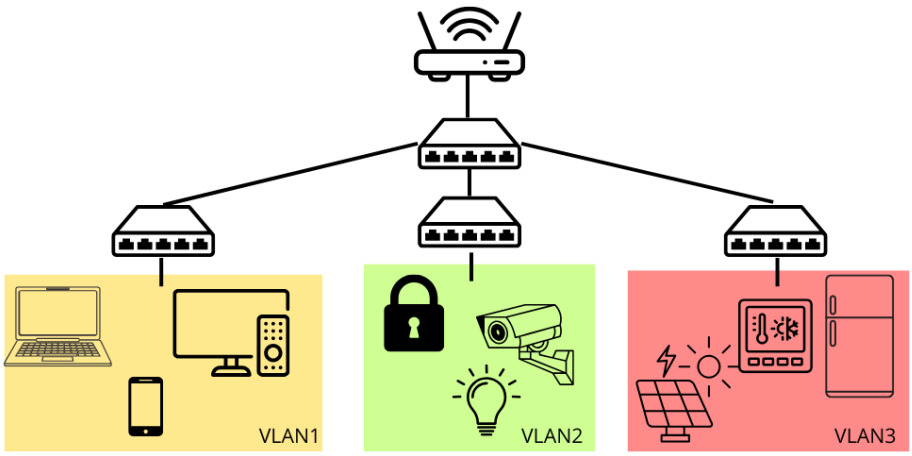
Az okosotthonok folyamatosan bővülő ökoszisztémája növeli a támadási felületet, így a megfelelő hálózatbiztonsági stratégiák alkalmazása elengedhetetlen. Az egyik leghatékonyabb védelmi megoldás a hálózati szegmentáció és a tűzfalhasználat kombinálása, amely minimalizálja a kockázatokat és fokozza az otthoni rendszer biztonságát.

Hálózati szegmentáció jelentősége

A hálózati szegmentáció az okosotthon-hálózat logikai vagy fizikai elkülönítését jelenti különböző szektorokra, így csökkentve a potenciális fenyegetések terjedésének lehetőségét. Ez azt jelenti, hogy az IoT-eszközök nem ugyanazon a hálózati szegmensen futnak, mint a kritikus eszközök, például a számítógépek és mobiltelefonok. Az elkülönítés egyik legfontosabb előnye, hogy ha egy IoT-eszközt feltörnek, a támadó nem tudja könnyen elérni az érzékeny adatokat tartalmazó eszközöket vagy a hálózat többi részét.[28]

A hálózati szegmentáció főbb módszerei:

- Virtuális LAN-ok (VLAN) – A modern routerek és hálózati eszközök támogatják a VLAN-ok beállítását, amely lehetővé teszi az egyes eszközcsoportok elkülönítését. Például az IoT-eszközök egy külön VLAN-ba helyezhetők, így nem férnek hozzá a személyes vagy munkaeszközökhöz. Emellett javítják a hálózat teljesítményét, mivel az eltérő típusú forgalmak külön csatornán mozognak. Szabályozás szempontból is előnyös, hiszen be lehet állítani, hogy melyik eszközök kommunikálhatnak egymással. Külön lehet szabályozni, azt is, hogy milyen forgalmat engedélyezünk az adott VLAN-on, ezzel például az Iot eszközök közvetlen internetkapcsolatát le lehet tiltani, ami egy nagy biztonsági faktort jelent.[29]
- Vendéghálózatok – Sok modern router lehetőséget kínál vendéghálózat létrehozására,

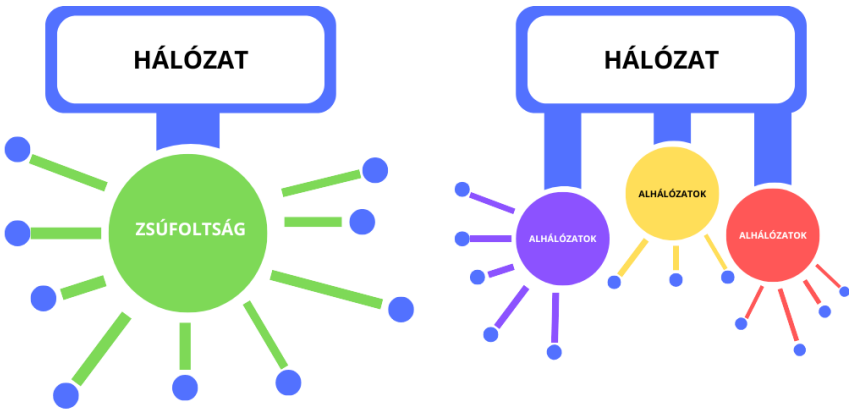


6. ábra – Egy lehetséges VLAN kiosztás egy okosotthonban – Saját szerkesztés

amely egy különálló Wi-Fi hálózatot biztosít a látogatók és ideiglenes eszközök

számára. Ez egy egyszerű és hatékony módja a hálózat szegmentálásának, amely megakadályozza a vendégek és nem megbízható eszközök hozzáférését az otthoni vagy vállalati hálózat érzékeny eszközeihez, például kamerákhoz, NAS szerverekhez vagy okosotthon-eszközökhöz. Egy megfelelően beállított vendéghálózat csökkenti a rosszindulatú szoftverek vagy támadások kockázatát, mivel a vendégek által használt eszközök nem érhetik el a főhálózatot. A biztonság érdekében érdemes a vendéghálózatot külön SSID-vel és jelszóval ellátni.[30]

- Subnetting (alhálózatok létrehozása) – Az alhálózatok kialakítása fejlettebb szegmentációs módszer, amely lehetővé teszi az eszközök külön hálózati tartományokba szervezését. Ez különösen hasznos az okosotthonokban és vállalati környezetekben, ahol az eszközök funkcióik szerint elkülöníthetők, például egy alhálózatban lehetnek a számítógépek és mobilok, egy másikban az IoT-eszközök, míg egy harmadikban a szórakoztató eszközök. Az alhálózatok segítenek csökkenteni a hálózati torlódást, mivel az eszközök nem osztoznak feleslegesen a sávszélességen. Emellett a biztonságot is növelik, hiszen egy fertőzött vagy támadás alatt álló eszköz nem érheti el az érzékeny adatokat vagy más eszközöket. Az alhálózatok VLAN-okkal kombinálva még hatékonyabb védelmet nyújtanak, mivel egy tűzfal vagy router szabályozhatja a szegmensek közötti forgalmat.[31]



7. ábra – Alhálózatok szemléltetése – Saját szerkesztés

A megfelelő hálózati szegmentációval az okosotthon-hálózat védettebbé válik a támadásokkal szemben, mivel a támadók mozgásterét jelentősen korlátozza az eszközök elkülönítése.

Behatolásérzékelő és anomáliadetektáló rendszerek

Az okosotthonok egyre nagyobb kiberbiztonsági kihívásokkal néznek szembe, mivel a hálózatba kapcsolt IoT-eszközök száma folyamatosan növekszik. Az érzékeny adatok és a hálózat védelme érdekében kulcsfontosságú a behatolásérzékelő rendszerek (Intrusion Detection Systems – IDS) és az anomáliadetektáló technológiák alkalmazása. Ezek a megoldások lehetővé teszik a gyanús tevékenységek azonosítását és a támadások megelőzését még azelőtt, hogy azok súlyos károkat okoznának.

Behatolásérzékelő rendszerek (IDS) az okosotthonokban

A behatolásérzékelő rendszerek célja az illetéktelen behatolások észlelése és azok gyors jelzése a felhasználók vagy biztonsági szolgálatok felé. Ezek a rendszerek érzékelőkből, vezérlőegységekből és riasztómechanizmusokból állnak, amelyek különböző módszerekkel képesek azonosítani a behatolási kísérleteket. A leggyakoribb érzékelőtípusok közé tartoznak a mozgásérzékelők, nyitásérzékelők, üvegtörésérzékelők, vibrációs érzékelők és hangalapú detektorok. A modern rendszerek gyakran integrálnak kamerás megfigyelést, amely lehetővé teszi a behatolás vizuális megerősítését is. Az intelligens rendszerek összekapcsolhatók más okoseszközökkel, például kamerákkal, világítással és okoszárakkal, így a behatolásérzékelők által adott jelzések automatikus válaszreakciókat indíthatnak el.[32]

Az IDS rendszerek két fő típusa:

1. Hálózati alapú behatolásérzékelő rendszer (NIDS – Network-based IDS)

   A teljes hálózati forgalmat figyeli, és elemzi az adatcsomagokat gyanús mintázatok után kutatva. Jellemzően az okosotthon-routerhez vagy egy dedikált hálózati eszközhöz kapcsolódik (Snort, Suricata).

2. Hosztalapú behatolásérzékelő rendszer (HIDS – Host-based IDS)

   Egy adott eszközön fut, és annak működését monitorozza. Figyeli a rendszerlogokat, fájlmódosításokat, jogosultságváltozásokat és egyéb belső folyamatokat (OSSEC, Wazuh).

A behatolásérzékelő rendszerek fő célja a gyors észlelés és riasztás, azonban az IDS önmagában nem tudja megakadályozni a támadásokat – erre a behatolásmegelőző rendszerek (IPS – Intrusion Prevention Systems) szolgálnak.[32]

Anomáliadetektáló rendszerek az IoT-eszközök biztonságában

Az anomáliadetektáló rendszerek (Anomaly Detection Systems – ADS) az IDS-ek továbbfejlesztett változatainak tekinthetők, mivel nemcsak előre meghatározott mintázatok alapján

keresnek fenyegetéseket, hanem a normális hálózati viselkedést is megtanulják, és attól való eltéréseket képesek azonosítani.

A leggyakoribb anomáliadetektáló rendszerek a következő technológiákra épülnek:

- Adatmintázatok elemzése: Az adatok folyamatos monitorozása és az eltérések azonosítása.
- Szenzorhálózatok: Különböző érzékelők adatait elemzik, hogy szokatlan változásokat észleljenek.
- Öntanuló algoritmusok: Gépi tanulás segítségével a rendszer folyamatosan javítja saját felismerési képességeit.

Míg a behatolásérzékelő rendszerek kifejezetten az illetéktelen behatolásokat hivatottak észlelni, az anomáliadetektálás szélesebb körű biztonsági és kényelmi funkciókat biztosít.[33]

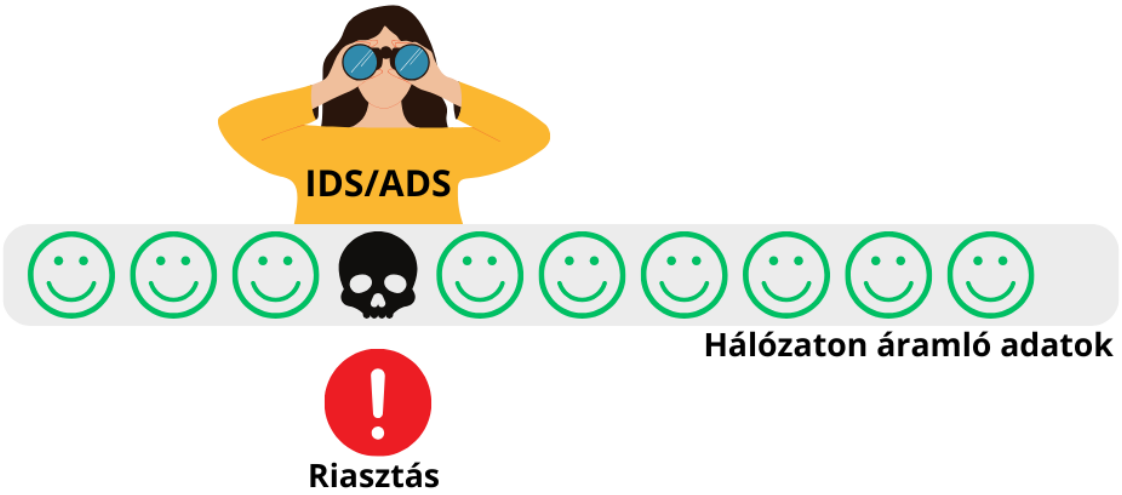
Gyakori fenyegetések, amelyeket az IDS és ADS felismerhet

- Brute force támadások: Az IDS képes észlelni, ha egy támadó folyamatosan próbál bejelentkezni egy rendszerbe különböző jelszavakkal.
- Szokatlan mozgások és tevékenységek: Az ADS érzékelheti, ha valaki olyan időpontban tartózkodik egy helyiségben, amikor általában nem szokott.
- Adathalászati és rosszindulatú forgalom: Az IDS figyelmeztethet, ha gyanús adatforgalmat észlel az otthoni hálózaton.
- Hirtelen energiafelhasználás-növekedés: Az ADS jelezheti, ha egy eszköz szokatlanul nagy mennyiségű energiát fogyaszt, ami akár egy meghibásodás vagy rosszindulatú program jele is lehet.
- Okoseszközök manipulálása: A rendszer észlelheti, ha egy ismeretlen vagy kompromittált eszköz próbálja átvenni az irányítást más eszközök felett.
- DDoS támadások: Az IDS figyelmeztethet, ha egy okosotthon hálózatát nagy mennyiségű adatforgalom éri, ami szolgáltatásmegtagadási támadásra utalhat.
- Fizikai biztonsági fenyegetések: Az ADS azonosíthatja a rendellenes viselkedést, például egy ablak vagy ajtó váratlan kinyitását, ami betörésre utalhat.[33]

IDS és ADS rendszerek telepítése okosotthonokban

Az anomáliadetektáló rendszerek telepítése egy okosotthonba összetett folyamat, amely több lépésből áll. Elsőként a megfelelő szenzorokat és eszközöket kell kiválasztani, ideértve a mozgásérzékelőket, hőmérsékletérzékelőket, kamerákat és más okoseszközöket. Ezt követően ki kell építeni a hálózati infrastruktúrát, amely stabil Wi-Fi vagy vezetékes kapcsolatot biztosít az eszközök közötti adatkommunikációhoz. A szoftveres rész magában foglalja a mesterséges intelligencia alapú algoritmusok telepítését és konfigurálását, amelyek az érzékelők által

szolgáltatott adatokat elemzik és észlelik az anomáliákat. Fontos az is, hogy az anomáliadetektáló rendszert integráljuk más okosotthon-megoldásokkal, például riasztórendszerekkel vagy világításvezérléssel, hogy egy átfogó védelmi rendszert hozzunk létre. A telepítés után elengedhetetlen a folyamatos karbantartás és a szoftveres frissítések biztosítása, hogy a rendszer mindig naprakész és hatékony maradjon.[34]



8. ábra – IDS / ADS egyszerűsített működése – Saját szerkesztés

Tűzfalak az okosotthonokban

A tűzfal – legyen az egy dedikált hardveres eszköz vagy szoftveresen integrált megoldás a routeren belül – képes szabályozni, mely eszközök milyen adatokat küldhetnek és fogadhatnak, valamint felismerni és blokkolni a gyanús adatforgalmat. Ezáltal jelentősen csökkenti annak esélyét, hogy egy rosszindulatú támadó hozzáférést szerezzen az otthoni hálózathoz.[35] [36]

Milyen fenyegetéseket képes szűrni a tűzfal?

Egy jól beállított tűzfal képes azonosítani és blokkolni a nem engedélyezett bejövő kapcsolatokat, például, ha egy ismeretlen IP-cím próbál meg hozzáférni egy otthoni kamerához. Emellett a kifelé irányuló adatforgalmat is szabályozza, így megakadályozható, hogy egy fertőzött eszköz kapcsolatba lépjen egy parancs- és vezérlőszerverrel (C&C server), például egy botnet hálózat részeként.[37] [36]

A tűzfalak képesek észlelni portscan-eket, azaz amikor egy támadó próbálja feltérképezni, hogy milyen szolgáltatások futnak az otthoni hálózaton. Emellett naplózhatják a forgalmat, így egy gyanús aktivitás visszakereshető és elemezhető. Több modern megoldás – különösen a vállalati szintű vagy haladó otthoni tűzfalak – már alkalmazás- és tartalomszűrést is kínálnak, amelyekkel például blokkolhatók a kéretlen reklámok, vagy korlátozható a gyermekek hozzáférése bizonyos weboldalakhoz.[37] [36]

Tűzfalak típusai

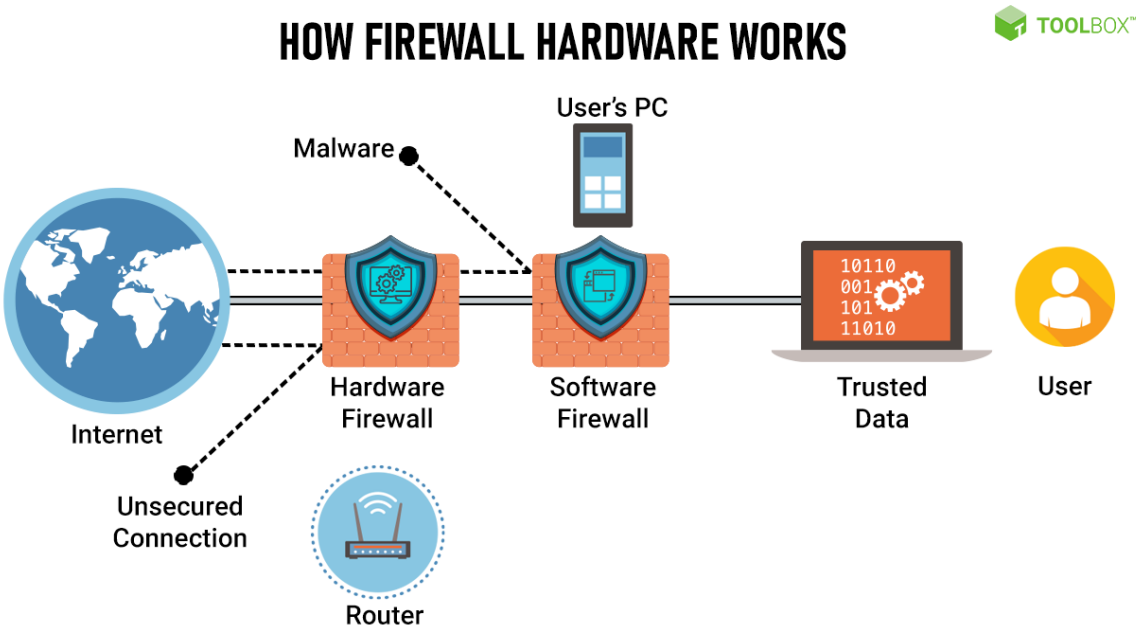
Az okosotthonokban alkalmazott tűzfalak kulcsszerepet játszanak az IoT (Internet of Things) eszközök védelmében, mivel ezek az eszközök gyakran ki vannak téve különböző kibertámadásoknak. A tűzfalak elsődleges feladata a hálózati forgalom monitorozása és szabályozása, ezáltal megakadályozva az illetéktelen hozzáféréseket és adatlopásokat. Az IoT eszközök védelmére többféle tűzfaltípus alkalmazható, melyek közül a leggyakoribbak a következők:

1. Hálózati tűzfalak (Network Firewalls): Ezek a tűzfalak a belső hálózat és az internet közötti határvonalon helyezkednek el, és minden bejövő és kimenő forgalmat ellenőriznek. Általában hardveres eszközök formájában jelennek meg, mint például routerek vagy dedikált tűzfalberendezések. Feladatuk, hogy megakadályozzák a nem kívánt forgalom bejutását a hálózatba, ezáltal védelmet nyújtva az okosotthon eszközeinek.[38]

2. Hosztalapú tűzfalak (Host-Based Firewalls): Ezeket a tűzfalakat közvetlenül az egyes IoT eszközökre telepítik, és elsősorban az adott eszköz helyi forgalmát figyelik. Céljuk az illetéktelen hozzáférések megakadályozása az adott eszköz szintjén, kiegészítve ezzel a hálózati tűzfalak nyújtotta védelmet.[38]

3. Következő generációs tűzfalak (Next-Generation Firewalls, NGFW): Ezek a tűzfalak a hagyományos tűzfalak funkcióit ötvözik fejlett biztonsági képességekkel, mint például behatolásmegelőző rendszerek (IPS), mély csomagellenőrzés és alkalmazás-szintű szűrés. Az NGFW-k képesek azonosítani és blokkolni a kifinomultabb támadásokat is, így fokozott védelmet nyújtanak az okosotthonok számára. [38]

A megfelelő tűzfaltípus kiválasztása és implementálása elengedhetetlen az okosotthonok biztonságának növelése érdekében, figyelembe véve a hálózat méretét, az eszközök számát és a felhasználók egyedi igényeit.[38]



9. ábra – Szoftveres és hardveres tűzfalak a hálózatban - https://www.spiceworks.com/it-security/network-security/articles/top-10-firewall-hardware-devices/

Port Forwarding és UPnP kockázatai az okosotthonokban

Az okosotthonok egyik legnagyobb kihívása a külső hozzáférés biztosítása anélkül, hogy veszélybe sodornánk az otthoni hálózat biztonságát. Két gyakran alkalmazott, de jelentős biztonsági kockázatokat rejtő megoldás a port forwarding (porttovábbítás) és az Universal Plug and Play (UPnP). Ezek a mechanizmusok lehetővé teszik a külső eszközök számára, hogy elérjék az otthoni hálózatban lévő IoT-eszközöket, azonban helytelen konfiguráció esetén súlyos sebezhetőségeket eredményezhetnek. [39]

Port Forwarding (Porttovábbítás) kockázatai

A port forwarding egy olyan hálózati beállítás, amely lehetővé teszi, hogy egy külső eszköz az interneten keresztül elérje az otthoni hálózat egy meghatározott eszközét vagy szolgáltatását. Az okosotthonok esetében gyakran alkalmazzák például IP-kamerák, intelligens vezérlőközpontok vagy távoli hozzáférést igénylő rendszerek esetében.[39]

Támadási felület növekedése

A port forwarding növeli a hálózat támadási felületét azáltal, hogy nyitott portokat hoz létre a routeren, amelyeket támadók könnyen feltérképezhetnek portszkennelési technikákkal. Az olyan eszközök, mint a Shodan vagy az Nmap, lehetővé teszik a támadók számára, hogy azonosítsák ezeket a nyitott portokat és a hozzájuk kapcsolódó szolgáltatásokat. A Shodan például egy keresőmotor, amely az internetre csatlakoztatott eszközök és nyitott portjaik információit gyűjti össze, így bárki számára hozzáférhetővé téve ezeket az adatokat. Az Nmap pedig egy nyílt forráskódú eszköz, amelyet hálózati adminisztrátorok és támadók egyaránt használnak nyitott portok és futó szolgáltatások felderítésére. [40]

Gyenge hitelesítés és brute-force támadások

Ha egy nyitott port mögött egy gyenge hitelesítéssel védett szolgáltatás található (például alapértelmezett felhasználónév-jelszó párossal működő IP-kamera), akkor egy támadó könnyen brute-force támadással megszerezheti a hozzáférést. Az ilyen támadások különösen elterjedtek az IoT-eszközök ellen, mivel sok gyártó nem biztosít megfelelő védekezési mechanizmusokat.[41]

Man-in-the-Middle (MitM) támadások és adatlopás

A port forwarding révén elérhető eszközök gyakran nem titkosítják megfelelően az adatforgalmat. Ha egy támadó képes lehallgatni a hálózati forgalmat, akkor érzékeny adatokat (például bejelentkezési adatokat vagy videófolyamokat) szerezhet meg.[42]

Botnetekbe való bevonás

A nyitott portokon keresztül elérhető sebezhető eszközök gyakran botnetek célpontjaivá válnak. Az olyan hírhedt IoT-botnetek, mint a Mirai, több százezer nyitott porttal rendelkező eszközt fertőztek meg, hogy DDoS-támadásokat hajtsanak végre.[43]

Universal Plug and Play (UPnP) kockázatai

A Universal Plug and Play (UPnP) egy olyan hálózati protokoll, amely megkönnyíti az eszközök automatikus konfigurációját egy helyi hálózaton belül. Az UPnP lehetővé teszi az IoT-eszközök számára, hogy automatikusan kinyissanak portokat a routeren anélkül, hogy a felhasználónak kézzel kellene konfigurálnia azokat. Bár ez kényelmes, komoly biztonsági problémákat is okozhat.[44]

Automatikus portmegnyitás és kontrollálhatatlan hozzáférés

Az UPnP egyik fő problémája, hogy a hálózatba csatlakozó eszközök automatikusan kérhetik a routertől portok megnyitását. Ez azt jelenti, hogy egy fertőzött vagy rosszindulatú alkalmazás képes lehet kinyitni egy hátsó kaput a támadók számára anélkül, hogy a felhasználó tudna róla.[44]

Külső támadók kihasználhatják az UPnP sérülékenységeit

Számos router és eszköz olyan UPnP implementációt használ, amely sérülékeny támadásokkal szemben. Az olyan támadások, mint a UPnProxy, lehetővé teszik a támadók számára, hogy egy otthoni routert proxyként használjanak más célpontok támadására.[44]

IoT-eszközök és rosszindulatú szoftverek

Az UPnP-t gyakran használják IoT-eszközök, amelyek biztonsági frissítései elmaradhatnak. Egy kompromittált IoT-eszköz kihasználhatja az UPnP-t a hálózat további eszközeinek megfertőzésére vagy további portok megnyitására.[44]

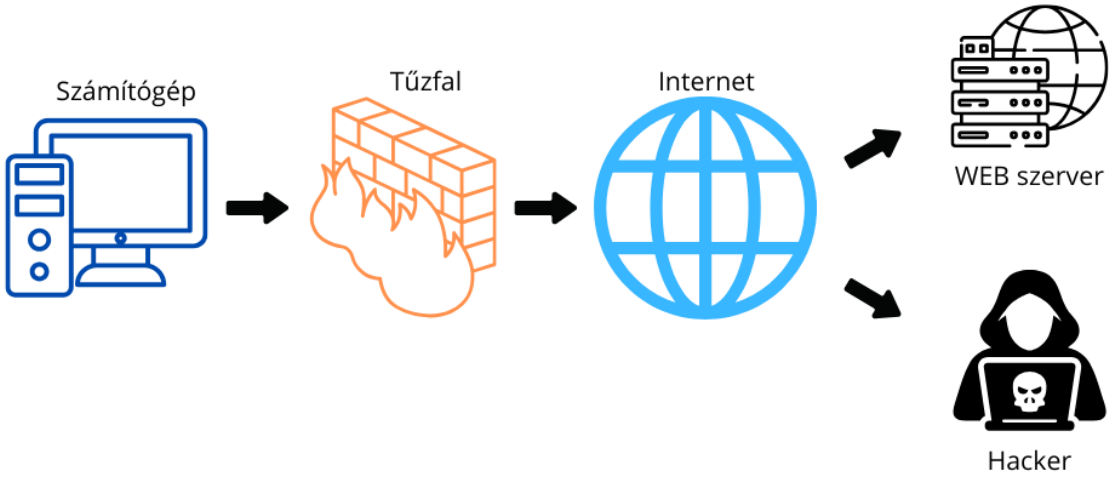
Hogyan csökkenthetők ezek a kockázatok?

Port Forwarding helyett biztonságos alternatívák használata

Egy VPN használatával a távoli hozzáférést biztonságos csatornán keresztül lehet megoldani, anélkül, hogy nyitott portokat kellene létrehozni. Sok modern IoT-eszköz felhőalapú távoli hozzáférési megoldásokat kínál, amelyek titkosított kapcsolatot biztosítanak anélkül, hogy a felhasználónak manuálisan kellene portokat nyitnia.[39]

Az UPnP letiltása, ha nincs rá szükség

A router beállításaiban érdemes letiltani az UPnP-t, ha nincs rá feltétlenül szükség. Ha mégis szükséges az UPnP használata, akkor rendszeresen ellenőrizni kell a router naplóit, hogy milyen eszközök nyitottak portokat.[44]



10. ábra- UPnP hátránya – Saját szerkesztés

Zero Trust megközelítés alkalmazása okosotthon-hálózatokban

Az okosotthonok elterjedésével egyre nagyobb hangsúlyt kap a kiberbiztonság, különösen a Zero Trust biztonsági modell alkalmazása. Ez a megközelítés a „soha ne bízz, mindig ellenőrizz” elven alapul, ami azt jelenti, hogy minden eszköz, felhasználó és alkalmazás ellenőrzésre kerül, függetlenül attól, hogy a hálózaton belül vagy kívül található.[45]

A Zero Trust alapelvei között szerepel a legkisebb jogosultság elve, amely a hozzáférést a lehető legszűkebb körre korlátozza, valamint a folyamatos ellenőrzés, amely a hozzáférést a változó körülményekhez igazítja. A mikroszegmentáció, vagyis a hálózat kisebb, elkülönített szegmensekre bontása, és az eszközintegritás ellenőrzése is fontos elemei a modellnek.[45]

Az okosotthonokban a Zero Trust alkalmazása számos előnnyel jár, például csökkenti a támadási felületet, korlátozza a támadások terjedését, javítja az adatvédelmet és növeli a hálózat feletti láthatóságot és kontrollt. Ugyanakkor kihívásokat is jelent, például az IoT-eszközök sokfélesége és korlátozott erőforrásai, a folyamatos ellenőrzés komplexitása, valamint a felhasználói szokások és a kényelem figyelembevétele.[45]

A Zero Trust megvalósítása érdekében fontos az identitás- és hozzáféréskezelés erős hitelesítési módszerekkel, a hálózati mikroszegmentáció, az eszközök biztonságának rendszeres frissítése, az adatvédelem adattitkosítással és adatvesztés-megelőzéssel, valamint a folyamatos monitorozás és elemzés biztonsági események naplózásával és anomáliadetektálással.[45]

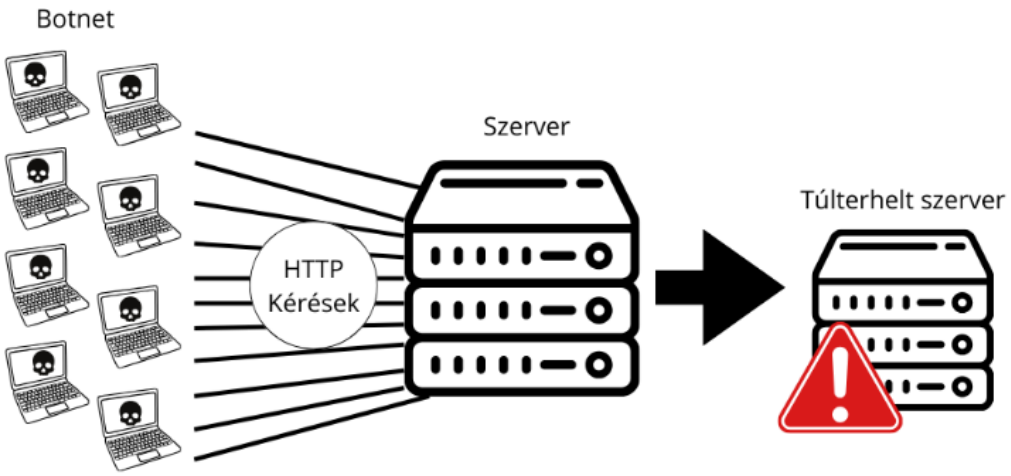
11. ábra- Zero Trust Security szemléltetése – Saját szerkesztés

Túlterheléses támadások (DDoS) és botnetek

Az okosotthonok elterjedésével párhuzamosan növekszik a kiberbiztonsági fenyegetések száma is, különösen a túlterheléses támadások (Denial of Service – DoS) és a botnetek jelentette veszélyek. Ezek a támadások nemcsak az egyéni felhasználókat, hanem a globális infrastruktúrát is veszélyeztethetik.

Túlterheléses támadások

A DDoS (Distributed Denial of Service) támadás egy olyan túlterheléses támadás, amelynek célja, hogy egy adott hálózati szolgáltatást, weboldalt vagy szervert elérhetetlenné tegyen azáltal, hogy hatalmas mennyiségű forgalmat generál felé, meghaladva annak kezelési kapacitását. A támadás alapelve, hogy nagyszámú, fertőzött eszközből – úgynevezett botnetből – egyidejűleg indítanak kéréseket az áldozati rendszer felé, ezzel kimerítve annak erőforrásait, például a sávszélességet, a CPU-t vagy a memóriát. A támadások többféle módszerrel történhetnek, például volumetrikus támadásokkal, amelyek hatalmas adatforgalmat generálnak és túlterhelik a hálózatot, vagy protokollalapú támadásokkal, amelyek az infrastruktúra gyengeségeit kihasználva foglalják le az elérhető kapcsolatokat. Emellett léteznek alkalmazásrétegi támadások, amelyek célzottan egy adott szolgáltatás, például egy weboldal HTTP-kérésekkel való elárasztásával igyekeznek leállítani annak működését. A DDoS támadások különösen veszélyesek, mivel gyakran nehezen szűrhetők, hiszen a támadó forgalom összetéveszthető a legitim felhasználói kérésekkel. A védekezés érdekében különféle technológiákat alkalmaznak, például forgalomszűrést, amely azonosítja és blokkolja a gyanús csomagokat, valamint terheléselosztást, amely a beérkező kéréseket több szerver között osztja el a túlterhelés csökkentése érdekében. Ezenkívül a behatolást megelőző rendszerek (IPS) és tűzfalak segíthetnek a DDoS-forgalom kiszűrésében, míg a nagyvállalatok és szolgáltatók gyakran felhőalapú DDoS-védelmi megoldásokat alkalmaznak, amelyek képesek a támadási minták gyors elemzésére és a rosszindulatú forgalom blokkolására. [46]

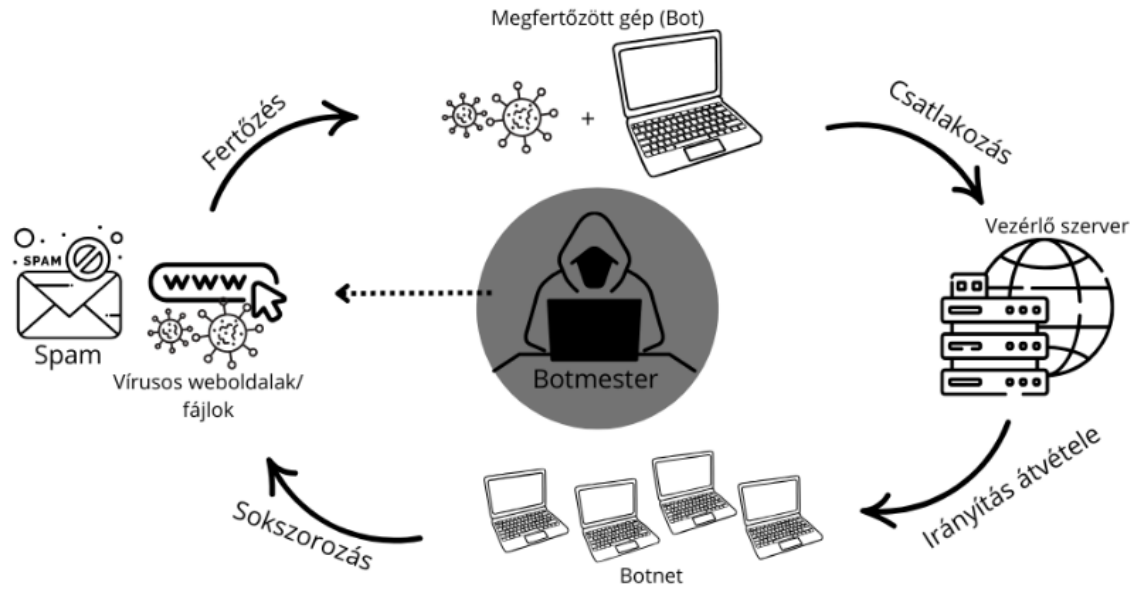


12. ábra Szolgáltatás-túlterhelés alapú DDoS támadás – Saját szerkesztés

Botnetek

A botnet egy olyan hálózat, amelyet kártékony szoftverekkel megfertőzött eszközökből – számítógépekből, szerverekből vagy IoT-eszközökből – építenek ki, és amelyet egy támadó távolról, központilag vagy decentralizált módon irányíthat. Ezeket a fertőzött eszközöket, amelyeket gyakran "botoknak" vagy "zombigépeknek" neveznek, a tulajdonosuk tudta nélkül használják fel különböző rosszindulatú tevékenységekre. A botnetek kialakulása általában egy többlépcsős folyamat eredménye, amely első lépésben a célzott eszköz megfertőzésével kezdődik, jellemzően adathalász e-maileken, biztonsági rések kihasználásán vagy rosszindulatú szoftverek terjesztésén keresztül. A kompromittált eszköz ezt követően csatlakozik egy Command and Control (C&C) szerverhez vagy egy peer-to-peer (P2P) hálózathoz, amelyen keresztül a támadó utasításokat küldhet. A botnetek főként elosztott szolgáltatásmegtagadási (DDoS) támadások, nagymennyiségű kéretlen e-mail (spam) küldése, adatlopás, kártékony programok terjesztése vagy akár kriptovaluta-bányászat céljából működnek. Az ilyen hálózatok elleni védekezés érdekében kritikus fontosságú az erős hitelesítési módszerek – például hosszú, egyedi jelszavak és kétlépcsős azonosítás – alkalmazása, az operációs rendszerek és szoftverek rendszeres frissítése, valamint a tűzfalak és vírusvédelmi rendszerek aktív használata. Emellett elengedhetetlen a felhasználók kiberbiztonsági tudatosságának növelése, mivel a legtöbb botnet-fertőzés emberi figyelmetlenségből vagy biztonsági hiányosságok kihasználásával valósul meg.[47]

Az IoT-eszközök, mint például az okosotthonokban használt kamerák, termosztátok vagy intelligens hűtőszekrények, gyakran gyenge biztonsági beállításokkal rendelkeznek. Ez lehetőséget ad a támadóknak arra, hogy ezeket az eszközöket megfertőzzék és botnetekbe integrálják. Egy ilyen botnet segítségével a támadók hatalmas mennyiségű adatforgalmat generálhatnak, amely túlterheli a célzott rendszereket, így azok elérhetetlenné válnak a felhasználók számára. [48]



13. ábra – Botnet támadás - Saját szerkesztés (https://www.radware.com/RadwareSite/MediaLibraries/Images/Cyberpedia/Bot%20Manager/what-is-botnet-1.jpg alapján átalakítva)

Energetikai rendszerek veszélyeztetése

A botnetek nemcsak az online szolgáltatásokat, hanem a kritikus infrastruktúrákat is veszélyeztethetik. Egyes kutatások szerint a nagy elektromos teljesítményű okoseszközökből – például légkondicionálókból vagy fűtőberendezésekből – álló botnetek képesek manipulálni az áramfelvételt. A kompromittált eszközök szinkronizált ki- és bekapcsolásával frekvencia instabilitást okozhatnak az elektromos hálózatban, ami akár generátorok leállásához és üzemzavarokhoz vezethet.

Milyen eszközök kompetenciák kellenek egy okosotthon biztonságos fenntartásához?

Szükséges eszközök

Az okosotthon biztonságos fenntartása egy komplex feladat, amely számos eszközt és kompetenciát igényel. A biztonságos okosotthon alapja egy erős Wi-Fi router, amely WPA3 titkosítással és naprakész firmware-rel rendelkezik. Fontos a vendég Wi-Fi hálózat beállításának lehetősége, valamint a tűzfal és IDS/IPS funkciók megléte. A hálózati forgalom szűrésére hardveres vagy szoftveres tűzfal, illetve speciálisan IoT-eszközökre optimalizált tűzfal szükséges. A behatolásérzékelő és -megelőző rendszerek (IDS/IPS) a hálózati forgalom elemzésével segítenek a gyanús tevékenységek észlelésében és blokkolásában. A távoli hozzáférés biztonságosabbá tételéhez virtuális magánhálózat (VPN) alkalmazása ajánlott.

A biztonságos jelszóhasználat érdekében jelszókezelő szoftver használata javasolt, amely erős és egyedi jelszavak generálására és tárolására szolgál. A kétfaktoros hitelesítés (2FA) bekapcsolása minden lehetséges eszközön és szolgáltatásban elengedhetetlen. A számítógépeken és mobil eszközökön vírusirtó, rosszindulatú szoftverek elleni és kémprogramok elleni szoftverek, valamint az IoT-eszközök biztonsági szoftverei nyújtanak védelmet. A hálózat szegmentációjához VLAN-ok létrehozására képes router vagy switch szükséges.[49]

Szükséges kompetenciák

A biztonságos okosotthon fenntartásához szükséges kompetenciák a hálózati ismeretektől a biztonsági tudatosságig terjednek. Fontos az IP-címek, alhálózatok, portok és protokollok ismerete, valamint a Wi-Fi hálózatok beállításának és karbantartásának képessége. A felhasználóknak tisztában kell lenniük a leggyakoribb kiberbiztonsági fenyegetésekkel, a biztonságos jelszóhasználattal és böngészési szokásokkal, valamint a szoftverek és firmware-ek frissítésének fontosságával. Az IoT-eszközök működésének, biztonsági beállításainak, frissítésének és karbantartásának ismerete is elengedhetetlen. A hálózati és biztonsági problémák azonosításának és megoldásának képessége, valamint a GDPR és egyéb adatvédelmi előírások ismerete is fontos. A zéró bizalom biztonsági modelljének megértése és alkalmazása is hozzájárul a biztonságos okosotthon kialakításához.

A biztonságos okosotthon fenntartása folyamatos odafigyelést és frissítést igényel. A felhasználóknak tisztában kell lenniük azokkal a kockázatokkal, amelyekkel az okosotthonok használata jár, és a biztonsági rendszereket rendszeresen ellenőrizni kell. Az okosotthon biztonságának fenntartása egy

folyamatos folyamat, amely megköveteli a felhasználóktól, hogy naprakészek legyenek a legújabb biztonsági fenyegetésekkel és megoldásokkal kapcsolatban.

14. ábra – Egy megfelelően védett okosotthon – Saját szerkesztés

Szubjektív vélemény összegzésként

Úgy gondolom, hogy az okosotthonok térnyerése gyorsabb lesz, mint azt az átlagemberek gondolják, hiszen az is szubjektív, hogy ma mit nevezünk okosotthonnak, illetve melyik otthon számít már annak. A technológia gyorsabban fejlődik, mint valaha köszönhetően a mesterséges intelligenciának. Az AI támadási szempontból nagyobb veszélyt, míg a támadások kivédésére használt AI nagyobb biztonságot jelent. A jelenlegi okosotthonok védelmét fenntartani nagyon sok figyelmet és pénzt igényel, tehát csak alapos átgondolás és utánajárás, vagy szakértők felkeresése után ajánlanám, hogy átalakítsák a kevésbé hozzáértők az otthonaikat. A kényelmi funkció vonzza az embereket elsősorban, pedig a védelmi szempont az én nézőpontom szerint sokkal fontosabb faktor.

Véleményem szerint egy okosotthon több előnnyel jár, mint hátránnyal, ugyanakkor nem szabad azt gondolnia senkinek, hogy „miért pont én lennék a célpont?”, ugyanis a kiberbűnözők számos ilyen áldozatot ejtettek az évek során, ahol az „áldozat” saját maga adta meg az érzékeny adatokat, nem a hálózatról vagy valamilyen eszközről lopták el.

Források

[1] „Az IoT eszközök az üres irodákban is dolgoztak – sajnos”, Bitport. Elérés: 2025. április 5. [Online]. Elérhető: https://bitport.hu/az-iot-eszkozok-az-ures-irodakban-is-dolgoztak-sajnos/

[2] M. R. F. https://www.marketresearchfuture.com, „Smart Home Market Size, Trends | Growth Report - 2032”. Elérés: 2025. április 5. [Online]. Elérhető: https://www.marketresearchfuture.com/reports/smart-home-market-974

[3] O. Traynor, „Security Challenges: Misconfigured IOT Devices”, CybelAngel. Elérés: 2025. április 5. [Online]. Elérhető: https://cybelangel.com/misconfigured-iot/

[4] „15% of All IoT Device Owners Don’t Change Default Passwords”, BleepingComputer. Elérés: 2025. április 5. [Online]. Elérhető: https://www.bleepingcomputer.com/news/security/15-percent-of-all-iot-device-owners-dont-change-default-passwords/

[5] „Figyelmeztetés elavult szoftverek miatt bekövetkezett incidensért”, gdpr.news.hu. Elérés: 2025. április 5. [Online]. Elérhető: https://gdpr.news.hu/cikkek/figyelmeztetes-elavult-szoftverek-miatt-bekovetkezett-incidensert/

[6] „Importance of Firmware Updates for IoT | CodingDrills”. Elérés: 2025. április 5. [Online]. Elérhető: https://www.codingdrills.com/tutorial/network-security-tutorial/iot-firmware-updates

[7] „MQTT and M2M: Do You Know Who Owns Your Machine’s Data? | Trend Micro (IN)”. Elérés: 2025. április 5. [Online]. Elérhető: https://www.trendmicro.com/vinfo/in/security/news/internet-of-things/mqtt-and-m2m-do-you-know-who-owns-your-machines-data

[8] „Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable”. Elérés: 2025. április 5. [Online]. Elérhető: https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

[9] A. Sharma, „Smart lock bug could let hackers locate you and unlock your door, remotely”, Security Report. Elérés: 2025. április 5. [Online]. Elérhető: https://securityreport.com/smart-lock-bug-could-let-hackers-locate-you-and-unlock-your-door-remotely/

[10] „Security Issues With Smart Thermostats: Protecting your Home | Smart living Way”. Elérés: 2025. április 5. [Online]. Elérhető: https://smartlivingway.com/security-issues-with-smart-thermostats/

[11] „New report finds over 90% of IoT device transactions are unencrypted”, Perle Systems. Elérés: 2025. április 5. [Online]. Elérhető: https://perle.com/articles/new-report-finds-over-90-of-iot-device-transactions-are-unencrypted-40185159.shtml

[12] N. Levy, „Amazon confirms that employees listen to Alexa conversations to help improve digital assistant”, GeekWire. Elérés: 2025. április 5. [Online]. Elérhető: https://www.geekwire.com/2019/amazon-confirms-employees-listen-alexa-conversations-help-improve-digital-assistant/

[13] „New research reveals alarming security and privacy threats in smart homes | News | University of Calgary”. Elérés: 2025. április 5. [Online]. Elérhető: https://ucalgary.ca/news/new-research-reveals-alarming-security-and-privacy-threats-smart-homes

[14] Magyarország G. D. és Kft V.-D. A., „Egyszerűen feltörhető a gyenge jelszóval védett wifi hálózat”, G DATA Magyarország. Elérés: 2025. április 5. [Online]. Elérhető: https://virusirto.hu/blogbejegyzesek/2018/09/19/egyszeruen-feltorheto-a-gyenge-jelszoval-vedett-wifi-halozat/

[15] „Beépített és alapértelmezett adatvédelem: hogyan alakítsuk technikai és egyéb rendszereinket, hogy segítse az adatkezelési folyamatainkat? (GDPR sorozat) - Tudástár”. Elérés: 2025. április 6. [Online]. Elérhető: https://www.nonprofit.hu/tudastar/Beepitett-es-alapertelmezett-adatvedelem-hogyan-alakitsuk-technikai-es-egyeb-rendszereinket-hogy-segitse-az-adatkezelesi-folyamatainkat-GDPR-sorozat?utm_source=chatgpt.com

[16] „Milyen adatbiztonsági intézkedéseket vár el a GDPR az adatkezelőktől?”, GDPR. Elérés: 2025. április 6. [Online]. Elérhető: https://gdpr.blog.hu/2020/03/02/milyen_adatbiztonsagi_intezkedeseket_var_el_a_gdpr_az_adatkezeloktol

[17] „ISO/IEC 27001 tanúsítás - Információbiztonság, kiberbiztonság és adatvédelem”, SGSCorp. Elérés: 2025. április 6. [Online]. Elérhető: https://www.sgs.com/hu-hu/services/iso-iec-27001-tanusitas-informaciobiztonsag-kiberbiztonsag-es-adatvedelem
[18] „ETSI EN 303 645 Cybersecurity Standard for Consumer IoT Devices”. Elérés: 2025. április 6. [Online]. Elérhető: https://www.intertek.com/iot/cybersecurity/etsi-en-303-645/
[19] „NIST Cybersecurity for IoT Program”, *NIST*, szept. 2019, Elérés: 2025. április 6. [Online]. Elérhető: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program
[20] „5 tipp az okosotthonunk védelmére - Trade magazin”. Elérés: 2025. április 6. [Online]. Elérhető: https://trademagazin.hu/hu/5-tipp-az-okosotthonunk-vedelmere/
[21] „IoT-eszkozok-biztonsagi-kerdesei_I_CTI_jelentes.pdf”. Elérés: 2025. április 6. [Online]. Elérhető: https://nki.gov.hu/wp-content/uploads/2022/09/IoT-eszkozok-biztonsagi-kerdesei_I_CTI_jelentes.pdf
[22] „Uniós szabvány készült a konzumer IoT eszközök biztonságossá tételéhez”, Nemzeti Kibervédelmi Intézet. Elérés: 2025. április 6. [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/unios-szabvany-keszult-a-konzumer-iot-eszkozok-biztonsagossa-tetelehez/
[23] S. Sharma, „IoT Connectivity Architecture: Engineering Guide to Enterprise-Scale Implementation”. Elérés: 2025. április 6. [Online]. Elérhető: https://www.wevolver.com/article/iot-connectivity-architecture-engineering-guide-to-enterprise-scale-implementation
[24] „Z-Wave vs. ZigBee”, Security.org. Elérés: 2025. április 6. [Online]. Elérhető: https://www.security.org/home-security-systems/z-wave-vs-zigbee/
[25] „Zigbee vs. Z-wave: Key Differences”, Spiceworks Inc. Elérés: 2025. április 6. [Online]. Elérhető: https://www.spiceworks.com/tech/iot/articles/zigbee-vs-z-wave/
[26] „Build With Matter | Smart Home Device Solution”, CSA-IOT. Elérés: 2025. április 8. [Online]. Elérhető: https://csa-iot.org/all-solutions/matter/
[27] „What is Matter?”, Google Home Developers. Elérés: 2025. április 8. [Online]. Elérhető: https://developers.home.google.com/matter/overview
[28] „A hálózattervezés kihívásai a biztonság és teljesítmény érdekében”, RelNet Technológia Kft. Elérés: 2025. április 7. [Online]. Elérhető: https://relnet.hu/a-halozattervezes-kihivasai-a-biztonsag-es-teljesitmeny-erdekeben/
[29] „Network Configuration VLANS, Home Assistant, and Smart Home Devices - Configuration”, Home Assistant Community. Elérés: 2025. április 7. [Online]. Elérhető: https://community.home-assistant.io/t/network-configuration-vlans-home-assistant-and-smart-home-devices/634122
[30] J. Fritsch, „Securing your Smart Home Devices: Use a Guest Network”, AllTheThings. Elérés: 2025. április 7. [Online]. Elérhető: https://www.allthethings.best/securing-your-smart-home-devices-use-a-guest-network/
[31] N. E. Ouadi, „Understanding Subnetting: Simplifying IP Address Management”, Medium. Elérés: 2025. április 7. [Online]. Elérhető: https://medium.com/@elouadinouhaila566/understanding-subnetting-simplifying-ip-address-management-ad096c4c863d
[32] „What is an Intrusion Detection System (IDS)? | IBM”. Elérés: 2025. április 7. [Online]. Elérhető: https://www.ibm.com/think/topics/intrusion-detection-system
[33] Hiraltalsaniya, „Anomaly Detection with Unsupervised Machine Learning”, Simform Engineering. Elérés: 2025. április 7. [Online]. Elérhető: https://medium.com/simform-engineering/anomaly-detection-with-unsupervised-machine-learning-3bcf4c431aff
[34] „Installing the IDS Appliance”, Cisco. Elérés: 2025. április 7. [Online]. Elérhető: https://www.cisco.com/c/en/us/td/docs/security/ips/4-0/installation/guide/hwchap1.html
[35] „Mindent amit a tűzfalról tudnod kell | INFOSYS - WebShop”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.infosys-admin.hu/antivirus/mindent-amit-a-tuzfalrol-tudnod-kell/
[36] „IBM i”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.ibm.com/docs/hu/i/7.3.0?topic=options-firewalls
[37] „Tűzfal - védelem a számítógépes hálózatokban | ESET”, Tűzfal. Elérés: 2025. április 8. [Online]. Elérhető: https://www.eset.com/hu/tuzfal/
[38] „Firewall For IoT Devices: Enhance Your Smart Home Security”. Elérés: 2025. április 8. [Online]. Elérhető: https://reolink.com/blog/firewall-for-iot-devices/

[39] „Port Forwarding – SmartHome Ninja”. Elérés: 2025. április 8. [Online]. Elérhető: https://smarthomeninja.hu/diy-projektek/port-forwarding/
[40] J. Gallagher, „How to See What Your Router is Exposing to the Internet”, PIA VPN Blog. Elérés: 2025. április 8. [Online]. Elérhető: https://www.privateinternetaccess.com/blog/how-to-see-what-your-router-is-exposing-to-the-internet/
[41] A. A. Rawi, N. Jabeur, és R. W. Anwar, „Generative AI-Based Tool for Brute Forcing IoT Devices’ Default Credentials”.
[42] „What is MITM (Man in the Middle) Attack | Imperva”, Learning Center. Elérés: 2025. április 8. [Online]. Elérhető: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
[43] „Robothálózat (botnet)”, Nemzeti Kibervédelmi Intézet. Elérés: 2025. április 8. [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/
[44] István S., „Mi az UPnP és miért veszélyes? | INFOSYS - WebShop”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.infosys-admin.hu/megoldasok/mi-az-upnp-es-miert-veszelyes/
[45] A. Vakulov, „Secure Your Home Network With Zero Trust Security Best Practices”, Forbes. Elérés: 2025. április 8. [Online]. Elérhető: https://www.forbes.com/sites/alexvakulov/2025/03/06/secure-your-home-network-with-zero-trust-security-best-practices/
[46] „Mi az a DDoS-támadás? | Microsoft Biztonság”. Elérés: 2025. április 8. [Online]. Elérhető: https://www.microsoft.com/hu-hu/security/business/security-101/what-is-a-ddos-attack
[47] „Botnet | ESET Glossary”. Elérés: 2025. április 8. [Online]. Elérhető: https://help.eset.com/glossary/hu-HU/botnet.html
[48] „Bot | ESET Glossary”. Elérés: 2025. április 8. [Online]. Elérhető: https://help.eset.com/glossary/hu-HU/bot.html
[49] C.-F. Kft, „OT biztonsági megoldások: ipari tűzfal, IPS/IDS, NAT és VPN”. Elérés: 2025. április 8. [Online]. Elérhető: https://info.comforth.hu/ics-ot-cybersecurity-ips-ids-tuzfal-vpn-nat

2.44. Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF INFORMATICS

IPAR 4.0 TECHNOLÓGIÁK

Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben

Mózes Márton
[redacted]
2024/2025/2

Tartalom

Bevezetés 4

1. Adaptív autonóm rendszerek és tanulási folyamatok 5

1.1 A gépi tanulás szerepe a CPS rendszerekben 5

1.2 Mélytanulás és autonóm döntéshozatal 5

1.3 Adaptivitás és környezeti változásokhoz való alkalmazkodás 6

1.4 Esettanulmányok és gyakorlati példák 6

1.5 Kihívások és jövőbeli irányok 6

2. Ipari mesterséges intelligencia pipeline-ok 7

2.1 Az MI pipeline felépítése ipari környezetben 8

2.2 Főbb ipari alkalmazások 8

2.3 Technológiai integrációs szempontok 9

2.4 Kihívások és jövőbeli irányok 10

3. MLOps és MES rendszerek 10

3.1 Az MLOps fogalma ipari környezetben 11

3.2 MES rendszerek és szerepük 11

3.3 MLOps integrálása a MES rendszerekbe 11

3.4 Előnyök az ipari termelés szempontjából 12

3.5 Kihívások és megoldások 13

3.6 Jövőbeli kilátások 13

4. Digitális ikrek alkalmazása a gyártási folyamatokban 13

4.1 A digitális iker fogalma és architektúrája 13

4.2 A digitális ikrek szerepe a gyártásban 14

4.3 Szimuláció és predikció 14

4.4 Integráció mesterséges intelligenciával 14

4.5 Előnyök 15

4.6 Kihívások 15

4.7 Jövőbeli trendek 15

5. CPS és mesterséges intelligencia alkalmazása különböző ágazatokban 15

5.1 Mezőgazdaság: Precíziós gazdálkodás MI-vel és szenzorhálózatokkal 16

5.2 Orvostudomány: Személyre szabott gyógyászat MI és CPS integrációval 16

5.3 Honvédelem: Intelligens döntéshozatali rendszerek 17

5.4 Összegzés 18

6. A gépi látás szerepe a CPS rendszerekben 19

6.1 Ipari automatizálás 19

6.2 Közlekedésirányítás 20
6.3 Biztonságtechnika 21
6.4 Gépi látás előnyei CPS-ben 21
6.5 Összegzés 21
7. Intelligens otthonok optimalizálása: Szenzoradatok szerepe az energiahatékonyságban és komfortnövelésben 22
7.1 Az intelligens otthonok architektúrája 22
7.2 Energiahatékonyság szenzoradatok segítségével 22
7.3 Komfortnövelés MI segítségével 23
7.4 Gépi tanulási algoritmusok a smart home rendszerekben 23
7.5 Adatbiztonság és adatvédelem 24
7.6 Összefoglalás 24
Záró gondolatok: 24
Források: 25

Bevezetés

A technológiai fejlődés egyik legdinamikusabban fejlődő területe napjainkban a mesterséges intelligencia (MI), amely egyre meghatározóbb szerepet tölt be a különböző iparágak működésében. Az MI algoritmusok képesek hatalmas mennyiségű adat feldolgozására, összefüggések felismerésére és intelligens döntések meghozatalára – mindezt egyre inkább valós időben, emberek közvetlen beavatkozása nélkül. Ezzel párhuzamosan fejlődnek a **kiber-fizikai rendszerek** (Cyber-Physical Systems – CPS), amelyek az információs technológia és a fizikai világ szoros integrációját valósítják meg. Ezek a rendszerek érzékelők, vezérlők, hálózatok és számítógépek segítségével képesek valós idejű adatgyűjtésre, -feldolgozásra és -reakciókra, miközben fizikai folyamatokkal lépnek kölcsönhatásba.

Az MI és CPS találkozása nem pusztán technológiai konvergencia, hanem egy újfajta rendszergondolkodás alapját is képezi, amely lehetővé teszi **adaptív, autonóm és tanulásra képes rendszerek** kialakítását. A hagyományos, statikus automatizált rendszerekkel szemben ezek az intelligens CPS megoldások képesek a környezeti változások felismerésére és azokhoz való dinamikus alkalmazkodásra. A gépi tanulás (Machine Learning – ML) és mélytanulás (Deep Learning – DL) algoritmusai kulcsszerepet játszanak abban, hogy a CPS rendszerek önálló tanulási és predikciós képességeket szerezzenek. Ennek köszönhetően a rendszerek nemcsak reagálnak a környezet változásaira, hanem előre is képesek jelezni bizonyos eseményeket, például egy gép meghibásodását vagy egy adott termelési szakasz optimalizálási lehetőségét.

A dolgozat központi célja annak részletes feltérképezése, hogy miként integrálhatók a mesterséges intelligencia különböző technológiái – mint például az ML pipeline-ok, MLOps gyakorlatok, digitális ikrek vagy számítógépes látás – a CPS rendszerekbe, és hogyan járulhatnak hozzá az adaptivitás, autonómia és hatékonyság növeléséhez. A tanulmány különös figyelmet fordít az ipari alkalmazásokra, de kitér a mezőgazdaság, az egészségügy, a honvédelem és az otthoni automatizálás területére is, ahol a MI+CPS rendszerek ígéretes megoldásokat kínálnak komplex problémákra.

Az elméleti háttér bemutatása mellett a dolgozat célja, hogy **rendszerszintű áttekintést** adjon az MI és CPS integrációs lehetőségeiről, különös tekintettel a gyakorlati megvalósításokra és technológiai kihívásokra. A témakör multidiszciplináris jellegéből adódóan a dolgozat elemzi az informatikai, elektronikai, gépészeti és üzleti szempontokat egyaránt, miközben konkrét példákon és esettanulmányokon keresztül szemlélteti a modern technológiák alkalmazását a valós világban.

Az MI alapú CPS rendszerek kulcsfontosságú szereplői lehetnek a negyedik ipari forradalom (Ipar 4.0) és a jövő digitális társadalmának, hiszen lehetővé teszik az **intelligens gyárak**, **önvezető járművek**, **precíziós mezőgazdasági rendszerek** vagy éppen **személyre szabott orvoslási megoldások** működését. A dolgozat célja, hogy hozzájáruljon e terület mélyebb megértéséhez, miközben gyakorlati szempontokat és jövőbeli irányokat is bemutat.

1. Adaptív autonóm rendszerek és tanulási folyamatok

A kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) olyan integrált technológiai megoldások, amelyek fizikai komponenseket (például szenzorokat, vezérlőegységeket, aktuátorokat) hálózatba kötött számítógépes rendszerekkel kombinálnak, lehetővé téve a valós idejű adatgyűjtést, feldolgozást és visszacsatolt működést. A hagyományos, előre programozott működésű CPS-ekkel szemben egyre nagyobb az igény az olyan rendszerek iránt, amelyek **adaptív módon**, azaz tanulásra és alkalmazkodásra képesen tudnak reagálni a környezeti változásokra. Ezt a képességet a mesterséges intelligencia – különösen a gépi tanulás (Machine Learning – ML) és a mélytanulás (Deep Learning – DL) – biztosítja, amelyek lehetővé teszik az **autonóm működést** a CPS rendszerekben.

1.1 A gépi tanulás szerepe a CPS rendszerekben

A gépi tanulás algoritmusai képesek adatminták alapján modelleket tanítani, amelyeket később predikciós és döntéshozatali folyamatok során alkalmaznak. A CPS rendszerek által begyűjtött szenzoradatok – például hőmérséklet, nyomás, rezgés, energiafogyasztás vagy mozgásadatok – folyamatosan tanulmányozhatók ML segítségével, így az adott rendszer működése **folyamatosan finomhangolható** [1].

A tanulás két fő módon járul hozzá az adaptivitáshoz:

- **Offline tanulás:** az adatok alapján előre betanított modellek vezérlik a működést. Ilyenek például a minőségellenőrzési rendszerek képfeldolgozó algoritmusai.
- **Online vagy valós idejű tanulás:** a rendszer folyamatosan alkalmazkodik az újonnan érkező adatokhoz, például egy okos robotkar, amely ismeretlen tárgyakat is képes manipulálni az élő szenzoradatok alapján.

1.2 Mélytanulás és autonóm döntéshozatal

A **mélytanulás** (DL) a gépi tanulás egyik speciális ága, amely többrétegű neurális hálózatokat alkalmaz a komplex mintázatok azonosítására. A DL kiemelkedő szerepet játszik azokban a CPS rendszerekben, ahol **nagy mennyiségű, strukturálatlan adat** keletkezik, például képek, hangok, időfüggő szenzorsorozatok formájában.

Az autonóm rendszerek működéséhez elengedhetetlen a mély tanuló modellek által biztosított:

- **környezetérzékelés** (pl. számítógépes látás vagy szenzorfúzió révén),
- **állapotfelismerés** (például rejtett Markov-modellek vagy RNN-ek segítségével),
- **döntéshozatal**, amely történhet szabályalapú rendszerekkel, vagy megerősítéses tanulással (reinforcement learning, RL)[2].

Például egy autonóm jármű esetében a DL modellek valós időben azonosítják az úton lévő akadályokat, értelmezik a közlekedési táblákat, és előre jelzik más közlekedők mozgását, lehetővé téve a biztonságos és autonóm navigációt.

1.3 Adaptivitás és környezeti változásokhoz való alkalmazkodás

Az egyik legfontosabb kihívás a CPS rendszerekben az **alkalmazkodóképesség** kialakítása. A dinamikusan változó környezet – például változó termelési követelmények, szezonális változások, gépek állapotromlása – miatt a rendszernek képesnek kell lennie a viselkedésének módosítására. A tanulás itt azt jelenti, hogy a rendszer:

- észleli a változást (detekció),
- azonosítja a változás jellegét (diagnózis),
- és módosítja a működését (adaptáció).

Ez a folyamat gyakran **MLOps** eszköztárral valósul meg, amely automatizálja az ML modellek újratanítását, validálását és telepítését a valós rendszerekbe. Az alkalmazkodás sikerességét a tanulási algoritmus robusztussága, a rendelkezésre álló adatok minősége és a rendszer architektúrája határozza meg.

1.4 Esettanulmányok és gyakorlati példák

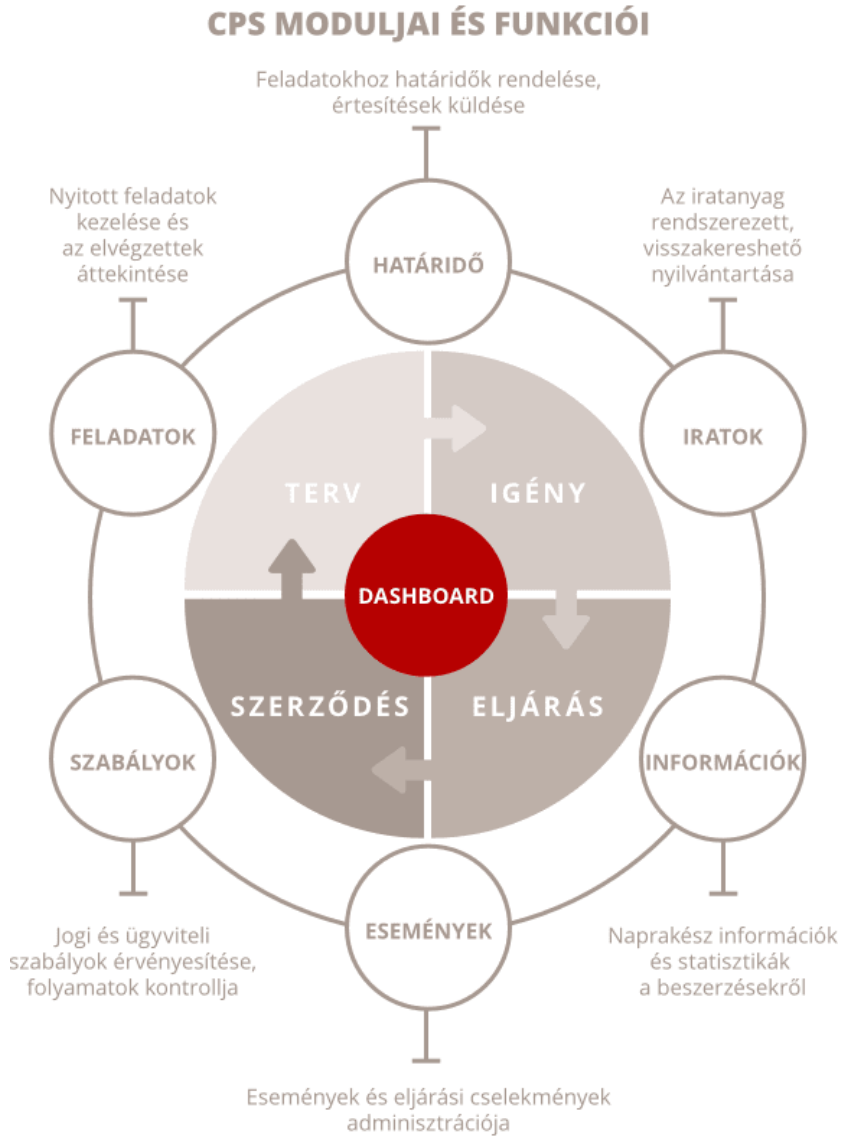
- **Prediktív karbantartás (Predictive Maintenance):** gépi tanulással a gépek állapotából származtatott minták alapján előrejelezhető, mikor fog egy gép meghibásodni, így optimalizálható a karbantartási ciklus [3].
- **Energiaoptimalizálás okos épületekben:** az MI képes megtanulni az épület használati szokásait és ehhez igazítva szabályozni a fűtést, világítást vagy szellőzést.
- **Robotika:** mobil robotok, drónok és ipari karok mozgásukban és működésükben is autonóm módon képesek alkalmazkodni a környezethez, például ember-robot kollaboratív gyártósorokon.

1.5 Kihívások és jövőbeli irányok

A tanulásra képes, autonóm CPS rendszerek kialakításának több akadálya is van:

- **Adatbiztonság:** a nagy mennyiségű érzékeny adat feldolgozása biztonsági és adatvédelmi problémákat vet fel.
- **Magyarázhatóság (Explainable AI – XAI):** a döntések átláthatósága elengedhetetlen a bizalom kialakításához különösen érzékeny területeken (pl. orvosi vagy katonai alkalmazások).
- **Valósidejűség:** a tanulási algoritmusoknak gyorsan kell reagálniuk az eseményekre, ami komoly számítási kapacitást igényel.

A jövő CPS rendszerei várhatóan egyre több **edge computing** (peremhálózati számítás) megoldást használnak, hogy a tanulási folyamatokat helyben, késleltetés nélkül tudják végrehajtani. Emellett a **megerősítéses tanulás**, az **önfelügyelt tanulás** és a **federált tanulás** is fontos szerephez jutnak, különösen elosztott rendszerekben.



1. ábra CPS Moduljai és funkciói

2. Ipari mesterséges intelligencia pipeline-ok

Az ipari automatizálás új korszakát hozta el a mesterséges intelligencia (MI), amely a hagyományos, szabályalapú rendszerek helyébe lépve képes összetett adathalmazokból tanulni, predikciókat készíteni és döntéseket támogatni. A gépi tanulás (ML) és mélytanulás (DL) technológiák integrációja az ipari folyamatokba lehetővé teszi a gyártás hatékonyságának, megbízhatóságának és rugalmasságának jelentős javítását. Ennek keretrendszerét képezi az ún. **ipari MI pipeline**, amely az adatok gyűjtésétől kezdve a modellek implementációján át a működésük monitorozásáig terjed.

2.1 Az MI pipeline felépítése ipari környezetben

Az ipari MI pipeline általában az alábbi főbb szakaszokra bontható[4]:

1. **Adatgyűjtés (Data Ingestion):** Szenzorok, IoT-eszközök, MES (Manufacturing Execution System), ERP és SCADA rendszerek biztosítják az adatok elsődleges forrásait. Az adatok típusa lehet időfüggő (pl. hőmérséklet), képi (pl. hibafelismerés), vagy strukturált (pl. termelési naplók).
2. **Adattisztítás és előfeldolgozás:** Az ipari adatok gyakran zajosak, hiányosak vagy redundánsak. A hatékony tanulás érdekében szükség van normalizálásra, szűrésre, hiányzó értékek kezelésére és adatszinkronizálásra[5].
3. **Jellemzők kiválasztása és mérnöki munka:** A cél az adatokból olyan jellemzők (feature-ök) kinyerése, amelyek jól reprezentálják az adott folyamat állapotát. Ez magában foglalhat statisztikai mutatókat (átlag, szórás), spektrális jellemzőket (FFT), vagy képfeldolgozási paramétereket.
4. **Modellezés:** Gépi tanulási algoritmusokat alkalmaznak a predikció, osztályozás vagy anomáliadetektálás céljából. Elterjedt modellek ipari környezetben: döntési fák (RF), SVM, neurális hálók (CNN, LSTM), valamint hibrid modellek.
5. **Értékelés és optimalizáció:** Keresztvalidáció, hiperparaméter-hangolás és metrikák (pl. F1-score, ROC-AUC, RMSE) segítségével történik a modellek értékelése és finomhangolása.
6. **Implementáció és élesítés:** A modellek integrálása történhet edge eszközökön, lokális szervereken vagy felhőalapú rendszerekben, a rendszer követelményeinek megfelelően.
7. **Monitorozás és visszacsatolás:** Az MI rendszer folyamatos felügyelet alatt áll, beleértve a modell drift detektálását és az újratanítást is, amely különösen fontos a dinamikusan változó ipari környezetben[6].

2.2 Főbb ipari alkalmazások

2.2.1 Termelésoptimalizálás

Az MI algoritmusok képesek optimalizálni az erőforrás-felhasználást, a gépek kihasználtságát és a munkafolyamatokat. Például egy gyártósoron az MI előre jelezheti, mely konfigurációk mellett csökken leginkább a selejtarány, vagy maximalizálható a termelési volumen.

- **Példa:** Egy autóipari vállalat neurális hálókat alkalmaz a gyártósor különböző szegmensein keletkező adatok korrelációjának azonosítására, így optimalizálva a gépátállások időzítését és sorrendjét.

2.2.2 Prediktív karbantartás (Predictive Maintenance)

A prediktív karbantartás célja a meghibásodások előrejelzése még azok bekövetkezése előtt. Ehhez az MI modellek időfüggő szenzoradatokat (pl. rezgés, hőmérséklet, nyomás) elemeznek, és mintázatokat keresnek a rendellenes működésre utaló jelek alapján.

- **Algoritmusok:** RNN, LSTM, autoencoderek és SVM egyaránt alkalmazhatók, attól függően, hogy időfüggő vagy statikus adatokról van szó.
- **Esettanulmány:** Egy gyártóüzem ventilátorainak állapotát figyelve egy gépi tanuló modell képes volt 92%-os pontossággal előre jelezni a csapágykopás mértékét, lehetővé téve az időben történő beavatkozást.

2.2.3 Minőségbiztosítás (Quality Control)

A gyártott termékek minőségének ellenőrzése gyakran manuálisan vagy egyszerű szabályalapú rendszerekkel történik. A mesterséges intelligencia lehetővé teszi a **valós idejű képfeldolgozáson** és **mintázatfelismerésen** alapuló automatizált ellenőrzést.

- **Alkalmazás:** CNN alapú modellek képesek felismerni repedéseket, szennyeződéseket vagy más hibákat akár mikroszkopikus szinten is.
- **Előnyök:** Nagy sebesség, alacsony hibatolerancia, taníthatóság új hibákra. A rendszer képes az új hibákat is detektálni folyamatos tanulással.

2.3 Technológiai integrációs szempontok

2.3.1 Szoftveres környezet

A pipeline implementációja történhet különféle MI platformokon:

- **Open-source eszközök:** TensorFlow, PyTorch, Scikit-learn
- **MLOps rendszerek:** MLflow, Kubeflow, Azure ML – ezek támogatják a modellek élettartam-kezelését, verziózását, CI/CD integrációt.

2.3.2 Hardveres támogatás

A tanítás és predikció igényei eltérőek:

- **Edge computing:** kis késleltetésű, beágyazott rendszerek (pl. NVIDIA Jetson, Intel Movidius).
- **Cloud computing:** skálázhatóság és nagy számítási kapacitás (pl. Amazon SageMaker, Google Vertex AI).

2.3.3 Integráció ipari rendszerekbe

Az MI pipeline sikeressége nagymértékben függ attól, hogy mennyire zökkenőmentesen illeszthető be a meglévő ipari informatikai környezetbe:

- **MES (Manufacturing Execution System)**
- **ERP rendszerek**
- **SCADA és PLC eszközök**

A sikeres integrációhoz szabványosított interfészek (OPC-UA, MQTT) és biztonságos adatátvitel szükséges.

2.4 Kihívások és jövőbeli irányok

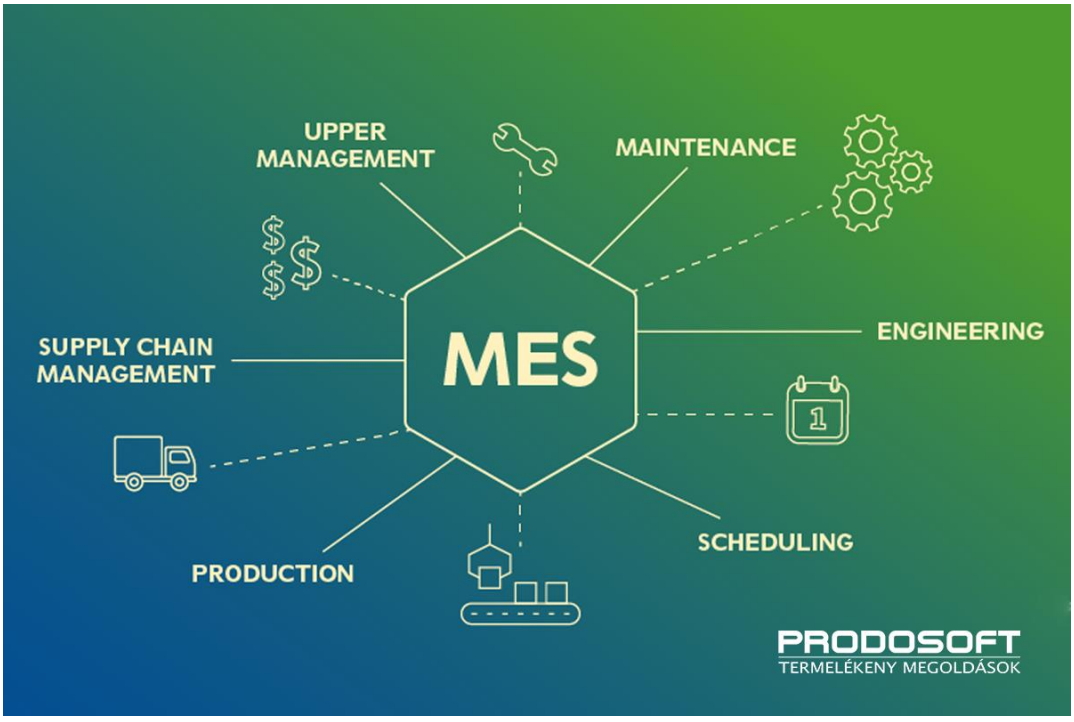
Bár az ipari MI pipeline-ok jelentős előrelépést kínálnak, több technikai és szervezeti kihívással is számolni kell:

- **Adatminőség:** A nem konzisztens, hiányos vagy torzított adatok gátolják a modellek megbízhatóságát.
- **Adatsilók megszüntetése:** Sok ipari vállalatnál az adatok el vannak különítve a rendszerek között, ami akadályozza a holisztikus optimalizálást.
- **Modelldrift:** A környezet változásával a tanított modellek pontossága romlik, újratanítás válik szükségessé.
- **Munkaerőhiány:** Az MI bevezetése új típusú szakértelmet igényel, amely hiányzik sok hagyományos ipari szereplőnél.

A jövőben várhatóan a **federált tanulás**, a **peremhálózati mesterséges intelligencia** és a **központi MLOps-platformok** további áttörést hoznak az ipari gépi tanulás skálázásában és fenntartásában.

3. MLOps és MES rendszerek

A mesterséges intelligencia (MI) gyártási környezetbe történő integrációja nem pusztán modellek kifejlesztését jelenti, hanem azok teljes életciklusának menedzselését. Ennek kulcsfontosságú eszköze az **MLOps** (Machine Learning Operations), amely az MI-fejlesztés DevOps-szerű keretrendszere. Az MLOps segítségével az ipari cégek képesek **automatikusan, skálázható módon és megbízhatóan** integrálni az MI-megoldásokat a **gyártásirányítási rendszerekbe (MES – Manufacturing Execution Systems)**, ezzel növelve a termelés hatékonyságát és rugalmasságát.



2. ábra MES rendszer, annak helye és szerepe

3.1 Az MLOps fogalma ipari környezetben

Az MLOps célja az MI rendszerek fejlesztésének, tesztelésének, telepítésének és monitorozásának **automatizálása és szabványosítása[7]**. Míg a klasszikus gépi tanulási projektek sokszor ad-hoc módon készülnek, az ipari alkalmazás megköveteli a **folyamatos működést, reprodukálhatóságot, verziókezelést, skálázhatóságot és robusztusságot**.

Az MLOps legfőbb komponensei:

- **Adatpipeline menedzsment** (Data versioning, lineage)
- **Modellek verziókezelése** és tárolása
- **CI/CD folyamatok MI modellekhez**
- **Automatizált modellek tréningje és retréningje**
- **Monitorozás és alulteljesítés észlelése** (model drift)
- **Auditálás és megfelelés** (pl. ISO 26262 autóiparban)

3.2 MES rendszerek és szerepük

A **Manufacturing Execution System (MES)** olyan szoftverrendszer, amely az üzemi szintű gyártási műveletek valós idejű nyomon követését és vezérlését végzi. Kapcsolatot biztosít az **üzemek fizikai infrastruktúrája** (gépek, szenzorok, PLC-k) és a **vállalati szintű információs rendszerek** (pl. ERP – Enterprise Resource Planning) között[8].

Főbb funkciók:

- Műszakirányítás és termelési ütemezés
- Minőségellenőrzés és hibadetektálás
- Karbantartáskövetés
- Raktárkezelés és anyagáramlás kontroll

A MES rendszerek az adatgyűjtés egyik fő forrásai, és kiváló belépési pontok az MI pipeline számára.

3.3 MLOps integrálása a MES rendszerekbe

3.3.1 Technikai architektúra

A **MES** gyűjti az adatokat, amelyeket az **MLOps pipeline** előfeldolgoz, modellez, majd a modell predikcióit visszacsatolja a MES-be vagy közvetlenül a gépekhez. Az MLOps rendszer így **valós idejű** döntéstámogatást nyújt.

3.3.2 Alkalmazási példák

- **Prediktív karbantartás:** MES rögzíti a gépek állapotát (pl. rezgés, hőmérséklet). Az MLOps pipeline egy ML modellt treníroz, amely előre jelzi az esetleges meghibásodásokat.

- **Adaptív termelés:** A MES-ből származó selejtarány-adatok alapján az MLOps pipeline újratanítja a modellt, amely javaslatot tesz a gyártási paraméterek optimalizálására.
- **Minőségellenőrzés:** A képfeldolgozó rendszerekből származó adatok feldolgozása, modellek frissítése automatikusan történik a MLOps pipeline-ban.

3.3.3 DevOps és MLOps összehasonlítása

Jellemző	**DevOps**	**MLOps**
Cél	Szoftververziók kezelése és üzemeltetés	ML modellek fejlesztése, deployolása
Verziókezelés	Kód	Kód + Adat + Modell
Tesztelés	Unit / Integration	Adatvalidálás, Modellvalidálás
Monitorozás	CPU, memória, logok	Modelldrift, predikciós hiba, adatszórás

3.4 Előnyök az ipari termelés szempontjából

1. Skálázhatóság

Az MLOps rendszerek lehetővé teszik több modell, több gyártósor és több lokáció párhuzamos kezelését. Egy jól konfigurált pipeline egyszerre képes több száz gyártási entitás prediktív modelljének futtatására.

2. Hatékonyság

Az automatizált tréning és deployálás időt és humánerőforrást takarít meg. A modellek frissítése és újratréningelése gyorsan, beavatkozás nélkül történik.

3. Reagálóképesség

A gyorsan változó környezeti feltételekhez való alkalmazkodás lehetősége jelentősen megnöveli a termelés rugalmasságát.

4. Reprodukálhatóság és átláthatóság

A modellverziók, adatforrások és feature-k változásai dokumentáltak, ami elengedhetetlen a gyártási auditok során.

3.5 Kihívások és megoldások

Kihívás	Lehetséges megoldás
Komplex integráció MES rendszerekkel	API-rétegek és OPC-UA protokoll segítségével szabványos adatkapcsolatok hozhatók létre, amelyek lehetővé teszik a különböző rendszerek közötti hatékony kommunikációt.
Modelldrift kezelése	A drift-detektorok és automatikus újratanítás lehetővé teszik, hogy a modell alkalmazkodjon a változó gyártási környezethez.
Verziókezelés és auditálhatóság	Az MLflow és DVC biztosítja a modellek verziókövetését, visszakereshetőségét és a fejlesztési lépések átláthatóságát.
Biztonsági aggályok	VPN-ek, titkosított adatkapcsolatok és szerepkör-alapú hozzáférés-kezelés (RBAC) növelik a rendszer védelmét az illetéktelen hozzáférés ellen.

3.6 Jövőbeli kilátások

A **felhőalapú MLOps platformok** (pl. Azure ML, AWS SageMaker) egyre szélesebb körű integrációt kínálnak MES rendszerekhez. A jövőben várhatóan elterjednek a **peremhálózati MI-megoldások** (Edge AI), amelyek lehetővé teszik az MI modellek **valós idejű, helyszíni működését**. Ezzel csökken a késleltetés és a hálózati függőség, növelve a rendszer megbízhatóságát.

4. Digitális ikrek alkalmazása a gyártási folyamatokban

A **Digitális iker (Digital Twin)** technológia egyre fontosabb szerepet tölt be az ipari digitalizációban, különösen a **kiber-fizikai rendszerek (CPS)** környezetében. A digitális iker nem csupán egy statikus modell, hanem egy **dinamikus, élő reprezentáció**, amely valós idejű adatokat használ a fizikai objektumok viselkedésének szimulálására, előrejelzésére és optimalizálására.

4.1 A digitális iker fogalma és architektúrája

A digitális iker egy fizikai entitás (pl. gép, gyártósor, termék) **digitális másolata**, amely folyamatos adatkapcsolatban áll az eredeti rendszerrel[10]. Ez lehetővé teszi a **monitorozást, szimulációt, predikciót** és döntéstámogatást.

A digitális iker rendszer fő komponensei:

1. **Fizikai entitás:** Szenzorokkal felszerelt gép vagy rendszer
2. **Adatgyűjtő infrastruktúra:** IoT szenzorok, SCADA, MES rendszerek
3. **Digitális modell:** A rendszer viselkedését leíró matematikai vagy gépi tanulási modell

4. **Kommunikációs interfész:** Valós idejű adatkapcsolat biztosítása (pl. MQTT, OPC-UA)
5. **Vizualizációs és analitikai felület:** Dashboardok, 3D szimulációk, AR/VR

4.2 A digitális ikrek szerepe a gyártásban

A gyártási folyamatok egyre komplexebbek, így a valós idejű megértésük és optimalizálásuk kulcsfontosságú. A digitális ikrek segítenek:

- **A működés valós idejű monitorozásában**
- **Szimulációk futtatásában – „mi lenne, ha" típusú kérdésekre**
- **Hibák előrejelzésében és elhárításában**
- **Erőforrás- és energiaoptimalizálásban**
- **Termékélettartam modellezésében és testreszabásában**

Konkrét ipari példák:

- **Autóipar:** A BMW digitális ikert használ a teljes gyártósor optimalizálására még a fizikai rendszer felépítése előtt[11].
- **Élelmiszeripar:** Nestlé a digitális ikerrel szimulálja az ellátási láncot és az energiafelhasználást.
- **Gyógyszeripar:** Gyártóberendezések folyamatparamétereinek valós idejű követése a megfelelőségi szabványok biztosítására (pl. GMP, FDA).

4.3 Szimuláció és predikció

A digitális ikrek egyik fő előnye, hogy valós idejű adatokkal kombinálva lehetővé teszik:

- **Folyamatok előrejelzése:** Pl. gépalkatrészek várható élettartama.
- **Szabályozási paraméterek tesztelése szimulált környezetben:** Valós beavatkozás nélküli próbák.
- **Többszörös szcenáriók összehasonlítása:** Például anyagválasztás vagy gyártási tempó hatása.

A szimulációk lehetnek **fizikai alapú modellek** (pl. mechanikai szimuláció) vagy **adatvezérelt modellek** (ML alapú előrejelzés).

4.4 Integráció mesterséges intelligenciával

A digitális ikrek hatékonyságát jelentősen növeli a **gépi tanulás és mesterséges intelligencia** bevonása:

- **Anomáliadetektálás:** Szokatlan viselkedés felismerése a fizikai rendszerhez képest.
- **Prediktív karbantartás:** AI előre jelzi a potenciális meghibásodásokat.
- **Önoptimalizáló gyártás:** A digitális iker folyamatosan tanul a működésből, és javaslatokat tesz a paraméterek finomhangolására.

4.5 Előnyök

Előny	Leírás
Valós idejű döntéstámogatás	Gyors reakciók környezeti változásokra
Költségcsökkentés	Hibák szimulációja még beavatkozás előtt
Termékminőség javítása	Pontosabb folyamatkontroll
Termelés rugalmassága	Különböző konfigurációk gyors tesztelése
Fenntarthatóság	Energiafogyasztás optimalizálása szimulációval

4.6 Kihívások

Bár a digitális iker technológia ígéretes, több kihívással is szembe kell nézni:

- **Adatintegráció:** Sokféle adatforrás szinkronizálása (MES, SCADA, ERP)
- **Skálázhatóság:** Nagy számú gép valós idejű másolatának kezelése
- **Szabványosítás:** Hiányoznak az egységes ipari szabványok
- **IT-biztonság:** Érzékeny működési adatok védelme
- **Szakértelem igénye:** A digitális modell felépítése multidiszciplináris tudást kíván

4.7 Jövőbeli trendek

A digitális ikrek jövője az **autonóm rendszerek** és a **felhő- + peremalapú MI kombinációjában** rejlik. A **Metaverse és AR/VR alapú interfészek** révén lehetőség nyílik arra, hogy a digitális ikreket nemcsak monitorozzuk, hanem **immerszív módon is interakcióba lépjünk velük**.

A legfejlettebb rendszerekben a digitális iker **önfejlesztő rendszerként** működik, amely automatikusan alkalmazkodik a környezethez, újratanítja modelljeit, és optimalizálja működését.

5. CPS és mesterséges intelligencia alkalmazása különböző ágazatokban

A **kiber-fizikai rendszerek (Cyber-Physical Systems, CPS)** és a **mesterséges intelligencia (AI)** integrációja forradalmasítja az ipar mellett a mezőgazdaságot, egészségügyet és a honvédelmet is. Ezekben az ágazatokban a **valós idejű adatgyűjtés, döntéshozatal és adaptív viselkedés** alapvetően új működési paradigmákat eredményez. A következőkben három jelentős szektort vizsgálunk meg részletesen.

3. ábra Mesterséges intelligencia használata cégeknek a Marketingben

5.1 Mezőgazdaság: Precíziós gazdálkodás MI-vel és szenzorhálózatokkal

5.1.1 Kontextus és kihívások

A modern mezőgazdaság célja a **termelékenység növelése és fenntarthatóság biztosítása** a természeti erőforrások megőrzése mellett. A CPS alapú rendszerek szenzoradatokra épülve képesek optimalizálni az inputokat (víz, műtrágya, növényvédő szer), miközben az AI segít a döntések meghozatalában.

5.1.2 Technológiai összetevők

- **Szenzorhálózatok:** Talajnedvesség, pH, hőmérséklet, páratartalom, fényintenzitás mérése.
- **Dronok és képfeldolgozás:** Növényállapot, betegségek felismerése.
- **Gépi tanulás:** Betegségek automatikus detektálása, hozam előrejelzés.
- **Edge computing:** Lokális adatfeldolgozás gyors döntéshozatalhoz.

5.1.3 Példák

- **John Deere** önvezető traktorai és okos permetezőrendszerei valós idejű adatgyűjtéssel és gépi tanulással működnek[12].
- **Climate FieldView**: Felhőalapú rendszer, amely szenzoradatokat és gépi tanulást kombinál a talaj- és növényanalízisre.

5.2 Orvostudomány: Személyre szabott gyógyászat MI és CPS integrációval

5.2.1 Kontextus

Az egészségügy digitális átalakulásának középpontjában az **adatalapú diagnosztika és terápia** áll. CPS rendszerek segítségével a beteg állapota valós időben követhető, míg az AI algoritmusok a személyre szabott kezelést támogatják.

5.2.2 Kulcstechnológiák

- **Orvosi képfeldolgozás (DL):** MRI, CT, röntgen képek elemzése.
- **Genetikai adatelemzés:** Genomszekvenálás alapján predikciók pl. rák hajlamra.
- **Viselhető eszközök (IoT):** Szívritmus, vércukorszint, alvásmonitorozás.
- **Digitális ikrek a gyógyászatban:** Beteg-specifikus szimulációk (pl. gyógyszerhatás előrejelzése).

4. ábra Orvosi képfeldolgozás: a formázástól az értelmezésig

5.2.3 Példák

- **IBM Watson Health** elemzi az onkológiai eseteket és terápiás javaslatot tesz több ezer kutatás alapján.
- **DeepMind Health (Google):** Retina szkennelés alapján mesterséges intelligenciával előre jelzi a vakságot okozó állapotokat.

Előnyök:

Előny	Példa
Gyorsabb diagnózis	Tüdőrák korai felismerése AI-val CT-képek alapján
Kezelés személyre szabása	Genetikai profil alapján célzott terápia
Folyamatos betegmonitorozás	IoT eszközök + CPS rendszer

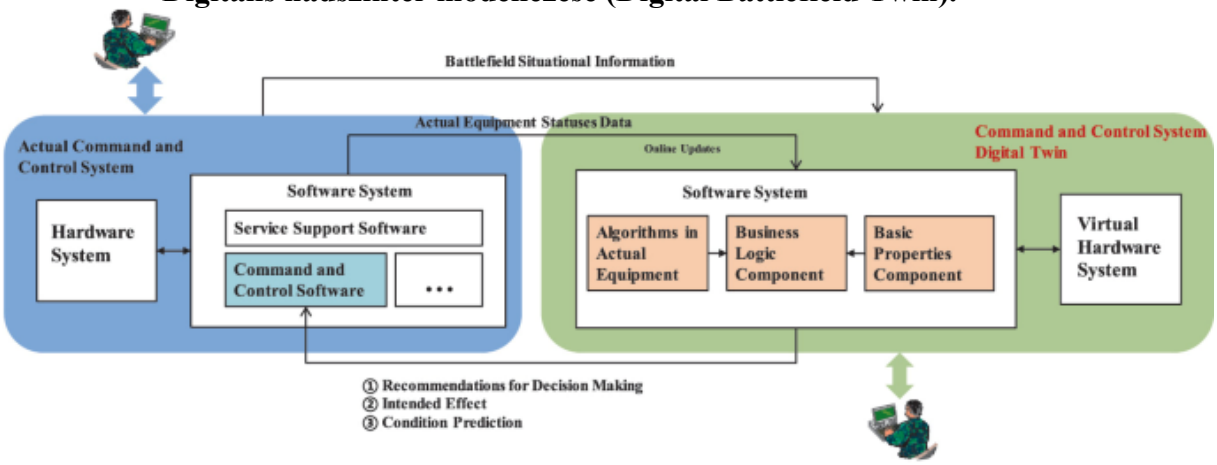
5.3 Honvédelem: Intelligens döntéshozatali rendszerek

5.3.1 Kontextus

A katonai rendszerek nagy mértékben támaszkodnak valós idejű helyzetértékelésre, gyors és pontos döntéshozatalra. CPS és MI integrációja itt nemcsak előnyt, hanem biztonsági követelményt is jelent.

5.3.2 Alkalmazási területek

- **Autonóm rendszerek:** Drónok, szárazföldi robotok önálló navigációja és célazonosítása.
- **Prediktív fenyegetés-azonosítás:** Mesterséges intelligencia segítségével anomáliafelismerés (pl. ellenséges mozgások).
- **Hálózati biztonság:** MI-alapú kiberfenyegetés-észlelés.
    - **Digitális hadszíntér modellezése (Digital Battlefield Twin).**



5. ábra Digitális iker csatatér kialakítása a vezetés és irányítás központi szerepével

5.3.3 Példák

- **DARPA's OFFSET program**: Autonóm drónrajok alkalmazása városi környezetben történő taktikai műveletekhez[13].
- **Project Maven (USA)**: Katonai drónfelvételek elemzése mélytanulás segítségével a célpontok automatikus felismeréséhez.

Etikai kérdések

- **Autonóm fegyverek problémája**
- **Döntéshozatal átláthatósága**
- **Civil célpontok védelme**

5.4 Összegzés

A különböző szektorokban tapasztalható **MI és CPS konvergencia** révén egyre inkább **adaptív, intelligens és autonóm rendszerek** jönnek létre. A mezőgazdaságban a fenntartható és precíz gazdálkodás, az egészségügyben a személyre szabott gyógyászat, a honvédelemben pedig a valós idejű stratégiai döntéshozatal terén mutatkoznak meg leginkább ezek az előnyök. A kihívások ellenére a technológiai fejlődés ezen ágazatokban is gyors és hatékony változásokat hoz.

6. A gépi látás szerepe a CPS rendszerekben

A **gépi látás (computer vision, CV)** a mesterséges intelligencia egyik kulcsterülete, amely lehetővé teszi a számítógépek és beágyazott rendszerek számára a vizuális információk észlelését, értelmezését és feldolgozását. A **kiber-fizikai rendszerek (CPS)** kontextusában a gépi látás olyan szenzorrendszert jelent, amely **kameraalapú észlelést** és **valós idejű döntéshozatalt** tesz lehetővé automatizált folyamatok irányításához és felügyeletéhez.

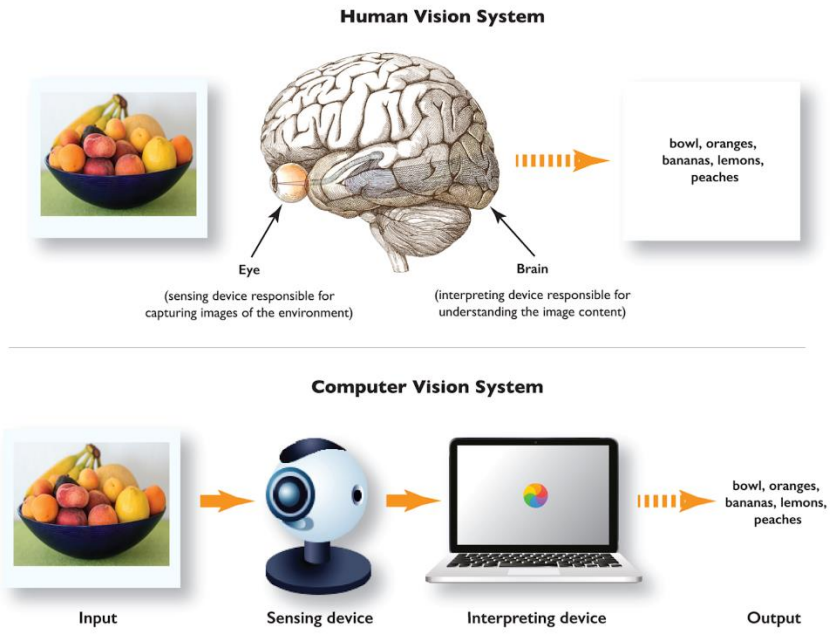
6.1 Ipari automatizálás

6.1.1 Minőségellenőrzés és hibadetektálás

Az ipari termelés során a gépi látás kulcsszerepet játszik a **minőségbiztosítás automatizálásában**. A kamerák valós időben pásztázzák a gyártósorokon áthaladó alkatrészeket, míg a CV-algoritmusok képesek detektálni:

- Felületi hibákat (karcolás, repedés)
- Méretbeli eltéréseket
- Helytelen összeszerelést

A **mélytanulás-alapú detektorok** képesek tanulni a tipikus hibákat, így az új típusú eltérések felismerésére is alkalmasak[14].



6. ábra Gépi látás összehasonlítása az emberi látással

6.1.2 Robotikai irányítás

A gépi látás támogatja az **ipari robotkarok vezérlését** például a:

- Célpont-azonosításban
- Precíziós megfogásban
- Dinamikus mozgástervezésben (pl. futószalagon mozgó tárgyak követése)

Példa: A **Fanuc** és a **KUKA** robotkarjai beépített 2D/3D kamerarendszerekkel azonosítják a tárgyakat, és képesek azokat irányba állítani vagy szortírozni.

6.1.3 Előnyök

- **Sebesség**: Milliszekundumos reakcióidő
- **Pontosság**: Mikron szintű hibadetektálás
- **Költségcsökkentés**: Kevesebb selejt és emberi hiba

6.2 Közlekedésirányítás

6.2.1 Forgalomfigyelő rendszerek

A városi és autópályás közlekedésirányítás során a gépi látás lehetővé teszi:

- **Járműszámlálás** és **áramlási elemzés**
- **Rendszámtábla-felismerés (ANPR)** bírságolás és beléptetés céljából
- **Torlódás- vagy balesetészlelés** valós időben

Példa: A **Budapesti Közlekedési Központ (BKK)** forgalomfigyelő rendszerei képesek gépi látással azonosítani a torlódásokat és automatikusan adaptálni a lámpák vezérlését.

6.2.2 Autonóm járművek

Az autonóm közlekedés egyik alappillére a látásalapú szenzorhasználat. A gépjárművekben alkalmazott kamerák és MI-modellek az alábbi funkciókat látják el:

- **Sávdetekció**
- **Közlekedési táblák felismerése**
- **Gyalogosok, kerékpárosok és más járművek követése**

Ezek a látásalapú érzékelők gyakran **LIDAR-ral és radarral** együtt működnek egy szenzorfúziós rendszerben.

6.2.3 AI-alapú forgalom-optimalizáció

A kamerákból érkező képadatok alapján mesterséges intelligencia vezérelheti:

- Zöld hullámokat
- Dinamikus forgalomterelést
- Torlódások predikcióját

6.3 Biztonságtechnika

6.3.1 Arc- és mozgásfelismerés

A biztonságtechnikai rendszerek egyik legfontosabb eleme a **felismerés és riasztás**. Gépi látással lehetőség nyílik:

- **Arcazonosításra** (pl. belépési rendszerekben)
- **Viselkedéselemzésre** (pl. illetéktelen mozgás, szokatlan aktivitás)
- **Mozgásdetekcióra** sötétben is (pl. hőkamerával)

Példa: A kínai **"Skynet" rendszer** képes országos szinten követni személyeket nyilvános kamerákból származó képek alapján.

6.3.2 Objektumkövetés és behatolásjelzés

- Érzékeli, ha egy személy átlép egy határvonalat vagy elhagyott csomag jelenik meg.
- Repülőtereken, katonai létesítményeknél kiemelten fontos.

6.3.3 Etikai és adatvédelmi aggályok

- **Adatkezelés**: Arcadatok tárolása
- **Megfigyelés**: Folyamatos videómonitorozás
- **Hamis pozitív riasztások** veszélye (pl. viselkedéselemző rendszereknél)

6.4 Gépi látás előnyei CPS-ben

Alkalmazási terület	Gépi látás előnye
Ipar	Gyors, precíz minőségellenőrzés
Közlekedés	Valós idejű torlódásfigyelés
Biztonság	Részletes személy- és viselkedés-azonosítás

6.5 Összegzés

A **gépi látás a CPS rendszerek egyik legkritikusabb érzékelési technológiája**, mely lehetővé teszi a valós világban történő események digitális értelmezését. Az ipari gyártás, közlekedésirányítás és biztonságtechnika példái is mutatják, hogy a kameraalapú adatfeldolgozás nemcsak hatékony, de adaptív és autonóm működést is támogat. Az algoritmusok fejlődésével és a számítási kapacitások bővülésével ezek a rendszerek egyre megbízhatóbbak és intelligensebbek lesznek.

7. Intelligens otthonok optimalizálása: Szenzoradatok szerepe az energiahatékonyságban és komfortnövelésben

Az **intelligens otthonok (smart homes)** a kiber-fizikai rendszerek egyik legismertebb és legdinamikusabban fejlődő alkalmazási területét képezik. Ezek a rendszerek különféle **szenzorokkal, aktuátorokkal és mesterséges intelligenciával** integrált környezetek, melyek célja a lakók kényelmének növelése, az energiafelhasználás optimalizálása, valamint a biztonság és automatizáció biztosítása.

7.1 Az intelligens otthonok architektúrája

Egy tipikus intelligens otthon a következő fő komponensekből áll:

- **Szenzorok**: hőmérséklet, páratartalom, mozgás, fény, CO_2, hang, ajtó/ablak nyitás
- **Vezérlők / aktuátorok**: termosztát, árnyékolók, világítás, fűtés/hűtés, háztartási eszközök
- **Gateway és vezérlőlogika**: edge vagy felhőalapú központi egység
- **MI-alapú döntéshozatal**: időalapú szabályok, felhasználói szokások tanulása, predikció

A szenzoradatok folyamatos gyűjtésével és feldolgozásával a rendszer képessé válik **valós idejű döntések meghozatalára** és **tanulásra** a felhasználói preferenciák alapján[15].

7.2 Energiahatékonyság szenzoradatok segítségével

7.2.1 Intelligens fűtés, hűtés és világítás

Az energiafogyasztás optimalizálásának egyik legfontosabb területe a **fűtés-hűtés és világítás vezérlése**. A rendszer:

- **Hőmérsékletszenzor** alapján szabályozza a termosztátot, figyelembe véve a kültéri időjárást is.
- **Mozgásérzékelőkkel** lekapcsolja a fűtést vagy világítást nem használt helyiségekben.
- **Fényérzékelőkkel** szabályozza a mesterséges világítást a természetes fényviszonyokhoz igazítva.

7.2.2 Időalapú és prediktív vezérlés

A gépi tanulás segíthet a rendszernek előre jelezni, mikor tartózkodnak otthon a lakók, és **előfűteni vagy -hűteni** az otthont ennek megfelelően.

Példa: A Nest termosztát megtanulja a lakók napi rutinját, és ennek alapján szabályozza a hőmérsékletet, akár 10–15%-os energia-megtakarítást is eredményezve[16].

7.2.3 Integráció napelemekkel és energiatárolással

A modern intelligens otthonokban a rendszer képes **napelemekkel és akkumulátorokkal** együttműködni:

- Optimalizálja a fogyasztást a napenergia rendelkezésre állásához.
- Tölti az akkumulátort alacsony tarifás időszakban, és kisüti csúcsidőben.

7.3 Komfortnövelés MI segítségével

7.3.1 Szokások tanulása és automatizáció

A gépi tanulás képes felismerni az egyéni **életviteli mintákat**:

- Mikor szeret a felhasználó világítást vagy zenét?
- Milyen hőmérsékletet részesít előnyben különböző napszakokban?

A rendszer alkalmazkodik ezekhez és személyre szabott szolgáltatást nyújt.

7.3.2 Hangvezérlés és természetes nyelvfeldolgozás

A hangalapú asszisztensek, mint a Google Assistant, Alexa vagy Siri, **természetes módon** teszik lehetővé az otthoni eszközök vezérlését. A CV és NLP integráció révén a lakók képesek akár látás- és mozgásérzékeléssel kombinált hangutasításokkal is vezérelni a környezetet.

7.3.3 Komfort az egészségi állapot figyelembevételével

Az intelligens otthon képes monitorozni a levegőminőséget (CO_2, VOC), a zajszintet és a fényviszonyokat. Idősek esetében az elesésdetekció vagy pulzusszám monitorozás szintén a komfort és biztonság kombinációját szolgálja.

7.4 Gépi tanulási algoritmusok a smart home rendszerekben

A leggyakrabban alkalmazott MI-algoritmusok:

Algoritmus	**Alkalmazási terület**
K-means clustering	Szokásminták klaszterezése
Decision Trees	Eszközvezérlési szabályok automatikus generálása
Neural Networks	Hőmérséklet- vagy energiafogyasztás predikció
Reinforcement Learning	Valós idejű döntéshozatal tanulása

7.5 Adatbiztonság és adatvédelem

Az intelligens otthonok egyik kritikus kihívása az adatvédelem:

- A lakók napi rutinja, jelenléte, szokásai érzékeny információk.
- A rendszer gyakran felhőkapcsolattal rendelkezik – adatátvitel és -tárolás során titkosítás szükséges.
- Edge computing lehet alternatíva: az adatok helyben történő feldolgozása csökkenti a kockázatot.

7.6 Összefoglalás

Az intelligens otthonok nem csupán kényelmi funkciókat nyújtanak, hanem aktívan hozzájárulnak az energiahatékonysághoz és a fenntartható életmódhoz. A **szenzoradatok feldolgozása és MI-alapú elemzése** lehetővé teszi a dinamikus vezérlést, tanulást és adaptív működést. Az autonóm és önfejlődő otthonrendszerek egyre elérhetőbbé válnak, de a további fejlődésük záloga az adatbiztonság, a szabványosítás és az interoperabilitás.

Záró gondolatok:

A mesterséges intelligencia integrációja a kiber-fizikai rendszerekbe (CPS) napjaink egyik legdinamikusabban fejlődő technológiai irányzata, amely jelentős hatást gyakorol az ipari, mezőgazdasági, egészségügyi és védelmi szektorokra egyaránt. Az MI-alapú adaptív rendszerek révén a CPS-ek képesek valós idejű döntéseket hozni, alkalmazkodni a környezet változásaihoz, és autonóm módon optimalizálni működésüket. Az olyan technológiák, mint a gépi tanulás, digitális ikrek, MLOps vagy a számítógépes látás, új szintre emelik a hatékonyságot, megbízhatóságot és prediktív képességet. Ugyanakkor az MI és CPS konvergenciája új kihívásokat is felvet – például a rendszerbiztonság, adatvédelem vagy etikai kérdések terén –, amelyek megoldása nélkülözhetetlen ahhoz, hogy ezek a technológiák széles körben és fenntartható módon legyenek alkalmazhatók a jövőben.

Források:

[1] M. Lee et al., "Machine Learning for Cyber-Physical Systems: Challenges and Opportunities,"

[2] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, May 2015.

[3] A. Jardine et al., "A review on machinery diagnostics and prognostics implementing condition-based maintenance," *Mechanical Systems and Signal Processing*, vol. 20, no. 7, pp. 1483–1510, 2006.

[4] B. Zhang et al., "An Industrial Artificial Intelligence Pipeline: Challenges and Case Studies," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 3, pp. 1994–2005, Mar. 2021.

[5] F. Chollet, *Deep Learning with Python*, Manning Publications, 2018.

[6] A. Ghosh and M. Lee, "Lifecycle Management of ML in Industrial CPS," *ACM Journal on Emerging Technologies*, vol. 16, no. 4, pp. 1–19, 2020.

[7] M. Villela, "MLOps: Continuous Delivery and Automation Pipelines in Machine Learning," *O'Reilly Media*, 2021.

[8] L. Monostori et al., "Cyber-physical systems in manufacturing," *CIRP Annals*, vol. 65, no. 2, pp. 621–641, 2016.

[9] M. Zaharia et al., "Accelerating the Machine Learning Lifecycle with MLflow," *IEEE Data Eng. Bull.*, vol. 41, no. 4, pp. 39–45, Dec. 2018.

[10] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in *Transdisciplinary Perspectives on Complex Systems*, Springer, 2017, pp. 85–113.

[11] R. Rosen et al., "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.

[12] J. Evans and P. Smith, "Precision Agriculture: Smart Farming with Sensors, AI, and Robotics," *IEEE Industrial Electronics Magazine*, vol. 14, no. 3, pp. 23–31, Sept. 2020.

[13] DARPA, "OFFSET: Offensive Swarm-Enabled Tactics,".

[14] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[15] M. Mozer, "The neural network house: An environment that adapts to its inhabitants," *AAAI Spring Symposium*, 1998.

[16] S. Darby, "Smart metering: What potential for householder engagement?" *Building Research & Information*, vol. 38, no. 5, pp. 442–457, 2010.

[17] Industry 4.0 and Digital Twins in Manufacturing https://www.researchgate.net/publication/328982819_Design_of_a_high-effective_fault-tolerance_double-stator_magnetless_vernier_machine_for_direct-drive_robotics

[18] MLOps: Continuous delivery and automation pipelines in machine learning https://cloud.google.com/architecture/mlops-continuous-delivery-and-automation-pipelines-in-machine-learning

[19] Smart Home Technologies and Sensor Systems https://www.mdpi.com/1424-8220/20/17/4767

2.45. Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF INFORMATICS

IPAR 4.0 TECHNOLÓGIÁK

Mesterséges intelligencia és alkalmazásai CPS keretrendszerekben

Mózes Márton
[redacted]
2024/2025/2

Tartalom

Bevezetés 4

1. Adaptív autonóm rendszerek és tanulási folyamatok 5

1.1 A gépi tanulás szerepe a CPS rendszerekben 5

1.2 Mélytanulás és autonóm döntéshozatal 5

1.3 Adaptivitás és környezeti változásokhoz való alkalmazkodás 6

1.4 Esettanulmányok és gyakorlati példák 6

1.5 Kihívások és jövőbeli irányok 6

2. Ipari mesterséges intelligencia pipeline-ok 7

2.1 Az MI pipeline felépítése ipari környezetben 8

2.2 Főbb ipari alkalmazások 8

2.3 Technológiai integrációs szempontok 9

2.4 Kihívások és jövőbeli irányok 10

3. MLOps és MES rendszerek 10

3.1 Az MLOps fogalma ipari környezetben 11

3.2 MES rendszerek és szerepük 11

3.3 MLOps integrálása a MES rendszerekbe 11

3.4 Előnyök az ipari termelés szempontjából 12

3.5 Kihívások és megoldások 13

3.6 Jövőbeli kilátások 13

4. Digitális ikrek alkalmazása a gyártási folyamatokban 13

4.1 A digitális iker fogalma és architektúrája 13

4.2 A digitális ikrek szerepe a gyártásban 14

4.3 Szimuláció és predikció 14

4.4 Integráció mesterséges intelligenciával 14

4.5 Előnyök 15

4.6 Kihívások 15

4.7 Jövőbeli trendek 15

5. CPS és mesterséges intelligencia alkalmazása különböző ágazatokban 15

5.1 Mezőgazdaság: Precíziós gazdálkodás MI-vel és szenzorhálózatokkal 16

5.2 Orvostudomány: Személyre szabott gyógyászat MI és CPS integrációval 16

5.3 Honvédelem: Intelligens döntéshozatali rendszerek 17

5.4 Összegzés 18

6. A gépi látás szerepe a CPS rendszerekben 19

6.1 Ipari automatizálás 19

6.2 Közlekedésirányítás 20
6.3 Biztonságtechnika 21
6.4 Gépi látás előnyei CPS-ben 21
6.5 Összegzés 21
7. Intelligens otthonok optimalizálása: Szenzoradatok szerepe az energiahatékonyságban és komfortnövelésben 22
7.1 Az intelligens otthonok architektúrája 22
7.2 Energiahatékonyság szenzoradatok segítségével 22
7.3 Komfortnövelés MI segítségével 23
7.4 Gépi tanulási algoritmusok a smart home rendszerekben 23
7.5 Adatbiztonság és adatvédelem 24
7.6 Összefoglalás 24
Záró gondolatok: 24
Források: 25

Bevezetés

A technológiai fejlődés egyik legdinamikusabban fejlődő területe napjainkban a mesterséges intelligencia (MI), amely egyre meghatározóbb szerepet tölt be a különböző iparágak működésében. Az MI algoritmusok képesek hatalmas mennyiségű adat feldolgozására, összefüggések felismerésére és intelligens döntések meghozatalára – mindezt egyre inkább valós időben, emberek közvetlen beavatkozása nélkül. Ezzel párhuzamosan fejlődnek a **kiber-fizikai rendszerek** (Cyber-Physical Systems – CPS), amelyek az információs technológia és a fizikai világ szoros integrációját valósítják meg. Ezek a rendszerek érzékelők, vezérlők, hálózatok és számítógépek segítségével képesek valós idejű adatgyűjtésre, -feldolgozásra és -reakciókra, miközben fizikai folyamatokkal lépnek kölcsönhatásba.

Az MI és CPS találkozása nem pusztán technológiai konvergencia, hanem egy újfajta rendszergondolkodás alapját is képezi, amely lehetővé teszi **adaptív, autonóm és tanulásra képes rendszerek** kialakítását. A hagyományos, statikus automatizált rendszerekkel szemben ezek az intelligens CPS megoldások képesek a környezeti változások felismerésére és azokhoz való dinamikus alkalmazkodásra. A gépi tanulás (Machine Learning – ML) és mélytanulás (Deep Learning – DL) algoritmusai kulcsszerepet játszanak abban, hogy a CPS rendszerek önálló tanulási és predikciós képességeket szerezzenek. Ennek köszönhetően a rendszerek nemcsak reagálnak a környezet változásaira, hanem előre is képesek jelezni bizonyos eseményeket, például egy gép meghibásodását vagy egy adott termelési szakasz optimalizálási lehetőségét.

A dolgozat központi célja annak részletes feltérképezése, hogy miként integrálhatók a mesterséges intelligencia különböző technológiái – mint például az ML pipeline-ok, MLOps gyakorlatok, digitális ikrek vagy számítógépes látás – a CPS rendszerekbe, és hogyan járulhatnak hozzá az adaptivitás, autonómia és hatékonyság növeléséhez. A tanulmány különös figyelmet fordít az ipari alkalmazásokra, de kitér a mezőgazdaság, az egészségügy, a honvédelem és az otthoni automatizálás területére is, ahol a MI+CPS rendszerek ígéretes megoldásokat kínálnak komplex problémákra.

Az elméleti háttér bemutatása mellett a dolgozat célja, hogy **rendszerszintű áttekintést** adjon az MI és CPS integrációs lehetőségeiről, különös tekintettel a gyakorlati megvalósításokra és technológiai kihívásokra. A témakör multidiszciplináris jellegéből adódóan a dolgozat elemzi az informatikai, elektronikai, gépészeti és üzleti szempontokat egyaránt, miközben konkrét példákon és esettanulmányokon keresztül szemlélteti a modern technológiák alkalmazását a valós világban.

Az MI alapú CPS rendszerek kulcsfontosságú szereplői lehetnek a negyedik ipari forradalom (Ipar 4.0) és a jövő digitális társadalmának, hiszen lehetővé teszik az **intelligens gyárak**, **önvezető járművek**, **precíziós mezőgazdasági rendszerek** vagy éppen **személyre szabott orvoslási megoldások** működését. A dolgozat célja, hogy hozzájáruljon e terület mélyebb megértéséhez, miközben gyakorlati szempontokat és jövőbeli irányokat is bemutat.

1. Adaptív autonóm rendszerek és tanulási folyamatok

A kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) olyan integrált technológiai megoldások, amelyek fizikai komponenseket (például szenzorokat, vezérlőegységeket, aktuátorokat) hálózatba kötött számítógépes rendszerekkel kombinálnak, lehetővé téve a valós idejű adatgyűjtést, feldolgozást és visszacsatolt működést. A hagyományos, előre programozott működésű CPS-ekkel szemben egyre nagyobb az igény az olyan rendszerek iránt, amelyek **adaptív módon**, azaz tanulásra és alkalmazkodásra képesen tudnak reagálni a környezeti változásokra. Ezt a képességet a mesterséges intelligencia – különösen a gépi tanulás (Machine Learning – ML) és a mélytanulás (Deep Learning – DL) – biztosítja, amelyek lehetővé teszik az **autonóm működést** a CPS rendszerekben.

1.1 A gépi tanulás szerepe a CPS rendszerekben

A gépi tanulás algoritmusai képesek adatminták alapján modelleket tanítani, amelyeket később predikciós és döntéshozatali folyamatok során alkalmaznak. A CPS rendszerek által begyűjtött szenzoradatok – például hőmérséklet, nyomás, rezgés, energiafogyasztás vagy mozgásadatok – folyamatosan tanulmányozhatók ML segítségével, így az adott rendszer működése **folyamatosan finomhangolható** [1].

A tanulás két fő módon járul hozzá az adaptivitáshoz:

- **Offline tanulás:** az adatok alapján előre betanított modellek vezérlik a működést. Ilyenek például a minőségellenőrzési rendszerek képfeldolgozó algoritmusai.
- **Online vagy valós idejű tanulás:** a rendszer folyamatosan alkalmazkodik az újonnan érkező adatokhoz, például egy okos robotkar, amely ismeretlen tárgyakat is képes manipulálni az élő szenzoradatok alapján.

1.2 Mélytanulás és autonóm döntéshozatal

A **mélytanulás** (DL) a gépi tanulás egyik speciális ága, amely többrétegű neurális hálózatokat alkalmaz a komplex mintázatok azonosítására. A DL kiemelkedő szerepet játszik azokban a CPS rendszerekben, ahol **nagy mennyiségű, strukturálatlan adat** keletkezik, például képek, hangok, időfüggő szenzorsorozatok formájában.

Az autonóm rendszerek működéséhez elengedhetetlen a mély tanuló modellek által biztosított:

- **környezetérzékelés** (pl. számítógépes látás vagy szenzorfúzió révén),
- **állapotfelismerés** (például rejtett Markov-modellek vagy RNN-ek segítségével),
- **döntéshozatal**, amely történhet szabályalapú rendszerekkel, vagy megerősítéses tanulással (reinforcement learning, RL)[2].

Például egy autonóm jármű esetében a DL modellek valós időben azonosítják az úton lévő akadályokat, értelmezik a közlekedési táblákat, és előre jelzik más közlekedők mozgását, lehetővé téve a biztonságos és autonóm navigációt.

1.3 Adaptivitás és környezeti változásokhoz való alkalmazkodás

Az egyik legfontosabb kihívás a CPS rendszerekben az **alkalmazkodóképesség** kialakítása. A dinamikusan változó környezet – például változó termelési követelmények, szezonális változások, gépek állapotromlása – miatt a rendszernek képesnek kell lennie a viselkedésének módosítására. A tanulás itt azt jelenti, hogy a rendszer:

- észleli a változást (detekció),
- azonosítja a változás jellegét (diagnózis),
- és módosítja a működését (adaptáció).

Ez a folyamat gyakran **MLOps** eszköztárral valósul meg, amely automatizálja az ML modellek újratanítását, validálását és telepítését a valós rendszerekbe. Az alkalmazkodás sikerességét a tanulási algoritmus robusztussága, a rendelkezésre álló adatok minősége és a rendszer architektúrája határozza meg.

1.4 Esettanulmányok és gyakorlati példák

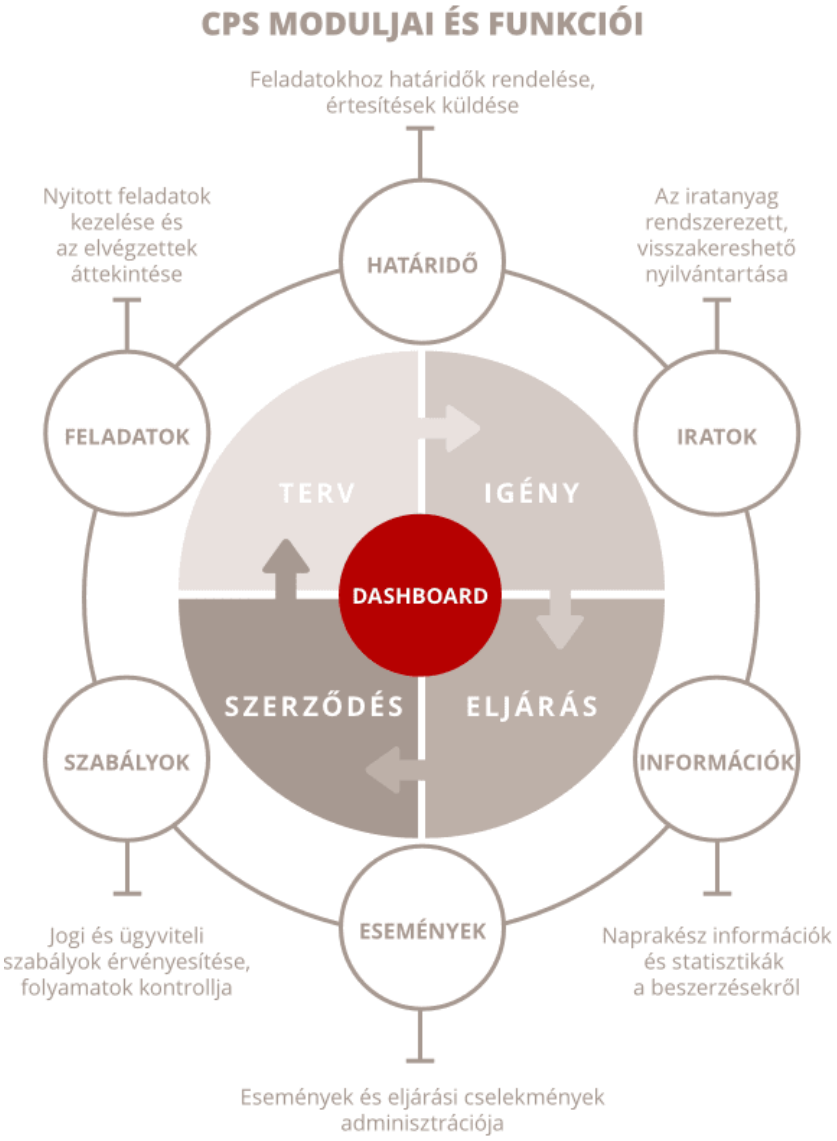
- **Prediktív karbantartás (Predictive Maintenance):** gépi tanulással a gépek állapotából származtatott minták alapján előrejelezhető, mikor fog egy gép meghibásodni, így optimalizálható a karbantartási ciklus [3].
- **Energiaoptimalizálás okos épületekben:** az MI képes megtanulni az épület használati szokásait és ehhez igazítva szabályozni a fűtést, világítást vagy szellőzést.
- **Robotika:** mobil robotok, drónok és ipari karok mozgásukban és működésükben is autonóm módon képesek alkalmazkodni a környezethez, például ember-robot kollaboratív gyártósorokon.

1.5 Kihívások és jövőbeli irányok

A tanulásra képes, autonóm CPS rendszerek kialakításának több akadálya is van:

- **Adatbiztonság:** a nagy mennyiségű érzékeny adat feldolgozása biztonsági és adatvédelmi problémákat vet fel.
- **Magyarázhatóság (Explainable AI – XAI):** a döntések átláthatósága elengedhetetlen a bizalom kialakításához különösen érzékeny területeken (pl. orvosi vagy katonai alkalmazások).
- **Valósidejűség:** a tanulási algoritmusoknak gyorsan kell reagálniuk az eseményekre, ami komoly számítási kapacitást igényel.

A jövő CPS rendszerei várhatóan egyre több **edge computing** (peremhálózati számítás) megoldást használnak, hogy a tanulási folyamatokat helyben, késleltetés nélkül tudják végrehajtani. Emellett a **megerősítéses tanulás**, az **önfelügyelt tanulás** és a **federált tanulás** is fontos szerephez jutnak, különösen elosztott rendszerekben.



1. ábra CPS Moduljai és funkciói

2. Ipari mesterséges intelligencia pipeline-ok

Az ipari automatizálás új korszakát hozta el a mesterséges intelligencia (MI), amely a hagyományos, szabályalapú rendszerek helyébe lépve képes összetett adathalmazokból tanulni, predikciókat készíteni és döntéseket támogatni. A gépi tanulás (ML) és mélytanulás (DL) technológiák integrációja az ipari folyamatokba lehetővé teszi a gyártás hatékonyságának, megbízhatóságának és rugalmasságának jelentős javítását. Ennek keretrendszerét képezi az ún. **ipari MI pipeline**, amely az adatok gyűjtésétől kezdve a modellek implementációján át a működésük monitorozásáig terjed.

2.1 Az MI pipeline felépítése ipari környezetben

Az ipari MI pipeline általában az alábbi főbb szakaszokra bontható[4]:

1. **Adatgyűjtés (Data Ingestion):** Szenzorok, IoT-eszközök, MES (Manufacturing Execution System), ERP és SCADA rendszerek biztosítják az adatok elsődleges forrásait. Az adatok típusa lehet időfüggő (pl. hőmérséklet), képi (pl. hibafelismerés), vagy strukturált (pl. termelési naplók).
2. **Adattisztítás és előfeldolgozás:** Az ipari adatok gyakran zajosak, hiányosak vagy redundánsak. A hatékony tanulás érdekében szükség van normalizálásra, szűrésre, hiányzó értékek kezelésére és adatszinkronizálásra[5].
3. **Jellemzők kiválasztása és mérnöki munka:** A cél az adatokból olyan jellemzők (feature-ök) kinyerése, amelyek jól reprezentálják az adott folyamat állapotát. Ez magában foglalhat statisztikai mutatókat (átlag, szórás), spektrális jellemzőket (FFT), vagy képfeldolgozási paramétereket.
4. **Modellezés:** Gépi tanulási algoritmusokat alkalmaznak a predikció, osztályozás vagy anomáliadetektálás céljából. Elterjedt modellek ipari környezetben: döntési fák (RF), SVM, neurális hálók (CNN, LSTM), valamint hibrid modellek.
5. **Értékelés és optimalizáció:** Keresztvalidáció, hiperparaméter-hangolás és metrikák (pl. F1-score, ROC-AUC, RMSE) segítségével történik a modellek értékelése és finomhangolása.
6. **Implementáció és élesítés:** A modellek integrálása történhet edge eszközökön, lokális szervereken vagy felhőalapú rendszerekben, a rendszer követelményeinek megfelelően.
7. **Monitorozás és visszacsatolás:** Az MI rendszer folyamatos felügyelet alatt áll, beleértve a modell drift detektálását és az újratanítást is, amely különösen fontos a dinamikusan változó ipari környezetben[6].

2.2 Főbb ipari alkalmazások

2.2.1 Termelésoptimalizálás

Az MI algoritmusok képesek optimalizálni az erőforrás-felhasználást, a gépek kihasználtságát és a munkafolyamatokat. Például egy gyártósoron az MI előre jelezheti, mely konfigurációk mellett csökken leginkább a selejtarány, vagy maximalizálható a termelési volumen.

- **Példa:** Egy autóipari vállalat neurális hálókat alkalmaz a gyártósor különböző szegmensein keletkező adatok korrelációjának azonosítására, így optimalizálva a gépátállások időzítését és sorrendjét.

2.2.2 Prediktív karbantartás (Predictive Maintenance)

A prediktív karbantartás célja a meghibásodások előrejelzése még azok bekövetkezése előtt. Ehhez az MI modellek időfüggő szenzoradatokat (pl. rezgés, hőmérséklet, nyomás) elemeznek, és mintázatokat keresnek a rendellenes működésre utaló jelek alapján.

- **Algoritmusok:** RNN, LSTM, autoencoderek és SVM egyaránt alkalmazhatók, attól függően, hogy időfüggő vagy statikus adatokról van szó.
- **Esettanulmány:** Egy gyártóüzem ventilátorainak állapotát figyelve egy gépi tanuló modell képes volt 92%-os pontossággal előre jelezni a csapágykopás mértékét, lehetővé téve az időben történő beavatkozást.

2.2.3 Minőségbiztosítás (Quality Control)

A gyártott termékek minőségének ellenőrzése gyakran manuálisan vagy egyszerű szabályalapú rendszerekkel történik. A mesterséges intelligencia lehetővé teszi a **valós idejű képfeldolgozáson** és **mintázatfelismerésen** alapuló automatizált ellenőrzést.

- **Alkalmazás:** CNN alapú modellek képesek felismerni repedéseket, szennyeződéseket vagy más hibákat akár mikroszkopikus szinten is.
- **Előnyök:** Nagy sebesség, alacsony hibatolerancia, taníthatóság új hibákra. A rendszer képes az új hibákat is detektálni folyamatos tanulással.

2.3 Technológiai integrációs szempontok

2.3.1 Szoftveres környezet

A pipeline implementációja történhet különféle MI platformokon:

- **Open-source eszközök:** TensorFlow, PyTorch, Scikit-learn
- **MLOps rendszerek:** MLflow, Kubeflow, Azure ML – ezek támogatják a modellek élettartam-kezelését, verziózását, CI/CD integrációt.

2.3.2 Hardveres támogatás

A tanítás és predikció igényei eltérőek:

- **Edge computing:** kis késleltetésű, beágyazott rendszerek (pl. NVIDIA Jetson, Intel Movidius).
- **Cloud computing:** skálázhatóság és nagy számítási kapacitás (pl. Amazon SageMaker, Google Vertex AI).

2.3.3 Integráció ipari rendszerekbe

Az MI pipeline sikeressége nagymértékben függ attól, hogy mennyire zökkenőmentesen illeszthető be a meglévő ipari informatikai környezetbe:

- **MES (Manufacturing Execution System)**
- **ERP rendszerek**
- **SCADA és PLC eszközök**

A sikeres integrációhoz szabványosított interfészek (OPC-UA, MQTT) és biztonságos adatátvitel szükséges.

2.4 Kihívások és jövőbeli irányok

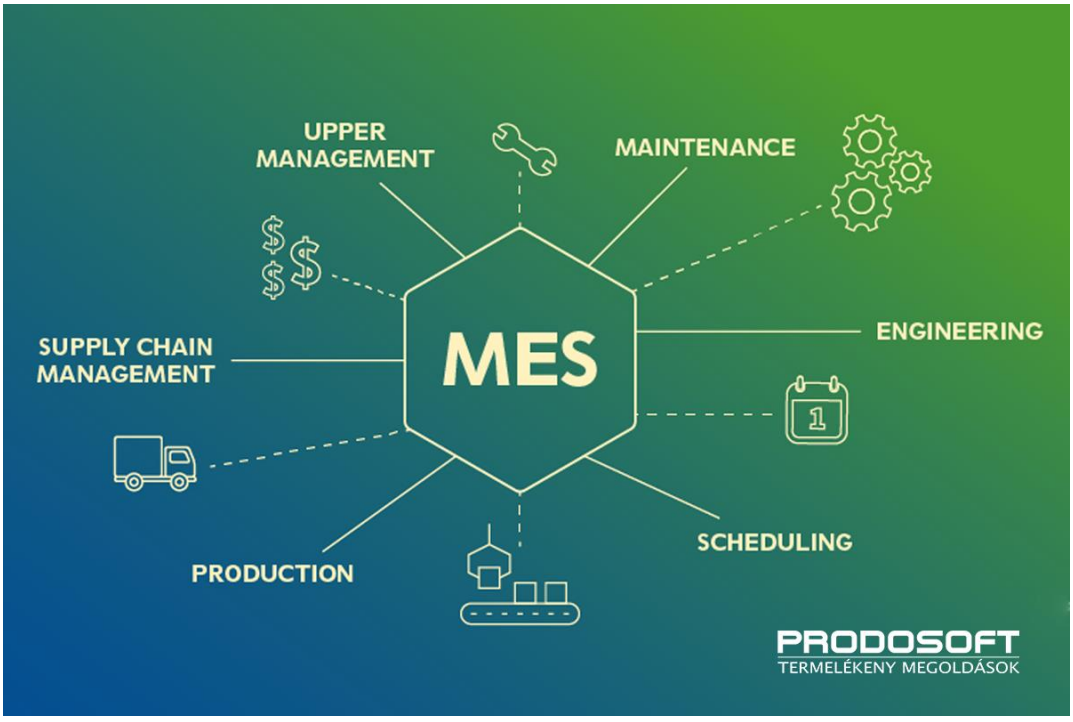
Bár az ipari MI pipeline-ok jelentős előrelépést kínálnak, több technikai és szervezeti kihívással is számolni kell:

- **Adatminőség:** A nem konzisztens, hiányos vagy torzított adatok gátolják a modellek megbízhatóságát.
- **Adatsilók megszüntetése:** Sok ipari vállalatnál az adatok el vannak különítve a rendszerek között, ami akadályozza a holisztikus optimalizálást.
- **Modelldrift:** A környezet változásával a tanított modellek pontossága romlik, újratanítás válik szükségessé.
- **Munkaerőhiány:** Az MI bevezetése új típusú szakértelmet igényel, amely hiányzik sok hagyományos ipari szereplőnél.

A jövőben várhatóan a **federált tanulás**, a **peremhálózati mesterséges intelligencia** és a **központi MLOps-platformok** további áttörést hoznak az ipari gépi tanulás skálázásában és fenntartásában.

3. MLOps és MES rendszerek

A mesterséges intelligencia (MI) gyártási környezetbe történő integrációja nem pusztán modellek kifejlesztését jelenti, hanem azok teljes életciklusának menedzselését. Ennek kulcsfontosságú eszköze az **MLOps** (Machine Learning Operations), amely az MI-fejlesztés DevOps-szerű keretrendszere. Az MLOps segítségével az ipari cégek képesek **automatikusan, skálázható módon és megbízhatóan** integrálni az MI-megoldásokat a **gyártásirányítási rendszerekbe (MES – Manufacturing Execution Systems)**, ezzel növelve a termelés hatékonyságát és rugalmasságát.



2. ábra MES rendszer, annak helye és szerepe

3.1 Az MLOps fogalma ipari környezetben

Az MLOps célja az MI rendszerek fejlesztésének, tesztelésének, telepítésének és monitorozásának **automatizálása és szabványosítása[7]**. Míg a klasszikus gépi tanulási projektek sokszor ad-hoc módon készülnek, az ipari alkalmazás megköveteli a **folyamatos működést, reprodukálhatóságot, verziókezelést, skálázhatóságot és robusztusságot**.

Az MLOps legfőbb komponensei:

- **Adatpipeline menedzsment** (Data versioning, lineage)
- **Modellek verziókezelése** és tárolása
- **CI/CD folyamatok MI modellekhez**
- **Automatizált modellek tréningje és retréningje**
- **Monitorozás és alulteljesítés észlelése** (model drift)
- **Auditálás és megfelelés** (pl. ISO 26262 autóiparban)

3.2 MES rendszerek és szerepük

A **Manufacturing Execution System (MES)** olyan szoftverrendszer, amely az üzemi szintű gyártási műveletek valós idejű nyomon követését és vezérlését végzi. Kapcsolatot biztosít az **üzemek fizikai infrastruktúrája** (gépek, szenzorok, PLC-k) és a **vállalati szintű információs rendszerek** (pl. ERP – Enterprise Resource Planning) között[8].

Főbb funkciók:

- Műszakirányítás és termelési ütemezés
- Minőségellenőrzés és hibadetektálás
- Karbantartáskövetés
- Raktárkezelés és anyagáramlás kontroll

A MES rendszerek az adatgyűjtés egyik fő forrásai, és kiváló belépési pontok az MI pipeline számára.

3.3 MLOps integrálása a MES rendszerekbe

3.3.1 Technikai architektúra

A **MES** gyűjti az adatokat, amelyeket az **MLOps pipeline** előfeldolgoz, modellez, majd a modell predikcióit visszacsatolja a MES-be vagy közvetlenül a gépekhez. Az MLOps rendszer így **valós idejű** döntéstámogatást nyújt.

3.3.2 Alkalmazási példák

- **Prediktív karbantartás:** MES rögzíti a gépek állapotát (pl. rezgés, hőmérséklet). Az MLOps pipeline egy ML modellt treníroz, amely előre jelzi az esetleges meghibásodásokat.

- **Adaptív termelés:** A MES-ből származó selejtarány-adatok alapján az MLOps pipeline újratanítja a modellt, amely javaslatot tesz a gyártási paraméterek optimalizálására.
- **Minőségellenőrzés:** A képfeldolgozó rendszerekből származó adatok feldolgozása, modellek frissítése automatikusan történik a MLOps pipeline-ban.

3.3.3 DevOps és MLOps összehasonlítása

Jellemző	**DevOps**	**MLOps**
Cél	Szoftververziók kezelése és üzemeltetés	ML modellek fejlesztése, deployolása
Verziókezelés	Kód	Kód + Adat + Modell
Tesztelés	Unit / Integration	Adatvalidálás, Modellvalidálás
Monitorozás	CPU, memória, logok	Modelldrift, predikciós hiba, adatszórás

3.4 Előnyök az ipari termelés szempontjából

1. Skálázhatóság

Az MLOps rendszerek lehetővé teszik több modell, több gyártósor és több lokáció párhuzamos kezelését. Egy jól konfigurált pipeline egyszerre képes több száz gyártási entitás prediktív modelljének futtatására.

2. Hatékonyság

Az automatizált tréning és deployálás időt és humánerőforrást takarít meg. A modellek frissítése és újratréningelése gyorsan, beavatkozás nélkül történik.

3. Reagálóképesség

A gyorsan változó környezeti feltételekhez való alkalmazkodás lehetősége jelentősen megnöveli a termelés rugalmasságát.

4. Reprodukálhatóság és átláthatóság

A modellverziók, adatforrások és feature-k változásai dokumentáltak, ami elengedhetetlen a gyártási auditok során.

3.5 Kihívások és megoldások

Kihívás	Lehetséges megoldás
Komplex integráció MES rendszerekkel	API-rétegek, OPC-UA alapú interfészek
Modelldrift kezelése	Drift-detektorok és automatikus retréning
Verziókezelés és auditálhatóság	MLflow, DVC használata
Biztonsági aggályok	VPN, titkosított adatkapcsolatok, RBAC

3.6 Jövőbeli kilátások

A **felhőalapú MLOps platformok** (pl. Azure ML, AWS SageMaker) egyre szélesebb körű integrációt kínálnak MES rendszerekhez. A jövőben várhatóan elterjednek a **peremhálózati MI-megoldások** (Edge AI), amelyek lehetővé teszik az MI modellek **valós idejű, helyszíni működését**. Ezzel csökken a késleltetés és a hálózati függőség, növelve a rendszer megbízhatóságát.

4. Digitális ikrek alkalmazása a gyártási folyamatokban

A **Digitális iker (Digital Twin)** technológia egyre fontosabb szerepet tölt be az ipari digitalizációban, különösen a **kiber-fizikai rendszerek (CPS)** környezetében. A digitális iker nem csupán egy statikus modell, hanem egy **dinamikus, élő reprezentáció**, amely valós idejű adatokat használ a fizikai objektumok viselkedésének szimulálására, előrejelzésére és optimalizálására.

4.1 A digitális iker fogalma és architektúrája

A digitális iker egy fizikai entitás (pl. gép, gyártósor, termék) **digitális másolata**, amely folyamatos adatkapcsolatban áll az eredeti rendszerrel[10]. Ez lehetővé teszi a **monitorozást, szimulációt, predikciót** és döntéstámogatást.

A digitális iker rendszer fő komponensei:

1. **Fizikai entitás:** Szenzorokkal felszerelt gép vagy rendszer
2. **Adatgyűjtő infrastruktúra:** IoT szenzorok, SCADA, MES rendszerek
3. **Digitális modell:** A rendszer viselkedését leíró matematikai vagy gépi tanulási modell
4. **Kommunikációs interfész:** Valós idejű adatkapcsolat biztosítása (pl. MQTT, OPC-UA)
5. **Vizualizációs és analitikai felület:** Dashboardok, 3D szimulációk, AR/VR

4.2 A digitális ikrek szerepe a gyártásban

A gyártási folyamatok egyre komplexebbek, így a valós idejű megértésük és optimalizálásuk kulcsfontosságú. A digitális ikrek segítenek:

- **A működés valós idejű monitorozásában**
- **Szimulációk futtatásában – „mi lenne, ha" típusú kérdésekre**
- **Hibák előrejelzésében és elhárításában**
- **Erőforrás- és energiaoptimalizálásban**
- **Termékélettartam modellezésében és testreszabásában**

Konkrét ipari példák:

- **Autóipar:** A BMW digitális ikert használ a teljes gyártósor optimalizálására még a fizikai rendszer felépítése előtt[11].
- **Élelmiszeripar:** Nestlé a digitális ikerrel szimulálja az ellátási láncot és az energiafelhasználást.
- **Gyógyszeripar:** Gyártóberendezések folyamatparamétereinek valós idejű követése a megfelelőségi szabványok biztosítására (pl. GMP, FDA).

4.3 Szimuláció és predikció

A digitális ikrek egyik fő előnye, hogy valós idejű adatokkal kombinálva lehetővé teszik:

- **Folyamatok előrejelzése:** Pl. gépalkatrészek várható élettartama.
- **Szabályozási paraméterek tesztelése szimulált környezetben:** Valós beavatkozás nélküli próbák.
- **Többszörös szcenáriók összehasonlítása:** Például anyagválasztás vagy gyártási tempó hatása.

A szimulációk lehetnek **fizikai alapú modellek** (pl. mechanikai szimuláció) vagy **adatvezérelt modellek** (ML alapú előrejelzés).

4.4 Integráció mesterséges intelligenciával

A digitális ikrek hatékonyságát jelentősen növeli a **gépi tanulás és mesterséges intelligencia** bevonása:

- **Anomáliadetektálás:** Szokatlan viselkedés felismerése a fizikai rendszerhez képest.
- **Prediktív karbantartás:** AI előre jelzi a potenciális meghibásodásokat.
- **Önoptimalizáló gyártás:** A digitális iker folyamatosan tanul a működésből, és javaslatokat tesz a paraméterek finomhangolására.

4.5 Előnyök

Előny	Leírás
Valós idejű döntéstámogatás	Gyors reakciók környezeti változásokra
Költségcsökkentés	Hibák szimulációja még beavatkozás előtt
Termékminőség javítása	Pontosabb folyamatkontroll
Termelés rugalmassága	Különböző konfigurációk gyors tesztelése
Fenntarthatóság	Energiafogyasztás optimalizálása szimulációval

4.6 Kihívások

Bár a digitális iker technológia ígéretes, több kihívással is szembe kell nézni:

- **Adatintegráció:** Sokféle adatforrás szinkronizálása (MES, SCADA, ERP)
- **Skálázhatóság:** Nagy számú gép valós idejű másolatának kezelése
- **Szabványosítás:** Hiányoznak az egységes ipari szabványok
- **IT-biztonság:** Érzékeny működési adatok védelme
- **Szakértelem igénye:** A digitális modell felépítése multidiszciplináris tudást kíván

4.7 Jövőbeli trendek

A digitális ikrek jövője az **autonóm rendszerek** és a **felhő- + peremalapú MI kombinációjában** rejlik. A **Metaverse és AR/VR alapú interfészek** révén lehetőség nyílik arra, hogy a digitális ikreket nemcsak monitorozzuk, hanem **immerszív módon is interakcióba lépjünk velük**.

A legfejlettebb rendszerekben a digitális iker **önfejlesztő rendszerként** működik, amely automatikusan alkalmazkodik a környezethez, újratanítja modelljeit, és optimalizálja működését.

5. CPS és mesterséges intelligencia alkalmazása különböző ágazatokban

A **kiber-fizikai rendszerek (Cyber-Physical Systems, CPS)** és a **mesterséges intelligencia (AI)** integrációja forradalmasítja az ipar mellett a mezőgazdaságot, egészségügyet és a honvédelmet is. Ezekben az ágazatokban a **valós idejű adatgyűjtés, döntéshozatal és adaptív viselkedés** alapvetően új működési paradigmákat eredményez. A következőkben három jelentős szektort vizsgálunk meg részletesen.

3. ábra Mesterséges intelligencia használata cégeknek a Marketingben

5.1 Mezőgazdaság: Precíziós gazdálkodás MI-vel és szenzorhálózatokkal

5.1.1 Kontextus és kihívások

A modern mezőgazdaság célja a **termelékenység növelése és fenntarthatóság biztosítása** a természeti erőforrások megőrzése mellett. A CPS alapú rendszerek szenzoradatokra épülve képesek optimalizálni az inputokat (víz, műtrágya, növényvédő szer), miközben az AI segít a döntések meghozatalában.

5.1.2 Technológiai összetevők

- **Szenzorhálózatok:** Talajnedvesség, pH, hőmérséklet, páratartalom, fényintenzitás mérése.
- **Dronok és képfeldolgozás:** Növényállapot, betegségek felismerése.
- **Gépi tanulás:** Betegségek automatikus detektálása, hozam előrejelzés.
- **Edge computing:** Lokális adatfeldolgozás gyors döntéshozatalhoz.

5.1.3 Példák

- **John Deere** önvezető traktorai és okos permetezőrendszerei valós idejű adatgyűjtéssel és gépi tanulással működnek[12].
- **Climate FieldView**: Felhőalapú rendszer, amely szenzoradatokat és gépi tanulást kombinál a talaj- és növényanalízisre.

5.2 Orvostudomány: Személyre szabott gyógyászat MI és CPS integrációval

5.2.1 Kontextus

Az egészségügy digitális átalakulásának középpontjában az **adatalapú diagnosztika és terápia** áll. CPS rendszerek segítségével a beteg állapota valós időben követhető, míg az AI algoritmusok a személyre szabott kezelést támogatják.

5.2.2 Kulcstechnológiák

- **Orvosi képfeldolgozás (DL):** MRI, CT, röntgen képek elemzése.
- **Genetikai adatelemzés:** Genomszekvenálás alapján predikciók pl. rák hajlamra.
- **Viselhető eszközök (IoT):** Szívritmus, vércukorszint, alvásmonitorozás.
- **Digitális ikrek a gyógyászatban:** Beteg-specifikus szimulációk (pl. gyógyszerhatás előrejelzése).

4. ábra Orvosi képfeldolgozás: a formázástól az értelmezésig

5.2.3 Példák

- **IBM Watson Health** elemzi az onkológiai eseteket és terápiás javaslatot tesz több ezer kutatás alapján.
- **DeepMind Health (Google):** Retina szkennelés alapján mesterséges intelligenciával előre jelzi a vakságot okozó állapotokat.

Előnyök:

Előny	Példa
Gyorsabb diagnózis	Tüdőrák korai felismerése AI-val CT-képek alapján
Kezelés személyre szabása	Genetikai profil alapján célzott terápia
Folyamatos betegmonitorozás	IoT eszközök + CPS rendszer

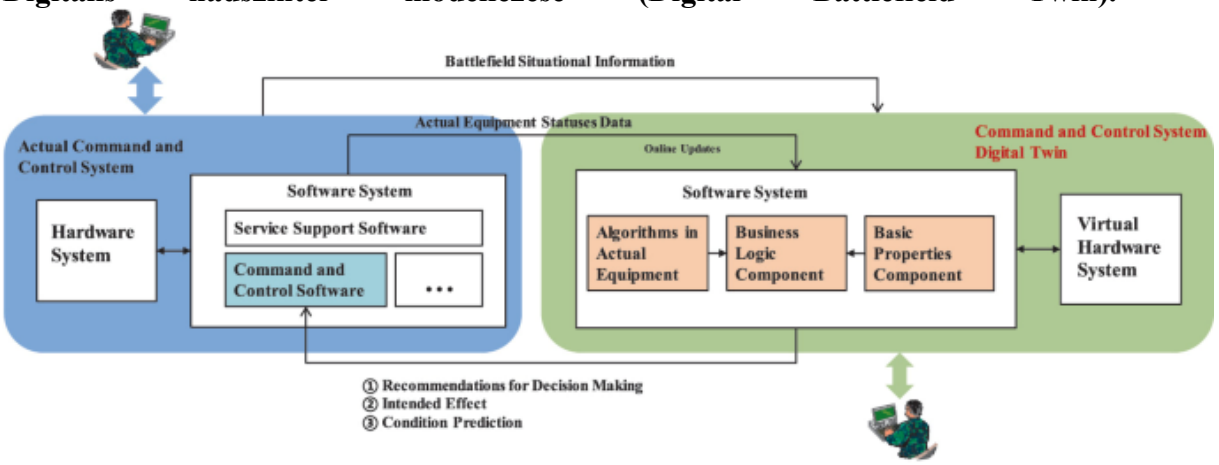
5.3 Honvédelem: Intelligens döntéshozatali rendszerek

5.3.1 Kontextus

A katonai rendszerek nagy mértékben támaszkodnak valós idejű helyzetértékelésre, gyors és pontos döntéshozatalra. CPS és MI integrációja itt nemcsak előnyt, hanem biztonsági követelményt is jelent.

5.3.2 Alkalmazási területek

- **Autonóm rendszerek:** Drónok, szárazföldi robotok önálló navigációja és célazonosítása.
- **Prediktív fenyegetés-azonosítás:** Mesterséges intelligencia segítségével anomáliafelismerés (pl. ellenséges mozgások).
- **Hálózati biztonság:** MI-alapú kiberfenyegetés-észlelés.
- **Digitális hadszíntér modellezése (Digital Battlefield Twin).**



5. ábra Digitális iker csatatér kialakítása a vezetés és irányítás központi szerepével

5.3.3 Példák

- **DARPA's OFFSET program**: Autonóm drónrajok alkalmazása városi környezetben történő taktikai műveletekhez[13].
- **Project Maven (USA)**: Katonai drónfelvételek elemzése mélytanulás segítségével a célpontok automatikus felismeréséhez.

Etikai kérdések

- **Autonóm fegyverek problémája**
- **Döntéshozatal átláthatósága**
- **Civil célpontok védelme**

5.4 Összegzés

A különböző szektorokban tapasztalható **MI és CPS konvergencia** révén egyre inkább **adaptív, intelligens és autonóm rendszerek** jönnek létre. A mezőgazdaságban a fenntartható és precíz gazdálkodás, az egészségügyben a személyre szabott gyógyászat, a honvédelemben pedig a valós idejű stratégiai döntéshozatal terén mutatkoznak meg leginkább ezek az előnyök. A kihívások ellenére a technológiai fejlődés ezen ágazatokban is gyors és hatékony változásokat hoz.

6. A gépi látás szerepe a CPS rendszerekben

A **gépi látás (computer vision, CV)** a mesterséges intelligencia egyik kulcsterülete, amely lehetővé teszi a számítógépek és beágyazott rendszerek számára a vizuális információk észlelését, értelmezését és feldolgozását. A **kiber-fizikai rendszerek (CPS)** kontextusában a gépi látás olyan szenzorrendszert jelent, amely **kameraalapú észlelést** és **valós idejű döntéshozatalt** tesz lehetővé automatizált folyamatok irányításához és felügyeletéhez.

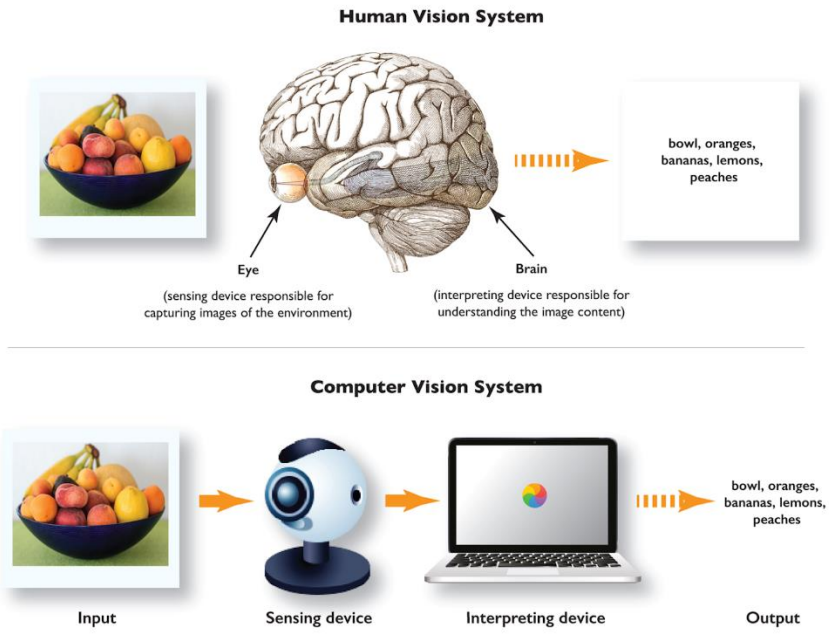
6.1 Ipari automatizálás

6.1.1 Minőségellenőrzés és hibadetektálás

Az ipari termelés során a gépi látás kulcsszerepet játszik a **minőségbiztosítás automatizálásában**. A kamerák valós időben pásztázzák a gyártósorokon áthaladó alkatrészeket, míg a CV-algoritmusok képesek detektálni:

- Felületi hibákat (karcolás, repedés)
- Méretbeli eltéréseket
- Helytelen összeszerelést

A **mélytanulás-alapú detektorok** képesek tanulni a tipikus hibákat, így az új típusú eltérések felismerésére is alkalmasak[14].



6. ábra Gépi látás összehasonlítása az emberi látással

6.1.2 Robotikai irányítás

A gépi látás támogatja az **ipari robotkarok vezérlését** például a:

- Célpont-azonosításban
- Precíziós megfogásban
- Dinamikus mozgástervezésben (pl. futószalagon mozgó tárgyak követése)

Példa: A **Fanuc** és a **KUKA** robotkarjai beépített 2D/3D kamerarendszerekkel azonosítják a tárgyakat, és képesek azokat irányba állítani vagy szortírozni.

6.1.3 Előnyök

- **Sebesség**: Milliszekundumos reakcióidő
- **Pontosság**: Mikron szintű hibadetektálás
- **Költségcsökkentés**: Kevesebb selejt és emberi hiba

6.2 Közlekedésirányítás

6.2.1 Forgalomfigyelő rendszerek

A városi és autópályás közlekedésirányítás során a gépi látás lehetővé teszi:

- **Járműszámlálás** és **áramlási elemzés**
- **Rendszámtábla-felismerés (ANPR)** bírságolás és beléptetés céljából
- **Torlódás- vagy balesetészlelés** valós időben

Példa: A **Budapesti Közlekedési Központ (BKK)** forgalomfigyelő rendszerei képesek gépi látással azonosítani a torlódásokat és automatikusan adaptálni a lámpák vezérlését.

6.2.2 Autonóm járművek

Az autonóm közlekedés egyik alappillére a látásalapú szenzorhasználat. A gépjárművekben alkalmazott kamerák és MI-modellek az alábbi funkciókat látják el:

- **Sávdetekció**
- **Közlekedési táblák felismerése**
- **Gyalogosok, kerékpárosok és más járművek követése**

Ezek a látásalapú érzékelők gyakran **LIDAR-ral és radarral** együtt működnek egy szenzorfúziós rendszerben.

6.2.3 AI-alapú forgalom-optimalizáció

A kamerákból érkező képadatok alapján mesterséges intelligencia vezérelheti:

- Zöld hullámokat
- Dinamikus forgalomterelést
- Torlódások predikcióját

6.3 Biztonságtechnika

6.3.1 Arc- és mozgásfelismerés

A biztonságtechnikai rendszerek egyik legfontosabb eleme a **felismerés és riasztás**. Gépi látással lehetőség nyílik:

- **Arcazonosításra** (pl. belépési rendszerekben)
- **Viselkedéselemzésre** (pl. illetéktelen mozgás, szokatlan aktivitás)
- **Mozgásdetekcióra** sötétben is (pl. hőkamerával)

Példa: A kínai **"Skynet" rendszer** képes országos szinten követni személyeket nyilvános kamerákból származó képek alapján.

6.3.2 Objektumkövetés és behatolásjelzés

- Érzékeli, ha egy személy átlép egy határvonalat vagy elhagyott csomag jelenik meg.
- Repülőtereken, katonai létesítményeknél kiemelten fontos.

6.3.3 Etikai és adatvédelmi aggályok

- **Adatkezelés**: Arcadatok tárolása
- **Megfigyelés**: Folyamatos videómonitorozás
- **Hamis pozitív riasztások** veszélye (pl. viselkedéselemző rendszereknél)

6.4 Gépi látás előnyei CPS-ben

Alkalmazási terület	Gépi látás előnye
Ipar	Gyors, precíz minőségellenőrzés
Közlekedés	Valós idejű torlódásfigyelés
Biztonság	Részletes személy- és viselkedés-azonosítás

6.5 Összegzés

A **gépi látás a CPS rendszerek egyik legkritikusabb érzékelési technológiája**, mely lehetővé teszi a valós világban történő események digitális értelmezését. Az ipari gyártás, közlekedésirányítás és biztonságtechnika példái is mutatják, hogy a kameraalapú adatfeldolgozás nemcsak hatékony, de adaptív és autonóm működést is támogat. Az algoritmusok fejlődésével és a számítási kapacitások bővülésével ezek a rendszerek egyre megbízhatóbbak és intelligensebbek lesznek.

7. Intelligens otthonok optimalizálása: Szenzoradatok szerepe az energiahatékonyságban és komfortnövelésben

Az **intelligens otthonok (smart homes)** a kiber-fizikai rendszerek egyik legismertebb és legdinamikusabban fejlődő alkalmazási területét képezik. Ezek a rendszerek különféle **szenzorokkal, aktuátorokkal és mesterséges intelligenciával** integrált környezetek, melyek célja a lakók kényelmének növelése, az energiafelhasználás optimalizálása, valamint a biztonság és automatizáció biztosítása.

7.1 Az intelligens otthonok architektúrája

Egy tipikus intelligens otthon a következő fő komponensekből áll:

- **Szenzorok**: hőmérséklet, páratartalom, mozgás, fény, CO_2, hang, ajtó/ablak nyitás
- **Vezérlők / aktuátorok**: termosztát, árnyékolók, világítás, fűtés/hűtés, háztartási eszközök
- **Gateway és vezérlőlogika**: edge vagy felhőalapú központi egység
- **MI-alapú döntéshozatal**: időalapú szabályok, felhasználói szokások tanulása, predikció

A szenzoradatok folyamatos gyűjtésével és feldolgozásával a rendszer képessé válik **valós idejű döntések meghozatalára** és **tanulásra** a felhasználói preferenciák alapján[15].

7.2 Energiahatékonyság szenzoradatok segítségével

7.2.1 Intelligens fűtés, hűtés és világítás

Az energiafogyasztás optimalizálásának egyik legfontosabb területe a **fűtés-hűtés és világítás vezérlése**. A rendszer:

- **Hőmérsékletszenzor** alapján szabályozza a termosztátot, figyelembe véve a kültéri időjárást is.
- **Mozgásérzékelőkkel** lekapcsolja a fűtést vagy világítást nem használt helyiségekben.
- **Fényérzékelőkkel** szabályozza a mesterséges világítást a természetes fényviszonyokhoz igazítva.

7.2.2 Időalapú és prediktív vezérlés

A gépi tanulás segíthet a rendszernek előre jelezni, mikor tartózkodnak otthon a lakók, és **előfűteni vagy -hűteni** az otthont ennek megfelelően.

Példa: A Nest termosztát megtanulja a lakók napi rutinját, és ennek alapján szabályozza a hőmérsékletet, akár 10–15%-os energia-megtakarítást is eredményezve[16].

7.2.3 Integráció napelemekkel és energiatárolással

A modern intelligens otthonokban a rendszer képes **napelemekkel és akkumulátorokkal** együttműködni:

- Optimalizálja a fogyasztást a napenergia rendelkezésre állásához.
- Tölti az akkumulátort alacsony tarifás időszakban, és kisüti csúcsidőben.

7.3 Komfortnövelés MI segítségével

7.3.1 Szokások tanulása és automatizáció

A gépi tanulás képes felismerni az egyéni **életviteli mintákat**:

- Mikor szeret a felhasználó világítást vagy zenét?
- Milyen hőmérsékletet részesít előnyben különböző napszakokban?

A rendszer alkalmazkodik ezekhez és személyre szabott szolgáltatást nyújt.

7.3.2 Hangvezérlés és természetes nyelvfeldolgozás

A hangalapú asszisztensek, mint a Google Assistant, Alexa vagy Siri, **természetes módon** teszik lehetővé az otthoni eszközök vezérlését. A CV és NLP integráció révén a lakók képesek akár látás- és mozgásérzékeléssel kombinált hangutasításokkal is vezérelni a környezetet.

7.3.3 Komfort az egészségi állapot figyelembevételével

Az intelligens otthon képes monitorozni a levegőminőséget (CO_2, VOC), a zajszintet és a fényviszonyokat. Idősek esetében az elesésdetekció vagy pulzusszám monitorozás szintén a komfort és biztonság kombinációját szolgálja.

7.4 Gépi tanulási algoritmusok a smart home rendszerekben

A leggyakrabban alkalmazott MI-algoritmusok:

Algoritmus	**Alkalmazási terület**
K-means clustering	Szokásminták klaszterezése
Decision Trees	Eszközvezérlési szabályok automatikus generálása
Neural Networks	Hőmérséklet- vagy energiafogyasztás predikció
Reinforcement Learning	Valós idejű döntéshozatal tanulása

7.5 Adatbiztonság és adatvédelem

Az intelligens otthonok egyik kritikus kihívása az adatvédelem:

- A lakók napi rutinja, jelenléte, szokásai érzékeny információk.
- A rendszer gyakran felhőkapcsolattal rendelkezik – adatátvitel és -tárolás során titkosítás szükséges.
- Edge computing lehet alternatíva: az adatok helyben történő feldolgozása csökkenti a kockázatot.

7.6 Összefoglalás

Az intelligens otthonok nem csupán kényelmi funkciókat nyújtanak, hanem aktívan hozzájárulnak az energiahatékonysághoz és a fenntartható életmódhoz. A **szenzoradatok feldolgozása és MI-alapú elemzése** lehetővé teszi a dinamikus vezérlést, tanulást és adaptív működést. Az autonóm és önfejlődő otthonrendszerek egyre elérhetőbbé válnak, de a további fejlődésük záloga az adatbiztonság, a szabványosítás és az interoperabilitás.

Záró gondolatok:

A mesterséges intelligencia integrációja a kiber-fizikai rendszerekbe (CPS) napjaink egyik legdinamikusabban fejlődő technológiai irányzata, amely jelentős hatást gyakorol az ipari, mezőgazdasági, egészségügyi és védelmi szektorokra egyaránt. Az MI-alapú adaptív rendszerek révén a CPS-ek képesek valós idejű döntéseket hozni, alkalmazkodni a környezet változásaihoz, és autonóm módon optimalizálni működésüket. Az olyan technológiák, mint a gépi tanulás, digitális ikrek, MLOps vagy a számítógépes látás, új szintre emelik a hatékonyságot, megbízhatóságot és prediktív képességet. Ugyanakkor az MI és CPS konvergenciája új kihívásokat is felvet – például a rendszerbiztonság, adatvédelem vagy etikai kérdések terén –, amelyek megoldása nélkülözhetetlen ahhoz, hogy ezek a technológiák széles körben és fenntartható módon legyenek alkalmazhatók a jövőben.

Források:

[1] M. Lee et al., "Machine Learning for Cyber-Physical Systems: Challenges and Opportunities,"

[2] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, May 2015.

[3] A. Jardine et al., "A review on machinery diagnostics and prognostics implementing condition-based maintenance," *Mechanical Systems and Signal Processing*, vol. 20, no. 7, pp. 1483–1510, 2006.

[4] B. Zhang et al., "An Industrial Artificial Intelligence Pipeline: Challenges and Case Studies," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 3, pp. 1994–2005, Mar. 2021.

[5] F. Chollet, *Deep Learning with Python*, Manning Publications, 2018.

[6] A. Ghosh and M. Lee, "Lifecycle Management of ML in Industrial CPS," *ACM Journal on Emerging Technologies*, vol. 16, no. 4, pp. 1–19, 2020.

[7] M. Villela, "MLOps: Continuous Delivery and Automation Pipelines in Machine Learning," *O'Reilly Media*, 2021.

[8] L. Monostori et al., "Cyber-physical systems in manufacturing," *CIRP Annals*, vol. 65, no. 2, pp. 621–641, 2016.

[9] M. Zaharia et al., "Accelerating the Machine Learning Lifecycle with MLflow," *IEEE Data Eng. Bull.*, vol. 41, no. 4, pp. 39–45, Dec. 2018.

[10] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in *Transdisciplinary Perspectives on Complex Systems*, Springer, 2017, pp. 85–113.

[11] R. Rosen et al., "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.

[12] J. Evans and P. Smith, "Precision Agriculture: Smart Farming with Sensors, AI, and Robotics," *IEEE Industrial Electronics Magazine*, vol. 14, no. 3, pp. 23–31, Sept. 2020.

[13] DARPA, "OFFSET: Offensive Swarm-Enabled Tactics,".

[14] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[15] M. Mozer, "The neural network house: An environment that adapts to its inhabitants," *AAAI Spring Symposium*, 1998.

[16] S. Darby, "Smart metering: What potential for householder engagement?" *Building Research & Information*, vol. 38, no. 5, pp. 442–457, 2010.

[17] Industry 4.0 and Digital Twins in Manufacturing https://www.researchgate.net/publication/328982819_Design_of_a_high-effective_fault-tolerance_double-stator_magnetless_vernier_machine_for_direct-drive_robotics

[18] MLOps: Continuous delivery and automation pipelines in machine learning https://cloud.google.com/architecture/mlops-continuous-delivery-and-automation-pipelines-in-machine-learning

[19] Smart Home Technologies and Sensor Systems https://www.mdpi.com/1424-8220/20/17/4767

2.46. LoRa-WAN technológia LoRa-WAN technológia alkalmazása CPS rendszerekben

LoRa-WAN technológia

LoRa-WAN technológia alkalmazása CPS rendszerekben

Molnár Roland

Mérnökinformatika, molnar.roland090@gmail.com

Kulcsszavak: LoRa-WAN, CPS, ipari automatizálás, okos városok, precíziós mezőgazdaság, kritikus infrastruktúrák, vezeték nélküli kommunikáció, energiahatékonyság, adatátvitel, hálózati architektúra, biztonság, skálázhatóság, 5G, edge computing, mesterséges intelligencia, Wi-Fi, ZigBee, Sigfox, NB-IoT, IoT, adatvédelem, kriptográfia, AES, ECC, redundancia, hálózati szegmentálás, előrejelző karbantartás, hibrid megoldások, frekvenciasávok, adatsebesség, hatótávolság, költséghatékonyság

Tartalomjegyzék

1 Bevezetés....4
1.1 Miért fontos megvizsgálni a LoRa-WAN technológia felhasználását a CPS rendszerekben?. 4
1.2 Alapelv alkalmazási területei - Hogyan működjön a LoRa-WAN hálózatban?....5
1.3 A háló architektúrája - mibőL épül fel és hogyan működnek egymással?.... 5
1.4 Frekvenciatartományok használata az adott frekvenciasávon és ennek jelentősége....6
1.5 Az energiahatékonyság és az átviteli sebesség kérdéseiről beszélünk. Mennyi az energiafogyasztás, és milyennek a rendelkezésére álló átviteli sebesség?....7
2 Az LoRa-WAN jelentősége az CPS rendszerekben.... 7
2.1 Előnyök más vezeték nélküli megoldásokkal szemben. Miben különbözik például az előny az Wi-Fi-hoz képest?....7
2.2 Milyen ipari területeken használható az alkalmasság?....7
3 Gyakorlati felhasználások [13]....8
3.1 Okos városok és a LoRa-WAN használata [6]....8
3.1.1 Okos városok - Forgalomirányítás LoRa-WAN segítségével....8
3.1.2 Irodai épület berendezéseinek megfigyelése....8
3.2 Precíziós mezőgazdaság – Melyek az előnyei a mezőgazdaság területén?....9
3.2.1 Állattenyésztés figyelemmel követése....9
3.3 Mező- és gazdaságfejlesztés automatizálása.... 9
4 Az ipari automatizálás szerepe az ipari folyamatok megerősítésében....9
4.1 Gépek állapotának monitorozása és jóslás alapú karbantartás....9
4.2 Folyamatok automatizálása és irányítása.... 10
4.3 Monitorozás az energiaellátó hálózat....10
5 Kritikus infrastruktúráink védelme.... 10
5.1 Biztonsági és méretezőképes problémák.... 11
5.1.1 Adatvédelem és biztonságos adatkezelés kérdéseinek, és azok megoldására irányuló lépésekről....11
5.1.2 Biztonsági kockázatok....11
5.1.2.1 Adatvédelmi veszedelmek és kockázatok.... 11
5.1.2.2 Esettanulmányok példaképek....11
5.2 Hálózat Védelmi intézkedések rendszerek....12
5.3 Fontossági fokozat és jelentőség - jelentőség....13
5.4 Hatékony kommunikáció módszerei a hatékonyság növelésére....13
5.5 Módszerek.... 14

6 Milyen fajta újdonságok megjelenése várható a közelgő időszakban?.....14
6.1 Edge számítástechnika és LoRa-WAN alkalmazása..... 14
7 Összehasonlítás LoRa-WAN és más kommunikációs technológiák között [14].....15
7.1 Wi-Fi hálóra épülő ZigBee technológia valamint Sigfox és NB-IOT protokoll és az 5. generációs mobiltechnológia között mily nézőpontok alapulhatnak az összevetésre?.....15
7.2 Kiadások [5]..... 16
7.3 LoRa-WAN technológia lehetővé teszi nagyszámú eszköze hatékony kezelését nagyméretű adatkapacitással rendelkező háló hátterének segítségével. [4].....16
7.4 Az energiahatékonyság kiemelt fontosságú terület a fenntartható fejlődés szempontjából. . 17
7.5 Mely helyzetekben érdemes ezeket a technológiai megoldásokat összekombinálni?.....18
7.5.1 Adatátviteli sebességgel és távoli információ átadással kapcsolatban.....18
7.5.2 Energiahatékonyság és teljesítmény..... 18
8 Szolgáltatások és programok.....18
8.1 Városok Infrastruktúrájának Figyelése.....19
8.2 Központosított eszköztár kezelése..... 19
9 LoRa-WAN és NB-Iot kombinációja.....19
9.1 LoRa-WAN és Sigfox kombinációja.....19
9.2 LoRa-WAN és ZigBee összekapcsolása.....19
9.3 LoRa-WAN és 5. generációs mobilhálózat (5) kombinációja.....19
9.4 LoRa-WAN és NB-Iot technológiák összevonása.....20
9.5 LoRa-WAN és ZigBee összekapcsolása.....20
10 Összegzés.....20

1 Bevezetés

Az ipar 4. generációja az ipari termelés újfajta lehetőségeit kínálja az internetes eszközeinkkel, az adatok elemzésével és az automatizálással összekapcsolva. Ezt az újfajta ipari forradalmat arra tervezték, hogy az eszközök és rendszerek kommunikálhassanak egymással és önmagukban is képesek legyenek működni ezzel jelentősen növesztve mindazok hatékonyságát és innovációs lehetőségét. A kiber-fizikai rendszerek (CPS) kulcsfontosságú szerepet játszanak ebben az újfajta modellben mert ezek integrált számítógépes és fizikai elemek amelyek segítségével képesnek vagyunk valós időben figyelemmel követni és irányítani az ipari életfolyamatainkat.

Az ipari 4-es forradalom fontossága nemcsak az hatékonyság növelésében és az innovációban rejlik meg jelentős mértékben, hanem az egész értékláncon való integrációban és az ügyfélszállítások javításában is megtalálhatóak benne előnyei is nyomot hagynak ezekkel kapcsolatban. Az ipari 4-es forradalom képessé teszi az üzemeltetést arra szintre emelje, hogy számítógépes módszerrel tervezzenek valamint gyártsanak és szolgáltassanak. Műveleteket is végrehajthatnak ezzel, amely lehetővé teszi azt hogy az üzletek rugalmasabban reagáljanak az ügyfél igényeinek valamint és gyorsabban olyan új ösvényeket találjunk amelyek lehetnek hasznosak számunkra. Az CPS rendszerek kulcs elemeit képezik az ipari 4-es forradalomnak ezáltal, mert ezen intézkedések biztosítják azt, hogy egy adott pillanatban reálisan figyelni lehessen az ipari folyamatokat és vezetéseket ami egyértelműen növelni fogja annak hatékonyságát valamint elemzővé teszik innovációs lehetőségét.

A CPS rendszerek hatékony és megbízható adatkommunikációra van szükségük alacsony energiaszükséglet mellett ahhoz kapunk lehetőséget ipari automatizálás és infrastruktúrák felügyeletére. Az adatatviteli technologiak fejlődése és alkalmazása kulcsfontosságú az ipar 4.0 sikeres végrehajtásához. A CPS rendszereknek valós idejű adatokat kell gyűjtenie es közvetítenie hogy üzleteink gyorsan reagálhassanak az ügyfelek kéréseire és üzleti folyamataik változasáira.

A cikk központi célja az LoRa-WAN technológia alkalmazásának átfogó és rendszerezett áttekintése az CPS rendszerekben gyakorlati példákkal és esettanulmányokkal alátámasztva. Az elemző a technológia lehetőségeire és koraiára helyezi a hangsúly azonban segítve a további kutatásokat és fejlődéseket ezen a területen hozzáad a hatékonyabb és fenntarthatóbb kommunikációs megoldások elterjesztéséhez.

1.1 Miért fontos megvizsgálni a LoRa-WAN technológia felhasználását a CPS rendszerekben?

Az LoRa-WAN (Long Range Wide Area Network), egy vezeték nélküli kommunikációs technológia kifejezetten tervezett távoli adatátvitelhez és az alacsony fogyasztású eszközök számára. Ezért kínál több előnyt ,mint például hosszas átviteli távolság és az energiatakarékos gazdaságosság mellett alkalmassá is teszi az ipar és okos városokban történő felhasználásra is.

A LoRa-WAN technológia egyre több területre terjed ki és jelentős előnyöket kínál a CPS rendszerek számára. Fontos megvizsgálnunk tehát ennek a technológiának az alkalmazásából eredő előnyöket és kihívásokat a CPS rendszerekben és hogy hogyan hasonlítható össze más kommunikációs technológiákkal mint például a Wi-Fi vagy ZigBee vagy Sigfox vagy NB-IoT vagy 5G. A LoRa-WAN technológia lehetővé teszi az eszközeink között való kommunikációt hosszan tartó távolságokon és alacsony energiafogyasztás mellett is amely lényegesen növelheti az ipari alkalmazások hatékonyságát és innovatív lehetőségeit az okos városokban is.

A LoRa-WAN technológia egyik legnagyobb előnye az energiahatékonyságban rejlik: az eszközeink éves szintű energiafelhasználása mindössze néhány wattóra lehet a működéshez szükséges energiamennyiséget jelentősen csökkenti és lehetővé teszi hosszan tartó és fenntartható kommunikációs megoldások kialakítását is. A LoRa-WAN technológia másik pozitívuma a hosszan elérhető távközlés adja: ez lehetőséget biztosít eszközeinknek arra is hogy nagy távolságból kommunikáljanak egymással A széles körben elérhető alkalmazások ezáltal nőnek amelyek segítségével ipari vagy más hasonló proteszt állapotát valós időben felül tudjuk vizsgálni és távolról vezérelni is tudjuk.

1.2 Alapelv alkalmazási területei - Hogyan működjön a LoRa-WAN hálózatban?

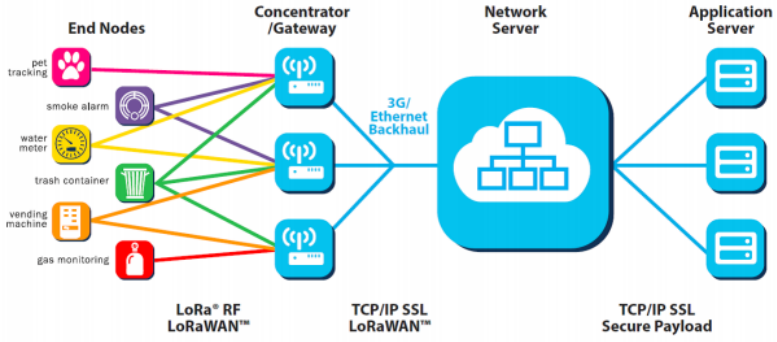
Az Lora-WAN (Long Range Wide Area Network), egy vezeték nélküli kommunikációs protokoll specifikusan kifejezetten távoli adatátvitelhez az alacsony energiaigényű eszközök számára tervezve van. Az Lora (Long Range), egy szórásos átviteli technológia amely engedi az Eszközök közötti kommunikációt nagyon hosszú távolságon. Az Lora-WAN protocol következőképpen működik:

Adat átvitelének folyamata az eszközön (pl. érzékelők vagy IoT eszközein) keresztül történik egy vagy több LoRa átvivő állomás felé. Ezek az állomások közvetítik az adatokat egy központosított szolgáltató szerver felé, amely feldolgozza és továbbítja az információkat a végfelhasználóhoz vagy egy másik rendszerhez.

Adatküldés módszereként az adatátviteli technológia LoRa egy rádiós átvitelt használó módszerét alkalmazza az adatok távol feladására alacsonyan frekvencián és kicsi energiafelhasználással együtt. Ezen keresztül az eszköze lehetővé teszik hogy nagyon messzi helyek közti kommunikációval egymást megértsék.

Adatátviteli sebesség: A LoRa-WAN technológia képes különböző adatsebességeken operálni azzal nagy mértékben megosztás az eszközök távolban és az üzenetek között és a következő újra adatok érdekét is tartalmaz is. Általában az adatkommunikáció sebessége kb 0,3 és 50 kb/s között mozog.

1.3 A háló architektúrája - miből épül fel és hogyan működnek egymással?(ábra 1)



Ábra 1: A végberendezések, átjárók (gateways), hálózati szerverek és alkalmazásszerverek közötti kapcsolat vizualizálása.[12]

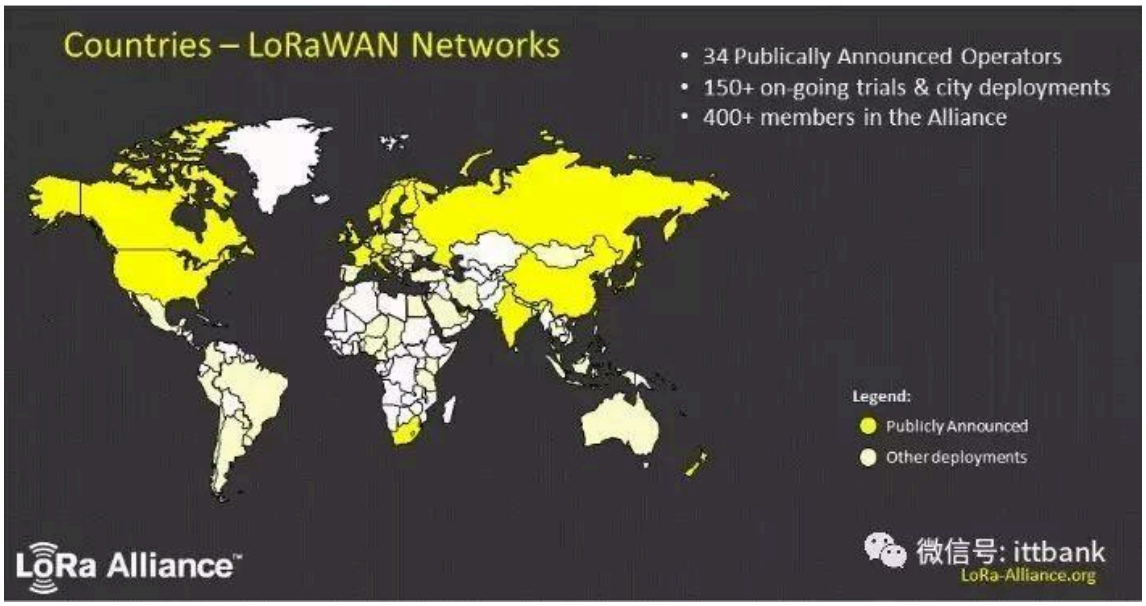
Végberendezések: Ezek az eszköztípusok olyan eszközei a LoRa-WAN hálózatnak amelyek képesek adatok továbbítására és fogadására rajta keresztül; például szenzorok,IoT eszköz vagy más bármilyen eszköz ami LoRa-WAN kommunikációra alkalmas.

Átkötő csomópontok (Gateways): Ezek az állomások fogadják az eszköz által továbbított adatokat, majd átküldik azokat egy központi szolgáltató szerver felé. A LoRa-WAN átkötő csomópontjai képesek több eszközzel egyszerűen kommunikálni és nagy távolságokon is hatékonyan dolgoznak.

Hálózati szerver (Network Server): A hálózati szerver felügyeli és tolmácsolja az átvivő állomások által kapott adatokat felhasználóknak vagy más rendszereknek. Emellett kezdve az eszközfelvevésekkel fogékony és protokollokat is irányít és adatvédelmi irányelveket is kezel.

1.4 Frekvenciatartományok használata az adott frekvenciasávon és ennek jelentősége

- 868 MHz (az Európai Unióban): Ez a frekvenciasávon Európa és más területein használják; nagy távolságú eszközközi kommunikációra alkalmas.
- 915 MHz (Észak-Amerika): Ennek a frekvenciasávnak az Észak-Amerikai régióban történő alkalmazása lehetővé teszi eszközeink közötti nagy távolságú kommunikációt.
- 433 MHz (Ázsia): Ez a frekvenciasávon kizárólag Ázsia országaiban használt, mely lehetővé teszi az eszközeink között történő kommunikációt rendelkező nagy távolságokon keresztül is.



Ábra 2: Az érzékelőktől induló rádiós jelátviteli útvonala a központi rendszerig.[12]

Ahogy az ábra 2-n is látható az elektromágneses hullámok frekvenciasávjának használata kiemelkedő fontosságú szerepet játszik abban a tényben, hogy lehetővé teszi a hosszan tartó távközlést az eszközeink között alacsony energiafelhasználással együtt. Ez rendelkezik jelentőséggel az ipari területeken és intelligens városokban való alkalmazás során is, ahol elengedhetetlen adatokat gyűjtése és tolmácsolás élesztése a nagyon távol es aspiráló pontok között.

1.5 Az energiahatékonyság és az átviteli sebesség kérdéseiről beszélünk. Mennyi az energiafogyasztás, és milyennek a rendelkezésére álló átviteli sebesség?

Az energiahatékonyság az egyik legfontosabb előnye a LoRa-WAN technológiának; lehetővé teszi az eszközeinket éves szintű csak néhány wattóra energiafelhasználással történő üzemeltetésre. Ez jelentős mértékben csökkenti az üzemeltetési költségeket és lehetővé teszi a hosszan tartó és fenntartható kommunikációs megoldások létrehozását.

A LoRa-WAN technológia esetén az adatátviteli sebesség általában 0,3 és 50 kbps között változik attól függően hogy milyen távol vannak egymástól az eszközeink és a központi állomások valamint a tolvaj tároló átfogadott mennyiségtől. Azt látjuk hogy ennek a sebességnek köszönhetően az eszközeink képesek valós idejű adatokat küldeni és fogadni amely jelentős mértékben növelni tudja a hatékonyságot és az innovációs lehetőségeket az ipari alkalmazásokban és okos városokban.

2 Az LoRa-WAN jelentősége az CPS rendszerekben

2.1 Előnyök más vezeték nélküli megoldásokkal szemben. Miben különbözik például az előny az Wi-Fi-hoz képest?

A LoRa-WAN lehetővé teszi a nagyon hosszan történő kommunikációt az eszközeik között nagy távolságokon is elérve ezzel a kapcsolatot a távolabbi helyeken is. Ezáltal kiemelkedően bővíti az alkalmazási lehetőségeket és az ipari automatizálás valamint okos városok hatékonyságát is növelhetjük ezzel a technológiával kapcsolatban például egy Wi-Fi háló csak néhány száz méteren belül működik míg a LoRa-WAN háló több kilométeres távon belül is képes kommunikálni [1].

Az alacsony energiafelhasználás egyik kulcsfontosságú előnye a LoRa-WAN technológiában az energiahatékonyság, amely lehetővé teszi az eszközeinek néhány watt éves energiafelhasználással való működését. Ennek következtében csökkennek az üzemeltetési költségeik és lehetővé teszik a hosszan tartó és fenntartható kommunikációs megoldások kialakítását. Például általában egy Wi-Fi eszköznél nagyobb az energiafogyasztás a LoRa-WAN eszközhöz.

Alacsony költségű megoldások alkalmazása esetén megfizethetővé válik az üzemek és ipari vállalatok számára tömegesen integrálni az eszközeiket hálózatokba anélkül jelentős költségeket viselni kelljen. Ez jelentősen bővilágítja az alkalmazási lehetőségeket és az hatékonyságot az ipari automatizálás és okos városok területén.

A LoRa-WAN nagy kapacitással rendelkezik és képes kezelni számos eszközt egyetlen átvivő állomáson keresztül, lehetővé téve az üzemeknek és ipari vállalatoknak nagy létszámban fejlesztik az IoT alkalmazásokat. Ennek jelentősége növelhető az alkalmazás lehetőségeivel és hatékonyabbá tehető az ipari automatizálásban és okos városokban.

2.2 Milyen ipari területeken használható az alkalmasság?

Az ipari területeken egyre szélesebb körben alkalmazásra kerülő LoRa-WAN technológia számos előnyt nyújt az ipari automatizálásban, okos városokban precíziós mezőgazdaságban és kritikus infrastruktúrája monitorozásában. Ezek közül néhány példa:

Az ipari automatizálásban a LoRa-WAN technológia lehetővé teszi az ipari folyamatok valós idejű figyelemmel kísérését és irányítását a hatékonyság és az innovációs lehetőségeik jelentős növelése érdekében. Például az érzékelőket és vezeték nélküli eszközök segítségével képesek vagyunk távolabbról is felügyelni és irányítani az ipari folyamatokat.

Az okos városokban használt LoRa-WAN technológia lehetővé teszi olyan alkalmazásokat, mint a közlekedés figyelemmel kísérése, a város infrastruktúrájának monitorozása és az épület belüli eszközeinek működtetése. Az érzékelőknél és vezeték nélkül működő eszköznél való alkalmazás révén például a város infrastruktúráját lehet távolabbról is figyelemmel kísérni és irányítani.

Precíziós mezőgazdaság: A LoRa-WAN technológia lehetővé teszi a mezőgazdasági folyamatok valós idejű figyelemmel kísérését és irányítását, ami szignifikánsan növelheti az hatékonyságot és az innovációs lehetőségeket is. Az érzékelőkhöz és vezeték nélküli eszközhöz használni segítségével például lehetségessé válik a mezőgazdasági folyamatok monitorozása és irányítása még nagyon távolabbi helyszínekről is.

A kritikus infrastruktúrákat monitorozása: A LoRa-WAN technológia lehetővé teszi a kritikus infrastruktúráknak a valós idejű figyelem alatt tartását és vezérlését, ami lényegesen javítja az hatékonyságot és az innovációs lehetőségeket is. Például érzékelőket és vezeték nélküli eszközt használva lehetségessé válik a kritikus infrastruktúráknak a nagyon távol eső helyek közvetlen felügyelete és irányítása is.

3 Gyakorlati felhasználások [13]

3.1 Okos városok és a LoRa-WAN használata [6]

Előnyök: A LoRa-WAN lehetővé teszi az utcákon és közlekedési infrastruktúrában elhelyezett érzékelőket valós időben figyelemmel kísérni. Ezek az érzékelő eszközei segítségével figyelemmel kísérhető a forgalom áramlása, a parkolóhelyek állapota és a közlekedési események alakulása.

Egy városban a közlekedés áramlatát LoRa-WAN érzékelők segítségével figyelemmel kísérhetik és az adatok valós ideje közvetítése lehetségessé válik számukra.. Ennek révén lehetőség nyílik a város közlekedés rendszereinek dinamikus reagálására a forgalom változtatása esetén például újratervezve a forgalmat vagy előrelátó módon kezelni a forgalom szabályosságát.

3.1.1 Okos városok - Forgalomirányítás LoRa-WAN segítségével

Előnyök: A LoRa-WAN segítségével a városok infrastruktúrája valós idejeben figyelemmel kísérhető és monitorozhatóvé válik Ez lehetővé teszi a város vezetésének az infrastruktúra problémáinak előre látható kezelését és a város életminőségének javítását.

Egy városban LoRa-WAN érzékelőket használnak ahhoz a középen található épületek állapotának figyelemmel követését és monitorozását lehetővé tegyük.Ezek a érzékelők például megfigyelhetik a középen található fények állapotát,a távolabb állásokat és a közlekedéshez kapcsolódó eseményeket is.

3.1.2 Irodai épület berendezéseinek megfigyelése

Előnyök: A LoRa-WAN technológia lehetővé teszi a köztéri eszközök vezérlését és figyelemmel kísérését valós időben. Ez segíti a városvezetést dinamikusan reagálnak a köztéri eszközök állapotára és javítani a város életminőségét.

Egy városban a LoRa-WAN vezérlőket használva lehetővé válik a közfények valós idejű szabályozása és monitorozása középületeken belül. Ezek a vezérlőegységeknél például lehetségessé teszik a közfények állapotának figyelemmel kísérését és a közlekedés események monitorozását is.

3.2 Precíziós mezőgazdaság – Melyek az előnyei a mezőgazdaság területén?

Előnyök: A LoRa-WAN lehetővé teszi a mezőgazdasági területeken elhelyezett érzékelőket azonnali figyelemmel kísérni és monitorozni. Ezek az érzékelő eszközei képesek nyomon követni a növénytermesztés állapotát, ellenőrizni a talaj állapotát és felügyelni a mezőgazdasági folyamatokat.

Az agrárterületeken a LoRa-WAN érzékelőinek használata lehetővé teszi a növénytermesztés állapotának figyelemmel kísérését és monitorozását. Ezek az eszközeke segítségével ellenőrizhetjük például a növények, a talaj állapotát és a mezőgazdasági folyamatokat is.

3.2.1 Állattenyésztés figyelemmel követése

Előnyök: A LoRa-WAN technológia lehetővé teszi a mezőgazdasági területeken elhelyezett érzékelőkből származó valós idejű adatok figyelemmel kísérését és monitorozását a háziállatok egészségének felügyelete céljából és az állattenyésztési folyamatok hatékonyabb megfigyeléséhező a mezőgazdasági infrastruktúra állapotának figyelemmel kísérése érdekében.

Az állattenyesztés területén LoRa-WAN érzékelőket használnak az állatok egészségének és viselkedésének nyomon követéséhért és megfigyeleséért.Hála ezeknek az egészségi státuszkövető eszközöknek például figyelemmel kísérhetjük az állatok jólétét és a tenyésztési folyamatokat is valamint az álláttenyesztesi infrastruktúra státuszának monitorozása is lehetségessé válik. [7]

3.3 Mező- és gazdaságfejlesztés automatizálása

Előnyök: A LoRa-WAN lehetővé teszi a mezőgazdasági műveleteik valós ideiglenes automatizálását és irányítását.Ahogy a mezőgazdasági cégeknél dinamikusan tudnak reagálni a mezőgazdasági műveleteik változtatásaiban és javíthatnak az hatékonyságán.

Egy művelés során a LoRa-WAN vezérlő használata lehetővé teszi a művelési folyamatok valós idejű automatizálását és irányítását. Az ilyen vezérlő segítségével például automatizálhatóak a művelési folyamatok, irányíthatóak a művelési folyamatok és monitorozhatóak is azok.

4 Az ipari automatizálás szerepe az ipari folyamatok megerősítésében

4.1 Gépek állapotának monitorozása és jóslás alapú karbantartás

A LoRa-WAN technológia lehetővé teszi az ipari gépek valós idejű figyelemmel kísérését és monitorozását a LoRa-WAN érzékelőket használva a gyártási üzemekben lehetővé teszik a gépek állapotának és az üzemeltetési adatok figyelemmel kísérését az előző karbantartási alkalmazásokra és az üzemeltetés költségeinek történő csökkentésére való felhasználásukkat. Az ipari automatizálásban az hatékonyságot és a fejlesztési lehetőségeket szem előtt tartják. [8]

4.2 Folyamatok automatizálása és irányítása

A LoRa-WAN technológia lehetővé teszi az ipari folyamatok valós idejű automatizálását és irányítását. Ez segíti az ipari vállalatokat abban, hogy rugalmasan reagáljanak a folyamatok változására és javítsák a hatékonyságot. Például egy gyárban a LoRa-WAN vezérlő eszközeinek felhasználásával automatizálható és irányítható az ipari folyamatok vezérlése és monitorozása is. Ezek az eszközök jelentősen növelik az effektivitást és az innovációs lehetőségeket az ipari automatizálás területén.

A LoRa-WAN technológia lehetővé teszi az ipari folyamatok energiafogyasztásának figyelemmel kísérését és optimalizálását. Az ipari vállalatok ezekkel a érzékelővel képesek lesznek ellenőrizni az energiafelhasználást és optimalizálnia azt a működés során ami jelentős mértékben csökkenthetik a kötelező kiadásokat. Például egy gyártó üzemben a LoRa-WAN érzékelőinél felhasználva lehetővé teszik az energia használat figyelemmel kísérését és optimalizálását, ami remek lehetőség az operatív költségek csökkentésére illetve az energia felhasználas javítására.

A LoRa-WAN technológia lehetővé teszi a gyártási folyamatok valós idejű monitorozását és optimalizálását ipari környezetben is. Az ilyen érzékelőrendszer segítségével az ipari cégeknél folyamatosan figyelemmel kísérhetik a gyártási folyamatokat és optimalizálhatják azokat is, ezáltal hatékonyabban működhetnek és nagyobb innovációs lehetőségeket teremthetnek maguknak is.

4.3 Monitorozás az energiaellátó hálózat

A LoRa-WAN technológia lehetővé teszi az energia hálózat valós időben figyelemmel kísérni és monitorozni. Ezek az érzékelők segítik a hálózatokat megfigyelni, követni a folyamatokat az üzemi adatokat gyűjtve. Például az energia hálóban a LoRa-WAN érzékelő jelek használatával lehetséges a hálózat állapotának figyelemmel kísérése és az üzemadatok összesítése is ezáltal csökkentheti az üzemeltetési kötséget és javíthatja a hálózat stabilitását. [9]

A LoRa-WAN technológia lehetővé teszi a vízhálóztatás valós idejű figyelemmel kísérését és monitorozását. Az ilyen érzékelők segítségével nyomon követni lehet a vízhálózat állapotát és folyamatát is, valamint gyűjteni az üzemeltetési adatokat is ezen rendszerekhez történő használatakor. A például egy vízhálózatban felhasznált LoRa-WAN érzékelő segítik a víz hálózat állapotának és üzemelési adatok gyűjtését is lehetővé teszik, hogy ezen információ használatakor az üzemelési költség csökkentését illetve a hálózat stabilizációját.

A LoRa-WAN technológia lehetőséget nyújt a környezeti állapot valós idejű figyelemmel kísérésére és monitorozására ismétlődően. Ezek a érzékelő berendezések alkalmasak a környezeti állapot figyelemmel kísérésében és a környezeti folyamatok monitorizálásában történő alkalmazásra valamint az azt követő környezeti üzemeltetés működtetésbe integrálásra történő adatgyűjtés során felhasználásra lehetőségét biztosító tevékenységhez is hasznosíthatóak.. Egy példát említve például egy LoRa-WAN érzékelős környezet szemléltetést is tartalmazó rendszerek eszközeivel lehet, hogy az állapotok megfigyelése, az üzemeltetést végző csoportok párbeszédbeli információnak gyűjtése is lehetővé válik mindenfajta költség csökkentését szolgáló intézkedésekre finanszirozási céllal.

5 Kritikus infrastruktúráink védelme

A LoRa-WAN technológia lehetővé teszi a kritikus infrastruktúráknak valós idejű figyelemmel kísérését és monitorozását a biztonság érdekében is fontos szerepet játszik. Az ilyen érzékelőeszközei segítik a kritikus infrastruktúráknak a folyamatok figyelemmel kísérését és az üzemadatok gyűjtését is hajthatja. Például a LoRa-WAN érzékelőinek való alkalmazása egy kritikus infrastruktúrában lehetővé teszi az állapotuk figyelemmel történő követését és az operatív információkat hogy gazdaságosabban működtethetőek legyenek és javíthatja ezen rendszerek biztonságát is.

Ezek az érzékelő eszközzel vehetnek előre jelző karbantartást végezhetnek javasolt emellett az üzemeltetés hatékonyságát és képességét csökkenteni az energia rendszeres leállásokat és kapcsolódási problémákat például egy energiatelep LoRa-WAN érzékelőivel előrejelző karbantartást végezhetnek amely kevesebbszer áll le és tapasztal problémát. Az energia áramrendszer hatékonyabban működik és biztonságosabb.

A LoRa-WAN technológia segítségével a kritikus infrastruktúrákat valós időben lehet figyelemmel kísérni és monitorozni. Ezek a érzékelő eszközei lehetővé teszik a kritikus infrastruktúráknál az állapot figyelemmel kísérését és a folyamatok monitorozását, valamint az üzemelési adatok gyűjtését is. Például LoRa-WAN érzékelőket használva egy kritikus infrastruktúrában lehetőség van az állapot figyelemmel kísérésére és az üzemelési adatok rögzítésére, mely segíthet csökkenteni az üzemeltetési költségeket és javítani a kritikus infrastruktúra működését is.

A működés folyamatait javítható és fejleszthető az innovációs lehetőségekkel is. Az üzemeltetés során az effektivitás és az innovációs lehetőségeket jelentősen megnövelhetik, például egy vízhálózatban. A LoRa-WAN által használt érzékelő hozzávetőleges elhelyezése optimalizálta illetve növelte ezáltal azt hatékonyabb és újszerűbb lehetőség teremtést.

5.1 Biztonsági és méretezőképes problémák

5.1.1 Adatvédelem és biztonságos adatkezelés kérdéseinek, és azok megoldására irányuló lépésekről.

Az együtt létnek a LoRa-WAN technológia egy széles körű területén való elterjesztése számos előnyt rejt magában; azonban biztonsági és skálázhatósági kihívásokkal kell szembenéznünk együttes használatakor érintve az adatvédelmet és hálózat stabilitást valamint a kommunikációs hatékonyság kérdéseire koncentrálnunk kell. [10]

5.1.2 Biztonsági kockázatok

5.1.2.1 Adatvédelmi veszedelmek és kockázatok

A LoRa-WAN hálózatokban az adatvédelem kritikus fontosságú szerepet játszik. A vezeték nélküli kommunikáció természetesen biztonsági kockázatokat rejt magában, például az adatok elfogását, megváltoztatását és hamisítását. Ezek a veszélyek érzékeny információkat szivároghatnak ki, szolgáltatások zavarhatnak meg, és potenciális fenyegetést jelenthetnek a kulcsfontosságú infrastruktúrára. Például ipari automatizálási és okos városi alkalmazásokban az engedély nélküli adathozzáférés súlyos biztonsági problémákhoz vezethet.

LoRa-WAN hálóknak szembe kell néznünk számos támadással ilyenekkel például DoS (Szolgáltatás Megtagadása), amelyek célja az eszközt vagy államot elérhetővé tevő eszközeinknél van tiltva Ezek ezek az általánosan széles adatforgalommal vagy hamis csomagok küldésével történnek ha az eszközt vagy rendszert túlzottan terhelik és nem érhetik el.

5.1.2.2 Esettanulmányok példaképek

Egy ipari parkban például számos érzékelő és vezeték nélkül használt eszközzel egy sikeres DoS támadás lehetővé teszi az üzemeltetés leállítását és az adatforgalom zavarását is egyaránt. Ebben az esetben a támadó átfogó adatforgalommal vagy hamis csomagjaikkal terheli túl az eszközöket vagy állomásokat ami által azok elérhetetlenek lehetnek.

Az adatvédelem biztosítása érdekében az LoRa-WAN technológia több kriptográfia módszerrel dolgozik együtt. Ezek közé tartozik az Advanced Encryption Standard (AES), valamint az Elliptic Curve Cryptography (ECC), amelyek segítségével titkosíthatjuk az adatokat és hitelesíthetjük az eszközt.

AES Titkosításról szólva az AES egy szimmetrikus kulcsú titkosítási algoritmus, amely lehetővé teszi az adatok biztonságos továbbítását. A LoRa-WAN eszközeinek és állomásainak kommunikációjában az adatokat AES titkosítással védelemmel látják el annak érdekében, hogy megelőzzék az adatok elfogását és módosítását.

Az ECC hitelesítés egy nyilvános kulcsú titkosítási eljárás, amely lehetővé teszi az eszköz hitelesítést. A LoRa-WAN eszközeink és állomásain történő kommunikáció során az eszközeinkkel ECC alapú hitelesítést végeznek el annak érdekében, hogy megakadályozza a hamis eszközeinek és állomások használatát.

5.2 Hálózat Védelmi intézkedések rendszerek

LoRa-WAN hálózat rendszereinkben több biztonsági intézkedést kell bevezetni annak érdekében,védelemmel ellássák magukat az esetleges támadások ellen.Ezek közé tartozik például az háló szegmentálása az adatforgalom figyelése és az illetéktelen behatolás érzékelőrendszerei.

Hálózati szegmentálás: A hálózát szegmentálásnak köszönhetően lehetőség nyílik arra, hogy egy LoRa-WAN hálózat több apróbb és biztonságosabb szegmensbe osztják fel,mely csökkenti az esetleges támadások hatótávját. Egy ipari parkban például,a hálózati szegmentálás köszönhetően az eszközök és állomásokat külön szegmensbe osztályozhatjuk, mely megakadályozza,hogy egy támadással hatást gyakoroljon az egész hálózatra.

Adatforgalom figyelemmel kísérése: A LoRa-WAN hálóknak fontos az adatforgalom figyelemmel kísérése annak érdekében, hogy előzetesen meg tudjanak küszöbölni támadásokat. Ezek a eszközöket lehetővé teszik az adatforgalom valós idejű ellenőrzését és a támadások észlelést is. Az adatát illetően például egy városban az adatforgalom figyelemmel kísérésével lehetőség van az eszközök, állomások közötti adatforgalom valós idejű ellenőrzésére, összekapcsolni és kimutatható tenni a támadásokat.

Intruder érzékelési rendszerek: Az intruder érzékelési rendszerek lehetővé teszik a LoRa-WAN hálózat a támadások észlelése és kezelése céljából. Ezek az eszközállományok képesek az eszközeik és állomásaik közötti kommunikáció során a támadások észlelése és kezelése is.. Például egy ipari parkban az intruder érzékelési rendszerek lehetővé teszik az eszközeik és állomásaik közötti kommunikáció során a támadások észlelése és kezelése is..

LoRa-WAN hálóinak biztosítaniuk kell felhasználóik és eszközeik azonosítását annak érdekében, hogy védettek legyenek az esetleges támadásokkal szemben. Fontos szerepet játszik ebben az eszközeink és felhasználóink hitelesítése valamint jogosultságaik ellenőrzése.

Az eszköz hitelesítés fontossága: A LoRa-WAN eszközei és állomásai számára elengedhetetlen a hitelesítés annak érdekében, hogy biztosítsák az adatok biztonságát. Ezek az eszközök lehetővé teszik az eszközeinek és állomások közötti kommunikáció során való egymás hitelesítését például egy ipari parkban ahhoz hogy megakadályozza a hamis eszközök és állomások használatát.

Az eszköz hitelesítés fontos szerepet játszik abban hogy csak az engedélyezett eszközök tudjanak kommunikálni a hálóval. Ez általában különleges eszköz azonosítókkal, titkos kulcsokkal vagy tanusítványokkal történik. A LoRa-WAN eszközei és állomásoknak is szükségük van hitelesítésével annak érdekében, hogy biztosítsák az adatvédelmet.

Például egy ipari automatizálási rendszerben több érzékelő és vezeték nélkülí eszközt használnak, amelyeknek hitelesítési eljárásra van szükségük az egymás közötti kommunikáció során. Ezáltal az eszközök és állomások megbíznak egymásban az adatok biztonságos továbbítása érdekében és megakadályozza az engedély nélküli eszközfelhasználást.

5.3 Fontossági fokozat és jelentőség - jelentőség

A hálózati megbízhatóság létfontosságú tényező a LoRa-WAN technológia hatékony felhasználásában. Az állandó és megbízható kommunikáció az eszközök és állomásain között elengedhetetlen az ipari automatizáció okos városokhozt és más kritikus felhasználásokhozt is.S instabil hálózással adatvesztéshez kommunikációs hibákra és eszközök elérhetetlenségéhez vezethetnek ami jelentős költségeket és biztonsági kockázatot okozhatnak.

Elérhetőség: Azért szükséges elérni az hálózat stabilitását különböző szinteken keresztül beleértve az infrastruktúra javítását és karbantartását is, hogy kezelhető legyen az adatforgalom és garantált legyen háló elemeinek redundanciája.

Infrastruktúra fejlődése: A fizikai infrastruktúra állandó fejlődtetése és frissítése nélkülözhetetlen ahhoz hogy az stabilitás megtartassa magát. Ezért gyakori ellenőrzés és frissítés szükséges az adott állomásoknak eszközeinek és az kapcsolódási pontoknak. Vegyünk például egy ipari parkot ahol sok érzékelö és vezeték nélküli eszköz dolgoznak, az infrastruktúra fejlődtetés biztosítsa azt, hogy az eszközök és állomások folyamatosan kommunikáljanak egymással közöttük.

Az adatforgalom kezelése: Az adatforgalom kezelése és optimalizálása jelentősen javítja a háló stabilitását és megbízhatóságát. Ezáltal a háló hatékonyan képes kezelni az adatok áramoltatását és csökkenti az adatvesztést valamint a kommunikációs hibákat is. Például egy okos városban számos eszközzel történő kommunikáció során az adatforgalom irányítása szavatolja az adatok valós idejű továbbítását és fogadását is.

Redundancia: A hálózati elemek feleslegessége garantálja azt a tényezőn kívüli szükségszerűséget hogy az egyes elemek hibája nem befolyásolja a háló intézmény teljesítményét. Nem érdemes figyelembe sem vennem több összekötő pont és átvivő állomás segítségét. De kell minden eszközhöz és állomáshoz rendeltetett több kapcsolódási pont és átvivő állomás ami minimalizálja az adat vesztést és kommunikációs hibákat. Példaképpen egy válságmenedzselés infrastruktúrában ahol tucatnyi érzékelés használata vezeték nélkül eszközök társítva a feleslegesség biztosítja azt hogy az eszközök és állomások valamint folyamatosan egymást keressék közvetlen kapcsolatot adjanak.

5.4 Hatékony kommunikáció módszerei a hatékonyság növelésére

A kommunikációs hatékonyság alapvető fontosságú a LoRa-WAN technológia sikeres alkalmazásában. Az effektív kommunikáció lehetővé teszi az eszközök és állomások között gyors és megbízható adatátvitelt; ez kulcsfontosságú az ipari automatizálásban és okos városokban való alkalmazások során is. Ha azonban a hatékonyság alacsony szintű lehetőséget ad az adatvesztésnek, a kommunikációs hibáknak és eszközök elérhetetlenek lesznek, ami jelentős költségeket okozhat valamint biztonsági problémákhoz vezethet.

5.5 Módszerek

Az kommunikáció hatékonyságának növelése különféle módon valósulhat meg,, ilyenek a adatátviteli sebesség növelése az adatforgalom optimalizálása és az adatvesztés minimalizálása.

Az adatátviteli sebesség növelése: Az adatátviteli sebesség fokozása lehetővé teszi az eszközök és állomásoknak az adatok gyorsabb és hatékonyabb átvitelét egymás között. Ez azt jelenti,hogy a hálózati képes nagyobb adatmennyiséget kezelni az adott időszakban,mely csökkenti az adatvesztést és kommunikációs hibákat is.Például egy ipari parkban ahol számos szenzor és vezeték nélküli eszköz funkcionális kommunikációját biztosítja.

Adatátvitel optimalizálása: Az adatátvitel optimalizálása lehetővé teszi az eszközeink és állomásainkkal való hatékonyabb és megbízhatóbb adatforgalmat biztosítani egymás között. Ez azt jelenti hogy a hálózat könnyebben és hatékonyabban kezelhetik az adatforgalmat ami csökkentheti az adatvesztések és kommunikációs hibák kockázatait. Például egy okos városban ahol sok készülék kommunikál egymással az Adatátvitel optimalizálása garantálja hogy az információkat valós időben továbbítsák és fogadják.

6 Milyen fajta újdonságok megjelenése várható a közelgő időszakban?

A LoRa-WAN technológia folyamatos fejlődéséhez teljesen elengedhetetlenek az előrelépés lehetőségeinek következő generációjának lehetőségeit és alkalmazásait tekintve.Ezeknek az innovációknak köszönhetően újdonságokat vezethetünk be és szolgáltatásokat fejlődhetünk ki,melyek tovább növelik technológia alkalmazhatóságát és hatékonyságát. A jövőbeli felfedését az újonnan kifejezetten integrált technológiákra, a adatkezelés és elemző rendszerek fejlődésével együtt valamint az újdonsült alkalmazások és szolgáltatások bevezetését is beleértve.

Azért egy LoRa-WAN technológia folyamatosan fejlődni és sok újdonság várható kiegészítést nyújt az alkalmazások számára és hatékonyságát növelve az alkalmazások területet és lehetőségeket is bővítik majdan.

Az egyik legígéretesebb fejlődési irány a 5G és a LoRa-WAN integrálása lehet. A 5G technológia nagy sebességet és kapacitást kínál, amely tökéletes kiegészítése a LoRa-WAN hosszan ható távközlésének és alacsony energiafogyasztásának általános hiányosságainak. Ezen lehetőség teszi lehetővé az eszközeink között valós idejű kommunikációt és adatátviteli sebesülése növelést az ipari automatizációban és okos városokban hasznosítva.

Egy intelligens városban például az 5G és LoRa-WAN kombinációja lehetővé teszi az utcákon és közlekedési infrastruktúrában található érzékelőknél az valós ideje figyelemmel kísérését és az adatok gyors tolmácsolását. Ezeknek köszönhetően a város közlekedés rendszere dinamikusan tud reagálni a forgalom változása és előrelátó módon kezelni a forgalom szabályszerűségét.

6.1 Edge számítástechnika és LoRa-WAN alkalmazása

Egy másik fejlődés iránya az élvonalbeliség és a LoRa-WAN összevonása lehetősége. Az élvonalbeliség lehetővé teszi az adatok közvetlenül az eszközeinken vagy a közelben lévő számítási erőforásokon történő feldolgozási képességét, ami csökkenti az adatátviteli időket és növelheti hálózati hatékonyságot is ezáltal a eszközeink gyorsabban választ adhatnak az érzékelő és valós idejű döntéseket hozhatnak. [11]

Az ipari parkokban például az edge computing és LoRa-WAN kombinációja segíti az ipari gépek valós idejű állapotfigyelését és az üzemeltetési adatok gyors feldolgozását. Ez megengedi az ipari vállalatoknak a prediktív karbantartást és a működési költségeik csökkentését.

A mesterséges intelligencia és a szokatlan tanulás egyaránt egyértelmű fontosságot kapnak a LoRa-WAN hálózat alkotó hálózati rendszerekben. Ezek az eszközök lehetővé teszik az adatok elemző vizsgálatát és az érzékelő alapuló előzetes megfigyeléseket is végrehajtanak ami jelentősen bővebb körű alkalmazhatóságot és teljesítést biztosítanak. Például mező gazdaságban a gépi tanulás és szokatlan tanulás segítségével előrelátást nyerhetünk a termesztett ültetvények állapotáról és analizálható üzemeltetés biztos adatokat amely nagymértékben fokozza a hatékonyságot és innovációs lehetőségeket is.

Adataink biztonságának és védelmének továbbfejlődésével számíthatunk az elkövetkező fejlődésekre is a jövőben. Az adatok védelme és az adatvesztések, valamint a kommunikációs hibák megakadályozása érdekében újonnan bevezetett kriptográfiai módszer és biztonsági protokollok segítségével garantálhatók leszel, például egy kulcsfontosságú infrastruktúrában az ilyen újdonságok bevezetése megóvják az adatokat és meghiúsítja az esetleges hibás kommunikációt is.

Az egészségügy területén egyik újdonság az okos egészségügy alkalmazása lehetőséget nyújt az egészségügyben használt eszközökről valós ideje figyelemmel kisérni és az adatok közvetítéshez felhasználni.A szakembereknek lehetőséget ad ez arra,hogy folyamatosan figyelemmel kísérhessék és értékelhessék betegeik állapotát ami sokat segít az egészségügy minőségének javításán.

Az intelligens mezőgazdaság egy másik újfajta alkalmazási területet kínál, amely lehetővé teszi a mezőgazdasági műveletek valós idejű ellenőrzését és adatok átvitelét. Ez lehetőséget teremthet a mezőgazdasági vállalatok számára arra, hogy dinamikusan reagáljanak a mezőgazdasági műveleteinek változásaira és növelhessék az hatékonyságát.

Az okos ipari szektor egy másik újfajta alkalmazási területet jelentő lehetőség az ipari folyamatok valós idejű megfigyelése és az adatok átvitele szempontjából is fontos szerepet játszik.. Ez segíti az ipari vállalatokat abban,, hogy dinamikusan reagálhassanak a gyártás során bekövetkező változásokra és növelhetjük hatékonyságukat.

7 Összehasonlítás LoRa-WAN és más kommunikációs technológiák között [14]

7.1 Wi-Fi hálóra épülő ZigBee technológia valamint Sigfox és NB-IOT protokoll és az 5. generációs mobiltechnológia között mily nézőpontok alapulhatnak az összevetésre?

Az IoT alkalmazásokban egyre elterjedtebb az LoRa-WAN technológia használata; azonban más kommunikációs technológiák is elérhetőek ezen felül Wi-Fi, ZigBee, Sigfox, NB-IoT és 5G formájában. Az egyes technológiák összevetésére különböző szempontok alapján van lehetőségünk, hogy megállapítsuk, melyik lenne legoptimálisabb egy adott alkalmazási helyzetben.

7.2 Kiadások [5]

A LoRa-WAN technológia alacsony költségű infrastruktúrát és eszközkészletet biztosít nagymértékű alkalmazások számára.

Wi-Fi használata drágább lehet nagyméretű területeken vagy sok eszközzel működtetve.

A ZigBee egy olcsó megoldás volt mindig is ám távig és kapacitást illetően korábban mindig korlatokkal küzdött.

Sigfox az egyik legköltségesebb alternatíva a kommunikációra vonatkozóan és csak egyirányú kommunikációt tesz lehetővé.

Az NB-IOT sokkal drágább lehetőségnek tűnhet az alacsony hatékonyság ellenére is.

A 4 generációs mobilhálózatok nagyon költik a pénzt de cserébe magas sebességet és kapacitást biztosítanak.

LoRa-WAN háló. Erős jelek nagy távolban (kilométerekre).

Wi-Fi jelentése vezeték nélküli háló, amely rövid távon (pár száz méteren belül) működik.

A ZigBee technológia rövid távközlési távon működik (néha csak négyzetméterekig terjed).

Sigfox egy olyan technológia, amely hosszan tud kommunikálni (akár kilométerek távjából is), azonban csak egyirányú kommunikációra képes.

NB-Iot technológia lehetővé teszi nagyon nagy távfelhasználását (akár több kilométerre is).

7.3 LoRa-WAN technológia lehetővé teszi nagyszámú eszköze hatékony kezelését nagyméretű adatkapacitással rendelkező háló hátterének segítségével. [4]

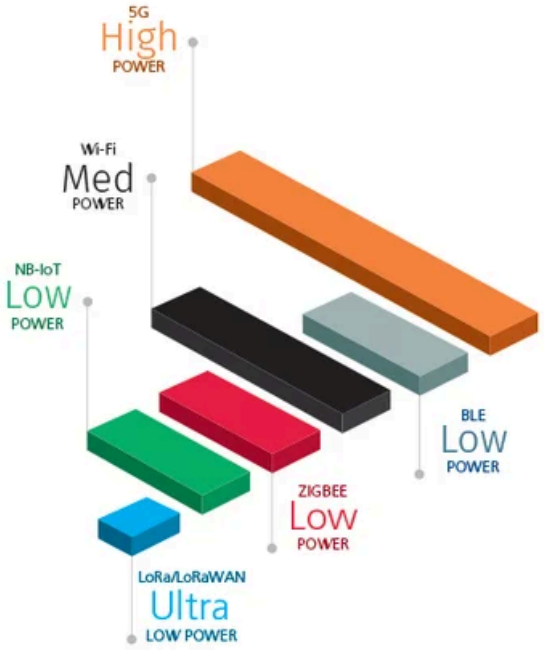
Wi-Fi kapcsolat korábban elérhető volt csak korai óráktól késő estig.

A ZigBee technológia korhatárolat és alacsonyköltségű lehetőség.

Sigfox egy korábban rövid kapacitású technológia volt és csak egyirányú kommunikációra képes volt.

NB-IOT technológia lehetővé teszi nagyszámú eszközzel való hatékony kommunikációt és kezelést.

A 6 G frekvencia lehetővé teszi nagy mennyiségű eszközzel való kommunikációt és gyors adatátvitelt is biztosít.



Ábra 3: Könnyen áttekinthető technológiai összehasonlítás a dokumentumban leírtak alapján.

7.4 Az energiahatékonyság kiemelt fontosságú terület a fenntartható fejlődés szempontjából. [2] (ábra 3)

LoRa-WAN rendszerrel rendelkező megoldások kiválóan alkalmasak hosszan tartó és távolabbi területeken történő felhasználásra is az alacsony energiafogyasztásának köszönhetően.

Wi-Fi kapcsolat esetén az energiatakarékosság alacsonynak bizonyulhat elsősorban akkor igaz ez ha gyors kommunikációra van szükségünk.

A ZigBee technológia energiatakarékos jellegű ugyanakkor vannak határai távméret és kapacitás szempontok szerint.

Sigfox egy nagyon energiatakarékos technológia lehetőséget ad a kommunikációra csak egy irányú kommunikációt biztosítva.

Az NB-IOT technológia energiatudatos módon működik és lehetővé teszi a hosszan távol létesített alkalmazások használatát is.

A 4-ik generációs mobilháló nem igazán hatékony az energiafelhasználás terén különösen nagyon gyors adatkommunikáció esetén.

LoRa-WAN technológia jellemzője az alacsonyan adatátviteli sebesség (kbps), ugyanakkor alkalmas hosszú távon való kommunikációra és alacsony energiafelhasználásra is.

Wi-Fi hálózatok lehetővé teszik a nagymértékű adatátvitelt nagyon gyors sebességgel (Mbps), ami alkalmas rövid távon való kommunikációra és nagymértékű sebességű adatforgalomra.

A ZigBee vezeték nélküli kommunikációs protokoll alacsony szintű adatátviteli sebesség jellemzi (kbps), de viszonylag alacsony költségű és energiatakarékosság is egyben.

Sigfox hálózat jellemzői között szerepel az alacsonyan sebes adatátvitel (kbps), mely csak egyirányú kommunikációra használható.

NB-IOT (Narrowband Internet of Things): Bár alacsonyak az adatátviteli sebességű, lehetőség van nagyszámú adat fogadására és hosszan tartó kommunikációra is a kibővített lefedettség és távoli elérés révén.

7.5 Mely helyzetekben érdemes ezeket a technológiai megoldásokat összekombinálni?

Az alkalmazások számára kedvező és előnyös lehetőségeket nyújt az egyes technológiák kombinálása által létrehozott kommunikációs technológiák alkalmazása.

Azáltal biztosíthatjuk a háló redundanciáját egy ipari parkban például ahol több érzékelő és vezeték nélküli eszközt használnak az LoRa-WAN és NB-IoT technológiák kombinálásával lehetővé válik az eszközök és állomások folyamatos kommunikációja még akkor is ha bármelyik technológiánál hiba lép fel.

7.5.1 Adatátviteli sebességgel és távoli információ átadással kapcsolatban

Az adatátviteli sebesség és tápfeszültség optimalizálásához mint az is megfontolandó lehet több kommunikációs technológia kombinálása Az okos városok például ahol sok eszközön keresztül kommunikálnak egymás között Wi-Fi és LoRa-WAN kombináció napjainkra gyorsan lehetővé teszi az eszközön kommunikálnak egymást megoldva miközben LoRa-WAN kezeli hosszan távolítsa el.

7.5.2 Energiahatékonyság és teljesítmény

Az energiahatékonyság és kapacitás optimalizálása érdekében érdemes több kommunikációs technológiát kombinálni. Például egy mezőgazdasági területen sok érzékelő és vezetéken keresztül működtetett eszközzel a ZigBee és a LoRa-WAN összekapcsolása lehetővé teszi az eszközeinekk energiahatékony kommunikációját egymás között úgy hogy a nagy kapacitást a LoRa-WAN kezelje.

8 Szolgáltatások és programok

Az egyes kommunikációs technológiák összekapcsolásának lehetősége számos előnyhöz és alkalmazások specifikus igényeknek való megfelelést teszi lehetővé ezek számára Az ilyen kombinációkat érdemes mérlegelni annak érdekében hogy az alkalmazások hatékonyságát és megbízhatóságát megerősítsük.

Az előnyök: A LoRa-WAN hosszan tartó átvitelének képessége és alacsony energiafogyasztása ideálisak az utcákon és közlekedési infrastruktúrában elhelyezett érzékelőket valós idejű figyelemmel kísérni. Az 5G magas sebességű és alacsony késleltetésű kapcsolata lehetővé teszi a közlekedési rendszerek dinamikus irányítását és az adatok gyors továbbítását, ami segíthet a forgalom optimalizálásában és az üzemeltetés költség megtakarításában.

8.1 Városok Infrastruktúrájának Figyelése

Előnyök: A LoRa-WAN hosszan tartó átviteli képességeivel és alacsony költségű megoldásaival ideálisan alkalmas a városok infrastruktúrájának valós idejű figyelemmel kísérésére, míg a ZigBee lehetővé teszi az infrastruktúra belső részeinek elemei figyelemmel kísérését és irányítását, miközben ezzel alacsonyan energiafelhasználással és működési költséggel működik, ezáltal lehetővé téve a város infrastruktúra optimalizálását és az üzemeltetési költségeinek csökkentését.

8.2 Központosított eszköztár kezelése

A LoRa-WAN hosszan tartó kommunikációs képessége kívül, alacsony költségével is megfelelek a középtávú eszközfelügyelet és valós idejű monitorozás igényeinél egy épületben vagy létesítményben. A Wi-Fi gyors kommunikációt és adattranszfert teszt lehetővé az eszközöök között, ami a középtávon történő eszköz mennyiség optimalizálását eredményezi, valamint az üzemeltetés kötségeket csökkenti.

9 LoRa-WAN és NB-Iot kombinációja.

Az előnyök közé tartozik a LoRa-WAN hosszan tartó közvetítő képessége és alacsony energiafelhasználásának alkalmassága a mezőgazdasági területeken elhelyezett érzékelőket valós időben figyelemmel kísérniheyeiz. Az NB-Iot is lehetővé teszi az adatok gyors átvitelét és a nagykamocságú kommunikációt, ami segíti a termelés optimalizálását és az üzemeltetés költségeinek csökkentését.

9.1 LoRa-WAN és Sigfox kombinációja.

Előnyök: A LoRa-WAN hosszan tartó kommunikációs képessége és alacsonyköltsége alkalmas az állattenyesztés területeken elhelyezett érzékelőkre valós idejű figyelemmel kíséréséhez. A Sigfox lehetőséget biztosít az adatok egyirányú továbbítására és az alacsony költségű kommunikációra.Ez lehetővé teszi az állattenyésztés optimalizálását és a működés költségek csökkentését.

9.2 LoRa-WAN és ZigBee összekapcsolása

Előnyök: A LoRa-WAN jelentős távközlési képességeivel és alacsony költségű működtetésével lehetővé teszi a mezőgazdasági tevékenységeket valós idejű automatizálásra és vezérlésének szükségességét.A ZigBee technológiának köszönhetően belül is figyelemmel kísérhető és irányítható a mezőgazdasági infrastruktúra, miközbe a költséggazdaságos üzemeltetést biztosítja. Alapvető funkciója az agráripari tevékenységeken belüli optimalizálás és a működtetés költség megtakarítása is.

9.3 LoRa-WAN és 5. generációs mobilhálózat (5) kombinációja.

Előnyök: A LoRa-WAN hosszan tartó adatküldés és alacsony energiafelhasználás miatt ideális az ipari gépek valós idejű állapot megfigyelése. Az 5G pedig gyors adatküldést és nagyképesítős kommunikációt tesz lehetővé, amely segíthet az ipari eljarasok optimalizálásában és a működés költségeinek csökkentésében.

9.4 LoRa-WAN és NB-Iot technológiák összevonása.

Az előnyökön belül a LoRa-WAN hosszan tartó átviteli képessége és alacsony könyvelésének előnyeit kihasználhatja az ipari feladatok valós idejű automatizálására és vezérlésével, míg az NB-IoT lehetővé teszi az adatok gyors átvitelét és nagymértékű kommunikációját, ezáltal segítve az ipari műveleteket optimalizálnia és munkaköltségét csökkenteni.

9.5 LoRa-WAN és ZigBee összekapcsolása.

Előnyök: A LoRa-WAN hosszan tartó átviteli képessége és alacsony költségessége ideálissá teszi az energiafogyasztás monitoringjára és optimalizálására. A ZigBee pedig lehetővé teszi az infrastruktúra belső területeinek megfigyelését és vezérlését, miközben az alacsony energiafelhasználás és költségcsökkentés szempontjából is hatékonyan működik. Ezen lehetőségeken keresztül az energiafogyasztás optimalizálható, valamint az üzemeltetéshez kapcsolódó költség csökkentése is megvalósíthatóvá válik.

10 Összegzés

A LoRa-WAN technológia egyre elterjedtebb és sokféle területen hasznosulhat a ipari automatizálásban az okos városokban a precíziós mezőgazdálkodásban és a kritikus infrastruktúrákat monitorozva. Ez a technológia lehetővé teszi az eszközök között való valós idejű kommunikációt és az adatok hatékony átvitelét nagy távolságokon és alacsony energiafogyasztással ami jelentősen növelhet benne az efficienciát és az innovációs lehetőségeket.

Nagyon nagy távolságú közvetítés: A LoRa-WAN technológia lehetővé teszi a nagyon nagy távolságú kommunikációt eszközeink között még a legtávolabbi helyeken is.

Alacsony energiaigényű működtetés: Az eszközeink csak némi évente megtermelt energia felhasználásával üzemelhetnek,, amely jelentősen csökkenti az üzemeltetés költségeit és lehetővé teszi a hosszan tartó kommunikációs megoldások kialakítását.

Alacsonyan tartott költségekkel járó előnyökkel jár a LoRa-WAN infrastruktúra és eszközeinek használata az általánosan olcsóbb Wi-Fi vagy NB-IoT alternatívákhozt képest, ennek révént nagymértékben lehetségesé válik a széles körben bevethető alkalmazások .

Jelentős kapacitású: Egy LoRa-WAN állomásnak képesnek kell lennie arra, hogy egyszerre több ezer eszközt kezeljen, ami lehetővé teszi számos érzékelő és eszközből integrálását egy közös hálóban.

Biztonsági és méretezési kihívások

A LoRa-WAN technológia számos biztonsági és méretbeli kihívást vet fel egyaránt. Ezek között található az adatvédelem kérdése is, valamint az hálózási stabilitás és kommunikációs hatékonyság problémák is. Az adatvédelem szempontjából kulcsfontosságúak az olyan kriptográfia módszerek, hálózati biztonsági mechanizmusok, valamint felhasználó- és eszköz hitelesítés, amelyek védelmet nyújtani. Hálózati stabilitás érdekében fontos az infrastruktúra fejlődése valamint az adatforgalom kezelés és redundancia kiépítése is elengedhetetlen. A kommunikációs hatékonyság növelése érdekében javasolt az adatátviteli sebesség emelése ,az adatforgalom optimalizálása és az adatvesztés csökkentése is.

Az LoRa-WAN technológia állandó fejlődésen megy keresztül és számos újdonság várható ami bővíti alkalmazási területeit és hatékonyságát továbbá az újdonságok között emelhető az integrált technológiák mint például az 5G és az edge computing valamint az adatkezelés és analizálás fejlődése is várhatóak. Az újonnan felmerülő alkalmazások között találhatóak okos egészségügy okos mezőgazdaság és okos ipari megoldások is.

Az alkalmazásoknak lehetősége van arra, hogy teljesítsék az igényeket és előnyökhöz jussanak az egyes technológiák kombinálásával az ipari parkokban és okos városokban is.

Az előzőleg kifejtett szövege szerint a LoRa-WAN technológia hatékony és alkalmazható kommunikációs megoldás az ipari automatizálásban és az okos városokban is megfelelő alkalmazást nyújtva különböző kritikus területeken. Az esetleges továbbfejlődés és kombinációs lehetőségeinek a technológia kihasználhatja az alkalmazási területeket teljesen optimalizálnia ipari működéseket vagy növelni a lehetőségeket innovatív módon.

ACKNOWLEDGMENTS

Szeretnék köszönetet mondani az alábbi szervezeteknek és személyeknek, akik hozzájárultak a jelen tanulmány publikálásához és előkészítéséhez:

LoRa Alliance: Az Alliance hálózati infrastruktúrájának és technológiai forrásainak használatával lehetővé tettem a LoRa-WAN technológia részletes elemzését.

Semtech: A Semtech támogatása és technológiai dokumentációja értékes információkat nyújtott a LoRa technológia működéséről és alkalmazásairól.

The Things Network: The Things Network közössége és erőforrásai értékesek voltak a LoRa-WAN hálózatok tervezéséhez és implementálásához.

Ezen szervezetek és személyek támogatása és erőforrásai jelentősen hozzájárultak a tanulmány elkészítéséhez és publikálásához. Örömmel említem mindenkit, akinek munkája és közreműködése lehetővé tette ezt a tanulmányt.

IRODALOMJEGYZÉK

[1] LoRa Alliance

Webcím: https://lora-alliance.org/about-lorawan/

Leírás: A LoRa Alliance hivatalos weboldala, ahol részletes információkat találhatunk a LoRa-WAN technológia hatótávjáról és alkalmazási lehetőségeiről.

[2] Semtech

Webcím: https://www.semtech.com/products/wireless-rf/lora

Leírás: A Semtech hivatalos weboldala, amely részletesen bemutatja a LoRa technológiát, beleértve az érzékelők és eszközök működését.

[3] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely tájékoztatást nyújt a LoRa-WAN technológia költségeiről és alkalmazási lehetőségeiről.

[4] The Things Network

Webcím https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely részletesen tárgyalja a LoRa-WAN technológia általános adatátviteli sebességét és hatótávját.

[5] The Things Network

Webcím: The Things Network - LoRaWAN Comparison

Leírás: The Things Network weboldala, amely összehasonlítja a LoRa-WAN-t más kommunikációs technológiákkal, mint például a Wi-Fi, ZigBee, Sigfox, NB-IoT és 5G.

[6] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN technológia alkalmazásait okos városokban, beleértve a közlekedési rendszerek figyelését, a városi infrastruktúra monitorozását és a középületi eszközök vezérlését.

[7] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN technológia alkalmazásait precíziós mezőgazdaságban, beleértve a növénytermelés figyelését, állattenyésztés figyelését és mezőgazdasági folyamatok automatizálását.

[8] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN technológia alkalmazásait ipari automatizálásban, beleértve a gépek állapotának figyelését, folyamatok automatizálását és energiagazdálkodást.

[9] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN technológia alkalmazásait kritikus infrastruktúrák monitorozásában, beleértve az energiaáramlási rendszerek figyelését, vízhálózatok monitorozását és környezeti monitorozást.

[10] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN hálózatokban alkalmazott biztonsági mechanizmusokat, beleértve az adatvédelmet, hálózati stabilitást és kommunikációs hatékonyságot.

[11] The Things Network

Webcím: https://www.thethingsnetwork.org/docs/

Leírás: The Things Network weboldala, amely bemutatja a LoRa-WAN technológia jövőbeli fejlesztési lehetőségeit, beleértve az új technológiák integrálását, adatkezelés és analízis fejlesztését és új alkalmazások bevezetését.

[12] What Is LoRa? A Complete Guide! (Border)

weboldal: https://boardor.com/blog/what-is-lora-a-complete-guide

Leírás: Képek az oldalról amelyek illusztrálásokra lettek használva.

[13] LoRaWAN - Most Common Applications and Use Cases

weboldal: https://www.iotforall.com/lorawan-most-common-applications-and-use-cases

Leirás: Az IoT For All cikkében számos gyakori LoRaWAN alkalmazási területet mutatnak be.

[14] Which IoT Technology Is Best for You?

weboldal: https://info.semtech.com/iot-network-comparison-infographic

Leirás:A Semtech oldalán található egy átfogó infografika, amely összehasonlítja a különböző IoT hálózati technológiákat, beleértve a LoRaWAN-t, NB-IoT-t, Zigbee-t, Wi-Fi-t, BLE-t és 5G-t.

2.47. Felhőalapú szolgáltatások hatása a videójáték-iparra

Ipar4.0 Beadandó Házi dolgozat

Felhőalapú szolgáltatások hatása a videójáték-iparra

Hallgató neve: Dobos Bálint ([redacted])1*

Gazdaságinformatikus, dobos.balint@hallgato.sze.hu

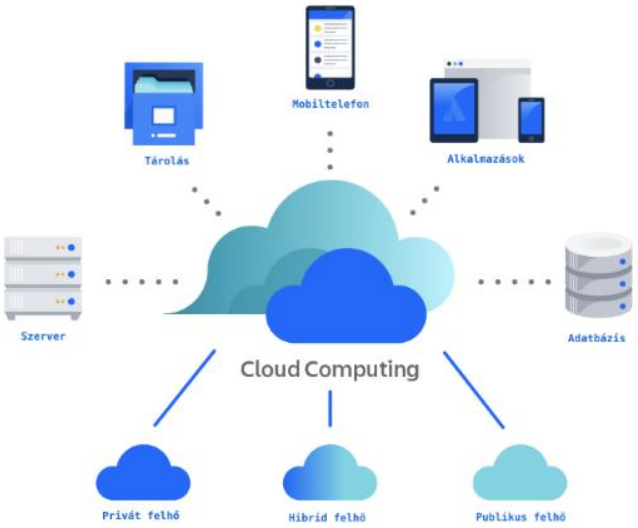
Kulcsszavak: gaming, tartalomgyártó, videójáték, minecraft

1 BEVEZETÉS

Az általam választott beadandó dolgozat témája a felhő alapú szolgáltatások ezen belül ennek története majd elterjedése. Folytatva annak típusaival és elterjedt alkalmazásaival. A továbbiakban pedig a külső hardvert alkalmazó, távoli eszközt használó, szórakoztatás céljából létre-jött, másnéven „cloud gaming" elterjedését fejtem ki. Az utóbbi személyes indíttatást keltett bennem, hogy erről írjak. Többek között azért is mert napi szinten az általános felhőalapú szolgáltatásokon kívül ezen lehetőségekkel is élek. Mindazonáltal ezzel is népszerűsíteni szeretném az alternatív „vas nélküli" lehetőségeket.

1.1 Definíciója

Maga a szószerkezet, mint felhőalapú számítástechnika az angol „cloud computing" szóból ered mely a számítástechnika 2010-es évek egyik fő ágazata. Több különböző típust tudunk meghatározni, amelyeket az 1. kép mutat be, de mindegyikben a közös, hogy nem egy adott helyben lévő hardveren futtatják, hanem egy külsős szolgáltatáson keresztül teszik elérhetővé melyből a felhasználó az üzemeltetési részletekről nincsen informálva. Mai értelmezésben vett cloud és cloud computing az ezredforduló hozta magával. Erre közre játszott, hogy óriási ipari és technológiai fejlődés indult el ebből kifolyólag a fogyasztói igény is megnőtt a számítástechnika felé több szempontból is. E miatt elengedhetetlen volt, hogy a számítástechnika igény szerinti teljesítményt nyújtson. Legyen szó adattárolásról vagy más hálózati szolgáltatásról. Előnyeihez sorolandó a biztonság, a sebesség, a földrajzi kiterjedtség, illetve a költségek optimalizáltsága a kapcsolódó tevékenységhez. [1].

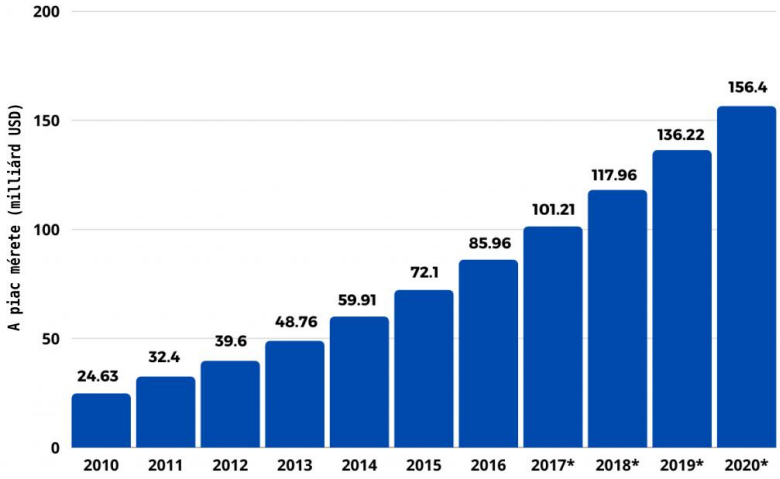


1. Kép: Cloud Computin és területei
https://www.atlassian.com/microservices/cloud-computing

1.2 Története a felhőalapú számítástechnikának

Magát a felhőalapú szolgáltatás eredetét két különböző nézőpontból szokták vizsgálni. Elsősorban az adott kifejezésről szól, mely egy Compaq nevezetű számítógépgyártó vállalatnál fordult elő 1996-ban egy belső dokumentáció során. Az elterjesztésében viszont a mára már rendkívül nagy hírnevet képviselő Amazon.com vette ki a nagyobb részét 2006-ban az Elastic Compute Cloude (EC2) értékesítésével. Maga a szoftver az Amazon Web Services más néven AWS felhő platformjának központi alkotó eleme. Az EC2 lehetővé teszi a felhasználóknak, hogy virtuális gépeket béreljenek maguknak, melyen saját alkalmazásaikat, programjaikat futtathatják. Az EC2 lehetővé teszi alkalmazások skálázható telepítését. [2] A piac méretének növekedése nagy mértékben nőtt és nőni is fog. Ezt a 2. kép reprezentálja.

A másik megközelítés szerint olyan technikai problémák megoldását vesszük figyelembe melyek a felhőalapú szolgáltatásokon alapulnak úgy, hogy korábban ezt a megnevezést még nem használták volna. Ebben az esetben viszont a történet egészen a hatvanas évekig nyúlhat vissza, mikor elsőként fejlesztették le majd teremtették meg az első olyan számítógépes rendszereket mellyel a számítógépes időt egyszerre több gépre, felhasználóra osztották szét. Tökéletes példa erre a telekommunikációs cégek, akik megosztották a dedikált vonalakat több ügyfél között ezzel az árakat csökkentették a minősége nem romlott. [3] [4].



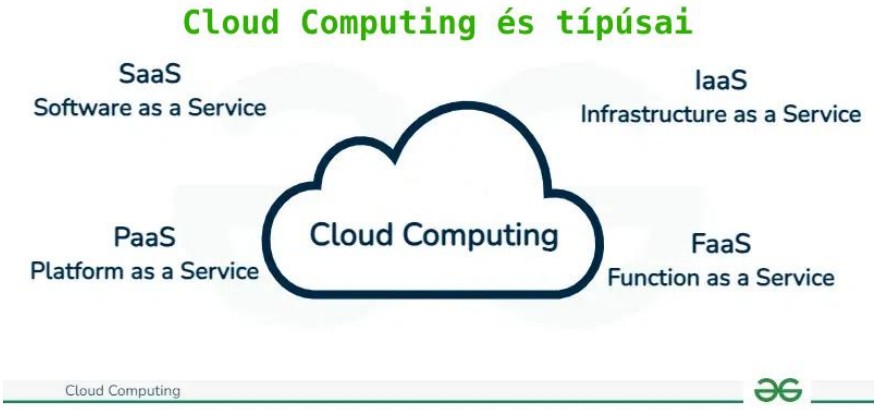
2. Kép: A piac mérete, becslések a jövőt tekintve (2018)
https://www.seasiainfotech.com/blog/history-and-evolution-cloud-computing/

2 HATÁSA AZ IPARI TERMELÉSRE

A cloud gaming működéséhez hatalmas számítási kapacitásra (adatközpontok, szerverparkok, hálózati infrastruktúra) van szükség. Ezeket az infrastruktúrákat ipari léptékben nagy gyártó cégek állítják elő (például szerverek, adatközpont-hűtő rendszerek, optikai kábelek gyártása). Tehát a cloud gaming kereslete közvetlenül hajtja az ipari termelést ezekben a szektorokban. Egyre nagyobb igény volt a szervergyártás mellett hűtési rendszerek és energiahatékony meg-oldások kifejlesztésére. [30] Maga a cloud gaming alacsony késleltetésű hálózatot követel meg, ez az igény gyorsította az 5G bevezetését és az IoT (Internet of Things) alkalmazásait többek között gyártóüzemekben a valós idejű adatfeldolgozással kapcsolatban (pl. prediktív karbantartás). [31] Ezzel párhuzamosan a különböző alkatrészek gyártási folyamatai digitalizálttá és automatikussá váltak. Bár a cloud gaming csökkenti a felhasználók oldalán szükséges csúcshardver igényét (nem kell gamer PC, elég egy okostévé vagy okostelefon), a háttérben megnövekedett szerver- és adatközpont-igény jelentkezik. Ez az ipari elektronikai gyártókat érinti, akik szerveralkatrészeket, hűtőrendszereket, áramellátó rendszereket gyártanak. A cloud gaming brutális energiafogyasztással jár, ami ráirányítja a figyelmet a zöld technológiák és energiahatékony adatközpontok ipari fejlesztésére. A vállalatok olyan innovációkat keresnek, amelyek csökkentik az energiaigényt, ezzel új ipari megoldások iránti keresletet generálva. [32] A cloud gaming globális piac, így az ipari termelés szempontjából is globális ellátási láncokat mozgat meg: Ázsiában gyártott félvezetők, Észak-Amerikában fejlesztett szerverek, Európá-ban üzembe helyezett adatközpontok. A geopolitikai változások (pl. chiphiány, exportkorlátozások) ezért nemcsak a játékosokat, hanem a mögöttes ipari szereplőket is érintik.

3 TÍPÚSAI

Mivel egy területen alkalmazott rendszerről van szó ebből eredően a felhasználói igények sokszor eltérnek. Számos különböző típus, modell és vagy szolgáltatás látott napvilágot. Annak érdekében, hogy a minél optimalizáltabb felhasználó barát megoldásokat tudjon nyújtani. A 3. kép mutatja be a típusokat.



3. Kép: Cloud Computing és típusai
https://www.geeksforgeeks.org/types-of-cloud/

3.1 Szolgáltatott szoftver

Az első típus a szolgáltatott szoftver másnéven Software as a Service (SaaS). Ez egy szoftver-szolgáltatási módszer, ahol központosítottan vannak tárolva az adatok legfőképpen egy internetes felhőben. Ezekhez a felhasználók leggyakrabban valamely klienesen keresztül (általában weblapon) nyerhetnek hozzáférést. A szolgáltatás széles körben elterjedt elsősorban könyvelésnél, számlázásnál vagy csoportos munkaszervezésnél. [5]

Természetesen ennek a rendszernek is vannak előnyei és hátrányai is. Talán egyik legmérv-adóbb hátránya, hogy ugyebár rengeteg webes alkalmazás fut rajta, mint például az e-mailok, számviteli rendszerek és kommunikációs programok. Az ügyfél vagy nem tudja vagy nem is akarja ellenőrizni a hálózat infrastruktúráját legyen szó magáról a hálózatról akár szerverekről, vagy magáról az operációs rendszerről. Ebből adódóan ezen rendszerek képességeivel sincs tisztában. Bár ebben a korlátozott beállítási opciók kivételt képeznek már ahol erre van lehetőség. A bérleti díja álltalában havi vagy éves szintű ezen modelleknek.

Népszerű szolgáltatott szoftverek közé sorolható a Google Apps, a Microsoft Office 365 vagy a Salesforce.

3.2 Platform szolgáltatás

A második típus a Platform as a Service (PaaS) azaz a platform szolgáltatások. Ez a modell a nevéből eredően ad egy platformot és arra vagy egymásra épülő szolgáltatások igényelhetőek a felvevő piac számára. Az alapja ennek a lehetőségnek, hogy az adott ügyfél a szolgáltató által felajánlott eszközök, programok segítségével hozzon létre egy számára megfelelő alkalmazást. És ezt a felhasználó ízlése szerint tudja konfigurálni, optimalizálni, mert teljesen ellenőrzése alatt tudja telepíteni a szoftvert ellenben az előző modellben felsorolt szolgáltatott szoftverrel szemben. A PaaS hatékony körülményeket tud teremteni, ha a prioritásunk az új alkalmazások fejlesztésére szánjuk, de a back-end hátterét és annak működtetését a szolgáltatóra szeretnénk bízni. A platform szolgáltatást két külön csoportba lehet sorolni. [6]

- Nyílt platform szolgáltatás
    - Lényege, hogy nyílt forráskódú szoftverrel dolgozik és ebből adódóan nem csak egy azon szolgáltatóhoz köthető.
- Alkalmazás szolgáltató környezetek

- Ezen rendszerek főként nem a felhasználóbarát megközelítést alkalmazzák, mint például a fejlesztőkörnyezet meglétét vagy hiba lekövetést és annak fejlesztését, hanem a biztonságra és a skálázhatóságra törekednek.

Ismertebb platform szolgáltatások az OpenShift, a Google App Engine, a Cloud Foundry, illetve az Amazon Web Services

3.3 Infrastrukturális szolgáltatás

A harmadik egyben utolsó típus az infrastrukturális szolgáltatás, avagy az Infrastructure as a Service (IaaS). Ez a modell számít a legalacsonyabb szintűnek, mert itt a szolgáltató egy az egyben számítógépet ad a kezünkben, ami lehet fizikai szerver, de legtöbb esetben virtuális számítógépként üzemel. A szolgáltató az egyszerű feladat, igénykör miatt nagy mennyiségű szervert tud a rendelkezésünkre bocsáltani melyhez gyakran plusz dolgokat is kaphatunk legyen szó választható operációs rendszerről vagy blokk alapú tárhelyről de lehet speciális tűzfal vagy IP-cím. Mivel általában ez egy nagyon összetett és dinamikus környezet, nem csak az alkalmazás időtartama vagy a tárhely után kell díjat fizetni, hanem a hálózati átvitel után is, amely akár óra, heti vagy havi díjas is lehet. [7]

Működési elve viszonylag egyszerű a felhasználónak először telepítenie kell egy operációs rendszert majd a hozzájuk használni kívánt alkalmazást. Itt viszont fontos leszögezni, hogy a használónak kell végrehajtania az esedékes frissítéseket, mind az operációs rendszeren, mind az alkalmazáson. Mint mindenhol itt is vannak kritériumok. A szolgáltatásnak a grafikus felület mellett egy programozásra képes felületet kell biztosítani, ami egy egyszerű parancssorral is megoldható.

Elterjedt infrastruktúra szolgáltatás az Amazon EC2 vagy a Google Compute Engine.

4 TELEPÍTÉSI MODELLEK

Többféle telepítési modell közismert melyet négy nagyobb csoportra tudunk osztani.

- Nyilvános/publikus felhő (public cloud)
  - Ez a legismertebb modell. Mindenki számára elérhető nagyrészük fogyasztói szegmensre összpontosít.
  - Ismertebb példák: AWS, Azure, Google Cloud Oracle Alibaba
- Magán felső (private cloud)
  - A magán felhő nevéből eredően egy ügyfél tudja használni. Maga az üzemeltetés lehet közvetlen az ügyfél vállalati környezetében esetleges adatközpontban vagy egy harmadik fél által nyújtott szolgáltatónál. Előnye és egyben célja a használatának az a magas biztosággal való rendelkezés.
  - Ismertebb példák: Virtual Network, Azure ExpressRoute
- Hibrid felső (hybrid cloud)
  - Elenevezése az előbb említett kettő típus kombinációjából ered csakúgy, mint funkciója. E kettő pozitív tulajdonságainak ötvözete. Ezen modellben a vállalatok a bizalmas vagy érzékeny adatokat a privát részben tárolják míg a támogatott szolgáltatásokat a nyilvános szegmensben foglal helyet, Így a cég felügyelete alatt maradnak az adatok anélkül, hogy kényes információk napvilágot látnának.
- Közösségi felhő (community cloud)
  - Ennek létezése a közösségi érdekekből ered, melyben több szervezet egymás között megosztott infrastruktúrája alkotja felhőt.

5 AZ IPARI TERMELÉSRE GYAKOROLT HATÁS

A technológiai fejlődés és a digitalizáció jelentős hatást gyakorolt az ipari termelésre. Az automatizálás és a robottechnológia bevezetése révén nőtt a termelés hatékonysága és pontossága, miközben csökkent az emberi munkaerőigény a monoton, ismétlődő feladatok esetében. Az intelligens gyártási rendszerek (pl. IoT, mesterséges intelligencia, prediktív karbantartás) lehetővé tették az ipari szerep

6 A VIDEÓJÁTÉKOK NÉPSZERŰSÉGE

Ahhoz, hogy megértsük miért van ekkora sikere a felhőn alapuló játékplatformoknak ismernünk a szolgáltatás nélküli játékélményt is. Sokan kérdőre vonják a videójátékokkal kapcsolatos munkákat legyen az influncer/streamer (online közvetítése egy adott videójátéknak) vagy akár egy világméretű szinten ismert e-sportoló. Elvégre egy erős függőséget okozó virtuális többek szájából erősen hangsúlyozott nem valós világban szerzett élményekben részesítenek minket. Főként szüleink és nagyszüleink vonnak minket kérdőre mikor megkérdezik, hogy a vizsgákra való tanulás helyett mégis mit csinálunk. És ekkor a kisebb rossz alaptézisből rávágjuk, hogy egész nap „gépeztünk”. Sajnos rengeteg időt el tudunk egy számunkra fontos fiktív világban tölteni. [8] Ezzel pedig sok ember volt és van így, ennek a népszerűségnek a növekedését a 4. kép mutatja be.

4. Kép: A játékosok számának tendenciája az évek során
https://explodingtopics.com/blog/number-of-gamers

6.1 A videójáték műfaja

Elsőként sokak számára abszurdnak is hangozhat, hogy a videójátékoknak vannak típusai, műfajai, de egy játék nem feltétlenül csak arról szól, hogy ész nélkül csapkodjuk a klaviatúrát és a játékban elszenvedett vereség után kettétörjük. A

városépítő vagy vasútirányító szimulátoroktól indulva a virtuális valóságon át akár egy második világháborús katona bőrébe is bújhatunk de még a Csillagok Háborújában fontos szerepet játszó jedik vagy rohamosztagosok szemszögébe is nyerhetünk betekintést.

6.2 A videójátékok típusai

Alább a legnépszerűbb kategóriákat ismertetem elvégre rendkívül sok műfaji képviselője van.

- Akció
    - Az egyik legnagyobb teret hódító kategória az az akció. A folyamatosan történő cselekmények főként a jó reflexeinkre mennek rá, de célzásunkat is igénybe veszi. Három kategóriára lehet bontani a játéknézet alapján (hogyan látunk rá irányítani kívánt harcosunkra).
    - FPS (First Person Shooter) vagy belső nézetű lövöldözős játék, ami olyan mintha belebújtál volna az általad irányított karakterbe és az ő szemszögéből láthatnánk az eseményeket. Legnépszerűbb FPS játékok: Call of Duty széria, Counter Strike: Global Offensive, Overwatch, Valorant
    - TPS (Thrird Person Shooter) avagy külső szemszögű lövöldözős játék. Nevéből adódóan olyan nézetet nyújt mintha egy harmadik személy rálátásból játszhatunk, aki kvázi mögöttünk van. Ide sorolandó az elmúlt években elterjedt battleroyal játékok is az éhezők viadalához hasonlóan adott számú embert kitesznek egy szigeten és az győz, aki utolsónak marad. Híres TPS játékok közé tartozik a Fortnite, Star Wars Battlefront II, Resident Evil széria, Grand Teft Autos széria (kiemelten az ötödik rész), Dark Souls 3 (soulslike játékok).
    - Oldalnézetes akciójáték, ez a típus a klasszikus kettő dimenziós megjelenési módot alkalmazza, ami annyit tesz, hogy oldalnézetből látjuk a játékot. Ilyenek például a Terraria, Cuphead, Inside, Ori And The Blind Forest, Mark Of The Ninja)
- Ügyességi, ismertebb nevén platformer játékok azon típusú videójátékok, ahol hősünkkel különböző akadályokon kell átjutnunk, (amik sok esetben egy ellenfél) platformok közti ugrálással és vagy speciális képességek alkalmazásával kell teljesíteni egy pályát. Emellett a pályán többféle érmét vagy tárgyat kell összegyűjteni egy nagyobb kincs vagy új fegyver megszerzése érdekében. Legelterjedtebb platformer játékok közé sorolandó A Super Mario széria, It Takes Two, Sonic széria, Ratchet & Clank: Rift Apart.
- Kaland játékok nevükből kiindulva egy történet orientált típusú. Az ilyen műfajú játékok egy személyre készültek és egy interaktív történetbéli felfedezésre invitálják a felhasználót. Kiemelkedő kaland játékok a Batman: Arkham széria, a Fallout széria és a Far Cry széria.
- Szerepjátékok azon játék típusok mikor egy adott szerepet öltünk magunkra, legyen az egy varácsló vagy egy felderítő, két fajtája van:
    - RPG (Role-Playing Game) műfaj leginkább a főleg külföldön elterjedt Dungeon and Dragons virtuális megfelelőjét adja. Adott egy történet melyben te vagy a főszereplőt és különböző döntéseket kell meghozni melyek hatással vannak az egész játékmenetre beleértve a végkimenetelre. Általában egyszemélyes játékok, mint például a remek könyvadaptáción alapult Witcher játékok, de e mellett akadnak többszemélyesek is, mint például a Diablo III
    - MMRPG (Massively Multiplayer Online Role-Playing Game) avagy a rendkívül sok szereplős online szerepjáték. Ha van olyan kategória melyre a legkönnyebben függőséget okoz, na ez az. Az alapkoncepció, hogy egy fiktív világban egy általad irányított karakterrel kell fejlődni mely a legmagasabb szintre

lépés után is rengetek tennivalót kínál fel. Legjobb példa erre a 2004-ben létrejött és a mai napig versenytárs nélküli World of Warcraft ahol Azeroth világában 10+ különböző fajból választhatsz azon belül is két különböző frakció van. A szintezés mellett folyamatosan fejleszteni kell a kazamatákban szerzett kosztümjeinket. A játék lehetőséget ad foglalkozások fejlesztésére minek termékét a helyi aukciós házban el tudjuk adni, továbbá ritka kedvencek vagy hátasok megszerzése is lehet célunk. Főleg ha annak az esélye, hogy megszerezzük akár 0,06% is lehet.

- Stratégiai játékok talán a legtöbb fejtörést okozó csoport elvégre a játékmenet folyamatos vagy körökre osztott és az opciók száma közel végtelen. A játékos bármikor adhat ki parancsokat, amelyek végrehajtása azonnal el is kezdődik. Egyik legkomplexebb ilyen játék a Civilization VI.

6.3 Videójátékok előnyei és pozitív hatási

Mint mindennek így a videójátékoknak is vannak előnyei és hátrányai is egyaránt. Előnyökkel kezdve több tanulmány is bizonyította, hogy a napi szintű játszás javíthatja a vizuális figyelmünket e mellett hatékonyabbá válhatunk a feladatok megváltoztatásában, gyorsabbak lehetnek olyan feladatokban, amelyekben vizuális keresést vagy objektumot kell megkülönböztetni legyen az alak vagy szín. Másfelől a videójátékok növelheti a pozitív értékeket, mivel rengetek olyan küldetés vagy játékon felüli kitüntetés van, ami a szolidaritásra a csapathoz tartozáshoz ad pozitív visszajelzést. Továbbá fejleszti az empátiát a szociális érzékenységet, növeli a kompetencia és önbecsülés érzését. Nem mellesleg fokozottan felhívja a csapatmunkában való részvételt, ami rendkívül hasznos tud lenni a munka világában főként, ha projekt orientált vállalatnál szeretnénk a későbbiekben dolgozni. De talán, ami a legfontosabb, hogy kikapcsolódást nyújt a hét fáradalmai után ezzel könnyed stresszlevezetésként is tökéletesen funkciónál.

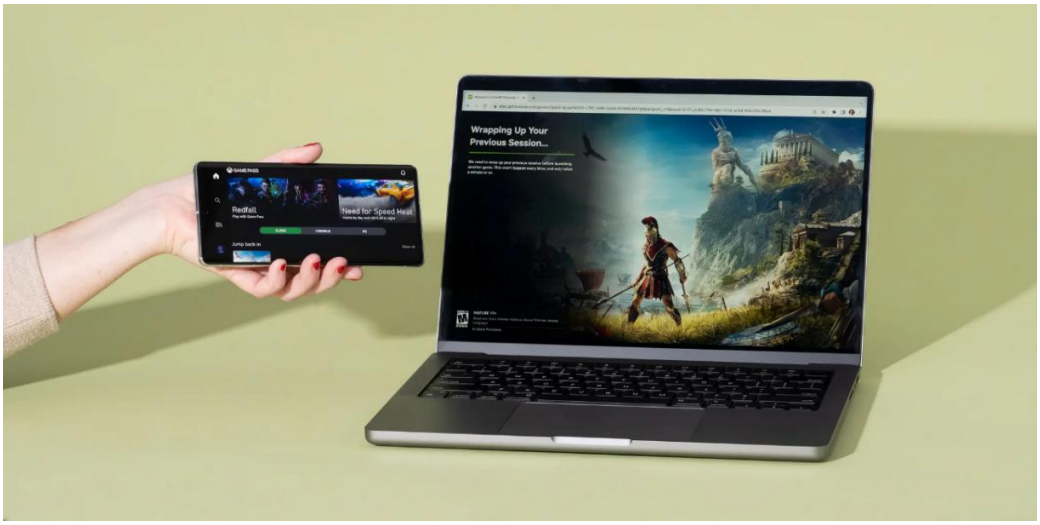
6.4 Videójátékok káros hatásai

Legelsőként, mint talán a legegyértelműbb az a maga a számítógép előtt való ülés. Ha még nem csinálunk semmit csak nézzük a monitort hosszas órákon keresztül szemünk jelentősen tud romlani főleg, ha a késő esti órákban még mindig az adott eszközt keressük kedvenc hősünkkel. De a hanyag testtártást is fokozza a monitor előtti görnyedés. Mindazonáltal mint minden a videójáték is lehet egy erős addikció. Sajnos a mai világban az internet elől közel lehetetlen elmenekülni főleg a mai generációs fiataloknak, akik abban élik konkrétan az életüket. És ha az életben nincs vagy kevés sikerélménye van az adott személynek sokkal szívesebben bújik, menekül el egy olyan világban, ahol ezen élményeket sokkal több aspektusból tudja befolyásolni. Ezért tud veszélyes lenni, mert lehetőséget kínál egy teljesen másik „valóságba", amiben általában sokkal jobban tudja élni az életét. E mellett, mint figyelem elterelő eszköz is válthat ki negatív hatásokat. Saját tapasztalatomból kiindulva az ember rengeteg olyan nehéz, rendkívül nem optimális szituációval találkozik az életben amire közel nulla ráhatása van és ezeket a problémákat nem tudja egyedül megoldani. Ahelyett, hogy segítséget kérne inkább tolja maga előtt, mint az egyetemisták a beadandókat. Nem a megoldást keresi, hanem a gondolattól való megszabadulást és ilyenkor találkozik olyan játékokkal, amik mentálisan annyira le tudják fárasztani az adott személyt, hogy nem lesz se energiája se affinitása a probléma megoldásához. A túlzott, több mint napi tíz óra játék után pedig ez válik a személy életévé és a virtuális életét helyezi prioritásba a valós helyett, melyből nem akar kiszabadulni. Ebből adódóan a szociális élete az illetőnek szépen lassan kezd megszűnni és az érdeklődési körének a spektruma is egyre szűkebbé válik. Na de mi van akkor, ha külső hatások miatt a függőséget nem tudja kielégíteni? Ekkor jön a sokak szerint minden játékosnál megtalálható agresszió mondhatni elvonási tünetek. Fontos leszögezni, hogy ezt nem csak függőség okozhatja, hanem a játékban több ideig tartó eredménytelenség is előhozhatja. Egy másik oldalról megfogva a negatív hatást, sok torzítás van a videójátékokban legyen emberi megjelenítés vagy valóságkép. Kicsit úgy tudnám hasonlítani, mint amikor valaki feltesz egy

képet valamely közösségi médiás platformra és a valóságot nem azt, hogy tükrözi, de még meg sem közelíti. Egy szó, mint száz reálisan kell hozzáállni a videójátékokhoz és mértékkel kell ezen dopamin szerzési letőséggel bánni.

7 FELHŐN ALAPULÓ JÁTÉKPLATFORMOK

A Gaming as a Service (GaaS) másnéven felhőalapú szolgáltatáson megvalósított szórakoztatóipari lehetőség. A 21. század egyik legnagyobb teret nyerő felhőalapú szolgáltatása. A felhőalapú játékplatformok hasonló módon működnek, mint a távoli asztali számítógépek és az igény szerinti videószolgáltatások mint például a Netfix, HBO GO, vagy a nemrégiben indult Disney +. A használni kívánt játékokat a szolgáltató a saját dedikált hardverén tárolja és távolról futtatja, mindazonáltal kliensszoftveren keresztül videóként közvetítik a játékos eszközére. A kliens szoftver kezeli a játékos inputjait, amelyeket visszaküldenek a szerverre, és a játékon belül végrehajtják. Egyes felhőalapú játékszolgáltatás legtöbbször virtualizált Windows-környezethez való hozzáférésen alapulnak, ezzel lehetőséget adva a felhasználók számára adott játékok letöltését és telepítését, ugyanúgy mintha otthon a saját vasunkra tennénk fel rég elfeledett alkalmazásunk. [9] Erre egy példát láthatunk az 5. képen.



5. Kép: GaaS illusztráció
https://www.nytimes.com/wirecutter/reviews/best-cloud-gaming-services/

7.1 Története, korai próbálkozások

A felhőalapú játéktechnológia első bemutatott megközelítése a G-Cluster (Game Cluster) volt, amely a 2000-es E3-on (sok éven keresztül megrendezett de sajnos a kovidnak köszönhetően mára már elhanyagolt éves szinten tartott világ méretű játékbemutatásra alkalmazott konferencia) mutatta be termékét és 2003 körül jelent meg. A kezdeti modelljükben 2005 körül a G-Cluster olyan PC-játékokat biztosított, melyeket saját szervereiken futtatták, video-on-demand szolgáltatók és köztesszoftver-szoftver-szolgáltatók támogatásával segítették szolgáltatásaikat a hálózatüzemeltetőknek, majd portálokon keresztül kínálták a játékokat a végfelhasználóknak. 2010-re a piac változásai miatt a G-Cluster modelljét úgy változtatta meg, hogy egy nagy szervergyártón keresztül biztosítsa játékait a hálózat üzemeltetőinek és közvetlenül a felhasználóknak. Ezt az újrafókuszálást a számítógépek számára elérhető, ingyenesen játszható játékok megnövekedett elérhetősége tette szükségessé, ami elvonta őket a G-Cluster szolgáltatásától, így a G-Cluster inkább az Internet Protocol televíziós (IPTV)

felhasználókra koncentrált, amiben megvolt a potenciál. 2010-ben mintegy hárommillió felhasználót vont maga köré A francia SFR távközlési szolgáltató 2010-ben indította el a G-Cluster játékszolgáltatást végfelhasználói számára, az Orange pedig 2012-ben követte a példát, és a játékszolgáltatást kínálta ügyfelei számára. Mindkét szolgáltatás kereskedelmi forgalomban azóta is működik, és felhőalapú játékot kínál ügyfelei számára tévén és mobilon.

7.2 Jelenlegi helyzet

Az első bejelentést a mai nap már közismert videókártya fejlesztő cég az Nvidia tette meg 2012 májusában, ami az Nvidea Grid (mai nevén GForce Now) névre hallgatott. A grafikus feldolgozóegységeket és szoftvereket használó hardverek kombinációjaként kezdetben a Gaikai-val szándékozott partnerre lépni a szolgáltatáshoz kapcsolódó játékok terén. Az Nvidia Gridje mellett az Ubitus GameCloud is bemutatkozott. A GameCloud-ot az Nvidia Gridjén alapuló „white-label" szolgáltatásnak tervezték, amelyet más szolgáltatók is használhattak arra, hogy játékstreamelést kínáljanak ügyfeleiknek. Ezzel is népszerűsíteni akarták az új innovációjuk elterjedését. A Grid hivatalosan az Nvidia Shield együtt látott napvilágot, ami az androidos televíziók részeként került bemutatásra a 2013-as Nemzetközi Szórakoztatóelektronikai Konferencia (Internacional Consumer Electronics Show/CES) során. A Grid/GeForce Now számos felhőalapú játékszolgáltatási partnerrel indult, köztük az Agawi, a Cloudunion, a Cyber Cloud, a G-Cluster, a Playcast és az Ubitus. A szolgáltatást először külföldön, Észak-Amerikában indították el 2014 novemberében, ahol korlátozott számú felhozatallal tettek elérhetővé, majd 2017-ben számítógépekre is kiterjesztették, beleértve a felhasználó Steam és Epic Games Store könyvtárának importálását is. Utóbbi két vállalatról láthatunk egy illusztrációt a 6. képen. Valószínű ez volt az egyik legnagyobb lépés, ami megsokszorozta a felhasználók számát elvégre csak a Steamen több mint 9.000 játék van, noha nem az összes játszható a felhőszolgáltatón, de százalékos arányban a mai napig viszi a prímet. Ezt az importáló modellt kritizálták a kiadók, köztük az Activision Blizzard (ha minden jól megy következő év nyarára a Microsoft teljesen felvásárolja) és a Bethesda Softworks, mivel a vásárlások csak személyi számítógépekre vonatkoztak, nem felhőalapú szolgáltatókon keresztül. Ebből adódóan a kiadók arra kényszerítették az Nvidiát, hogy vonja ki ezeket a címeket a szolgáltatásukból. Érdekesség, hogy a 2014-ben a Dragon Quest X-et a Nintendo 3DS-re hozták Japánban Ubitus streaming technológiával. A következő nagy lépés 2017-ben a francia Blade elindította el a Shadow néven ismert szolgáltatással, ahol a felhasználók egy távoli Windows 10-es példányt bérelhetnek egy adatközpontban, hozzáférve az akkori legerősebb Intel Xeon névén futó processzorhoz és az Nvidia Quadro grafikához. A szolgáltatás földrajzi elhelyezkedéshez kötött, így az egyik adatközponthoz való távolság alapján működött; kezdetben Franciaországban indult,[4] de 2019-re az Egyesült Államokban is megindult a terjeszkedés. Ezt követően több nagy név is elkezdett terjeszkedni a cloud gaming irányába.

6. Kép: Epic Games és Steam a két legnagyobb felhőszolgűltató
https://www.reddit.com/r/MortalKombat/comments/17enfqz/is_crossplay_between_steam_and_epic_games/

Többek között az Electronic Arts nevezetű cég, aki a Need For Speed franchiseról és a mikrotranzakciós botrányairól híres, elkezdett felvásárolni felhőalapú játékeszközöket és a témában elismert dolgozókat a GameFly-tól egy hivatalosan nem publikált összegért 2018 májusában Az EA ezt követően bejelentette a „Project Atlas” néven indított munkaprogramot, amely a mesterséges intelligencia, illetve a gépi tanulás körét boncolgatta a Frostbite technológiájának integrációjával. Ennek köszönhetően jött létre az, hogy egy „egységes” platformot hozzon létre. Mely a többjátékos magas felbontású távoli elérésű letőséget hozta magával. Ahol a prioritás a minimális késleltetési időre és az úgynevezett „crossplay” -re (több különböző platformon játszó felhasználók egyidejű játékára) irányult. A hírek hallatán a Google és a Microsoft sem akart kimaradni. Ezért egy hónapra rá ők is elkezdték saját projektjüket „Project Stream” néven. A következő évben a 2019-es Game Developers Conference rendezvényen a Google hivatalosan is bejelentette felhőalapú játékszolgáltatását, a Stadia-t, amely hivatalosan az év november 19-én indult. Májusban a Sony is bejelentette, hogy partnerséget kötött a Microsofttal, hogy felhőn alapuló közös megoldásokat dolgozzanak ki a részlegek között, beleértve a játékokat is. Innentől a többi már csak történelem. Az nem régiben megjelent Xbox Series S/X és a PlayStation 5 fizikai meghajtók nélkül is megjelentek és gyakorlatilag csak felhő alapon elérhetőek melyeknek a csak a tárhely adhat korlátozásokat. Mindezek mellett meg elindultak nem csak az imént említett eszközökre, hanem a videójátékok nagyon nagy részére az adott „game pass” - ok. Ami egy sima előfizetésben merül ki havidíjas vagy éves kiszerelésekben, természetesen az utóbbinál kedvezményt is kap a vásárló. Az előfizetés havi szinten valamilyen plusz dologhoz juttatja a játékost különböző játékokban a mellett, hogy ingyenesen megszerezhető címeket nyújt feléje. Amikkel tud játszani amíg tart az előfizetése. És ezt a modellt szinte az összes nagyobb videójáték fejlesztő vállalat átvette még az ingyenesen játszható játékok körében is (Free To Play/F2P). Sajnos ez a lépés a legtöbb általunk oly kedvelt játékra negatív hatással volt, mert a bónuszok olyan előnyökhöz juttatták az előfizetéses felhasználókat, amit F2P-ben játszó felhasználóknak lényegesen több időbe telik elérni, ha egyáltalán el lehet. Ebből adódóan egy új „kategória” született, ami hallatán a legtöbb ember inkább el sem kezdi az adott alkalmazást, ami nem más, mint a Pay To Win magyarul, ha fizetsz nyersz.
Napjainkban a legelterjedtebb felhőalapó játékszolgáltatók közé tartozik az Xbox Cloud Gaming, a Stadia, a GForce Nowy illetve a PlayStation Now.

7.3 Infrastruktúrája

A felhőalapú játékokhoz elengedhetetlen a megfelelő infrastruktúra ahhoz, hogy a szolgáltatások rendeltetésszerűen működjenek, ideértve a játékok futtatásához szükséges adatközpontokat és szerverfarmokat. Valamint az alacsony késleltetésű, nagy sávszélességű igénylő internetkapcsolatok elengedhetetlenek, hogy az élő közvetítéseken keresztül a felhasználókhoz eljussanak. A felhőalapú játékok megvalósíthatóságához szükséges hálózati infrastruktúra évekig nem volt elérhető. Ennek oka lehet a földrajzi elhelyezkedés vagy egyszerűen nem volt elérhető a fogyasztói piacok számára. A jó minőségű streaming videóktól való függőségük miatt a szolgáltatás rendszeres használatának lehetőségét egyes internetszolgáltatók által bevezetett adatkorlátok is korlátozhatják.

7.4 Fő szempontok

A felhőalapú játékszolgáltatás minőségének egyik fő tényezője a késleltetés, mivel a felhasználó bemenetei és azok érvénybe lépése közötti késés befolyásolhatja a játékmenetet. Főleg, ha az adott felhasználó a fentiekben említett FPS műfajú játékokkal szeretne játszani, mert itt a precíz bemenetektől függő, gyors tempójú játékoknál egy pillanat késés is jelentős befolyással van a játékmenetre. A késleltetés csökkentésére tett kísérletek közé tartozik a gyorsítótár használata, mivel a gyorsítótárazott adatok helyben tárolható és szükség esetén visszakereshetők. A szolgáltató dedikált hardvere időközönként frissíthető azzal a céllal, hogy optimalizálja a nagyobb felbontást és képkockasebességet (Frame Per Second/FPS) a renderelés és az adatfolyamok szempontjából. Az élmény minőségét, amely a felhasználó általános elégedettségi szintjét méri, szintén figyelembe kell venni.

7.5 Előnyei a felhőalapú játékszolgáltatóknak

A cloud gaming előnyei közé sorolandó, hogy nem kell a hiperinfláció és gazdasági válság közben költenünk többszázezer forintot egy saját számítógépre vagy új generációs konzolra. E mellett a tárhely miatt sem kell aggódni elvégre virtuális felhőbe történik a munkamenet mentése, továbbá a telepítés idején is tudunk spórolni. A cloud gaming számos számítástechnikai platformon is elérhetők, idesorolva a mobileszközöket, például okostelefonokat és táblagépeket, digitális médialejátszókat, mindazonáltal természetesen a kézi konzolok (Nintendo Switch), illetve az óriási teret hódító „next generation” konzolokat beleértve (Xbox Series X, PlayStation 5).

7.6 Kompromisszumok

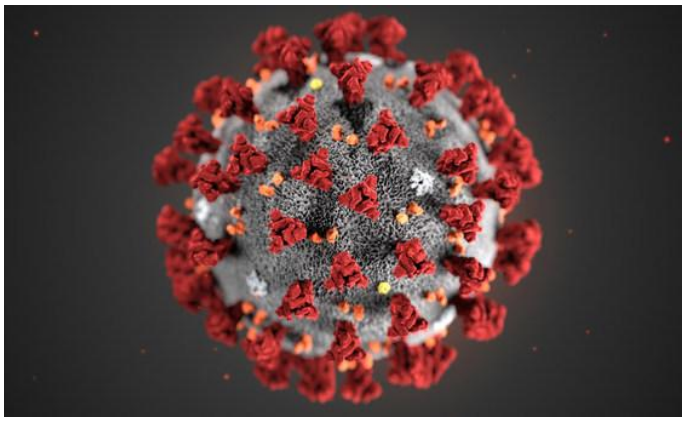
A felhőalapú játékokhoz azonban megbízható, de e mellett nagy sebességű internetkapcsolatra van szükség. Ez korlátozhatja a felhasználókat azokon a területeken, ahol nincsenek ilyen lehetőségek ezzel főként a nagyvárosokon kívül falukra vagy községekre gondolva, vagy ahol az adatkorlátok korlátozhatják a használatot. A forgalmi torlódások és a hálózati késleltetést befolyásoló egyéb problémák még tökéletes internkapcsolatok esetén is lehetnek ráhatással a szolgáltatás teljesítményére. Ezenkívül a felhőalapú játékok költségei a hagyományos terjesztésről a kiskereskedelmi egységeken és a digitális kirakatokon keresztül a felhőalapú játékszolgáltatásokat üzemeltető adatszerverek felé tolódnak el. Ezeknek a működtetési költségeknek a fedezésére a hagyományos disztribúcióhoz képest újszerű költségstruktúrákra van szükség. Ez általában egy alap előfizetési modell volt, de a szolgáltatás tartalmazta a felhőszolgáltatáson futtatható játékok vásárlásának költségeit is, még akkor is, ha a felhasználó nem birtokolja a játékot ugyanúgy, mint a kiskereskedelmi vagy digitális terjesztésnél.

8 A FELHŐALAPÚ SZOLGÁLTATÁSOK ELTERJEDÉSÉNEK FŐBB OKAI

A felhőalapú szolgáltatások elsősorban az említett technikai fejlődésnek köszönhető. De rengeteg külső tényező hatása is nyomott hagyott rajtuk. Ezen kiváltó okokat kategorizálom két fő pontba.

8.1 COVID-19

Ahogy a fentiekben említettem nem véletlenül 2019-re datálják a cloud gaming elterjedését, ugyanis ekkor ért be mind az országunkba, mind a világ összes pontjába a koronavírus. És a veszélyhelyzetre való tekintettel az általános kormányrendeleti intézkedéseken kívül a munkalehetőséget kínáló cégek átálltak egy online munkavégzésre, amit a mára elterjedt „home offce" kifejezés képvisel. Ugyebár ahhoz, hogy ezen munkatípus kördülékenyen menjen elengedhetetlen a felhőszolgáltatások alkalmazása. Kezdve egy közös Google Drivetól egészen egy távoli kapcsolatot létesítő rendszerrel, mint például a FortiClient. De nem csaka munka világát érintette a vírus, amiről egy illusztrációt láthatunk a 7. képen, hanem az oktatást is iskolákban, egyetemeken is át kellett állni az online oktatásra. Elengedhetetlenné vált a személyenkénti laptop vagy asztali számítógép. Annak érdekében, hogy be tudjanak csatlakozni a diákok az órákra a szülők pedig a megbeszélésekre.



7. Kép: Covid-19 vírus illusztráció
https://www.un.org/en/coronavirus

8.2 Mikrochip hiány

Másik fő ok az a mikrochip hiány. A koronavírus következménye, mert mindenkinek kellett egy eszköz, amin tudja a feladatát végezni. A hirtelen nagy igény miatt az áruházak, webshopok tartalékjaikat elkezdték felélni. Amit a kriptovaluták elterjedése csak hatványozott. Amíg a közel 3 millió Ft-os árfolyam volt nem volt probléma, de ez a szám 2021 márciusára csúcsosodott ki közel 18 millió Ft-ra. Nagyjából a kilencszeresére növekedett és már az is elkezdett vele foglalkozni, aki azt se tudta, hogy eszik vagy isszák. A Bitcoin bányászat alapjául a „vas" videókártyája szolgál, amely árak exponenciálisan megemelkedtek. Saját tapasztalatomból kiindulva egy hároméves használt kártyát az óriási infláció elején még el lehetett adni közel annyiért amennyiért újonnan lehetett venni és ez az ár a kicsúcsosodás idejére akár másfélszeresére ugrott. Ezt az abszurd helyzetet fokozta az is, hogy a Microsoft és a Sony bemutatta az új generációs konzoljaikat melyek szintén azokat a pár nanométeres chippeket használják. Ennek hatására óriási előrendelések jöttek már egy évre előre a Xbox Series X-re és a PlayStation 5-re, amiket a mai napig lényegesen nehezebb beszerezni. Az imént említett inflációs hatásoknak köszönhetően nem csak a PC-k és alkatrészeik drágultak meg hanem laptopok is főleg a „gamer" laptopok. Mivel

a fizetésekben nem látszik az inflációre reflektáló emelkedés ezért ezen cikkek beruházását vagy nélkülöznünk kell, vagy várni vele. Sokan köztük én is akadtunk rá a felhőn alapuló játékszolgáltatásokra mely a nehéz időben tudja kielégíteni a piaci igényt.

9 PIACI SZEREPLŐK ÉS VERSENYHELYZET

A felhőalapú játékszolgáltatások piaca az utóbbi években dinamikusan fejlődött, és számos nagy technológiai vállalat igyekszik meghatározó szereplőként megvetni a lábát ezen a területen. A legismertebb szereplők közé tartozik az NVIDIA GeForce NOW, amely lehetővé teszi a felhasználók számára, hogy saját játékgyűjteményüket streameljék egy felhőalapú környezetben. Az Xbox Cloud Gaming (korábban xCloud) a Microsoft Game Pass szolgáltatásába integrálva kínál több száz játékhoz való azonnali hozzáférést különböző eszközökön. A Sony PlayStation Now szolgáltatása már korábban megjelent a piacon, míg az Amazon Luna és a már leállított Google Stadia úttörőként próbálkozott új üzleti modellekkel, változó sikerrel.

A piaci verseny egyre kiélezettebbé válik, mivel a szolgáltatók nemcsak technológiai szinten – például késleltetéscsökkentés vagy grafikai teljesítmény – próbálnak versenyezni, hanem az árazás, a játékpaletta, valamint az eszközök közötti átjárhatóság tekintetében is. Emellett a regionális lefedettség és az infrastruktúra fejlettsége is fontos tényező a szolgáltatások elérhetőségében. Mivel a felhasználói élmény nagymértékben függ a hálózati kapcsolatok minőségétől, a verseny nemcsak a vállalatok között, hanem az internet- és infrastruktúra-fejlesztők között is zajlik. A piac jövője valószínűleg a technológiai integráció (pl. mesterséges intelligencia, 5G, edge computing) és a szolgáltatások diverzifikációja mentén fog formálódni.

9.1 Nagyobb szolgáltatók bemutatása

9.1.19.1.1. NVIDIA GeForce NOW

Az NVIDIA GeForce NOW egy felhőalapú játékszolgáltatás, amely lehetővé teszi a felhasználók számára, hogy saját, már meglévő játékaikat – például Steam, Epic Games vagy Ubisoft Connect fiókokon keresztül – streameljék bármilyen eszközre, legyen az PC, Mac, okostévé vagy mobiltelefon. A szolgáltatás nem tartalmaz önálló játékkatalógust, hanem a meglévő könyvtárakat használja, így a felhasználók nem kell, hogy újra megvásárolják a játékaikat. A platform nagy előnye a magas színvonalú grafikai teljesítmény, akár RTX technológiával (valós idejű ray tracing), valamint az alacsony késleltetésű játékélmény. [10] Az NVIDIA GeForce NOW színvilágát és logóját mutatja be a 8. kép.

8. Kép: NVIDIA GeForce NOW illusztráció
https://blogs.nvidia.com/blog/geforce-now-pc-gaming-everywhere/

9.1.2Xbox Cloud Gaming (xCloud)

A Microsoft Xbox Cloud Gaming – gyakran „xCloud”-ként emlegetett – szolgáltatása a Game Pass Ultimate előfizetés részeként érhető el, és lehetőséget nyújt arra, hogy a felhasználók több száz játékot streameljenek különféle eszközökön, beleértve a mobilokat, tableteket, PC-ket és Xbox konzolokat. A szolgáltatás különösen erős az Xbox ökoszisztéma integrációjában: a játékmentések, achievementek és játékosprofilok automatikusan szinkronizálódnak. A Microsoft masszív felhőinfrastruktúrája (Azure) támogatja a platform működését, amely lehetővé teszi a globális elérhetőséget és megbízható teljesítményt. [11] A Microsoft Xbox Cloud Gaming tehát több játékot foglal magában, ezt hivatott a 9. kép mutatni.

9. Kép: Xbox Cloud Gaming (xCloud) illusztráció
https://bytech.hu/xbox-cloud-gaming/

9.1.3PlayStation Now (ill. PlayStation Plus Premium)

A Sony PlayStation Now szolgáltatása volt az egyik első jelentős szereplő a felhőalapú játékszolgáltatások piacán, 2014-ben indult. 2022-től a szolgáltatás integrálódott a PlayStation Plus Premium csomagba. A felhasználók több száz klasszikus és újabb PlayStation-játékhoz férhetnek hozzá streamelhető vagy letölthető formában. A platform különösen vonzó lehet azoknak, akik régebbi PlayStation generációk (PS2, PS3) játékaival szeretnének játszani újabb hardvereken. [12] Ennek a két szolgáltatásnak a dizájnját és logóját láthatjuk a 10. képen.

10. Kép: PlayStation Now és PlayStation Plus illusztráció
https://gamerant.com/playstation-now-ps-plus-subscription-transfer/

9.1.4 Amazon Luna

Az Amazon Luna az Amazon által fejlesztett felhőalapú játékszolgáltatás, amely 2020-ban indult el először az Egyesült Államokban. A Luna előfizetés-alapú modellt használ, ahol a felhasználók különböző "csatornákra" fizethetnek elő – például Luna+, Ubisoft+, Retro Channel –, ezek különféle játékokat kínálnak, folyamatosan bővülő kínálattal. A platform támogatja a PC-ket, Mac-eket, Fire TV-t, mobiltelefonokat, valamint webes böngészőket is. Az Amazon a saját infrastrukturális hátterét (AWS) használja a játékstreameléshez, ami alacsony késleltetést és stabil teljesítményt ígér. A szolgáltatás egyik különlegessége a Twitch integráció, amely lehetővé teszi a játékosoknak, hogy közvetlenül kapcsolódjanak streamjeikhez. [13] A Twitch integráció ihlette az Amazon Luna dizájnját is színvilágot tekintve, ezt a 11. képen láthatjuk.

11. Kép: Amazon Luna illusztráció
https://www.aboutamazon.com/news/entertainment/what-is-amazon-luna

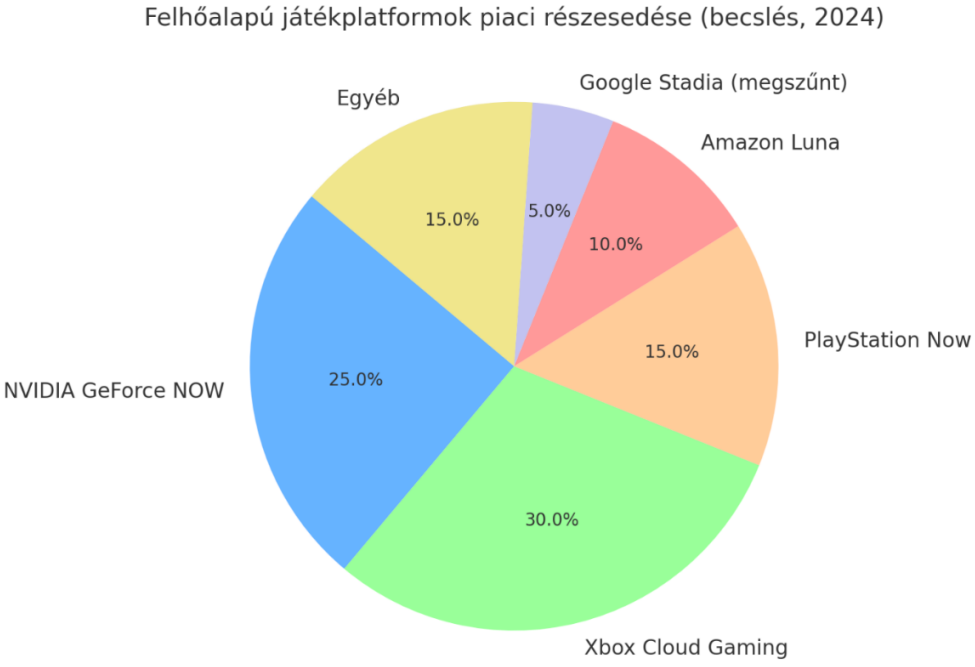
9.1.5 Google Stadia

A Google Stadia 2019-ben indult, és az egyik legismertebb – ám végül sikertelen – kísérlet volt a felhőalapú játékstreamelés piacán. A Stadia célja az volt, hogy bármilyen eszközön – böngészőben, mobilon, okostévén – konzolszintű játékélményt nyújtson letöltés és fizikai hardver nélkül. A szolgáltatás egyaránt kínált vásárolható játékokat és előfizetéses modellt (Stadia Pro). Bár technológiailag ígéretes volt (4K, HDR, alacsony késleltetés), a korlátozott játékkínálat, az üzleti modell hiányosságai és a piaci verseny miatt a Stadia 2023-ban hivatalosan megszűnt. Az eset tanulságos példaként szolgál arra, hogy a technológiai háttér önmagában nem garantál piaci sikert. [14] Külső megjelenése, marketing anyagai hasonlítanak a jellegzetes fehér Xbox One S reklám anyagaihoz. Ez is hordozhatott egy negatív megítélést magával, ami miatt sikertelen projekt lett a Google Stadia. Ezt a marketing anyagot a 12. kép mutatja be.

12. Kép: Google Stadia illusztráció
https://www.gamer365.hu/news/078d0690-36fc-11eb-9f4d-b79ef2e5a27b

9.2 Piaci részesedések, trendek és jövőbeni kilátások (statistikák, grafikonok, diagramok)

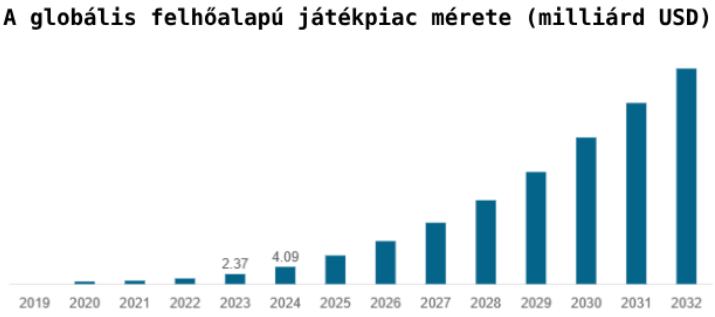
A felhőalapú játékpiac az elmúlt években jelentős növekedést mutatott, és a jövőbeni kilátások is ígéretesek. Az alábbiakban bemutatjuk a piaci részesedéseket, a jelenlegi trendeket és a várható fejlődési irányokat. A következő ábra mutatja be a piaci részesedést a már korábban említett szolgáltatásokat is tekintve.



13. Kép: A piaci részesedés aránya az említett szolgáltatások kontextusában

9.2.1Piaci részesedések és növekedés

A Frost & Sullivan 2022-es elemzése szerint a globális felhőalapú játékpiac B2C szegmense 2021-ben 1,6 milliárd USD bevételt termelt, és várhatóan 2025-re eléri a 13,05 milliárd USD-t, ami 69%-os éves növekedési ütemet jelent. Ugyanezen időszak alatt a felhasználók száma 60,6 millióról 349,4 millióra emelkedhet.
A Fortune Business Insights 2025 márciusi jelentése szerint a globális felhőalapú játékpiac mérete 2024-ben 9,71 milliárd USD volt, és előrejelzéseik alapján 2025-ben 15,74 milliárd USD-ra nő, majd 2032-re eléri a 121,77 milliárd USD-t, ami 33,9%-os éves növekedési ütemet jelent. [15] [16] Ezt a becslést mutatja a 14. kép.



14. Kép: A globális felhőalapú játékpiacának becslése
https://www.fortunebusinessinsights.com/cloud-gaming-market-102495

9.2.2Jelenlegi trendek

5G technológia hatása: Az 5G hálózatok elterjedése csökkenti a késleltetést és növeli az adatátviteli sebességet, ami javítja a felhőalapú játékok teljesítményét és élményét. Ez különösen fontos a mobil játékok terén, ahol a felhasználók egyre inkább elvárják a konzol minőségű élményt hordozható eszközökön is.
Mobil játékok térnyerése: A mobil játékok piaca jelentős növekedést mutat, 2023-ban több mint 90 milliárd USD bevételt generálva, ami a globális játékpiac felét teszi ki. A fejlettebb okostelefonok lehetővé teszik a magas minőségű játékok futtatását, és a felhőalapú szolgáltatások révén a játékok elérése még egyszerűbbé válik.
Okos TV-k és felhőalapú játékok integrációja: A gyártók, mint például az LG, együttműködnek a játékplatformokkal, hogy közvetlenül az okos TV-ken kínáljanak felhőalapú játékokat. Ez lehetővé teszi a felhasználók számára, hogy konzol vagy PC nélkül élvezhessék a legújabb játékokat. [17] [18]

9.2.3Jövőbeni kilátások

A felhőalapú játékpiac további növekedése várható, különösen az alábbi területeken:
Felhasználói bázis bővülése: A technológiai fejlődés és az internet-hozzáférés javulása révén egyre több felhasználó csatlakozhat a felhőalapú játékokhoz világszerte.
Új piacok megnyílása: A fejlődő országokban az infrastruktúra fejlesztése és az okoseszközök elterjedése új lehetőségeket teremt a szolgáltatók számára.
Technológiai innovációk: Az olyan technológiák, mint a mesterséges intelligencia és a virtuális valóság integrációja tovább növelheti a felhőalapú játékok vonzerejét és piaci részesedését.
Összességében a felhőalapú játékok piaca dinamikusan fejlődik, és a jövőben is jelentős növekedésre számíthatunk, amelyet a technológiai innovációk és a felhasználói igények változása hajt. [19]

10 TECHNOLÓGIAI KIHÍVÁSOK ÉS FEJLESZTÉSI IRÁNYOK

A felhőalapú játékszolgáltatások technológiai fejlődése számos lehetőséget rejt magában, ugyanakkor komoly kihívásokkal is szembesül. Az egyik legnagyobb technikai akadály a hálózati késleltetés (latency) és a sávszélesség kérdése. A felhőalapú játékok valós idejű adatkapcsolatot igényelnek a felhasználó és a távoli szerver között, így a gyenge vagy instabil internetkapcsolat jelentősen ronthatja a játékélményt. Ezenfelül a magas felbontású, 4K-s streamelés, valamint az egyre élethűbb grafikai megjelenítés növeli az adatátviteli igényeket, ami különösen problémás lehet alacsony infrastruktúrával rendelkező régiókban.

A fejlődési irányok között kiemelten fontos az 5G hálózatok és a szélessávú internet további terjedése, amelyek hozzájárulnak a késleltetés csökkentéséhez és a játékélmény stabilizálásához. Ezen túlmenően a peremhálózati számítástechnika (edge computing) alkalmazása lehetővé teszi, hogy a szerverek fizikailag közelebb kerüljenek a felhasználókhoz, így gyorsabb válaszidő érhető el. A jövőben várhatóan a mesterséges intelligencia és a gépi tanulás is egyre nagyobb szerepet kap a felhasználói élmény optimalizálásában – például a hálózati erőforrások dinamikus kezelése vagy játékbeli események előrejelzése terén.

10.1 Késleltetés és adatátviteli problémák

A felhőalapú szolgáltatások egyre fontosabb szerepet töltenek be a videójáték-iparban, különösen a játékstreaming platformok és az online multiplayer játékok terjedésével. E technológiák sikeres működéséhez azonban elengedhetetlen a stabil, nagy sávszélességű internetkapcsolat és az alacsony késleltetés. Ezek hiánya komoly kihívásokat jelenthet mind a fejlesztők, mind a játékosok számára. [20]

A késleltetés (latency) azt az időt jelöli, amely egy adatcsomag elküldése és a válasz visszaérkezése között telik el. A videójátékok esetében ez különösen kritikus tényező, mivel a valós idejű reakciók – például egy gombnyomásra történő karaktermozgás – kulcsfontosságúak a játékélmény szempontjából. Egy pár századmásodperces késés is frusztrációt válthat ki, főként kompetitív játékokban, ahol minden pillanat számít. [21]

A felhőalapú játékok – mint például a Microsoft xCloud, NVIDIA GeForce NOW, vagy a korábban működő Google Stadia – esetében a játék nem a játékos eszközén fut, hanem egy távoli szerveren. A felhasználó csupán a videófolyamot kapja vissza, miközben a vezérlési parancsokat (pl. billentyűlenyomás) elküldi a szervernek. Ez a modell kifejezetten érzékeny a késleltetésre, mivel minden egyes parancsnak az interneten keresztül kell eljutnia a szerverhez, majd annak válasza is vissza kell érkezzen – mindezt a lehető leggyorsabban.

Emellett az adatátviteli problémák, mint például csomagvesztés (packet loss), hálózati torlódás, vagy instabil kapcsolat szintén negatívan befolyásolják a felhasználói élményt. A videójel szakadozása, a képminőség csökkenése, illetve a vezérlés késedelme mind-mind a technológiai korlátokból fakadnak, és akadályozzák a felhőalapú játékplatformok széleskörű elfogadását.

A megoldások között szerepel a 5G hálózatok elterjedése, amelyek alacsony késleltetést és nagyobb adatátviteli sebességet ígérnek, valamint a játékstreaming infrastruktúra fejlesztése, mint például több regionális adatközpont létrehozása a felhasználókhoz közelebbi szerverek biztosítása érdekében. Emellett a videó tömörítési algoritmusok optimalizálása és a prediktív input-technológiák is hozzájárulhatnak a késleltetés csökkentéséhez.

Összességében a késleltetés és az adatátviteli problémák jelentős technikai kihívást jelentenek a felhőalapú szolgáltatások videójáték-ipari alkalmazásában, ugyanakkor az Ipar 4.0 technológiai fejlődése folyamatosan nyit új lehetőségeket ezek leküzdésére.

10.2 A mesterséges intelligencia szerepe a cloud gamingben

A mesterséges intelligencia (MI) egyre jelentősebb szerepet tölt be a cloud gaming technológiában, mind a felhasználói élmény javítása, mind az infrastruktúra optimalizálása területén. Az MI alkalmazásával a szolgáltatók hatékonyabban kezelhetik az erőforrásokat, csökkenthetik a késleltetést, és dinamikusan alakíthatják a játékminőséget a felhasználók internetkapcsolatának megfelelően. [20]

Az egyik legfontosabb terület az MI használatában a dinamikus videótömörítés és átvitel. A cloud gaming szolgáltatások valós időben tömörítik a játékmenet kép- és hangadatfolyamát, amelyet a felhasználó eszközére közvetítenek. Az MI algoritmusok folyamatosan elemzik a felhasználó internetkapcsolatának sebességét, stabilitását, valamint a játékon belüli mozgás komplexitását, és ezek alapján adaptívan módosítják a közvetített képminőséget és bitrátát, így csökkentve az adatvesztést és a késleltetést. [22]

Az MI segíti a hálózati forgalom előrejelzését is. A szolgáltatók az újonnan elérhető óriási adatmennyiséget feldolgozva képesek megjósolni a felhasználói aktivitások csúcsidőszakait, ezáltal időben tudják skálázni az infrastruktúrát. Ez javítja a szolgáltatás rendelkezésre állását, elkerülhetővé teszi a torlódásokat és leállásokat.

További fontos szerepe van az MI-nek a játékélmény prediktív javításában is. A rendszer tanul a felhasználó szokásaiból, kedvenc játékaiból, teljesítményéből, és ehhez igazodva automatikusan optimalizálja a szerveroldali beállításokat, csökkentve ezzel a betöltési időket és minimalizálva a megszakításokat. [23]

Az MI továbbá fontos szerepet játszik a biztonság és csalásfelismerés területén is, azaz a csalási kísérletek, a szoftvermanipulációk és a felhasználói anomáliák korai felismerésében, amely a cloud gaming platformok hosszútávú megbízhatóságát növeli. [24]

10.3 Környezeti hatások (Green IT és fenntarthatóság)

A felhőalapú szolgáltatások, különösen a cloud gaming, fontos szerepet tölthetnek be a fenntarthatóbb digitális jövő megteremtésében. A "Green IT" mozgalom a technológiai ipar környezetre gyakorolt hatásának csökkentését célozza, amelyben a cloud computing és ezen belül a cloud gaming is különösen ígéretes szereplő. [25]

A klasszikus gamer PC-k és konzolok által generált karbonlábnyom jelentős. Egy modern gamer PC évente több mint 1400 kWh energiát is fogyaszthat, összehasonlítva egy cloud gaming szolgáltatással, amely optimalizált adatközpontokat használ, és az energiahatékonyságot skálaszerűen növeli. [26]

A nagy technológiai vállalatok, mint a Microsoft (Azure), a Google (Google Cloud) és az Amazon (AWS) komoly lépéseket tesznek az adatközpontok zöldítése érdekében. Céljaik közé tartozik, hogy 2030-ra nettó zéró kibocsátást érjenek el, megújuló energiákra építve az összes szolgáltatásukat. [27]

A cloud gaming lehetővé teszi, hogy a felhasználóknak ne kelljen nagy energiaigényű helyi eszközöket üzemeltetniük, elég egy energiatakarékos kliens (pl. laptop, tablet, okostévé), miközben a nagy teljesítményt a szuperefficiens adatközpontok biztosítják. Ez csökkenti az egy főre eső energiafogyasztást és a berendezések elektronikai hulladékká válását is lassítja. [28]

Mindazonáltal fontos hangsúlyozni, hogy az adatközpontok is jelentős energiaigénnyel bírnak, ezért kulcsfontosságú, hogy a szolgáltatók folytassák a megújuló energiák felé való átállást, az adatközpontok hűtési rendszerének optimalizálását (pl. folyadékhűtés bevezetése) és az üzemeltetési hatékonyság további növelését. [29]

Összességében a cloud gaming - megfelelő irányítással és fenntartható energiaforrásokkal - hozzájárulhat a digitális ipar ökológiai lábnyomának jelentős csökkentéséhez.

10.4 Digitális ikrek az Ipar 4.0 kontextusában

A digitális ikrek (digital twins) az Ipar 4.0 egyik kulcstechnológiáját jelentik, amelyek valós idejű adatkapcsolat segítségével lehetővé teszik egy fizikai eszköz, gyártósor vagy akár egy teljes gyár virtuális másolatának létrehozását. Ezek a modellek nem csupán statikus másolatok, hanem dinamikusan frissülnek a szenzoradatok alapján, így valós időben követik a fizikai rendszer működését.
A digitális ikrek használatának fő előnyei közé tartozik:

- Prediktív karbantartás: a valós idejű adatok elemzésével előre jelezhetők a lehetséges meghibásodások.
- Folyamatoptimalizálás: a virtuális modell segítségével kísérletezés nélkül tesztelhetők különböző gyártási beállítások.
- Termék- és rendszerfejlesztés: a tervezési fázisban digitális szimulációval csökkenthető a prototípusok száma és a fejlesztési idő.

A digitális ikrek technológiája szoros kapcsolatban áll más Ipar 4.0 technológiákkal, mint a mesterséges intelligencia, IoT (Internet of Things), big data és felhőalapú számítástechnika. Együttes alkalmazásukkal lehetőség nyílik arra, hogy a gyártási rendszerek adaptívvá, önoptimalizálóvá és önjavítóvá váljanak – ami a jövő intelligens gyárainak alapkövét képezi. [33]
A digitális ikrek hatalmas potenciállal rendelkeznek általánosan az Ipar 4.0-át tekintve. Gondoljunk csak bele mennyi orvostudományi, biztonságtechnikai (vezetés), elemzés és adat származtatható ezzel a módszerrel. A szimulációk révén a már megtörtént eseményeket tudjuk „rekreálni" így tanulhatunk belőlük. Persze ehhez nagy mennyiségű információkra és szaktudásra van szükség.

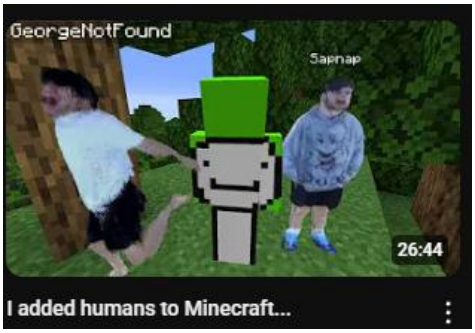
10.4.1 Digitális ikrek felhasználása a videójáték iparban

Napjaink egyik közkedvelt videójátéka a Minecraft. A Minecraft egy nyílt világú sandbox videojáték, amelyet eredetileg Markus Persson (ismertebb nevén Notch) fejlesztett, és 2011-ben jelent meg a Mojang Studios kiadásában. A játék lényege a felfedezés, építés és túlélés egy véletlenszerűen generált, kockákból álló világban. A Minecraft több játékmódot kínál, köztük a kreatív módot, ahol a játékos korlátlan erőforrásokkal építhet, valamint a túlélő módot, ahol a játékosoknak nyersanyagokat kell gyűjteniük, eszközöket készíteniük, és különféle ellenségekkel szembenézniük. A játék sikerének kulcsa a szabadság, a közösségi élmény és az oktatási potenciál, hiszen a Minecraft világszerte népszerű oktatási célokra is, például programozás vagy építészet tanítására. A játék egy ikonikus borítóképe látható a 15. képen.

15. Kép: Minecraft illusztráció
https://www.nintendo.com/en-gb/Games/Nintendo-Switch-games/Minecraft-1386505.html

A videójátékból rengeteg tartalom készül különböző korosztálynak, különböző jellegű tartalom. Az egyik legkiemelkedőbb tartalomgyártó Dream, aki főleg YouTube-ra gyárt videókat különböző ötletekkel a Minecraft világán belül. Ő volt az első, aki digitális ikreket alkalmazva játszott ebben a világban. [34]
Dream koncepciója azt takarja, hogy egy területen néhány kamerával, különböző optikai érzékelőkkel és egy VR szemüveggel (valamint a hozzátartozó eszközökkel pl controller) egy digitális ikret tudott létrehozni, így a teremben jelenlévő ember teljes egésze meg tud jelenni a Minecraft világában. Több videóstartalmat is készített már ezt a technológiát használva. Többek között a saját házáról egy arányos verziót épített a játékon belül a digitális ikerrel pedig körbe tudták járni. „Manhunt" videót is tudott ezt a technológiát felhasználva csinálni. Maga a Manhunt egy különleges műfaj, lényegében Player-vs-Player alapú műfaj, ahol az egyik csapat célja hogy a lehető legrövidebb idő alatt végig játssza a játékot. A másik csapat dolga ennek megakadályozása. Erre különféle szabályrendszerek léteznek. – *Azok most nem relevánsak dolgozatomat tekintve.* – Maga a technikai megvalósítás nagy kaput nyitott a „gaming" világban. Rengeteg lehetőség rejlik még a digitális ikrek felhasználásában a videójáték-ipart tekintve. Dream korszakalkotó ötlete remek példa erre. Egy relatív régi játékba bele tudott vinni még mérnöki és tudományos szemnek is izgalmas területet. Dream videóinak a borítóképeit láthatjuk a 16., a 17., a 18. és a 19. képen.

16. Kép: Dream: Minecraft Speedrunner VS TITAN video
https://www.youtube.com/watch?v=FxR_I6UVyIA



17. Kép: Dream: I added humans to Minecraft... video
https://www.youtube.com/watch?v=YHGMfQ1TDPA

18. Kép: Dream 20 YouTuber VS Titan video
https://www.youtube.com/watch?v=Vjz3rOsr_5A

19. Kép: Dream 3 Minecraft Speedrunners VS TITAN video
https://www.youtube.com/watch?v=WphbV44bsik

11 ÖSSZEFOGLALÁS, SAJÁT TAPASZTALAT

Összeségében az egész felhőbe való költözés véleményem szerint egy rendkívül innovatív és jó problémamegoldó lehetőség. A nagy covidban én is főállásban dolgoztam, amit a távoli elérések nélkül elég nehezen tudtam volna megoldani. A másik ilyen alternatív kommunikációs rendszer, amit azóta előszeretettel használok az a Microsoft Teams. És egy fuvarszervezéssel, szállítmányozással foglalkozó cég szempontjából a folyamatos informáltság elengedhetetlen.

Cloud gaming oldalról és lassan már több mint egy éve használom a GForce Now által kínált ingyenes verziót, amivel teljesen meg vagyok elégedve. Gyakorlatilag nem sok különbség van a havidíjas verzió között. Az ingyenes verzió lehetőséget ad maximum 1920x1080p és 60 Fps-es felbontásra amíg a fizetős verzió 2560x1440p és 120 Fps-t tud biztosítani. Mérvadó differencia lehet még, hogy az ingyenes verzió egy órás szekciókra osztja az egyhuzamban használt időt az előfizetéses akár nyolc órára is kitudja tolni azt. Na és igen, ha már szekciók mivel az Nvideanak is limitáltak a szerverei, ezért a nem fizetős felhasználónak egy várakozás sort kell kivárniuk amennyiben szeretnék használni. Megjegyzendő ez sokban függ attól milyen időintervallumban akarja használni a felhasználó, mert egy esti szekcióban mondjuk éjféltől egyig nincsen várakozási idő.

IRODALOMJEGYZÉK

[1] Wikipédia, “Felhőalapú számítástechnika,” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Felh%C5%91alap%C3%BA_sz%C3%A1m%C3%ADt%C3%A1stechnika [Accessed: Apr. 7, 2025].Sam Anzaroot and Andrew McCallum. 2013. UMass Citation Field Extraction Dataset. Retrieved May 27, 2019 from http://www.iesl.cs.umass.edu/data/data-umasscitationfield

[2] Microsoft, “What is cloud computing?” Azure, [Online]. Available: https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits [Accessed: Apr. 7, 2025].Chelsea Finn. 2018. Learning to Learn with Gradients. PhD Thesis, EECS Department, University of Berkeley.

[3] Wikipédia, “Amazon Elastic Compute Cloud,” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Amazon_EC2 [Accessed: Apr. 7, 2025].Matthew Van Gundy, Davide Balzarotti, and Giovanni Vigna. 2007. Catch me, if you can: Evading network signatures with web-based polymorphic worms. In Proceedings of the first USENIX workshop on Offensive Technologies (WOOT ’07) . USENIX Association, Berkley, CA, Article 7, 9 pages.

[4] Wikipédia, “Compaq,” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Compaq [Accessed: Apr. 7, 2025].David Harel. 1979. First-Order Dynamic Logic. Lecture Notes in Computer Science, Vol. 68. Springer-Verlag, New York, NY. https://doi.org/10.1007/3-540-09237-4

[5] Wikipédia, “Szoftver mint szolgáltatás (SaaS),” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Saas [Accessed: Apr. 7, 2025].

[6] Wikipédia, “Platform mint szolgáltatás (PaaS),” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Platform_szolg%C3%A1ltat%C3%A1s [Accessed: Apr. 7, 2025].R Core Team. 2019. R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

[7] Wikipédia, “Infrastruktúra mint szolgáltatás (IaaS),” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Infrastrukt%C3%BAra_szolg%C3%A1ltat%C3%A1s [Accessed: Apr. 7, 2025].John R. Smith and Shih-Fu Chang. 1997. Visual Seek: a fully automated content-based image query system. In Proceedings of the fourth ACM international conference on Multimedia (MULTIMEDIA ’96). Association for Computing Machinery, New York, NY, USA, 87–98. https://doi.org/10.1145/244130.244151

[8] Wikipédia, “Videójáték,” Wikipedia, [Online]. Available: https://hu.wikipedia.org/wiki/Vide%C3%B3j%C3%A1t%C3%A9k [Accessed: Apr. 7, 2025].

[9] Alper Yilmaz, Omar Javed, and Mubarak Shah. 2006. Object tracking: A survey. ACM Comput. Surv. 38, 4 (December 2006), 13–es. https://doi.org/10.1145/1177352.1177355

[10] NVIDIA Corporation, “GeForce NOW Cloud Gaming,” NVIDIA, [Online]. Available: https://www.nvidia.com/en-us/geforce-now/. [Accessed: Apr. 7, 2025].

[11] Microsoft Corporation, “Xbox Cloud Gaming (Beta) with Xbox Game Pass,” Xbox.com, [Online]. Available: https://www.xbox.com/en-US/xbox-game-pass/cloud-gaming . [Accessed: Apr. 7, 2025].

[12] Sony Interactive Entertainment, “PlayStation Plus Premium,” PlayStation.com, [Online]. Available: https://www.playstation.com/en-us/ps-plus/ . [Accessed: Apr. 7, 2025].

[13] Amazon.com, Inc., “Amazon Luna,” Amazon Games, [Online]. Available: https://www.amazon.com/luna/. [Accessed: Apr. 7, 2025].

[14] Google LLC, “Stadia - One place for all the ways we play,” Stadia Archive, [Online]. Available: https://stadia.google.com/. [Accessed: Apr. 7, 2025].

[15] Frost & Sullivan, "Global Cloud Gaming to Reach 349.4 Million Users by 2025", PR Newswire, 2022. [Online]. Available: https://www.prnewswire.com/news-releases/global-cloud-gaming-to-reach-349-4-million-users-by-2025--301533394.html

[16] Fortune Business Insights, Cloud Gaming Market Size, Share & COVID-19 Impact Analysis, 2025. [Online]. Available: https://www.fortunebusinessinsights.com/cloud-gaming-market-102495

[17] A. Nguyen, "Mobile Gaming in 2024", WIRED, Jan. 2024. [Online]. Available: https://www.wired.com/story/mobile-gaming-in-2024-backbone/

[18] MeriStation, "LG y Xbox se unen para potenciar el cloud gaming en Smart TV", AS.com, Mar. 2024. [Online]. Available: https://as.com/meristation/noticias/lg-y-xbox-se-unen-para-potenciar-el-cloud-gaming-en-smart-tv-n/

[19] R. Evans, "Cloud Gaming Market Trends and Predictions 2025", Ofoxil, 2024. [Online]. Available: https://ofoxil.net/cloud-gaming-future-market-trends-and-predictions-2025/

[20] M. Schwarz, "Artificial Intelligence in Cloud Gaming: Enhancing User Experience," IEEE Access, vol. 9, pp. 123456-123470, 2021.

[21] Y. Chen, H. Hu, "Real-time Video Compression Techniques in Cloud Gaming," IEEE Transactions on Multimedia, vol. 23, no. 2, pp. 345-356, Feb. 2021.

[22] T. Liu, S. Gupta, "Predictive Resource Allocation in Cloud Services," IEEE Transactions on Cloud Computing, vol. 8, no. 1, pp. 55-67, Jan.-Mar. 2020.

[23] K. Roy, A. Sarkar, "Machine Learning Based Optimization for Cloud Gaming Services," in Proc. IEEE Intl. Conf. Cloud Computing (CLOUD), 2022.

[24] J. Smith, P. Jones, "AI-based Cheating Detection in Online Games," IEEE Transactions on Games, vol. 13, no. 1, pp. 75-85, Mar. 2021.

[25] B. Brown, "Green IT and Sustainability Challenges in Cloud Infrastructure," IEEE Spectrum, vol. 58, no. 7, pp. 20-27, July 2021.

[26] E. Davis, "Energy Consumption in PC Gaming vs. Cloud Gaming," Journal of Sustainable Computing, vol. 6, pp. 35-45, 2022.

[27] Microsoft Corp., "Sustainability Commitments," [Online]. Available: https://www.microsoft.com/sustainability [Accessed: Apr. 28, 2025].

[28] Google LLC, "Environmental Impact of Cloud Gaming," [Online]. Available: https://cloud.google.com/sustainability [Accessed: Apr. 28, 2025].

[29] R. Patel, "Data Center Cooling and Energy Efficiency Strategies," IEEE Transactions on Sustainable Computing, vol. 5, no. 4, pp. 567-578, Oct.-Dec. 2020.

[30] Microsoft hatékony fenntarthatósági megoldásaival felgyorsíthatja előrehaladását https://www.microsoft.com/hu-hu/sustainability

[31] Ericsson Mobility Report https://www.ericsson.com/en/reports-and-papers/mobility-report

[32] Google Environmental Report (2024) https://sustainability.google

[33] F. Tao, Q. Qi, A. Liu and A. Kusiak, "Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," Engineering, vol. 5, no. 4, pp. 653–661, Aug. 2019. https://doi.org/10.1016/j.eng.2018.08.019

[34] I added humans to Minecraft https://youtu.be/YHGMfQ1TDPA?si=CJ2Qu0MxbOxJfwfA

2.48. A biztonságtechnika szerepe

IPAR 4.0 TECHNOLÓGIÁK

A biztonságtechnika szerepe

Csicsai Bajnok Nimród

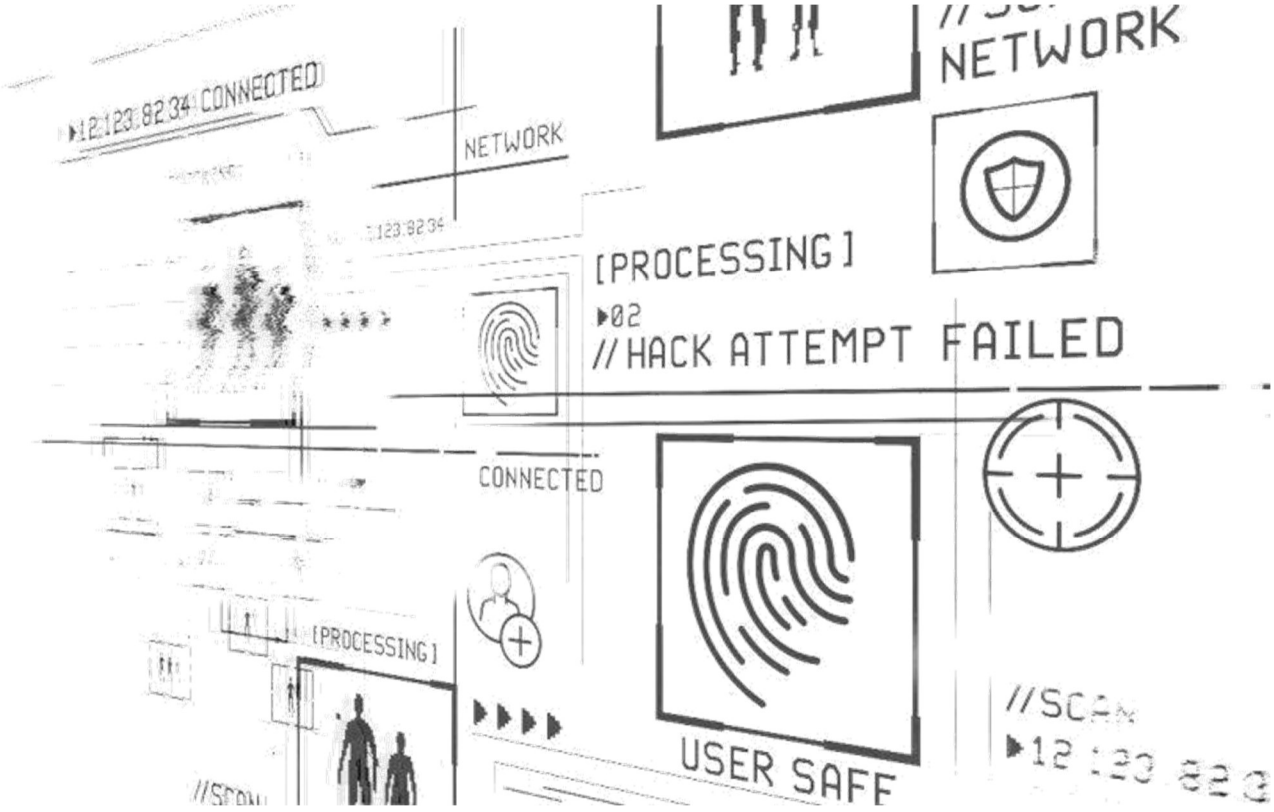
[redacted]

(GKNB_INTM087)

2024/2025/2

Tartalom

1. Mi is az a biztonságtechnika? 3
2. Védelem Fajtái 4
2.1. Mechanikus védelem 4
2.2. Elektronikus védelem 4
2.3. Élőerős, őrzés védelem 4
3. Biztonságtechnika funkciók szerinti besorolásai 5
3.1. Behatolás- és támadásjelző rendszerek 5
3.2. Videó-megfigyelő és képrögzítőrendszerek 5
3.3. Beléptető és munkaidőnyilvántartó rendszerek 5
3.4. Tűzjelző és vagy tűzoltó rendszerek 5
4. Biztonságtechnika legfontosabb eszközei 6
4.1. Elektronikus behatolás és támadás jelzők 6
4.2. A belső térvédelmi érzékelők 6
4.2.1. Mikrohullámú mozgásérzékelők 7
4.2.2. Kültéri mozgásérzékelők 7
4.3. Kézi támadásjelzők (gombok, kapcsolók) 8
4.4. Épületvédelmi érzékelők 8
4.4.1. Lépésérzékelők 9
4.4.5. Kerítésvédelem 10
4.4.6. Elektronikus behatolásjelző központok 12
5. Videósmegfigyelő rendszerek 13
5.1. Kamerák 13
5.2. Jelátalakítás 16
5.3. Rögzítő berendezések 16
6. Beléptető és munkaidőnyilvántartó rendszere 17
6.1. Azonosítók 17
7. Tűzjelző és vagy tűzoltó rendszerek 19
8. Vezérlők fajtái működési elv és jelfeldolgozás szerint 20
8.1. PIC alapú mikrovezérlő 20
8.2. PLC alapú mikrokontroller (Programozható logikai vezérlő) 21
9. Szabványosítás 22
9.1. Főbb feladatai 22
10. Összegzés és egyéni vélemény 23



1. ábra a biztonságtechnika

1. Mi is az a biztonságtechnika?

A biztonságtechnika napjaink elengedhetetlen témája. Az emberek, vállalkozások, társadalmak számos területen védik magukat a vagyonát, egészségét, létezését veszélyeztető tevékenységektől. Ehhez nyújt segítséget a biztonságtechnika számos lehetősége.

A biztonságtechnika interdiszciplináris tudomány, mely a tulajdon és személy védelmével foglalkozik. (Lásd: 1. ábra)

Tulajdonképpen ez egy olyan tudomány, mely több másik tudomány területet is érint. Ezen tudomány legfontosabb célja, a személy, élet és a vagyonvédelem, illetve ezek mellet még a különböző rendszerek felügyelete.

A biztonság köznapi értelemben valakinek vagy valaminek a veszélytől, kártól, jogtalan beavatkozástól, bántódástól védett állapota, helyzete. Technikai értelemben a biztonság egy objektum (vállalat, intézmény, bank, üzem, munkahely, termelőeszköz, lakás stb.) olyan állapotát jelenti, hogy rendellenes működése, meghibásodása esetén az emberekre és más objektumokra veszélyes következmények nem lépnek fel, nem keletkezik baleset vagy nagyobb

1 https://hu.wikipedia.org/wiki/Biztonságtechnika

anyagi kár, esetleg katasztrófa. A biztonságra egyaránt veszélyt jelenthetnek a vagyon és a személyek elleni támadások (betörések, rablás), a munkahelyi balesetek és ártalmak, a veszélyes anyagok, a tűzés robbanásveszély, az ipari és természeti katasztrófák. A biztonságra való törekvés egyik területe az annak érdekében megoldandó technikai, műszaki kérdések megvizsgálása, majd a kialakított feladatok végrehajtása.

Biztonságtechnikának nevezzük tehát a műszaki tudományok azon területét, amelynek feladata a különféle objektumok és rendszerek biztonságának növelése, az embert érő káros hatások és a vagyoni kár kockázatának csökkentése, igénybe véve ehhez műszaki, szervezési, egészségügyi, gazdasági intézkedéseket és eszközöket.[2]

A biztonságtechnikai rendszerek fejlesztésének célja, hogy a feladatra legmegfelelőbb rendszert tervezünk, célirányos eszközválasztással, Az egyik alapvető szabály, hogy tökéletes biztonság nem létezik, de törekedni kell az elérhető legmagasabb biztonsági szint létrehozására, kivitelezésére. Biztonsági rendszerek tervezésére és létrehozására csak hatósági engedéllyel rendelkező vállalkozhat.

2. Védelem Fajtái

2.1. Mechanikus védelem

Azokat a védelmi intézkedéseket, amelyek a védett létesítménybe, védett épületben, épületrészbe, vagy helyiségbe történő ellenőrzött bejutást mechanikai eszközökkel (rács, kerítés, falazatok, falak, zárszerkezetek, nyílászárók, stb.) szabályozzák, korlátozzák, vagy éppen megakadályozzák, mechanikai védelemnek nevezzük.[3]

2.2. Elektronikus védelem

Ezzel emelhetjük az tulajdon és személyvédelmet minél magasabb szintre kiegészítve vele a mechanikus védelmet. Minden olyan elektromos berendezés ingatlanon belül és kívül, mely illetéktelen behatolás vagy veszély esetén jelzést adhat a tulajdonosnak, vagy az arra illetékes biztonságtechnika szervezetnek elektronikus védelemnek számít. Ilyenek a riasztórendszerek, CCTV kamerás megfigyelőrendszerek, tűzjelzők, beléptetők, kaputelefon rendszerek és áruvédelmi eszközök.

2.3. Élőerős, őrzés védelem

Biztonságtechnikai szolgálatot ellátó személynek számítanak mindazok, akik a vagyonvédelmi feladatukat, szakmai tudásukat és tapasztalatukat felhasználva személyes jelenlétükkel látják el. Élőerős védelemnek számít a biztonsági őr, távfelügyeleti járőr, valamint a rendezvényeken jelenlévő helyszínt biztosító szolgálat és itt említhetjük meg a személyi testőrséget is.[4]

2 http://hadmernok.hu/154_03_kisss.pdf

3 https://lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Horvath_Tamas_ertekezes.pdf

4 https://www.alarmdirect.hu/biztonsagtechnika-ami-mar-nem-csak-egy-fogalom-szotarunkban-es-mindennapjainkban/

3. Biztonságtechnika funkciók szerinti besorolásai

3.1. Behatolás- és támadásjelző rendszerek

Feladat, hogy észlelje a jogosulatlan behatolást és azt jelezze élőerős kivonuló szolgálat vagy a hatóság felé (pl.: rendőrség). Ezen rendszerek folyamatosan fejlesztés alatt vannak a gyártó részéről.

Pl.: Paradox[5] rendszereknél már a fejlesztők fokozatosan bevonják a mesterséges intelligenciát is. A Paradox rendszerei – más gyártók megoldásaihoz hasonlóan – vezérelhetők applikációból is.

Behatolás jelző rendszerek

Pl.: Lakásriasztó

Behatolás jelző és beavatkozó rendszerek

Pl.: Pénzintézetek (füstgenerátor, elektromoszár vezérlés, fény vezérlés), akár üzletek.

3.2. Videó-megfigyelő és képrögzítőrendszerek

Ezek a rendszerek segítik egy objektumban vagy közterületeken történő mozgások, események követését és áttekintését. Amennyiben rögzítésre kerülnek a felvételek és nem csak azonnali megfigyelésre, akkor segítik a felderítést és a bizonyítási eljárásokat. Ezen belül megkülönböztetünk működés szerint analóg, digitális és hibrid rendszereket. [6]

3.3. Beléptető és munkaidőnyilvántartó rendszerek

A beléptető rendszerek az elektronikai védelem egyik meghatározó területe. Rendeltetése, hogy az adott területre csak engedéllyel rendelkező személy lépjen be és tartózkodjon. Objektumokon belül különböző részekre, területekre történő belépés is külön korlátozható.

Tehát a beléptető rendszer alapvetően szabályoz, azonban az objektum tulajdonosának, üzemeltetőjének van lehetősége a rendszer más szolgáltatásait is igénybe vennie munkaidő nyilvántartás, rendszámfelismerés stb. Alapvetően a beléptető rendszernek három fő funkciója van. A belépési jogosultság megállapítása, a belépő azonosítása és az áthaladás szabályozása.[7]

3.4. Tűzjelző és vagy tűzoltó rendszerek

Feladata, hogy egy adott objektumban esetlegesen keletkező tűz vagy más tűzjellemzők (füst, gyorshőmérséklet emelkedés) mihamarabbi észlelése. A rendszer az észlelés után értesíti a hatóságokat és vagy automatikus beavatkozást indít. A beavatkozás a hely jellegétől függően lehet habbal, halonnal, vízzel.

5 https://www.securifocus.com/hir/2022/9/22/paradox-uj-blueeye-applikacio

6 http://hadmernok.hu/142_03_kissics.pdf

7 https://ipit.hu/?module=KnowledgebasePost&ID=71

4. Biztonságtechnika legfontosabb eszközei

2. ábra Néhány példa a különböző eszközökre

https://epuletbiztonsag.hu/biztonsagtechnika/riasztorendszerek

Az alaprendszer felépítés tartalmazza az érzékelők, vezérlők(központ), kommunikációs csatornák és kimeneti eszközöket.

Érzékelő feladata az adott esemény bekövetkezésének érzékelése.

Vezérlő feladata a bemeneti információk feldolgozása, kiértékelése, beavatkozás kezdeményezése.

Kimeneti eszközök továbbítják a vezérlőktől kapott jelzéseket és létrehozzák a helyi jelzéseket, például hang- vagy fényjelzéseket.

Kommunikációs csatornák biztosítják az érzékelő központ és a kimeneti eszközök közötti információátvitelt.

4.1. Elektronikus behatolás és támadás jelzők

Az elektronikus behatolásjelző rendszerek telepítésének célja a mechanikai védelem kiegészítése, hogy az egyetlen beavatkozni képes védelem, az élőerős védelem időben intézkedhessen. A jól megtervezett és szakszerűen kivitelezett behatolásjelző rendszer már a mechanikai védelem megsértésének pillanatában jelez a helyszínen, illetve jelzést továbbít az élőerős szolgálatot ellátó felügyeleti központ felé. Amíg az élőerős védelmet biztosító szolgálat kiérkezik, addig a mechanikai védelem késlelteti az elkövető bejutását.

4.2. A belső térvédelmi érzékelők

Ezek az eszközök a mozgást érzékelik. Lehetnek mikrohullámú és passzív infra mozgásérzékelők.

A mikrohullámú mozgásérzékelők a Doppler elv alapján működnek. Az adóból kibocsátott 2,5; 6, vagy 10 GHz-es környezetről visszavert jelet veszi az antenna és továbbítja a vevőhöz. Ha a térben mozgás történik, akkor megváltozik a visszavert jel és riaszt.

A passzívinfra mozgásérzékelő az ember hő kibocsájtását érzékeli, és mivel az eltér a környezet által kibocsájtott hőmennyiségtől riaszt.

4.2.1. Mikrohullámú mozgásérzékelők

Aktív védelmi eszközök. Két típusa ismeretes: a Doppler mikrohullámú érzékelő és a mikrohullámú sorompó. Mindkét esetben az adó egység GHz-es tartományba eső rádiófrekvenciás jelet sugároz. Az első eszköz önmaga végzi a jel kibocsátását és a visszavert jel érzékelését, feldolgozását. Ha a lefedett térbe mozgó tárgy (személy) kerül, akkor a róla visszaverődő jel frekvenciája módosul. A mikrohullámú sorompó ezzel szemben egy adó és egy vevő berendezésből áll, ahol a jelkibocsátást az adó, míg a módosult jel érzékelését a vevő egység végzi. A két eszköz között egy térbeli szivar alakú zóna (úgynevezett Fresnel zóna) alakul ki. Ez utóbbi eszközt inkább periméter védelemként, míg az előzőt térvédelemként alkalmazzuk.

3. ábra mikrohullámú mozgásérzékelő
https://www.wentronic.com/en/microwave-motion-detector-96011

4.2.2. Kültéri mozgásérzékelők

Kültéri viszonyok között alkalmazhatók, nedvesség és por ellen, valamint a nap UV sugárzása ellen védettek. Az emberi test hőmérsékletének megfelelő infravörös spektrumba eső hősugárzás változását érzékelik. Alkalmazásuk hátránya, hogy az előttük mozgó nagyobb testű állatok, esetleges gyors hőmérsékletváltozások téves jelzést generálhatnak. Ennek kiküszöbölésére hőmérséklet kompenzációt és több érzékelőt vagy érzékelési módot alkalmaznak.

Az eszközöket általában térvédelemre használják, 10–20 méteres „látótávolság” és 90–140°-os „látószög” mellett. Az eszköz „ablakára” rakódott szennyeződés az érzékelés hatásfokát nagymértékben csökkenti, ezért ügyelni kell a fokozott karbantartásra, hanem passzívan figyeli a teret – ahogy ezt a neve is jelzi.[8]

4.ábra infravörös mozgásérzékelő
https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Toth-Toth_bizt-techn.pdf

Feladata tulajdonképpen az, hogy a megfigyelt terület infravörös tartományba eső sugárzását, különösen az emberi testmelegből származó hősugárzást érzékelje, és egy optikai

8https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Toth-Toth_bizt-techn.pdf

rendszer segítségével egy pontra fókuszálja. A fókuszpontban egy piroelektromos elven működő szenzor található, amelynek feladata, hogy a védett területen mozgó ember által kiváltott infrasugárzás szintjének – a környezet alap jelszintjéhez viszonyított – megváltozását villamos jelváltozássá alakítsa. A villamos jelek változását egy jelfeldolgozó áramkör kiértékeli és szükség esetén egy relé működtetésével riasztást vált ki.

A passzív infra érzékelők felépítése:

A PIR érzékelők az alábbi elemekből épülnek fel: érzékelőelem, optikai rendszer, jelfeldolgozó áramkör Az érzékelőelem a környezet hősugárzását, pontosabban annak változását érzékeli és az infravörös sugárzást villamos jelekké alakítja át.[9]

4.3. Kézi támadásjelzők (gombok, kapcsolók)

5.ábra Támadásjelző
https://forschnit.com/product-category/riasztorendszer/tamadasjelzok/

A támadás által veszélyeztetett személyek közelében kell elhelyezni őket. Lehetnek egyszerű nyomógombok, kapcsolók vagy lehajtható fedelű támadásjelző eszközök (3.25. ábra), amelyeknél a fedélben lévő mágnes a fedél lehajtásakor eltávolodik a készülékházban elhelyezett reed érzékelőtől, és így jelzést generál. Az eszközök működtetése kézzel történik, szerelhető rejtetten is, esetleg a pult aljába süllyesztve történik. Pénzszállítási útvonalon, trezor helyiségekben a falra szerelt változat a jellemzőbb. Az eszközökkel szemben támasztott közös követelmény, hogy működtetésük zajmentes legyen, és aktiválásuk minimális erőkifejtést igényeljen.

4.4. Épületvédelmi érzékelők

Az épület ablakain, ajtóin, falazatán, födémén és padlózatán helyezkednek el a felületvédelem érzékelői. Leggyakoribb érzékelők a nyitás-, az üvegtörés-, a falbontás érzékelők, valamint az infra sorompók.

A **nyitásérzékelők** az ajtókra és az ablakokra szerelt mechanikus kapcsolók vagy reed relés érzékelők, amelyek élesítés esetén az ajtó, illetve ablak nyitása esetén riasztó jelzést ad. A mechanikus kapcsoló egy rugós és érintkezős, viszonylag könnyen meghibásodó egység. Lehet nyomó- vagy billenő kapcsolós. Nyitás esetén zárja az áramkört, mely riaszt. A reed relés érzékelő két részből áll a mágnesből és a reléből. A mágnest a nyitható elembe, vagy elemre, a relét a tokba, vagy a tokra építik. Élesítés esetén nyitás után a mágnes elmozdul a relében az érintkezők zárják az áramkört és riaszt.

9https://www.qrface.hu/tanfolyam/Elektronikusvagyonvedelmirendszerszerelokidolgozotttetelek.pdf

Az **üvegtörés** érzékelők lehetnek az üvegre ragasztottak (higanykapcsolós, piezo elven működő), optikaiak, vagy akusztikusak. A higanykapcsolós érzékelőben a törés esetén keletkező rezgés hatására a két érzékelő között elmozduló higany csepp megszakítja az érintkezést és riaszt. A piezo kristály a törés esetén elektromos jelet bocsájt ki a riasztáshoz. Az optikai érzékelő az üvegfelületre bocsájtott és visszavert infra sugarak megváltozása esetén, az akusztikus pedig a töréshang észlelése esetén jelez.

6. ábra nyitásérzékelő
https://fensterplast.hu/reszletek/nyitaserzekelok

Az infra sorompó egy adó és egy vevő egységből áll. A behatoló megszakítja a két egység között lévő infravörös sugarat és ezáltal riaszt.[10]

7. ábra infra sorompó https://www.riasztokamera.com/kulteri-vedelem/

8. ábra üvegtörés érzékelő
http://bulisbiztonsag.hu/vagyonvedelem/22-e-uvegtores-erzekelo

4.4.1. Lépésérzékelők

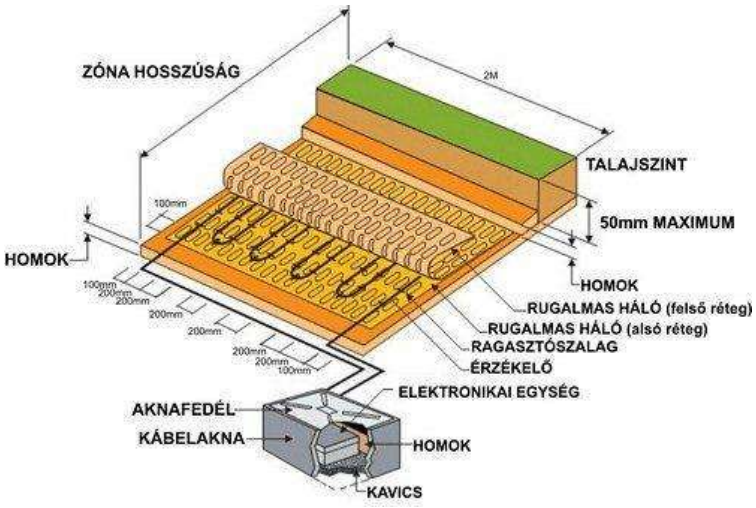
A lépésérzékelő rendszer a védendő objektum körül kialakított sávban, föld alá telepített szeizmikus érzékelő rendszer, amely jelzést bocsát ki, amint a felszínen mozgó személyt vagy gépjárművet észlel. Előnye, hogy a lépésérzékelővel védett területen (miután a földmunka nyomai eltűntek és a fű is kinőtt) gyakorlatilag semmilyen érzékelő vagy szerelvény nem látható, a rendszer észrevehetetlen, amíg nem lép működésbe. Hátránya a telepítéssel és a beállítással kapcsolatos nehézségek.

10 https://ipit.hu/index.php?module=KnowledgebasePost&ID=70

A szeizmikus behatolásvédelem a hadiiparból került át polgári felhasználására, de manapság a kiemelt biztonságú intézményeken (pl. fegyházak, félkatonai-, katonai objektumok, energiaszolgáltatók és más stratégiai fontosságú helyszínek) kívül alkalmazzák ipari vagy gazdasági szempontból védett létesítményeknél, például, víz- vagy gázkivitelezési helyeken vagy vízművek, erőművek, szerverparkok területén.

A lépésérzékelők fajtái:

- optikai szálas lépésérzékelő
- kapacitív lépésérzékelő
- folyadékos lépésérzékelő[11]



9. ábra lépésérzékelő
https://oktel.hu/szolgaltatas/kulteri-vedelem/lepeserzekelo/

4.4.5. Kerítésvédelem

A kerítésvédelem, más néven szenzorkábeles védelem, kifejezetten egy kiépített kerítés védelmére, az azon történő átmászás, átvágás, áttörés érzékelésére alkalmas. Általában 300 méternél hosszabb kerítések vagy falak esetén javasolt az alkalmazása.

A többi kültéri érzékelőkhöz hasonlóan itt is többféle megoldás létezik a kerítés vagy kerítésrészek védelmére, illetve a behatolás különböző formáinak érzékelésére. A megoldások közös jellemzője, hogy az érzékelő eszköz valamilyen technológiával rendelkező érzékelő kábel, amelyet a kerítésre rögzítenek.

Ez az ún. mikrofonkábel érzékeli a kerítés mozgását és a környezeti körülmények okozta zavarjeleket kiszűrve felismeri a valós behatolásra jellemző jelformát. Az érzékelőkábeles kerítésvédelem megvalósításhoz különböző működési elvű kábelezést alkalmazhatnak.

Az érzékelőkábeles kerítésvédelem megvalósításhoz különböző működési elvű kábelezést

alkalmazhatnak.

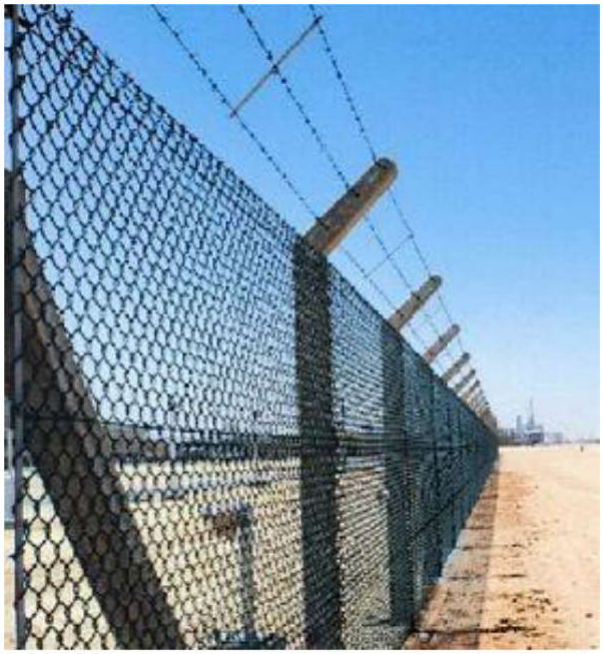
Az alábbi szenzorkábeles érzékelő rendszereket ismerjük:

- elektret technológiájú koaxiális érzékelő kábel;
- piezo elektromos technológiájú koaxiális kábel;
- lineáris mágneses érzékelő kábel;
- optikai érzékelő kábel.

11 https://www.qrface.hu/tanfolyam/Elektronikusvagyonvedelmirendszerszerelokidolgozotttetelek.pdf

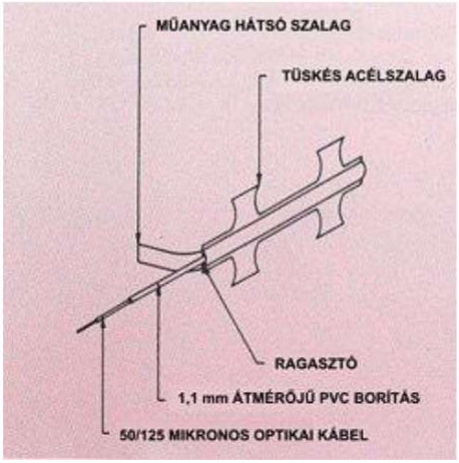
12 https://oktel.hu/szolgaltatas/kulteri-vedelem/keritesved

Az optikai szál, mint érzékelő sokkal jobb jellemzőkkel rendelkezik, mint például a réz alapú kábelek. Nem érzékeny az elektromágneses és rádiófrekvenciás zavarokra, nagyfeszültségű kábelek jelenlétére, napfényre, ködre, havazásra. Nem lehet észrevétlenül áthidalni vagy kiiktatni kábelszakaszt. Működési elve arra épül, hogy a kerítés átvágása vagy átmászása esetén az optikai szál elhajlik, így a szálban vezetett fény intenzitása, tulajdonságai megváltoznak. A kábel kimenetére kötött vevőegység kiértékeli a lézerfény megváltozásának intenzitását, jellegét és az előírtnál nagyobb változás esetén riasztási jelzést ad. Az optikai szálat drótfonatos, hegesztett fémhálós kerítéshez, téglafalhoz, épületfalhoz is lehet rögzíteni, illetve falban vezetni. Képes érzékelni az épület falának fúrására, áttörésére tett kísérleteket is. A kiépítéstől és az érzékelő kábel elhelyezésétől függően a rendszer felismeri a kerítés alatti és feletti átmászásra irányuló próbálkozást, az átvágást vagy a felmászást



10. ábra szenzorkábeles kerítés védelem
https://oktel.hu/szolgaltatas/kulteri-vedelem/keritesvedelem/

Kiemelt fontosságú objektumoknál alkalmazott speciális megoldás, amikor az optikai szál egy különleges kiképzésű (szögesdrót funkciót ellátó) éles acél szalagba van belepréselve és a szalag szakadása vált ki jelzést. Ennek a rendszernek a kiépítése utólag is megoldható, már kész kerítések tetejére történő ráépítéssel vagy a komplett kerítés is kialakítható az acélszalag segítségével.



11.ábra drót szerkezete
https://oktel.hu/szolgaltatas/kulteri-vedelem/keritesvedelem/

Kimeneti eszközök:

1. **Hangjelzők**: A hangjelzők riasztóhangot bocsátanak ki, amely figyelmezteti az embereket a veszélyre vagy incidensre. Ezek a hangjelzők lehetnek hangos szirénák, csengők vagy más hangjelző eszközök.

2. **Fényjelzők**: A fényjelzők fényjelzéseket bocsátanak ki, például villogó fényeket, hogy vizuális figyelmeztetést nyújtsanak a veszélyre vagy incidensre. Ezek a fényjelzők lehetnek villogó lámpák, LED-ek vagy más fényjelző eszközök.

3. **Kijelzők**: A kijelzők lehetővé teszik az információ megjelenítését vagy kommunikációját a riasztás típusáról vagy forrásáról, valamint a rendszer állapotáról. Például egy digitális kijelzőn megjeleníthetik a riasztás típusát vagy az érintett területet.

4. **Kommunikációs modul**: GPRS modul (General Packet Radio Service)

A GPRS segítségével a biztonságtechnikai rendszerek értesítéseket és riasztásokat küldhetnek a felhasználóknak vagy a biztonsági szolgáltatóknak. Például, ha egy riasztás vagy behatolás észlelhető, a rendszer automatikusan értesítést küldhet SMS-ben vagy e-mailben a felhasználóknak, vagy közvetlenül kapcsolatba léphet a biztonsági szolgáltatóval.

4.4.6. Elektronikus behatolásjelző központok

A behatolásjelző rendszer központi egysége – más néven a riasztóközpont – tulajdonképpen egy zárt, acéllemezből készült doboz vagy szekrény, amelyben egy elektronikus áramkör (a központ panel), egy transzformátor, egy akkumulátor és esetleg néhány további kiegészítő áramkör helyezkedik el. Szabotázsvédelemmel van ellátva a jogosulatlan nyitás, rongálás ellen. A műanyag dobozos riasztóközpontok alkalmazása nem felel meg sem a szabványoknak, sem a gyakorlati védelmi igényeknek. A központ elhelyezését úgy kell megoldani, hogy mindig a védett téren belülre kerüljön, lehetőleg illetéktelenek számára nehezen felderíthető vagy megközelíthető helyre felszerelve. A központi egység feladata,

12. ábra Központi panelre egy példa

hogy fogadja és feldolgozza a rákapcsolt érzékelők jelzéseit, a kezelőegységeken beütött kódokat és utasításokat, megszólaltassa a szirénákat, működésbe hozza a fényjelzőt, valamint – amennyiben a rendszer

távfelügyeletre van csatlakoztatva – elküldje a riasztási jelzést a 24 órás távfelügyeleti állomásnak.

A riasztóközpontokat a jelzéstovábbítás szempontjából is megkülönböztethetjük.

- Vezetékes központ Pl.: Paradox SP4000

- Vezeték nélküli vagy rádiós központ Pl.: DSC Alexor
- Hibrid (kombinált vezetékes és rádiós jelzésátvitelű) központ Pl.: Paradox Magellan sorozat[13]

5. Videósmegfigyelő rendszerek

5.1. Kamerák

A kamerák feladata az általuk látott természetes kép átalakítása elektromos jelekké, amelyek alkalmasak megfelelő átviteli csatornán történő továbbításra, képpé történő visszaalakításra, valamint rögzítésre. A fényinformáció elektromos jellé történő alakításban a fő szerepet az úgynevezett képérzékelő elem végzi. A képérzékelőknek két fő fajtáját különböztetjük meg ─ a CCD-t (Charge Coupled Device, töltéscsatolt elem) és a CMOS-t (Complementary Metal-Oxide Semiconductor, azaz komplementer fém-oxid) , mivel a többi technológia is valamilyen szinten e két csoportba sorolható be. Általánosságban elmondható, hogy a CCD elem előállítási költsége nagyobb, érzékenysége viszont jobb, mint a CMOS társáé, ráadásul ez utóbbi sokszor zajosabb képet produkál, viszont kisebb a fogyasztása.[14]

A CCD chip alkalmazási területe ma már annyira széles, hogy minden olyan jellegű technológiában, ahol a képi információt (analóg jelet) digitális jellé kell alakítani, ezt az eszközt alkalmazzák. Megtalálható a szkennerekben, digitális fényképezőgépekben, telefaxokban, digitális videókamerákban, valamint a CCTV rendszerekben alkalmazott analóg és IP kamerákban egyaránt, hogy csak néhány példát említsünk.[15]

A CCTV kamera rendszer használata széles körben alkalmazható a biztonság és felügyelet területén.

Biztonságtechnika szempontjából használják**:** üzletek, bankok, repülőterek, közlekedési csomópontok, parkolók és más közterületek területén a vagyonvédelem és a bűnmegelőzés céljából.

13 https://www.qrface.hu/tanfolyam/Elektronikusvagyonvedelmirendszerszerelokidolgozotttetelek.pdf

14 https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Toth-Toth_bizt-techn.pdf

15 https://www.qrface.hu/tanfolyam/Elektronikusvagyonvedelmirendszerszerelokidolgozotttetelek.pdf

13. ábra kamera rendszer

Az **IP-kamera** egy olyan digitális kamera, amely az internetprotokollt (IP) használja adatátvitelre, és így egy IP-hálózatra kapcsolódva kommunikál a külvilággal, szemben a hagyományos biztonsági (CCTV) kamerákkal, melyek analóg jeleket továbbítanak (jellemzően koaxiális kábelen), és szemben a webkamerákkal, melyek bár digitális eszközök, de adataikat csak egy működő számítógépre képesek továbbítani, annak USB-portjára csatlakozva.

Analóg Biztonsági Rendszerek

Az analóg kamera rendszerek a hagyományos megfigyelő rendszerek, amelyek a koaxiális kábeleken keresztül továbbítják a videójeleket. Az analóg kamerák olcsóbbak, mint az ***IP kamerák***, ***de*** kevesebb funkcióval rendelkeznek, és a képminőség sem olyan jó. Az analóg kamerák ideálisak lehetnek a költségvetési korlátozásokkal rendelkező helyszínek számára, ahol a képminőség nem elsődleges szempont.

Hibrid Megfigyelő Rendszerek

A hibrid megfigyelő rendszerek kombinálják az IP és az analóg kamerák előnyeit. Ezek a rendszerek képesek kezelni mind az analóg, mind az IP kamerákat, lehetővé téve a felhasználók számára, hogy fokozatosan frissítsék rendszerüket anélkül, hogy teljesen lecserélnék azt. A hibrid rendszerek ideálisak lehetnek azok számára, akik szeretnék kihasználni az IP kamerák előnyeit, de nem akarnak teljesen lemondani az analóg kamerákról.[16]

16 https://orkodo.hu/blog/kamera-rendszer-tipusai-ip-analog-hibrid-megoldasok

Analóg kamera rendszer jellemzői

- Az analóg kamera rendszerek hosszú ideje jelen vannak a biztonságtechnikai piacokon.
- Ezek a rendszerek a hagyományos koaxiális kábeleken keresztül továbbítják a videójelet.
- Az előnyük a megbízhatóság és az egyszerű telepítés, de a felbontásuk korlátozott.
- Hagyományosabb technológiát alkalmaznak, ezért az analóg kamera rendszer árak viszonylag olcsóbbak.
- Kábelek segítségével továbbítják a videojelet egy monitorra vagy rögzítőeszközre.
- Jellemzően könnyen kiépíthetők és általában költséghatékonyabbak.

IP alapú biztonsági kamera rendszer jellemzői (Digitális kamera rendszer alapú)

- Az IP (Internet Protocol) alapú kamera rendszerek a modern technológia csúcsát képviselik.
- Ezek a kamerák a hálózaton keresztül kommunikálnak, és magasabb felbontású képeket rögzítenek.
- Az IP kamerák lehetővé teszik a távoli hozzáférést, a felhőalapú tárolást és a bővíthetőséget.
- Digitális adatokat használnak, és az interneten keresztül továbbítják azokat.
- Nagyobb felbontású képekkel dolgoznak, és több funkció elérését teszik lehetővé, így ez a fajta kültéri kamera rendszer ár magasabb kategóriát képvisel.
- Rugalmasabb hálózati kapcsolattal rendelkeznek, amelyek lehetővé teszik egyaránt a távoli elérés és a videofelvételek könnyebb kezelését.[17]

14. ábra analóg és ip kamera rendszer https://www.spyglass.hu/single-post/analogesipkulonbseg

17 https://www.electrocool.eu/kamera-rendeszer

5.2. Jelátalakítás

Ahhoz, hogy megértsük a videó megfigyelő rendszereket, érdemes tisztában lenni néhány fogalommal.

Az információelméletben egy **jel** a kommunikációs csatorna állapotainak egy sorozata, amelyet üzenetté lehet dekódolni. Tehát egy olyan információs sorozat melyet hasznos üzenetté lehet átalakítani. Ennek két fajtája van analóg és digitális.[18]

Analóg

Az analóg jel „folytonos” jel, hiszen folytonosan együtt változik azzal, amit jelöl, egy tartományban bármely két állapot közti, minden állapotot fel tud venni. Az értelmezési tartománya és az értékkészlete is folytonos, a jel pedig minden időpillanatban értelmezhető. A valóság hű leírására alkalmasak.

Digitális

A digitális jelben csak számjegyeket használunk. Ilyenkor annak ellenére, hogy a jelenség folytonos (pl. idő múlása, hőmérséklet emelkedése, sebesség változása), a jel csak egy-egy adott pillanat értékét mutatja, csak bizonyos „lépés-közzel”, vagyis diszkrét értékeket vehet fel. A valóság tetszőleges pontosságú leírására alkalmas.

5.3. Rögzítő berendezések

Analóg: DVR

Digitális: NVR

DVR és NVR Különbségek

A DVR (Digital Video Recorder) és NVR (Network Video Recorder) közötti különbség a jelek kezelésében rejlik. Míg a DVR kizárólag analóg jeleket kezel, addig az NVR képes mind az analóg, mind a digitális jelek kezelésére. Mellesleg ez teszi az NVR-t ideális választássá a hibrid rendszerek számára.

18 https://marrk.me/book/informatika_tetelek.pdf

6. Beléptető és munkaidőnyilvántartó rendszere

A beléptető rendszerek az elektronikai védelem egyik meghatározó területe. Rendeltetése, hogy az adott területre csak engedéllyel rendelkező személy lépjen be és tartózkodjon. Objektumokon belül különböző részekre, területekre történő belépés is külön korlátozható.

Tehát a beléptető rendszer alapvetően szabályoz, azonban az objektum tulajdonosának, üzemeltetőjének van lehetősége a rendszer más szolgáltatásait is igénybe vennie munkaidő nyilvántartás, rendszámfelismerés stb. Alapvetően a beléptető rendszernek három fő funkciója van. A belépési jogosultság megállapítása, a belépő azonosítása és az áthaladás szabályozása.

A beléptető rendszer fő egységei:

1. a központi egység,
2. az olvasó terminálok
3. a vezérlő egységek.

Az olvasó terminál fő feladata érzékelni és továbbítani a vezérlő egység felé a belépő személyazonosítási jellemzőit. A vezérlő egység ezen adatok alapján azonosítja a belépőt, megállapítja a jogosultságát, vagy annak hiányát, és ezek függvényében vezérli a bejárat mechanikai, vagy elektromechanikai elven működő szerkezetét, mely lehet ajtó, sorompó, forgóvilla, forgókereszt, vagy gyorskapu.

Az azonosításra használt információ alapján a személyek azonosítására három alapvető módszer létezik.

1. A tudás alapú azonosítás esetén a személy olyan információ tudatában van, amit az azonosítási eljárás során ellenőrizni lehet. Ilyen információ lehet például egy jelszó, vagy a PIN kód is.
2. Birtok alapú azonosítás esetén már az azonosítás egy olyan eszközzel történik, amely a személy birtokában van, például egy kulcs, vonalkód, mágneskártya, chipkártya vagy smartcard.
3. A biometria alkalmazása, amikor a személy valamilyen fizikai vagy biológiai jellemzőjét felhasználva történik az ellenőrzés[19]

6.1. Azonosítók

RFID azonosítós beléptető rendszer

A leggyakoribb és korszerű azonosítási rendszer, amely az RFID technológiáján alapuló rádiós adatátvitellel működik. Hatalmas gyakorlati jelentősége abból származik, hogy segítségével adatokat lehet nyerni az adathordozó megérintése nélkül, mert az adatátvitel elektromos vagy mágneses hullámok segítségével történik.

19 https://ipit.hu/?module=KnowledgebasePost&ID=71

Chip-kártyával működő beléptető rendszer

Legegyszerűbb chip-kártyák egy tároló chipet, míg az intelligens (smart) változataik a tároló chipen kívül egy mikroprocesszort is tartalmaznak. Az utóbbiak lényegesen több információ tárolására alkalmasak. Beléptető rendszereknél csak nagyon ritkán alkalmazzák, Szilikon karkötős RFID azonosító kulcstartóra helyezhető RFID azonosító jellemzően a mobiltelefonokban, italautomatáknál, könyvtárakban, bankok azonosítási rendszerében találkozhatunk vele.

Kódkulccsal működő beléptető rendszer

A kódkulcsos beléptető rendszerben a belépésre jogosító eszköz egy elektronikus chipet tartalmazó kódkulcs (ibutton), amely gyakorlatilag csak formájában tér el a chipkártya működési elvétől. A kis méret miatt irodai, mechanikai ellenállóképessége miatt pedig, ipari körülmények között célszerű alkalmazni. Rendkívül megbízható, valamint az egyik legkisebb energiafogyasztású azonosítási rendszer. A kulcsot a kulcsolvasóhoz kell érinteni, az olvasása viszont igen rövid idő alatt (néhány ms) megtörténik. A mechanikai kopás a legjelentősebb hátránya. Vonalkódos beléptető rendszer Parkolási-, jegykiadó- és áruazonosító rendszerekben használatos a vonalkódos jegy, kártya, vagy matrica formájú vonalkódos azonosító. Az vonalkódos azonosítót telepített- (parkoló jegykiadó automata, forgóvillás kapu) és kézi leolvasóval is ellenőrizhetjük. A vonalkód fénymásolással könnyen hamisítható, ezért szigorúan védett beléptetésnél nem alkalmazzuk.

Mágneskártyás beléptető rendszer

Régebben a feliratozható, fényképpel ellátható mágneskártyák irodai-, banktechnikai-, parkolási-, pontgyűjtő rendszerekben, valamint beléptető rendszerekben is népszerűvé váltak. Nem korszerű technika, manapság már nem nagyon alkalmazzák, de pl. bankok bejárati ajtajánál még találkozhatunk ilyen megoldással. A mágneskártya mechanikai és mágnes érzékenysége miatt is ritkábban alkalmazzák.

15.ábra mágneskártyás belépés
https://graphax.hu/belepteto-rendszerek

PIN Kódos beléptető rendszer

Irodai-, ipari-alkalmazásokban lépcsőházaknál, kapubejáróknál, személyazonosításra alkalmazzák olyan esetekben, ahol a védettségi szint nem túl magas. Egy számkód beütésével azonosítja magát a személy. A számkódos rendszert a biztonság növelése érdekében kombinálhatjuk más azonosítókkal (pl. RFID kártyával).[20]

20 https://www.qrface.hu/tanfolyam/Elektronikusvagyonvedelmirendszerszerelokidolgozotttetelek.pdf

Biometrikus azonosítás

A személyek azonosításának harmadik és egyben legmegbízhatóbb módszere a biometrikus azonosítás, amely az emberi test valamely, gépek által is könnyen kezelhető, fizikai vagy biológiai jellemzőjét használja fel az ellenőrzés során, mint például az ujjnyomat, a hang, a szem, a kéz vagy akár az arc jellegzetes vonásait. A tudás- illetve a birtok alapú azonosítással szemben itt már ténylegesen magát a személyt azonosítjuk, nem pedig valamilyen más, közvetett jellemzőt, mint a jelszó vagy a kulcs. Ezáltal az azonosítás alapját képező tulajdonság nem lopható el, megfelelő technológiai megvalósítással pedig az is 23 biztosítható, hogy a mintavételezés valós élő személytől származzon, jelentősen csökkentve ezzel a megtévesztés lehetőségét. Csendes riasztásra is lehetőség van, hiszen kényszerítés esetén megoldható például, hogy ujjnyomat ellenőrzésnél egy másik – riasztást kiváltó - ujjat használjon a kényszerített alany, illetve hang alapú azonosítás esetén másik jelszó használata váltsa ki a riasztást, miközben az azonosítás és a beengedés is megtörténik.[21]

7. Tűzjelző és vagy tűzoltó rendszerek

Az automatikus tűzjelző rendszerek telepítésének célja a keletkező tűz korai észlelése, a beavatkozó szervek mielőbbi értesítése az emberéletek és az anyagi javak hatékony mentése érdekében. Az automatikus tűzjelző rendszerekkel szemben elvárás, hogy a helyi riasztás-jelzésen túl automatikus vezérlési feladatokat is képesek legyenek elvégezni. Ilyen vezérlési feladat például a légtechnikai berendezések ki-, illetve bekapcsolása, a felvonók vezérlése, tűzszakaszok lezárása, automatikus oltórendszerek vezérlése stb.

A tűzjelző rendszer elemei:

- automatikus tűzjelző központ
- táp/akkumulátor egység
- automatikus érzékelők
- manuális jelzésadók
- bemeneti, kimeneti modulok
- akusztikus jelzőeszközök
- átjelző eszközök
- Automatikus érzékelők csoportosítása

Beavatkozó rendszerek

• szórófejes vízpermetező

• vízzel árasztó rendszer

• halonnal oltó rendszer (halon: gáz és por elegye)

• tűzoltó habbal oltó rendszer

• különleges esetekben oxigén elvonásos égés lassító rendszer

16. ábra szórófejes vízpermetező https://startechengineering.ca/

21 https://ipit.hu/?module=KnowledgebasePost&ID=71

A tűzjelzés kiértékeléséért, valamint az egyes vezérlések aktiválásáért a tűzjelző központ felel. Működési elvük szerint két főbb típusú tűzjelző központ van, a hagyományos, illetve a címezhető, analóg tűzjelző központ.

Hagyományos tűzjelző központ:

A hagyományos tűzjelző központok esetén az érzékelők jelzőkörökön – ún. zónákon – keresztül csatlakoznak a központhoz és tűzjelzés esetén az egymással párhuzamosan kötött érzékelők egy jellemző ellenállásértéket kapcsolnak a jelzőkörre, így értesül a központ arról, hogy a jelzőkörön valamelyik eszköz tüzet érzékel. Ebből a működésből rögtön láthatóvá válik ezen rendszerek legnagyobb hátránya, miszerint nem azonosítható, hogy egy jelzőkörön melyik eszköz jelzett vagy hibásodott meg. Ez csak úgy lehetséges, ha egyenként megvizsgáljuk valamennyi eszköz LED-jét és amelyik jelzett az fog világítani. Ez a szemrevételezés csak addig lehetséges, amíg a tűzjelző központ riasztás állapotban van. Amennyiben hiba lép fel a jelzőkörön akkor valamennyi ahhoz csatlakoztatott eszköz kiesik a működésből. Éppen ezért a hagyományos elven működő központokat csak kisebb rendszerek esetén szokták alkalmazni.

Címezhető, analóg központok:

Analóg címezhető tűzjelző berendezések Nagy áttörést jelentett, amikor az automatikus érzékelők analóg módon lettek képesek az érzékelt tűzjellemző (hő, füst stb.) mennyiségével arányosan mért jelszintet továbbítani a TJK felé. A jelzőáramkörben már digitális kommunikáció zajlik a központ és a jelzőáramkörre felfűzött eszközök (automatikus érzékelők, kézi jelzésadók stb.) között. A központ folyamatosan felügyeli az érzékelők állapotát és működőképességét, lekérdezi azokat.[22]

A címezhető, analóg tűzjelző központokhoz az egyes érzékelők ún. hurkokon keresztül csatlakoznak. Azért hívják az érzékelőkört huroknak, mert visszatér a központhoz, így egy tervrajzon huroknak látszik. A visszatérő hurkos rendszerek óriási előnye, hogy két irányból is képesek megtáplálni a hurokeszközöket, így egy esetleges hurok szakadás esetén egyetlen érzékelő sem esik ki az érzékelésből. Továbbá ezen az tápellátást biztosító vezetéken keresztül az egyes hurokeszközök a központtal kommunikálni képesek. Ehhez szükséges, hogy mindegyiknek külön címe legyen, melynek segítségével azonosítható, hogy melyik eszköz és honnan jelez. Így a tűzeset pontosan és egyértelműen lokalizálhatóvá válik.[23]

8. Vezérlők fajtái működési elv és jelfeldolgozás szerint

8.1. PIC alapú mikrovezérlő

Nem fut alap program rajta (EEPROM).

Integrált perifériák--> EEPROM

> Kikapcsolás után is megmaradó adatok tárolását lehetővé memória. Egyes PIC-ek külön EEPROM-ot tartalmaznak erre a célra, más típusok esetében a programtároló Flash memóriát használhatjuk fel erre a célra.[24]

22 http://hadmernok.hu/153_03_mohaia.pdf

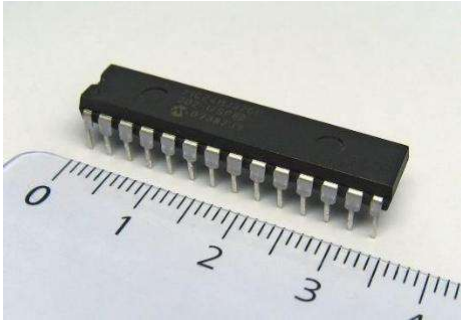
23 https://partnertech.hu/blog/induljunk_az_alapoktol/tuzjelzo_rendszer

24 https://hu.wikipedia.org/wiki/PIC_mikrovez%C3%A9rl%C5%91

Minden adatmemória rekesz egyben regiszterként is használható. Egyes regiszterek speciális jelentéssel rendelkeznek a külső hardver elemek vezérlésében. Azaz egyes regiszterek speciális jelentéssel rendelkeznek.

Értelmez egy bemeneti jelet és a beállítástól függően kommunikációt indít más eszköz felé.

Nem képes tamper jelzésre, azaz hiba védelemre.



17. ábra PIC mikrokontroller és a mérete
https://en.wikipedia.org/wiki/PIC_microcontrollers

Hol használjuk:

• Egyszerűbb, kártyás vagy kódos beléptető rendszerek

• Garázskapunyitók

Miért használjuk?

Egyszerű és költséghatékony rendszereket hozhatunk létre, olyan helyeken, ahol nincs magasbiztonsági szint követelmény.

Kommunikáció fajtái:

A PIC mikrovezérlő alapvetően csak vezetékes kommunikációra képes, de különböző önálló modulok használatával vezeték nélkül is használható.

8.2. PLC alapú mikrokontroller (Programozható logikai vezérlő)

A programozható logikai vezérlő (Programmable Logical Controller, PLC) az ipari szabályozások, illetve vezérlések megvalósítására elterjedten alkalmazott ipari kivitelű mikroszámítógép. Fontos jellemzője, hogy bemeneti és kimeneti egységeinek feszültségszintje illeszkedik az iparban használatos szintekhez.[25]

Ahogy a nevéből is adódik, ezen már ciklikus program fut, programozható. Ezáltal több beállítási lehetősége van. Képes analóg és digitális jel feldolgozására, bemeneten és kimeneten is.

18. ábra Példa egy PLC mikrokontrollerre
https://controlsolution.hu/termekek/plc-logikai-vezerlok/

Kommunikáció fajtái:

• Soros átvitel

• Támogatja az RS kommunikáció szabványokat

• Képes hálózati kommunikációra o ethernet, internet

• Bus kommunikáció o modbus, interbus, canbus

Felhasználása:
Vállalati behatolásjelzők és vállalati többzónás beléptetőrendszerek (komplex többzónás)

25 https://people.inf.elte.hu/toke/adda_ea.pdf

9. Szabványosítás

A **szabvány** elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb. A magyar szabványokat az 1995. évi XXVIII. törvény szabályozza.

A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény értelmében Magyarország nemzeti szabványügyi szervezete a Magyar Szabványügyi Testület (MSZT), amely az alapszabályának megfelelően működő köztestület és amely a törvény felhatalmazása alapján köztestületként a nemzeti szabványosítással összefüggő közfeladatokat kizárólagos jogkörrel látja el.

9.1. Főbb feladatai

- A nemzeti szabványok kidolgozása, jóváhagyása és közzététele, módosítása és visszavonása.
- Az európai szabványok nemzeti szabványként való közzététele, összhangban a kapcsolódó jogharmonizációs feladatok teljesítésével, illetve az európai szabványügyi szervezetek tagszervezetei számára előírt határidőkkel.
- A nemzetközi szabványok nemzeti szabványként való közzététele.
- Részvétel és képviselet a nemzetközi (ISO, IEC) és az európai (CEN, CENELEC, ETSI) szabványügyi szervezetek munkájában, illetőleg más érintett szervezetek részvételének összehangolása.
- Együttműködés az európai szabványügyi szervezetekkel és az Európai Unió tagállamainak nemzeti szabványügyi testületeivel.
- Szaktanácsadás és szakvélemény készítése nemzeti szabványügyi kérdésekben
- Felkérésre közreműködik az Európai Unió irányelvein alapuló magyar jogszabályok előkészítésében.[26]

Jelölések:

A magyar szabványok hivatalos jelölése a következő: a nemzeti jel MSZ a megkülönböztető sorszám xxxx- (egy szabványon belüli szabvány xxxx-x) a kibocsátás éve :yyyy

Nemzetközi szabvány: ISO

Európai szabvány: EN

Európai uniós szabvány honosítása: MSZ EN

Nemzetközi szabvány honosítása: MSZ ISO

Nemzetközi szabvány honosítása: MSZ IEC
Olyan nemzetközi szabvány, amit az unió is elfogadott: MSZ EN ISO

26 https://www.mszt.hu/hu-hu/mszt-rol

10. Összegzés és egyéni vélemény

Az beadandóm írása és a témával kapcsolatos utánanézések alatt mélyebben átgondoltam és megértettem, hogy a biztonságtechnikai rendszerek sokkal többet jelentenek számomra, mint pusztán eszközök a vagyonom védelmére. Ezek a rendszerek a mindennapi életünk szerves részeivé váltak, és hozzájárulnak ahhoz, hogy érzékeljem a biztonságot és a nyugalmat a környezetemben. Értékelem a rendszerek által nyújtott védelmet, és egyúttal megértem, hogy azok segítenek fenntartani a közösségi és egyéni biztonságot is. Összességében, az esszé megírása során ráébredtem arra, hogy a biztonságtechnikai rendszerek nem csupán technológiai eszközök, hanem életminőséget javító intézkedések is, amelyek nélkülözhetetlenek mindennapi életem során.

2.49. GSM technológiák összehasonlítása, alkalmazása CPS rendszerekben

GSM technológiák összehasonlítása, alkalmazása CPS rendszerekben

Györe Márk Róbert

BMI, gyore.mark.01@gmail.com

1 BEVEZETÉS

Az elmúlt évtizedekben a mobilkommunikáció meghatározó pillérévé vált a technológiai fejlődésnek, szerepe pedig messze túlmutat az emberi kapcsolattartás keretein. A digitális eszközök számának rohamos növekedése, az automatizálás előretörése és az adatalapú döntéshozatal térnyerése újfajta hálózati megoldások kialakítását követelte meg. A modern környezetben kiemelt szerepet töltenek be a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS), amelyek a fizikai folyamatokat és a digitális vezérlőmechanizmusokat szoros, dinamikus kapcsolatba hozzák. A CPS rendszerek szerves részét képezi a valós idejű adatgyűjtés, -feldolgozás és -megosztás, amelyhez stabil, biztonságos és hatékony kommunikációs infrastruktúrára van szükség. Az ipar 4.0, az okos városok, a közlekedési rendszerek, valamint a környezetfigyelési és egészségügyi alkalmazások mind ezen rendszerekre alapozva fejlődnek. A kiber-fizikai rendszerek kommunikációs igényei rendkívül változatosak: egyes alkalmazásokban az alacsony energiafelhasználás és a hosszú akkumulátor-élettartam a legfontosabb szempont, míg más területeken – például valós idejű vezérlőrendszerek esetében – a minimális késleltetés és a megbízható adatátvitel elengedhetetlen követelmény. Ezekre az igényekre reagálva születtek meg különböző mobilkommunikációs technológiák, mint például az NB-IoT (Narrowband IoT), amely kis sávszélességű, energiatakarékos adatkapcsolatot kínál, vagy az LTE-M (Long Term Evolution for Machines), amely gyorsabb adatátvitelt és alacsonyabb késleltetést biztosít. Az egyes technológiák közötti választás jelentősen befolyásolja a CPS rendszerek teljesítményét, költséghatékonyságát és hosszú távú megbízhatóságát, így az optimális megoldás kiválasztása kulcsfontosságú tervezési szemponttá vált.

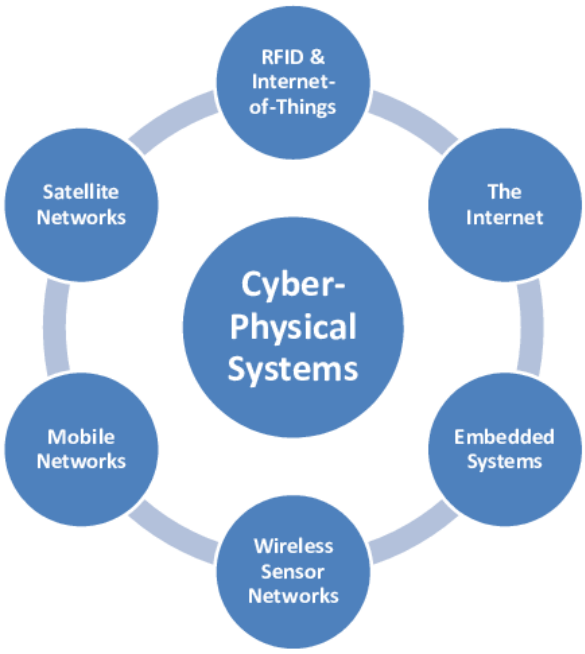
2 A KIBER-FIZIKAI RENDSZEREK BEMUTATÁSA

2.1 A KIBER-FIZIKAI RENDSZEREK (CPS) FOGALMA ÉS JELENTŐSÉGE

A kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) olyan integrált rendszerek, amelyek a fizikai világot és a digitális számítógépes rendszereket összekapcsolják, lehetővé téve a valós idejű adatgyűjtést, feldolgozást és vezérlést. A CPS rendszerek célja, hogy a fizikai rendszerekhez kapcsolódó információkat digitális módon dolgozzák fel, és a digitális rendszer segítségével vezéreljék vagy optimalizálják a fizikai folyamatokat. E rendszerek különösen fontosak azokban az alkalmazásokban, ahol az eszközök és a fizikai környezet közötti kölcsönhatások gyors és pontos elemzése szükséges [1]. A fizikai és digitális világ összekapcsolásának eredményeképpen a CPS rendszerek lehetővé teszik az automatizált döntéshozatalt és az intelligens irányítást, ahelyett, hogy az embereknek folyamatosan közvetlenül be kellene avatkozniuk [2].

A CPS rendszerek fő jellemzője a szoros integráció, amely lehetővé teszi a valós idejű adatgyűjtést, a rendszerek közötti folyamatos kommunikációt, valamint a rendszer egészére kiterjedő vezérlést és optimalizálást. A rendszer a fizikai környezetet szenzorokkal figyeli, és a kapott adatokat digitálisan feldolgozza, majd az alapján végrehajtja a szükséges beavatkozásokat. A gyors döntéshozatal és az adatok valós idejű feldolgozása kulcsfontosságú a kiber-fizikai rendszerek sikeres működéséhez [3].

A kiber-fizikai rendszerek hasznossága különösen nagy az ipari automatizálásban, a közlekedési rendszerekben, az egészségügyben, valamint az intelligens városok fejlesztésében. Az ipari alkalmazásokban a CPS rendszerek például az automatizált gyártósorok és a robotikai rendszerek működését biztosítják, amelynek során a valós idejű adatokat a számítógépes vezérlőrendszerek dolgozzák fel, hogy a fizikai folyamatok hatékonyabban, gyorsabban és kevesebb hibával történjenek [4]. Az egészségügyi alkalmazásokban a CPS rendszerek, mint például a betegmonitorozó rendszerek, az orvosi eszközök és a betegek közötti folyamatos kommunikációt teszik lehetővé, és biztosítják a gyors beavatkozást, ha az orvosi állapot változik [5]. A közlekedési rendszerek területén a CPS rendszerek például az önvezető járművek működését támogatják, amelyek érzékelik a környezetüket, és valós időben reagálnak a forgalmi helyzetekre, a balesetveszélyekre és az útviszonyokra [6]. A kiber-fizikai rendszerek számára alapvetően fontos a megbízható és hatékony kommunikáció. Az ilyen rendszerek közötti adatcsere kulcsfontosságú a sikeres működéshez, mivel a valós idejű adatgyűjtés és feldolgozás gyors, folyamatos kapcsolatot igényel a különböző komponensek között. Az optimális működés érdekében a kommunikációs protokollok, mint az NB-IoT és az LTE-M, amelyek alacsony energiafogyasztást és gyors adatátvitelt kínálnak, elengedhetetlenek [2][6].



1. ábra A Vision of Cyber Physical Internet - Scientific Figure on ResearchGate. (https://www.researchgate.net/figure/Large-Scale-Cyber-Physical-Systems-Components_fig1_228955564)

2.2 KOMMUNIKÁCIÓS KÖVETELMÉNYEK CPS RENDSZEREKBEN

A CPS rendszerek különböző alkalmazásai eltérő adatátviteli sebességet igényelnek. Azok a rendszerek, amelyek nagy mennyiségű adatot kezelnek, például az ipari automatizálásban vagy a videó alapú monitorozásban, szükségük van magas sávszélességre és gyors adatátvitelre [7]. Más rendszerek, amelyek egyszerűbb érzékelő adatokat dolgoznak fel, mint például az alacsony adatátviteli igényű IoT eszközök, alacsonyabb sebességgel is működhetnek, így optimalizálva az energiafelhasználást [8].

A késleltetés minimalizálása kulcsfontosságú a valós idejű alkalmazások számára. Az önvezető járművek, robotok vagy a gyártási folyamatok, amelyek azonnali reakciókat igényelnek, nem működhetnek hatékonyan hosszú késleltetések mellett [9]. A CPS rendszerekben alkalmazott kommunikációs protokolloknak képesnek kell lenniük gyors adatátvitelre, hogy a rendszer megfelelő időben és pontosan reagáljon a változásokra. Ennek biztosítása érdekében olyan kommunikációs infrastruktúrák szükségesek, amelyek garantálják az alacsony késleltetést és a megbízható adatátvitelt [10].

Az energiahatékonyság kulcsfontosságú szempont a kiber-fizikai rendszerek működésében, különösen azoknál az alkalmazásoknál, amelyek hosszú élettartamú akkumulátorokkal működnek, vagy amelyek mobil eszközöket használnak [11]. Az alacsony energiafogyasztás biztosítása érdekében a kommunikációs protokolloknak optimalizálniuk kell az adatátvitelt, minimalizálva az eszközök energiafelhasználását, miközben a rendszer továbbra is képes valós idejű kommunikációra és adatfeldolgozásra [12]. A megfelelő protokollok és megoldások alkalmazása elengedhetetlen az akkumulátor élettartamának növelése érdekében, miközben biztosítják a megbízhatóságot és az alkalmazások zavartalan

működését [13].

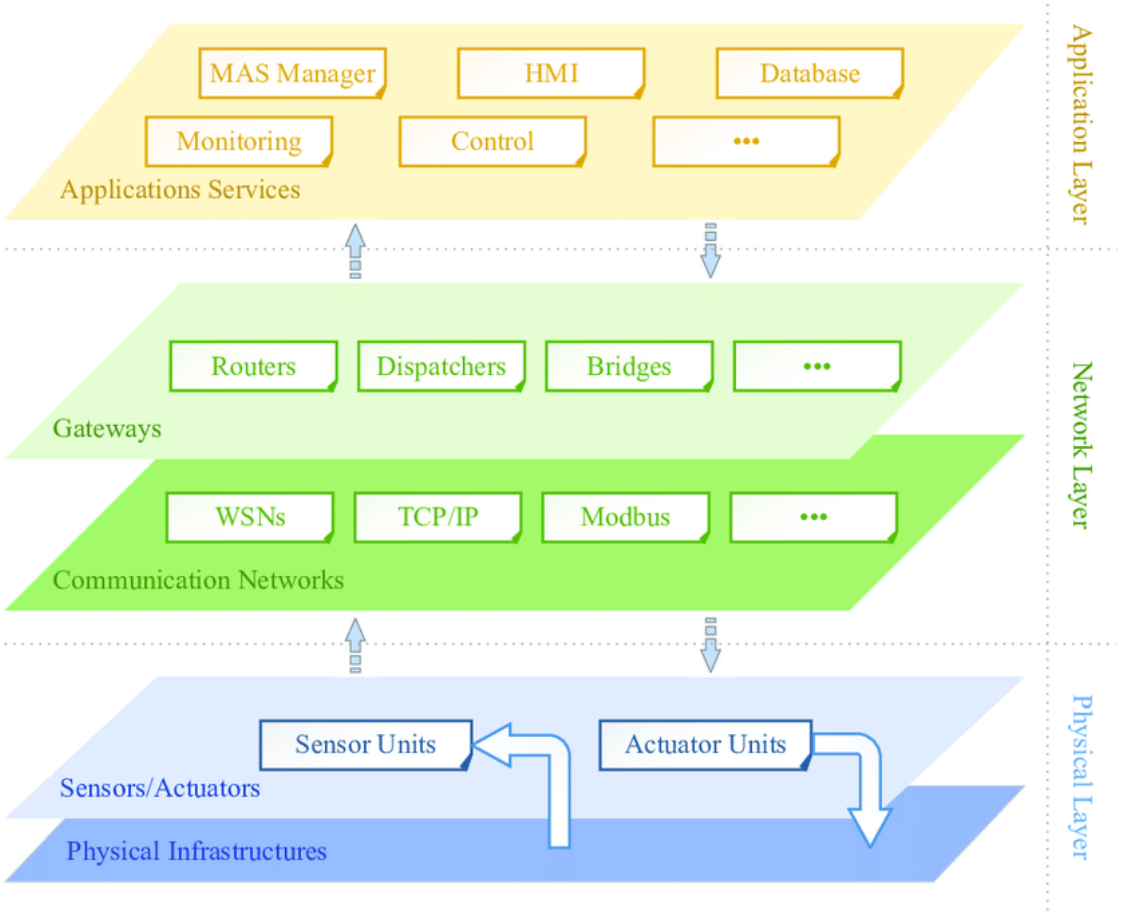
A kiber-fizikai rendszerek, különösen a távoli és mobil eszközökkel működő alkalmazások esetén, a hálózati lefedettség is kritikus tényező [14]. A különböző rendszerek működésének biztosítása érdekében fontos, hogy a kommunikációs hálózatok képesek legyenek biztosítani a szükséges lefedettséget, akár városi, akár vidéki vagy ipari környezetben [15]. A széleskörű hálózati lefedettség garantálja, hogy az eszközök képesek legyenek folyamatos adatcserére és megbízható kapcsolatot tartsanak fenn a rendszer többi komponensével [16]. Az IoT eszközökkel működő CPS alkalmazások számára a hálózati tervezés és a megfelelő protokollok kiválasztása különösen fontos, hogy a hálózati kapcsolatokat az alkalmazások igényeihez igazítsák [17].

2.3 KIBER-FIZIKAI RENDSZEREK ARCHITEKTÚRÁJA

2.3.1 HAGYOMÁNYOS 3 RÉTEGŰ ARCHITEKTÚRA

Ez az egyik legelterjedtebb architektúra, amelyet az ipari és más valós idejű rendszerekben alkalmaznak. A 3 réteg a következőkből áll:

- **Érzékelő réteg (Perception Layer):** Ez a rendszer legalsó rétege, amely a fizikailag észlelt adatokat gyűjti szenzorok és aktuátorok segítségével. A réteg feladata az érzékelés és a fizikai adatok biztosítása.
- **Adatfeldolgozó réteg (Network Layer):** Az adatokat a különböző hálózati protokollokon keresztül továbbítják, amely az adatokat gyűjti és eljuttatja a feldolgozó rendszerhez. Az adatok itt továbbítódnak, és közvetlenül kapcsolódnak a felhőalapú vagy központi adatfeldolgozó rendszerekhez.
- **Vezérlési réteg (Application Layer):** Ez a réteg az adatokat feldolgozza és döntéseket hoz a rendszer számára, amely alapján beavatkozások történhetnek. A vezérlés itt lehet helyi vagy központi, és alkalmazás specifikus döntéseket hozhat, például automatizált vezérlést vagy prediktív elemzéseket.



2. ábra Architecture of a cyber-physical system (Fig. 1)

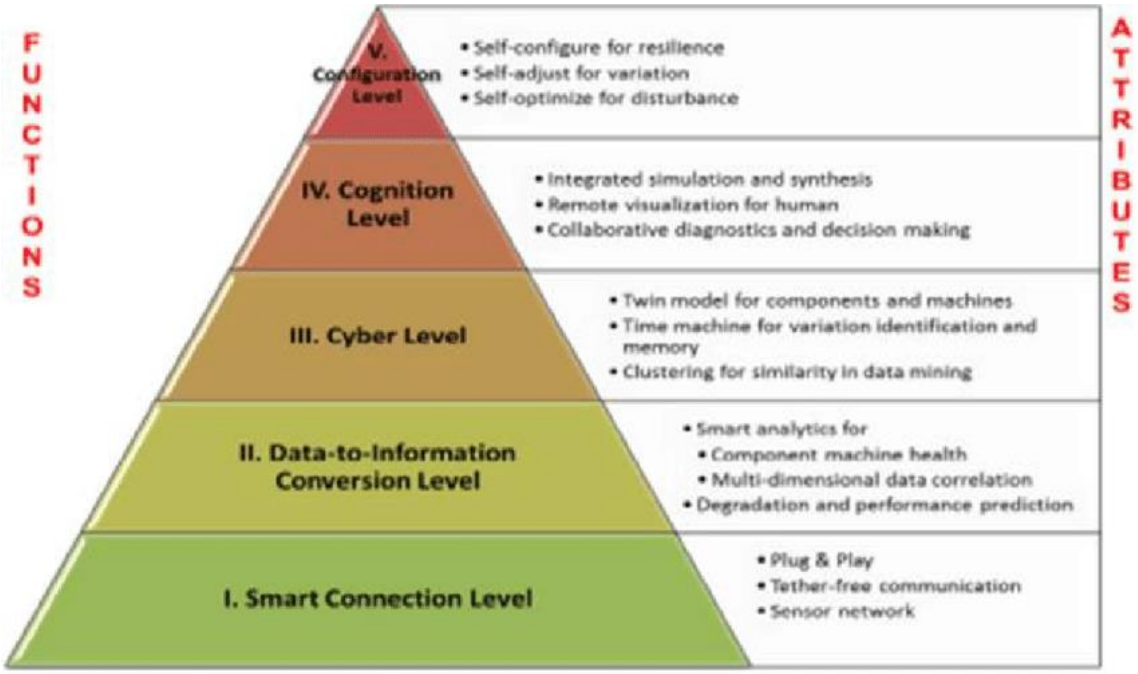
https://www.researchgate.net/publication/331600306_A_Distributed_Multi-Agent_Framework_for_Resilience_Enhancement_in_Cyber-Physical_Systems

2.3.2 5C ARCHITEKTÚRA

A **5C architektúra** a kiber-fizikai rendszerek (CPS) egyik alapvető modellje, amely az adatgyűjtéstől kezdve a döntéshozatalig a rendszeren belüli adatfeldolgozást és -kommunikációt szabályozza. A 5C modell az alábbi komponensekre épül, mindegyik egy-egy kulcsfontosságú feladatot lát el a rendszer működésében:

- **Connection (Kapcsolódás):** Ez a réteg biztosítja a kiber-fizikai rendszer eszközei közötti kapcsolatokat.
- **Cognition (Kogníció):** A kognitív réteg a begyűjtött adatokat elemzi és feldolgozza, hogy értékes információkat nyújtson.

- **Cyber (Kiber):** Ez a réteg a számítógépes rendszerek és alkalmazások működését felügyeli, és kezeli az adatokat a virtuális környezetben.
- **Control (Irányítás):** Ez a réteg felelős a valós idejű válaszokért és döntésekért. Az irányítási réteg valós időben reagál a kognitív rétegből származó információkra, és vezérli a rendszer működését.
- **Coordination (Koordináció):** A koordinációs réteg biztosítja a különböző rendszerkomponensek közötti szinkronizációt és a rendszer integrálását.



3. ábra 5C architecture for implementation of Cyber-Physical System.

https://www.researchgate.net/figure/C-architecture-for-implementation-of-Cyber-Physical-System_fig1_341493061

3 CPS RENDSZEREK FIZIKAI RÉTEGÉBEN HASZNÁLT PROTOKOLLOK

3.1 A GSM ALAPÚ TECHNOLÓGIÁK FEJLŐDÉSE

A GSM technológia kezdeti célja a digitális mobiltelefonos kommunikációs rendszer kialakítása volt. Az 1980-as évek végén kezdték el fejleszteni, és az első hivatalos szabványokat az 1990-es évek elején hozták létre. A GSM elsődleges előnyei közé tartozott a nagyobb adatátviteli sebesség, a megbízhatóság és az erősebb titkosítás a korábbi analóg rendszerekhez képest. A szabvány az 1G mobiltelefonhálózatokkal szemben egy teljesen digitális hálózati architektúrát vezetett be, amely az egész világon elterjedt, és azóta alapvetően meghatározta a mobiltelefonos kommunikáció fejlődését.[19]

A GSM eredetileg csak szöveges üzenetek (SMS) küldésére és hangalapú kommunikációra szolgált, de idővel az adatok gyorsabb, hatékonyabb átvitele és a különféle multimédiás szolgáltatások iránti igények is felmerültek.[20]

- GPRS és EDGE

A GSM fejlődését követően két fontos szabványt vezettek be, amelyek jelentősen megnövelték a mobil hálózatok adatátviteli sebességét. Az első jelentős előrelépés a GPRS (General Packet Radio Service) volt, amely lehetővé tette az adatcsomagok dinamikus átvitelét, nemcsak hang és szöveges üzenetek, hanem adatforgalom számára is. A GPRS alapvetően az IP-alapú adatátvitelt tette lehetővé a mobilhálózatokban, ezzel új lehetőségeket teremtve az internet és alkalmazásalapú szolgáltatások elérésére.[21]

A következő mérföldkő az EDGE (Enhanced Data rates for GSM Evolution) technológia bevezetése volt, amely tovább növelte az adatátviteli sebességet a GSM-hálózatokon belül. Az EDGE technológia segítségével a GSM-hálózatok képesek voltak gyorsabb adatátvitelre, és már olyan szolgáltatások is elérhetővé váltak, mint a mobilinternet böngészése és multimédiás üzenetek (MMS) küldése.[22]

- UMTS és HSPA

Bár a GPRS és az EDGE már jelentős előrelépést hoztak, a következő nagy fejlődést a harmadik generációs mobilkommunikációs rendszerek jelentették. Az UMTS (Universal Mobile Telecommunications System) és a hozzá kapcsolódó HSPA (High Speed Packet Access) szabványok bevezetésével lehetőség nyílt a szélessávú mobilinternet hozzáférésre, jelentősen megnövelve az adatátviteli sebességet és a hálózatok kapacitását.[23][24]

Az UMTS a GSM-hálózatok továbbfejlesztett verziója volt, amely már lehetővé tette a nagy sebességű adatátvitelt, és az első mobilvideóhívásokat is támogatta. A HSPA kiegészítő technológia, amely az UMTS hálózatok sebességét javította, a modern mobiladatforgalom egyik alappillérét képezte.

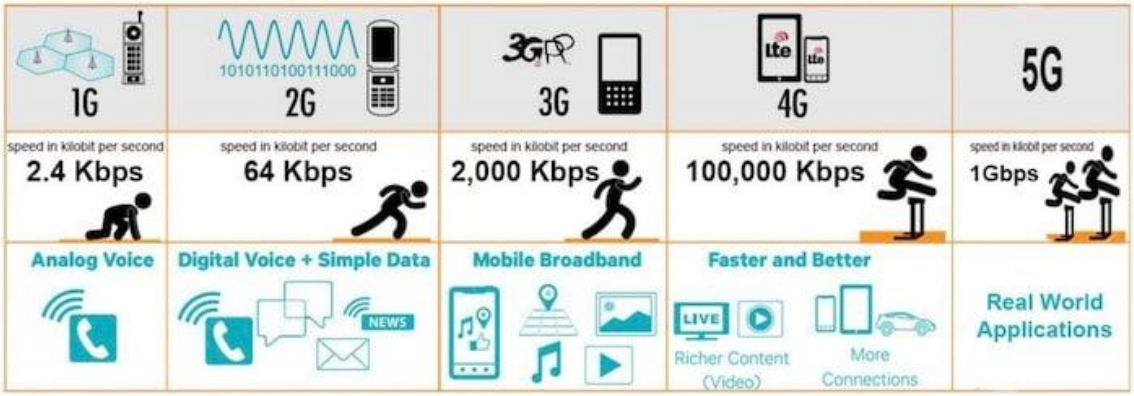
- LTE, 4G

A következő mérföldkő a 4G LTE (Long Term Evolution) technológia volt, amely gyökeresen megváltoztatta a mobil adatátvitelt. Az LTE gyors adatátviteli sebességet és alacsony késleltetést kínált, és lehetővé tette a széles körű alkalmazások, mint a HD videóhívások, zökkenőmentes mobilvideó streaming és a nagy sávszélességű internet-hozzáférés használatát. Az LTE technológia a mobilhálózatok számára új lehetőségeket teremtett, különösen az ipari és fogyasztói alkalmazásokban.[25]

- LTE-M és NB-IoT: Az IoT és CPS környezetekhez igazodó megoldások

Az LTE technológia újabb iterációi, mint az LTE-M és az NB-IoT, kifejezetten az IoT (Internet of Things) és a kiber-fizikai rendszerek igényeire lettek optimalizálva. Az LTE-M (Long Term Evolution for Machines) és az NB-IoT (Narrowband IoT) célja a nagy lefedettségű, energiatakarékos, és hosszú távú kapcsolat biztosítása alacsony sávszélességű eszközök számára. Ezek a megoldások ideálisak a kisebb adatforgalmat generáló eszközök számára, mint például az érzékelők, amelyek folyamatos adatokat küldenek és fogadnak a kiber-fizikai rendszerek vezérlőegységeivel.[26]

Az LTE-M és az NB-IoT technológiák különösen fontos szerepet játszanak a kiber-fizikai rendszerekben, mivel lehetővé teszik a valós idejű adatátvitelt alacsony energiafogyasztás mellett, és biztosítják a nagy lefedettséget, amit sok IoT alkalmazás igényel.



4. Ábra. Wireless Communication Technologies

https://ioarp.org/ioarp-admin-panel/upload/articles/1460357886_IDL-ICCN15-011.pdf (Fig. 1.)

3.2 CPS RENDSZEREKBEN HASZNÁLT PROTOKOLLOK

A fizikai réteg elsődleges feladata a bitek megbízható továbbítása két eszköz között egy meghatározott átviteli közegen keresztül. Ez a réteg felelős az adatok elektronikus vagy rádióhullámos jellé alakításáért, valamint az eszközök közötti tényleges kapcsolat létrehozásáért. Támogatja az adatátvitel különböző módjait, például a soros vagy párhuzamos, illetve szinkron vagy aszinkron kommunikációt. Emellett biztosítja a hordozó hozzáférés vezérlését (pl. mikor kezdhet el egy eszköz adatot küldeni), valamint definiálja a fizikai csatlakozók, jeltípusok, feszültségszintek és időzítések paramétereit, amelyek elengedhetetlenek a kommunikációs lánc többi rétege számára.

3.2.1 VEZETÉKES RENDSZEREKBEN HASZNÁLT PROTOKOLLOK

- **Modbus (RTU/TCP):** Egy nyílt ipari protokoll, amelyet főként PLC-k és egyéb vezérlők közötti kommunikációra használnak. Az RTU változat soros vonalon működik (pl. RS-485), míg a TCP változat Etherneten keresztül kommunikál. Egyszerű struktúrája miatt széles körben alkalmazott.
- **CAN (Controller Area Network):** Autóipari eredetű soros buszrendszer, amely determinisztikus üzenetkezelést tesz lehetővé. Kiemelkedően megbízható, időkritikus adatátvitelre optimalizált protokoll, széles körben alkalmazott ipari automatizálásban is.
- **OPC UA (Open Platform Communications Unified Architecture):** Egy magas szintű, platformfüggetlen protokoll, amely ipari rendszerek közötti adatcserét tesz lehetővé. Támogatja a hálózati biztonságot, valamint a strukturált és modellezett adatok átadását Ethernet-alapú környezetben.

- **EtherCAT (Ethernet for Control Automation Technology):** Nagy sebességű, determinisztikus Ethernet-alapú ipari protokoll. Valós idejű vezérlőrendszerekhez készült, és közvetlenül támogatja a szenzorok és aktuátorok szinkronizált működését.

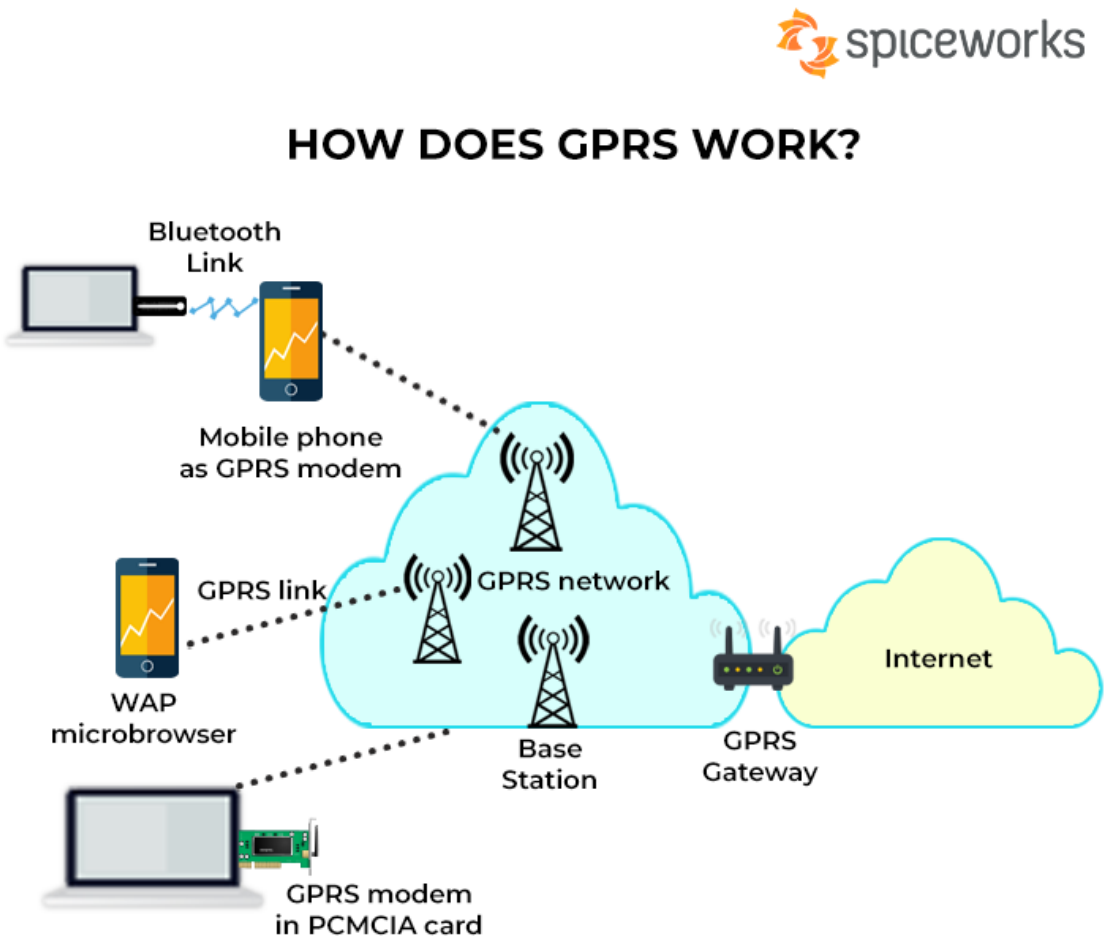
3.2.2 VEZETÉK NÉLKÜLI RENDSZEREKBEN HASZNÁLT PROTOKOLLOK

- **LoRa (Long Range):** Alacsony fogyasztású, nagy hatótávolságú vezeték nélküli protokoll, amely ideális választás kültéri környezetmonitorozási és mezőgazdasági CPS alkalmazásokhoz. Tipikusan kis mennyiségű adatot közvetít ritkán.
- **Zigbee (IEEE 802.15.4):** Rövid hatótávolságú, alacsony energiaigényű protokoll, mely elsősorban szenzorhálózatokban, okos otthonokban és ipari CPS rendszerekben használatos. Több csomópontból álló hálózatok építését teszi lehetővé.
- **Bluetooth Low Energy (BLE):** Egy energiatakarékos, rövid hatótávolságú protokoll, amely elsősorban mobil és hordozható eszközökhöz alkalmazható. Alkalmas egészségügyi, logisztikai és viselhető CPS eszközök kommunikációjára.
- **NB-IoT (Narrowband IoT):** Mobilhálózati technológiára épülő vezeték nélküli protokoll, amelyet kis mennyiségű adat, de nagy számú eszköz hosszú távú és megbízható kommunikációjára terveztek. Ideális például okosmérőkben és környezetmonitorozásban.
- **LTE-M (LTE Cat-M1):** Szintén mobilhálózati alapú megoldás, de nagyobb sávszélességet és alacsonyabb késleltetést kínál, mint NB-IoT. Alkalmas dinamikusabb, mozgó CPS alkalmazásokhoz (pl. járművek, egészségügyi monitorozás).

4 CPS RENDSZEREKBEN HASZNÁLT GSM PROTOKOLLOK

4.1 RÉGEBBI PROTOKOLLOK

- **GPRS (General Packet Radio Service):** A GPRS a GSM (2G) hálózatok kiterjesztéseként jelent meg az 1990-es évek végén, kereskedelmi forgalomban 2000 körül kezdett elterjedni. A GPRS elsőként tette lehetővé a csomagkapcsolt adatátvitelt mobilhálózatokon keresztül, így hatékonyabbá vált a kisebb adatmennyiségek küldése és fogadása. A rendszer úgy működik, hogy a GSM-csatornákat időosztásos módszerrel osztja fel a felhasználók között, lehetővé téve az osztott erőforrás-használatot.[21]

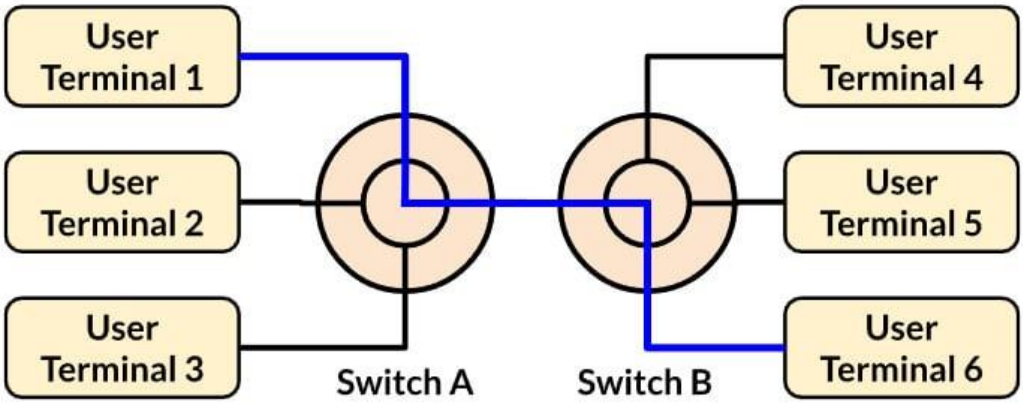


5. Ábra. How does GPRS work?

https://www.spiceworks.com/tech/networking/articles/what-is-gprs/

- **EDGE (Enhanced Data Rates for GSM Evolution):** Az EDGE a GPRS továbbfejlesztett változata, amelyet 2.75G-ként is szokás említeni. Először 2003 körül jelent meg kereskedelmi használatban. A technológia a GPRS-sel kompatibilis maradt, de újabb modulációs eljárásokat (8PSK) vezetett be, amelyek segítségével jelentősen növelni lehetett az adatátviteli sebességet. Ezzel lehetővé vált akár videóstream vagy nagyobb állományok átvitele a mobilhálózaton keresztül.[22]

- **CSD (Circuit Switched Data):** A CSD a GSM rendszerek legelső adatátviteli szolgáltatása volt, amely a klasszikus vezetékes modemekhez hasonlóan kapcsolt vonali kapcsolatot alkalmazott. Ez a technológia az 1990-es évek elején került bevezetésre, de már akkor is jelentős korlátai voltak, mivel a teljes GSM csatornát lefoglalta a kapcsolat időtartamára. Mivel nem volt hatékony a rendelkezésre álló sávszélesség kihasználása, fokozatosan háttérbe szorult.[29]



6. Ábra. Diagram of circuit switching network communication connecting user 1 and 6.

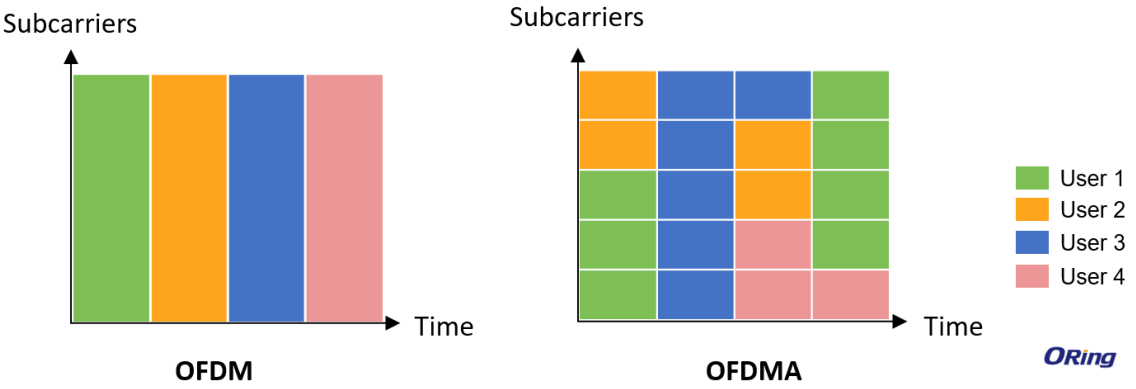
https://resources.pcb.cadence.com/blog/2024-all-about-circuit-switching-network-communication

	GPRS	EDGE	CSD
Hálózati generáció	**2G (GSM)**	**2.75G (GSM alapú)**	**2G (GSM)**
Megjelenés éve	**~2000**	**~2003**	**~1991**
Átviteli mód	**Csomagkapcsolt**	**Csomagkapcsolt**	**Kapcsolt vonali**
Elméleti maximális sebesség	**114 kbps**	**384 kbps**	**9.6 kbps**
Valós átviteli sebesség	**35–50 kbps**	**100–200 kbps**	**~9.6 kbps**
Moduláció	**GMSK**	**8PSK**	**-**
Kapcsolat típusa	**Megosztott**	**Megosztott**	**Folyamatos (lefoglalt)**
Kompatibilitás	**GSM alapú**	**GPRS-szel kompatibilis**	**GSM alapú**

4.2 ÚJFAJTA PROTOKOLLOK

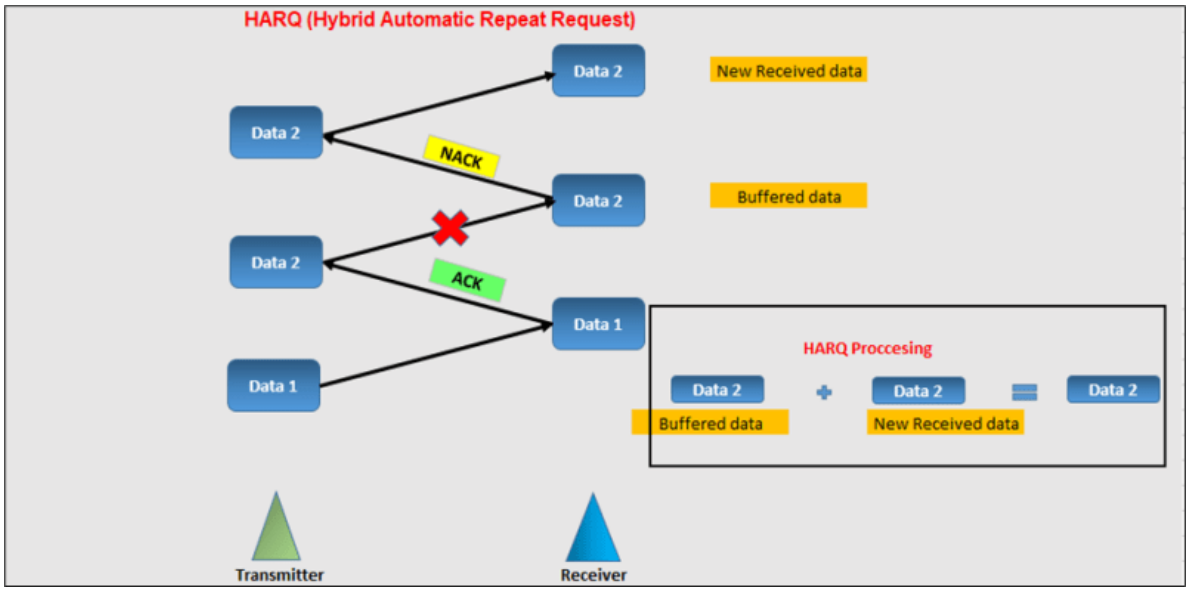
4.2.1 LTE-M

Fizikai réteg és moduláció: Az LTE-M hálózatok fizikai rétege ugyanúgy az OFDMA (Orthogonal Frequency Division Multiple Access) technológiát használja, mint az LTE, de az IoT alkalmazásokhoz szükséges sávszélességet és energiatakarékosságot figyelembe véve az LTE-M hálózatok kisebb adatmennyiségeket is képesek kezelni. A fizikai szinten az LTE-M a 1.4 MHz-es sávszélességet használja, amely lehetővé teszi a nagy hatótávolságú és alacsony sávszélességű adatátvitelt. A modulációs technika a QPSK (Quadrature Phase Shift Keying) vagy 16-QAM (Quadrature Amplitude Modulation) lehet, amely biztosítja a robusztus adatátvitelt különböző környezetekben, különösen akkor, amikor a jel erőssége gyengül vagy interferenciák lépnek fel. A csatorna kódolás és dekódolás a HARQ (Hybrid Automatic Repeat reQuest) mechanizmust alkalmazza, amely javítja az adatátvitel megbízhatóságát és csökkenti a hibaarányokat.[27]



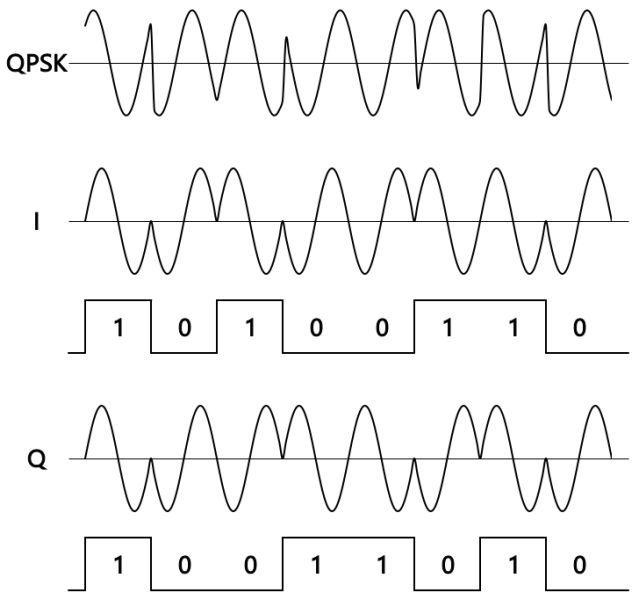
7. Ábra. Orthogonal frequency-division multiple access

https://oringnet.com/en/knowledge-base/how-does-wifi6-ofdma-work



8. Ábra. Hybrid Automatic Repeat Request (HARQ)

https://techlteworld.com/harq-hybrid-automatic-repeat-request-in-lte/



9. Ábra. Quadrature Phase-Shift Keying (QPSK)

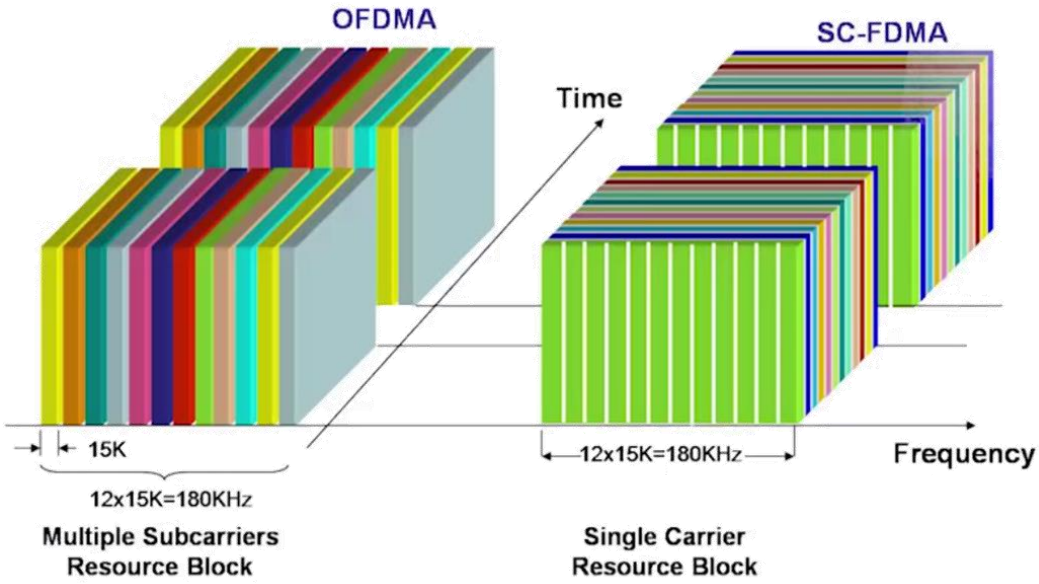
https://ensatellite.com/qpsk/

Hálózati erőforrás-kezelés: Az LTE-M az alacsonyabb energiafogyasztásra és a hosszú akkumulátor-élettartamra optimalizáltak. Ehhez a hálózatok az alvó módokat és az eszközök közötti diszkrét adatátviteli időszakokat használják. A hálózati erőforrások, mint például a PRB-k (Physical Resource Blocks) dinamikusan vannak kiosztva, figyelembe véve az eszközök igényeit, és az adatátvitelt gyakran kisebb időablakokban végzik.[27]

Rádiós interfész és sávszélesség-kezelés: Az LTE-M az alap LTE hálózaton kívül működik, de a rádiós interfész specifikus módosításai segítenek az eszközök közötti hatékony kommunikációban. A sávszélességkezelés az adattovábbítás során a kisebb csomagok és az alacsonyabb adatátviteli sebesség révén csökkenti a szükséges rádiós spektrumot. Az LTE-M emellett képes a jobb lefedettséget biztosítani a mélyebb beltéri helyeken és a távolabbi területeken, az alacsonyabb jelerősség mellett is.[27]

4.2.2 NB-IOT:

Fizikai réteg és moduláció: Az NB-IoT szintén az OFDMA technológiát használja, de a sávszélesség jelentősen csökkentett, és csak 200 kHz-et használ a kommunikációra. Ez lehetővé teszi a hálózatok számára, hogy széleskörű lefedettséget biztosítsanak az alacsony sebességű adatátvitel esetén. A fizikai rétegben az NB-IoT az SC-FDMA (Single-Carrier Frequency Division Multiple Access) modulációt alkalmazza, amely az alacsonyabb szintű energiafogyasztásra van optimalizálva, és kifejezetten a távoli, ritkán kommunikáló eszközökhöz tervezték.[28]



10. Ábra. Simplified LTE Architecture

https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2014_2/rafaelreis/ofdma_scfdma.html

Adatátvitel és hálózati erőforrás-kezelés: Az NB-IoT a hálózati erőforrásokat rendkívül hatékonyan kezeli. A kisebb adatcsomagok és az alacsony sebességű adatátvitel révén az NB-IoT lehetővé teszi a hosszú akkumulátor-élettartamot. A fizikai rétegben az NB-IoT az alacsony jelerősségű és alacsony sávszélességű adatátvitelt támogatja, miközben csökkenti a szükséges rádiós spektrumot. Az eszközök számára beállíthatók az alvó módok és a minimális aktiválási idő, hogy maximális energiahatékonyságot érjenek el.[28]

Jelkezelés és hálózati lefedettség: Az NB-IoT kiemelkedő képessége a mélyebb beltéri lefedettség. Az alacsony sávszélesség és a nagyobb hatótávolságok révén képesek az NB-IoT eszközök kapcsolatot fenntartani akkor is, ha a jel erősen gyengül, például épületeken belül vagy föld alatti alkalmazásoknál. A csatornák és frekvenciák kifejezetten úgy lettek kialakítva, hogy a lehető legnagyobb lefedettséget biztosítsák a különböző környezetekben.[28]

	LTE-M	**NB-IoT**
Adatátviteli sebesség	**Magasabb adatátviteli sebesség (kb. 1 Mbps)**	**Alacsonyabb adatátviteli sebesség (kb. 100 kbps)**
Késleltetés	**Alacsony késleltetés (20-50 ms)**	**Magasabb késleltetés (kb. 1-2 másodperc)**

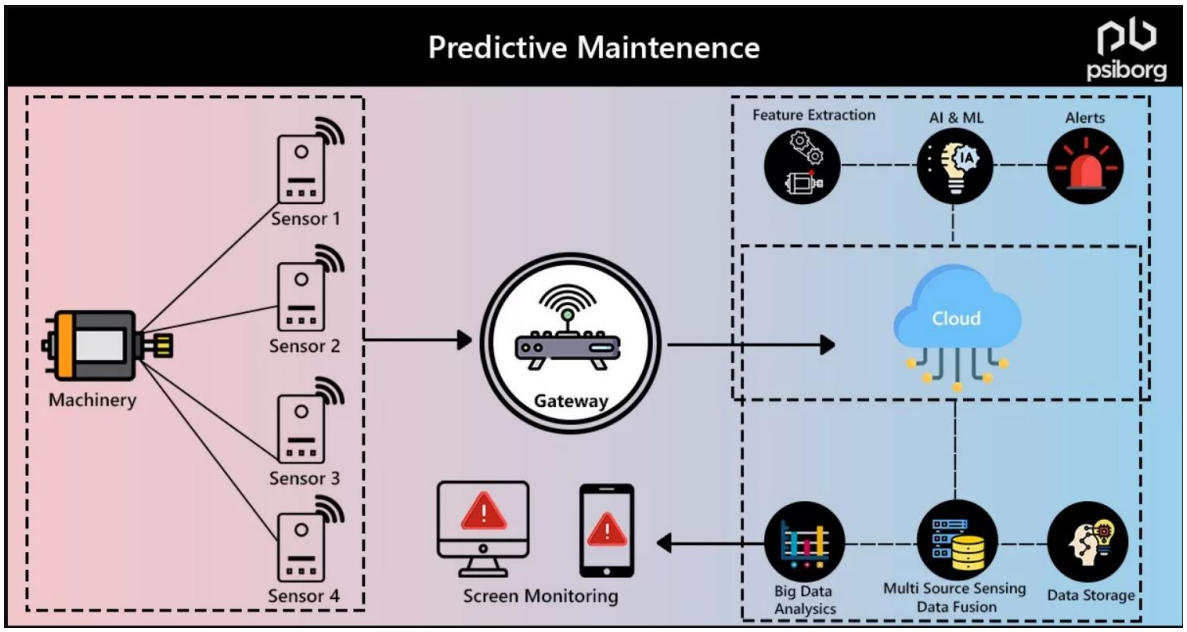
Energiahatékonyság	**Közepes energiafogyasztás**	**Nagyon alacsony energiafogyasztás, hosszú akkumulátor-élettartam**
Lefedettség	**Jó városi és ipari lefedettség, de nem annyira széleskörű, mint az NB-IoT**	**Kiváló lefedettség, különösen nehezen elérhető helyeken (pl. épületek, alagutak)**
Sávszélesség	**Szélesebb sávszélesség, ideális magas adatforgalomhoz**	**Keskeny sávszélesség, ideális alacsony adatforgalomhoz**
Valós idejű kommunikáció	**Alkalmas valós idejű kommunikációra**	**Nem ideális valós idejű kommunikációra**
Alkalmazási területek	**Ipari IoT, okos városok, eszközök közötti nagy adatforgalom**	**Szenzorok, mérőórák**

5 ALKALMAZÁSI LEHETŐSÉGEK A KIBER-FIZIKAI RENDSZEREKBEN

5.1 IPARI AUTOMATIZÁLÁS LS GYÁRTÁSI RENDSZEREK[27][28]

- **NB-IoT:**

  - **Prediktív karbantartás:** Az ipari rendszerek prediktív karbantartásának egyik kulcsfontosságú eleme az érzékelők folyamatos adatgyűjtése. Az alacsony energiafogyasztás és a hosszú akkumulátor-élettartam révén az NB-IoT kiváló választás a gépek és berendezések monitorozására, különösen olyan helyszíneken, ahol hosszú távú távfelügyelet szükséges.



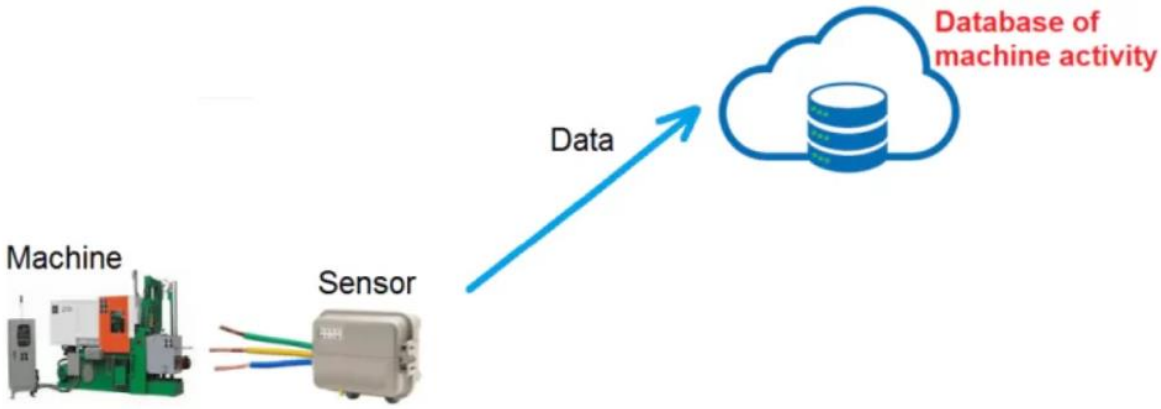
11. Ábra. Predective maintenence

https://psiborg.in/predictive-maintenance-using-iot/

- **Minőségellenőrzés automatizálása:** Az NB-IoT ideális megoldás lehet a minőségellenőrzési rendszerekhez, mivel a rendszer alacsony adatátviteli sebességet igényel, viszont folyamatos működést biztosít az alacsony energiafogyasztás és hosszú akkumulátor-élettartam révén.

- LTE-M:

- **Valós idejű gyártásfelügyelet:** A gyors adatátvitel és a valós idejű kommunikáció elősegíti a gyártósorok állapotának monitorozását, különösen olyan esetekben, ahol a gépek közötti folyamatos adatcsere szükséges a hatékonyság növelése érdekében.



12. Ábra. Machine monitoring and data collection

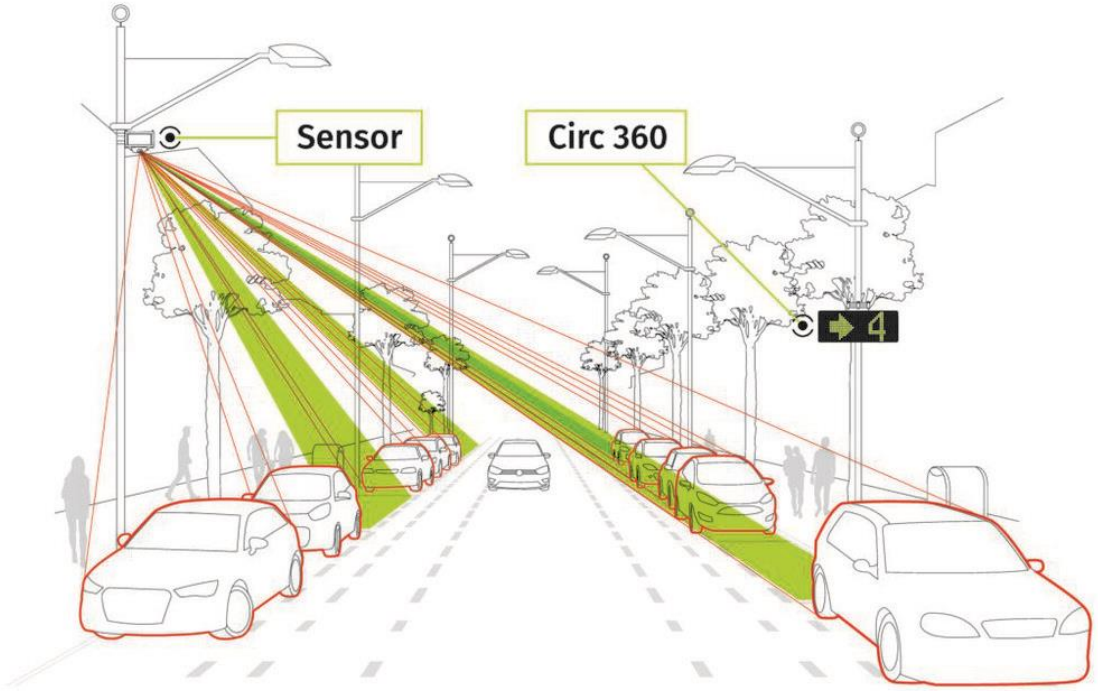
https://leanworxcloud.com/remote-machine-monitoring/

- **Eszközök mobilitása és újrakonfigurálása:** Az LTE-M előnyös lehet a dinamikus gyártási eszközök számára, mivel a hálózati lefedettség széleskörű és a rendszer képes gyors adatátvitelre, amely lehetővé teszi a folyamatos vezérlést és beállítást.

5.2 OKOS VÁROSOK ÉS KÖZLEKEDÉSI RENDSZEREK[27][28]

- NB-IoT:

- **Intelligens parkolás:** Az NB-IoT megfelelő a parkolási rendszerekhez, ahol az alacsony adatsebesség és alacsony energiafogyasztás kulcsfontosságú. A rendszer folyamatos adatgyűjtést végez, és nagy lefedettséget biztosít az alacsony adatátvitellel rendelkező parkolóhelyek monitorozásához.



13. Ábra. Smart Parking

https://www.cleverciti.com/en/resources/blog/how-does-smart-parking-work

- **Közvilágítás vezérlése:** A közvilágítási rendszerek számára az NB-IoT alkalmazása ideális, mivel alacsony adatsebességgel működik, és a hosszú akkumulátor-élettartam miatt ideális a folyamatos működésre, különösen olyan helyszíneken, ahol a költségek minimalizálása fontos.

- LTE-M:

- **Forgalomirányító rendszerek**
- **Tömegközlekedési eszközök nyomon követése**

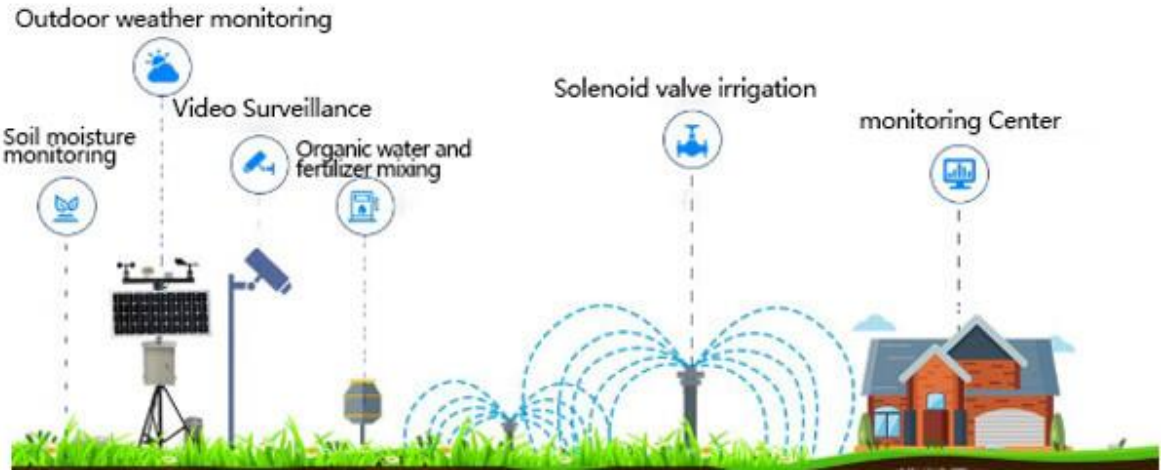
5.3 KÖRNYEZETMONITOROZÁSI ÉS MEZŐGAZDASÁGI ALKALMAZÁSOK[27][28]

- LTE-M:

- **Kártevő- és növénybetegség-felderítés:** Az LTE-M nagy adatsebessége és megbízhatósága előnyös lehet a kártevők vagy betegségek korai felismerésében, mivel gyors képfeldolgozást és adatátvitelt igényel, amely a növények állapotának gyors elemzését lehetővé teszi.

- NB-IoT:

- **Légköri és hőmérsékleti monitorozás:** Az alacsony adatsebesség és a nagy lefedettség ideális választás a légköri és hőmérsékleti adatok gyűjtésére, mivel a rendszer az egész földrajzi területet lefedheti, miközben biztosítja a szükséges adatátvitelt.
- **Talajnedvesség-figyelés:** Az NB-IoT tökéletes választás a talajnedvesség monitorozásához, mivel a szenzorok hosszú ideig működhetnek, és az alacsony adatátviteli sebesség lehetővé teszi a költséghatékony adatgyűjtést a mezőgazdasági területeken.



14. Ábra. The implementation of a scientific automated irrigation system

https://www.renkeer.com/soil-moisture-sensor-for-irrigation/

- **Árvíz- és vízminőség-figyelés:** Az árvíz- és vízminőség-figyelő rendszerek számára az NB-IoT ideális, mivel hosszú távú működést biztosít alacsony adatsebességgel és minimális energiafogyasztással, miközben széles területen biztosítja a kapcsolatot.

5.4 EGÉSZSÉGÜGYI RENDSZEREK ÉS TÁVFELÜGYELET[27]

- LTE-M:

- **Mentőszolgálat támogatása**: A mentőautókban lévő eszközök gyors adatátvitelét segíti az LTE-M, amely lehetővé teszi a valós idejű helymeghatározást és az orvosi adatok gyors szállítását az egészségügyi központok felé.

5.5 RÉGEBBI GSM TECHNOLÓGIÁK ALKALMAZÁSA CPS RENDSZEREKBEN[30][21][22]

A korai GSM-alapú technológiák, mint a GPRS, EDGE és CSD, még mindig jelen vannak bizonyos CPS rendszerekben, különösen olyan helyeken, ahol modern hálózati infrastruktúra nem elérhető, vagy ahol a meglévő rendszerek hosszú távú működése kulcsfontosságú. Ezek az alacsony sávszélességű, megbízható és széles körben támogatott technológiák különösen előnyösek lehetnek egyszerű adatkommunikációs feladatokhoz.

A. **GPRS (General Packet Radio Service)**
   - **Ipari rendszerek:** Távoli vezérlésű PLC-k és SCADA rendszerek, ahol alacsony sávszélesség is elegendő.
   - **Közlekedés:** Egyszerű járműkövetési rendszerek, amelyek időszakos adatküldést igényelnek.
   - **Energiaipar:** Alállomások és okos mérők GPRS-alapú adatátvitellel.

B. **EDGE (Enhanced Data rates for GSM Evolution)**
   - **Mezőgazdaság**: Távoli szenzorok és egyszerű gépmonitorozás mobilhálózaton keresztül.
   - **Környezetmonitorozás**: Időjárásállomások, levegőminőség-érzékelők, melyek nem igényelnek valós idejű kapcsolatot.
   - **Biztonságtechnika**: Régebbi biztonsági rendszerek (pl. kamerák vagy riasztók), amelyek időszakos frissítést küldenek.

C. **CSD (Circuit Switched Data)**
   - **Hagyományos automatizálási rendszerek:** Klasszikus gyártóberendezésekhez kapcsolódó GSM modemek.
   - **Rural IoT alkalmazások:** Olyan távoli vidéki környezetek, ahol csak 2G szolgáltatás érhető el.
   - **Egészségügy:** Régi generációs távdiagnosztikai eszközök, amelyek minimális adatátvitel mellett is működőképesek.

6 TESZT

- Nordic Semiconductor – LTE-M vs NB-IoT:

A Nordic Semiconductor blogbejegyzésében bemutatott teszt célja annak megértése volt, hogy az LTE-M és az NB-IoT hogyan teljesítenek különböző távolságoknál, valamint a két technológia energiafogyasztásának alakulása a távolság függvényében. A teszt során a jelerősséget, a válaszidőt és a kapcsolódási stabilitást mérték, amelyeket az alábbiak szerint összegeztek:

- **Energiafogyasztás különbségek:** Az LTE-M alacsonyabb energiafogyasztást mutatott, különösen akkor, amikor a távolság kicsi volt, mivel alacsonyabb adatsűrűséget igényel. Az NB-IoT azonban előnyösebb volt akkor, amikor az eszközök nagyobb távolságot kellett áthidaljanak, mivel erősebb jel- és lefedettségi képességekkel rendelkezik.
- **Alkalmazás területek:** Az LTE-M-et ajánlják olyan alkalmazásokhoz, ahol az eszközök gyors kommunikációra képesek, például real-time alkalmazások, biztonsági rendszerek, stb. Az NB-IoT inkább alacsonyabb adatsebességet igénylő, de több eszközt kezelő alkalmazások számára megfelelő, mint például vízmérők vagy szenzorhálózatok.
- **Teljesítmény és Lefedettség:** Az NB-IoT jobb teljesítményt mutatott sűrűn beépített környezetekben, míg az LTE-M sikeresebben működött nyílt terepen és kisebb távolságokon.

	LTE-M	NB-IoT
Also known as	“eMTC”,”LTE Cat-M1”	“LTE Cat-NB1” (3GPP rel 13) - "LTE Cat-NB2" (3GPP rel 14)
Bandwidth	1.4 MHz	200 kHz
Max Throughput (DL/UL)	300/375 kbps	30/60 kbps (NB1) - 127/169 kbps (NB2)
Range	Up to 4x	Up to 7x
Mobility/cell re-selection	Yes	Limited
Frequency deployment	LTE In-band	LTE In-band, guard band and GSM (Global System for Mobile) re-purposing
Deployment density	Up to 50,000 per cell	Up to 50,000 per cell
Module size	Suitable for wearables	Suitable for wearables
Power consumption	Up to 10 years of battery lifetime	Up to 10 years of battery lifetime

15. Ábra. Difference between LTE-M and NB-IoT

https://devzone.nordicsemi.com/nordic/nordic-blog/b/blog/posts/ltem-vs-nbiot-field-test-how-distance-affects-power-consumption

IRODALOMJEGYZÉK

[1] E. A. Lee, "Cyber-Physical Systems: Design Challenges," in *Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, 2008, pp. 363-369.

[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-Physical Systems: The Next Computing Revolution," in *Proceedings of the 47th IEEE International Conference on Design Automation*, 2010, pp. 731-736.

[3] L. Zhao and D. Li, "A Survey of Cyber-Physical Systems Architectures," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 72-80, Jan. 2017.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[5] F. Xia, L. Zhu, and J. Ma, "Internet of Things (IoT): A survey on enabling technologies, protocols, and applications," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 1-16, Dec. 2015.

[6] E. Vasilenko, V. Alexandrov, and A. Kravtsov, "Energy Efficient Communication in Cyber-Physical Systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 1875-1882, March 2018.

[7] D. R. Smith, "High-speed data transmission for industrial automation systems," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 3, pp. 1234-1245, March 2020.

[8] J. M. Lee, "Low-power sensor communication protocols in IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 1839-1847, July 2021.

[9] A. K. Singh et al., "Real-time data processing and low-latency systems for autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5512-5523, June 2021.

[10] S. Patel, "Communication infrastructures for low-latency CPS applications," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 2893-2902, May 2021.

[11] C. J. Wang, "Energy efficiency in wireless CPS networks," *IEEE Access*, vol. 9, pp. 4671-4682, 2021.

[12] L. Zhang and R. H. Liu, "Energy-aware data transmission strategies for CPS systems," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 738-746, February 2022.

[13] K. H. Lee, "Battery-life optimization in CPS networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 322-330, November 2021.

[14] M. T. Valente et al., "Wireless communication in mobile CPS applications," *IEEE Wireless Communications Letters*, vol. 9, no. 12, pp. 1987-1992, December 2020.

[15] H. N. Oskarsson and M. G. Bertozzi, "Network coverage and performance in IoT-enabled CPS," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2111-2122, May 2021.

[16] A. M. Zhang, "Designing network coverage strategies for CPS systems," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 7, pp. 2045-2052, July 2021.

[17] T. W. Shiu, "Protocoll selection for IoT-based CPS applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 1989-2002, 2021.

[18] Budi Mulyanti, „Development of Cyber-Physical System (CPS) implementation in industry 4.0” ResearchGate https://www.researchgate.net/publication/341493061_Development_of_Cyber-Physical_System_CPS_implementation_in_industry_40

[19] *"GSM,"* Wikipédia [Online]. Available: https://hu.wikipedia.org/wiki/GSM

[20] *"GPRS,"* Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/GPRS

[21] *"EDGE (telecommunication),"* Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/EDGE_(telecommunication)

[22] *"High Speed Packet Access,"* Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/High_Speed_Packet_Access

[23] *"Universal Mobile Telecommunications System,"* Wikipedia. [Online]. Available: https://hu.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

[24] *"4G,"* Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/4G

[25] *"LTE Cat M,"* u-blox, [Online]. Available: https://www.u-blox.com/en/technologies/lte-cat-m [Accessed: Apr. 29, 2025].

[26] Onomondo, "LTE-M IoT Guide: Everything You Need to Know," *Onomondo Blog*, Apr. 2023. [Online]. Available: https://onomondo.com/blog/lte-m-iot-guide/

[27] Onomondo, "What is NB-IoT? A Definitive Guide," *Onomondo Blog*, Apr. 2023. [Online]. Available: https://onomondo.com/blog/what-is-nb-iot-definitive-guide/#under-the-hood-nb-io-t-technology-and-functionality

[28] GeeksforGeeks, "Circuit Switching in Computer Network," *GeeksforGeeks*, [Online]. Available: https://www.geeksforgeeks.org/circuit-switching-in-computer-network/?ref=rbp

[29] A. Dsouza, "What is GPRS (General Packet Radio Service)?", *Spiceworks*, Apr. 4, 2023. [Online]. Available: https://www.spiceworks.com/tech/networking/articles/what-is-gprs/

2.50. IoT hálózatok biztonsági kihívásai és megoldásai ipari környezetben

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF COMPUTER SCIENCE

IoT hálózatok biztonsági kihívásai és megoldásai ipari környezetben

Féléves feladat Ipar 4.0 technológiák (GKNB_INTM087) tárgyból

Bigun Jázmin
[redacted]
Gazdaságinformatikus BSs
Gépészmérnöki, Informatikai és Villamosmérnöki Kar

Tartalom

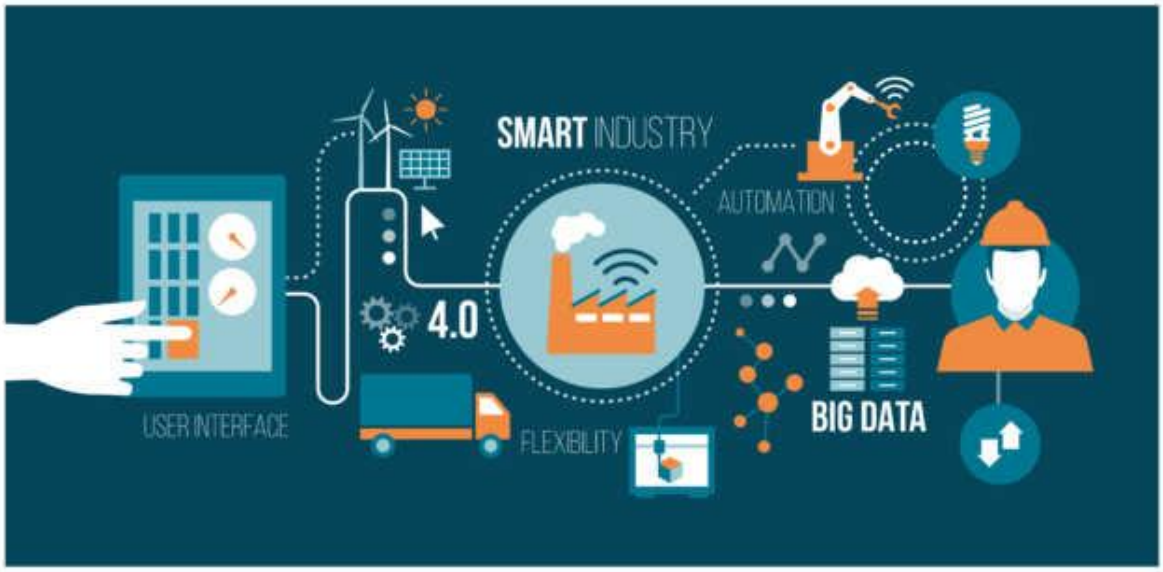
1. Bevezetés ... 3
2. Ipari IoT rendszerek és alkalmazási környezetük ... 3
2.1. A IIoT szerepe az Ipar 4.0-ban ... 4
2.2. A IIoT architektúra fő elemei ... 5
2.3. Tipikus ipari alkalmazások ... 6
2.4. A biztonság technikai kihívásai a IIoT-ben ... 6
3. Sebezhetőségek és támadási felületek ipari IoT környezetben ... 7
3.1. Gyenge hitelesítés és alapértelmezett jelszavak ... 7
3.2. Elavult szoftverek és frissítések hiánya ... 7
3.3. Nem megfelelő titkosítás és adatvédelem ... 8
3.4. Láthatóság hiánya és eszközkezelés problémái ... 9
4. Biztonsági kihívások ipari környezetben ... 10
4.1. Botnetek és DDoS támadások ... 10
4.2. Adatszivárgás és adatlopás ... 11
4.3. Fizikai hozzáférés és manipuláció ... 12
4.4. Szabályozási és jogi kihívások ... 13
5. Védekezési lehetőségek ipari IoT rendszerekben ... 13
5.1. Eszközök rendszeres frissítése ... 13
5.2. Erős jelszavak és többfaktoros hitelesítés ... 13
5.3. Adatok titkosítása és biztonságos kommunikáció ... 14
5.4. Hálózati szegmentáció és hozzáférés-szabályozás ... 15
5.5. Folyamatos monitorozás és anomália-észlelés ... 15
6. Szabályozási környezet ipari IoT rendszerekben ... 16
6.1. A NIS2 irányelv hatása ... 16
6.2. Magyarországi megfelelés és kihívások ... 16
7. Jövőbeli irányok az ipari IoT biztonságában ... 17
7.1. Prediktív biztonság és gépi tanulás ... 18
7.2. Zero Trust modell alkalmazása ... 18
8. Következtetések ... 19
Források: ... 20

1. Bevezetés

Az Internet of Things (IoT) technológia robbanásszerű fejlődése alapjaiban alakította át az ipari termelést és informatikai infrastruktúrákat. Az Ipar 4.0 korszakában a gyártósorok, érzékelők, robotkarok és gépi látással rendelkező beágyazott rendszerek egy intelligens, összekapcsolt hálózat részeként működnek – ez az ipari IoT (Industrial Internet of Things, IIoT). Ezek a technológiák egyre gyakrabban kiberfizikai rendszereket (Cyber-Physical Systems, CPS) alkotnak, ahol a fizikai folyamatokat digitális eszközök irányítják és figyelik meg.

Ezek rendszerek biztonsága azonban még nem tart lépést az elterjedtséggel. Az ipari IoT hálózatok, számos sebezhetőséggel rendelkeznek: gyenge hitelesítési mechanizmusokkal, elavult firmware-ekkel, hiányos titkosítással vagy nem megfelelő hálózati szegmentációval. Egy sikeres támadás nemcsak az informatikai infrastruktúrára jelent veszélyt, hanem közvetlenül fizikai károkat is okozhat.

A dolgozat célja, hogy részletesen bemutassa az ipari környezetben működő IoT rendszerek biztonsági kihívásait, azok lehetséges támadási felületeit, és feltárja azokat a gyakorlati és szabályozási megoldásokat, amelyek hozzájárulhatnak a biztonságosabb működéshez. A dolgozat a témát technikai szempontból, szűkített kontextusban tárgyalja, kiemelve a beágyazott rendszerek, hálózati kommunikációs protokollok és prediktív monitoring szerepét a védekezésben.



Ipari IoT

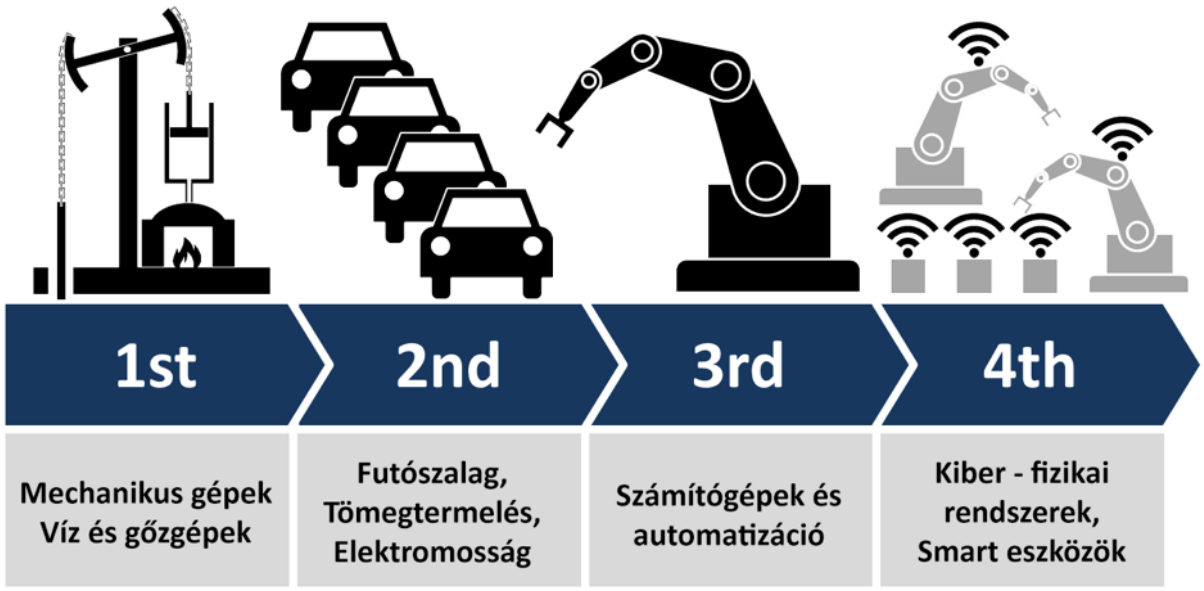
2. Ipari IoT rendszerek és alkalmazási környezetük

Az ipari IoT (IIoT) a klasszikus IoT technológia továbbfejlesztett, ipari célú alkalmazása, amely az Ipar 4.0 jövőjében kiemelkedően fontos szerepet játszik. Az IIoT célja, hogy a fizikai termelési folyamatokat összekapcsolja digitális hálózatokkal és intelligens adatelemző rendszerekkel. A szenzorhálózatok, vezérlők és beágyazott eszközök együttese lehetővé teszi a valós idejű adatgyűjtést, azonnali döntéshozatalt és automatizált beavatkozást. Ezeket azonban egyre komplexebb biztonsági kihívások közepette kell működtetni.

2.1. A IIoT szerepe az Ipar 4.0-ban

Az ipari Internet of Things (Industrial Internet of Things, IIoT) az Ipar 4.0 egyik alappillére, amely a gyártási és termelési rendszerek digitalizálására törekszik. A klasszikus IoT-tól eltérően a IIoT kifejezetten ipari környezetre optimalizált technológiákat alkalmaz, célja pedig a fizikai folyamatok valós idejű monitorozása, automatizálása és optimalizálása.

A IIoT rendszerek lehetővé teszik az összekapcsolt eszközök (gépek, szenzorok, aktuátorok) közötti kommunikációt, valamint az adatok továbbítását központi elemző rendszerek felé, például felhőszolgáltatásokba vagy lokális adatfeldolgozókba. Ezáltal javul a döntéstámogatás, csökken a karbantartási költség, és növekszik a termelés hatékonysága.

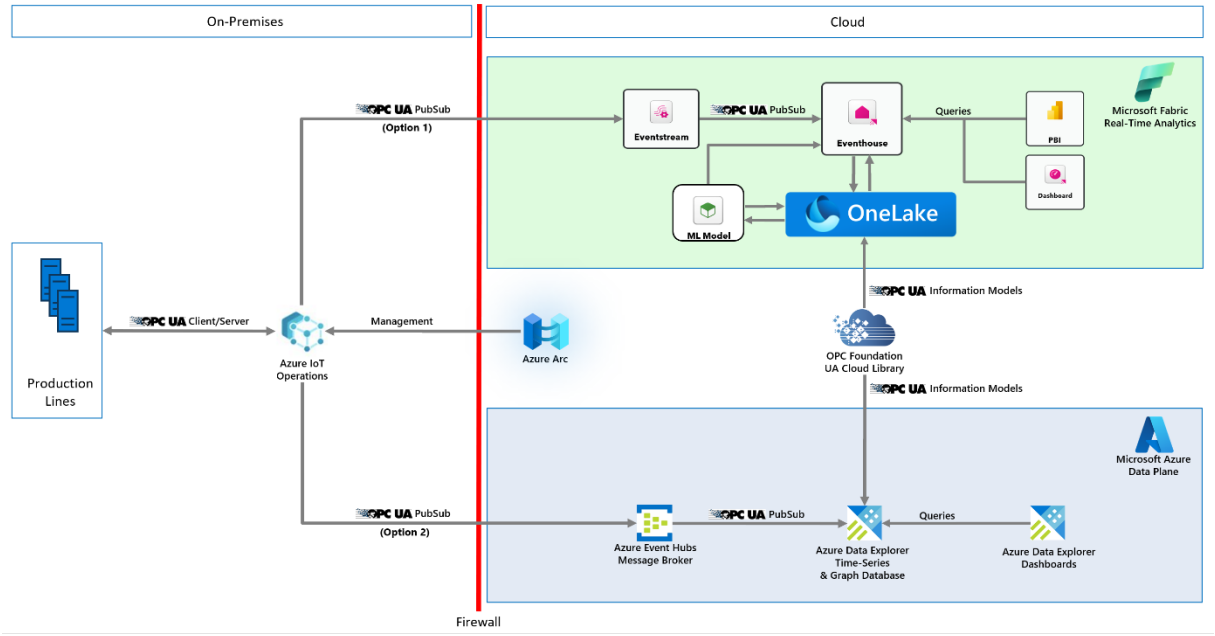


Ipar fejlődése

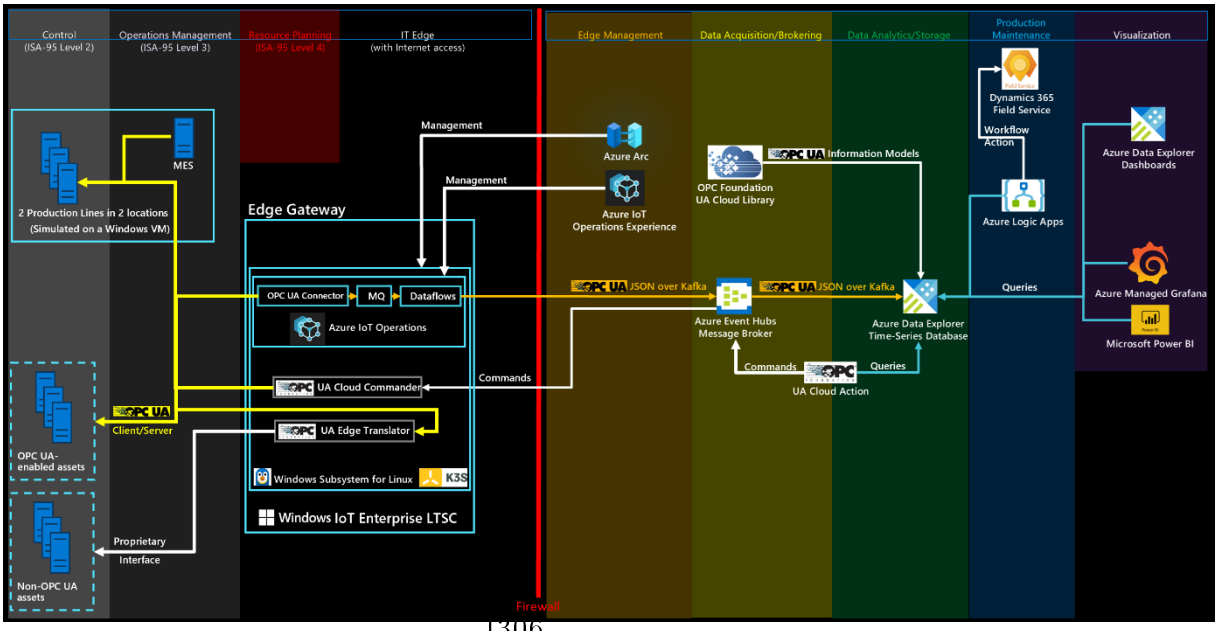
2.2. A IIoT architektúra fő elemei

A IIoT rendszerek általában több rétegből állnak, amelyeket hierarchikusan vagy hálózatos módon szerveznek:

- Peremeszközök (edge devices): Szenzorok, vezérlők, mikrokontrollerek, amelyek fizikai jeleket mérnek (pl. hőmérséklet, rezgés, áram).
- Gateway-ek: Ezek az eszközök gyűjtik az adatokat az érzékelőktől, előfeldolgozást végezhetnek, és továbbítják az információt magasabb szintek felé.
- Kommunikációs infrastruktúra: Itt jellemző protokollok például az MQTT, OPC UA, 5G vagy Ethernet TSN. Ezek determinisztikus és valós idejű adatátvitelt tesznek lehetővé ipari környezetben.
- Felhő vagy lokális adatfeldolgozás: A begyűjtött adatokat adatbázisokba és analitikai rendszerekbe továbbítják, ahol prediktív karbantartás, gépi tanulás és vizualizáció történhet.



Egyszerűsített architektúra



Az Azure opciót bemutató részletes architektúr

2.3. Tipikus ipari alkalmazások

A IIoT rendszerek számos alkalmazási területen jelen vannak, különösen a gyártás és logisztika automatizálásában:

- **Okosgyárak:** Az intelligens gyártósorok valós időben igazodnak a termelési igényekhez.
- **Prediktív karbantartás:** Az érzékelők segítségével előrejelezhető egy gép meghibásodása, így elkerülhető az állásidő.
- **SCADA rendszerek:** Folyamatirányító rendszerek, amelyek központilag vezérlik az egész gyártási folyamatot.
- **AGV-k (Automated Guided Vehicles):** Önállóan közlekedő járművek, amelyek anyagmozgatást végeznek gyárakban.

2.4. A biztonság technikai kihívásai a IIoT-ben

A IIoT rendszerek speciális biztonsági kihívásokkal néznek szembe, mivel fizikai és digitális elemeket is tartalmaznak, amelyek folyamatos kapcsolatban állnak egymással:

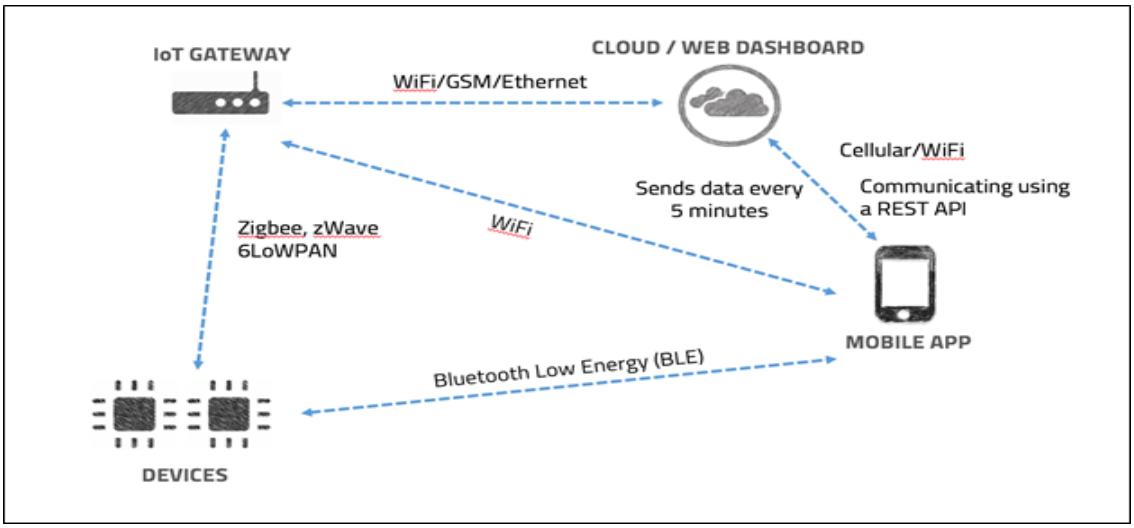
- **Kritikus működés:** Sok esetben emberi életek vagy jelentős pénzügyi kockázat függ a rendszerek megbízhatóságától.
- **Valós idejű működés:** A hálózat késleltetése vagy meghibásodása súlyos következményekkel járhat.
- **Beágyazott eszközök korlátozottsága:** Alacsony számítási kapacitás miatt nehezebb klasszikus védekezési mechanizmusokat (pl. titkosítás, tűzfal) alkalmazni.
- **Heterogén rendszerek:** Sokszor különböző gyártók eszközei kommunikálnak, eltérő protokollokkal és biztonsági szintekkel.

Az IoT és az IT biztonság

3. Sebezhetőségek és támadási felületek ipari IoT környezetben

3.1. Gyenge hitelesítés és alapértelmezett jelszavak

Számos ipari IoT eszköz (például vezérlők, szenzorhubok, SCADA terminálok) gyárilag beállított, nyilvánosan ismert jelszavakkal kerül forgalomba. Gyakori, hogy ezek a jelszavak nem kerülnek megváltoztatásra, ezáltal a támadók könnyedén hozzáférést szerezhetnek az eszközökhöz, akár teljes hálózati szintű irányítást is átvéve.



IoT-eszköz támadási felülete

3.2. Elavult szoftverek és frissítések hiánya

Az IIoT eszközök egy része nem rendelkezik automatikus frissítéssel, vagy a gyártó nem biztosít biztonsági frissítéseket. Sok esetben hiába van lehetőség frissítésre a felhasználó mégis elfelejti azokat. Emiatt az eszközök hosszú ideig ki lehetnek téve támadásoknak, ami komoly veszélyt jelent az ipari IoT rendszereknek.

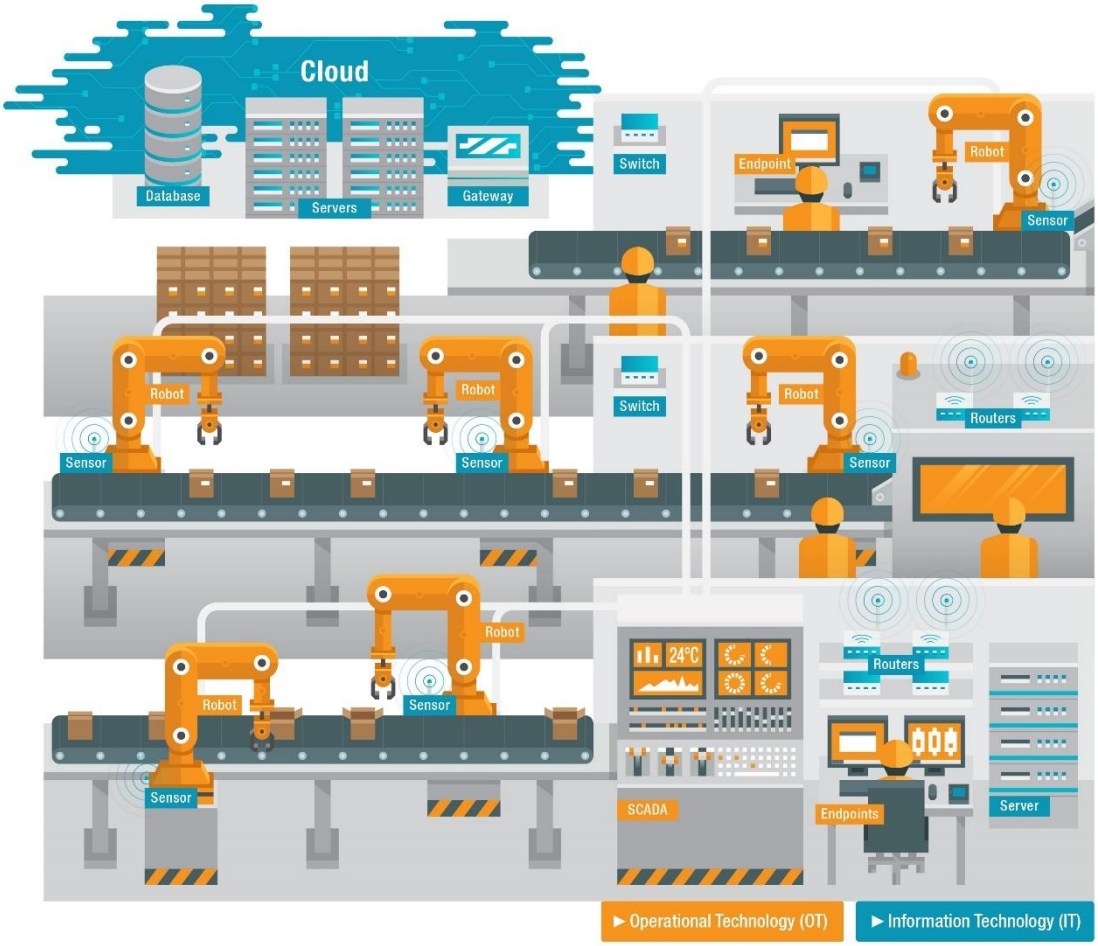
3.3. Nem megfelelő titkosítás és adatvédelem

Az adatvédelem kulcsfontosságú az IIoT környezetekben, mégis számos eszköz nem alkalmaz megfelelő titkosítási módszereket. A rendszerek érzékeny adatokat kezelhetnek (termelési paramétereket, energiafogyasztási adatokat, gépállapot-információkat), amelyeket gyakran titkosítás nélkül továbbítanak. A nem védett kommunikációs csatornák lehetőséget adnak lehallgatásra, adatmanipulációra vagy akár irányítási parancsok meghamisítására. Különösen problémás, ha kritikus eszközöket (pl. szelepeket, robotkarokat) irányítanak ilyen csatornákon keresztül.

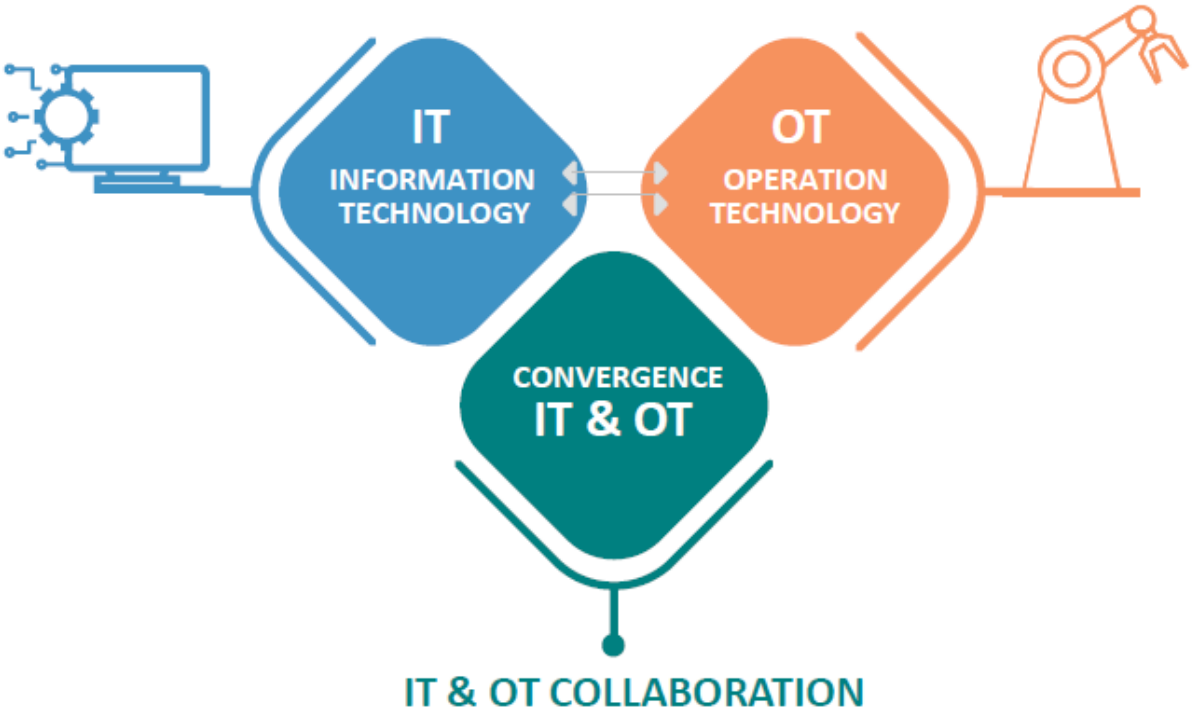
IoT eszközök hálózata

3.4. Láthatóság hiánya és eszközkezelés problémái

Ipari rendszerek esetén gyakran előfordul, hogy az üzemeltetők nem rendelkeznek teljes képpel a hálózatra csatlakoztatott összes eszközről. Egy régi, már nem használt szenzor vagy gateway akár hónapokon át aktív lehet anélkül, hogy bárki észrevenné. Ezek az eszközök komoly biztonsági kockázatot jelentenek, mivel jellemzően nem kapnak frissítést és nem figyelik őket folyamatosan. A láthatóság hiánya tehát közvetlenül hozzájárul a támadási felület növekedéséhez.



OT és IT gyári környezetben



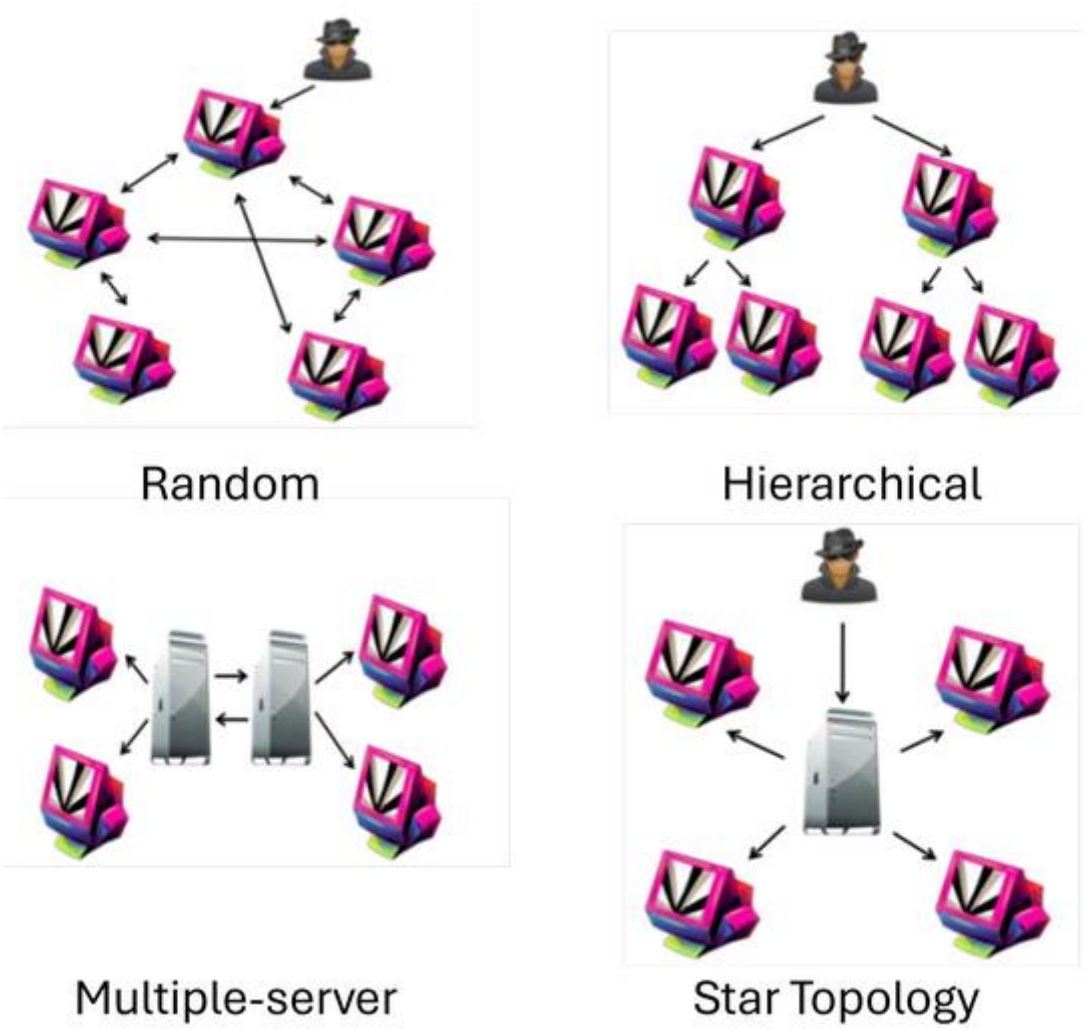
It és Ot együttműködése

4. Biztonsági kihívások ipari környezetben

Az ipari IoT környezetekben a sebezhetőségeken túl olyan összetett fenyegetések jelennek meg, amelyek gyakran több rétegben támadják meg a rendszereket. Ezek nem csupán technikai, hanem szabályozási, fizikai és szervezeti szinten is kihívásokat jelentenek.

4.1. Botnetek és DDoS támadások

Az IoT rendszerek könnyen kiberbűnözés áldozatává vállhatnak, ha a megfelelő biztonsági beállítások hiányosak. Az ilyen eszközöket a támadók gyakran használják elosztott szolgáltatásmegtagadási (DDoS) támadásokhoz, melyek során több ezer vagy akár millió fertőzött eszköz egyszerre árasztja el célpontját adatforgalommal. Egy IIoT infrastruktúra ellen irányuló sikeres DDoS támadás komoly következményekkel járhat: hálózati túlterhelést okozhat, megbéníthatja a gyártósorok irányítását, vagy szabotálhatja a valós idejű adatfeldolgozást. Ez nem csupán anyagi kárral, hanem a termelés biztonságát és minőségét veszélyeztető helyzettel is járhat. A botnetek elleni védekezés ezért kiemelt figyelmet igényel az IIoT rendszerek kialakítása és üzemeltetése során.



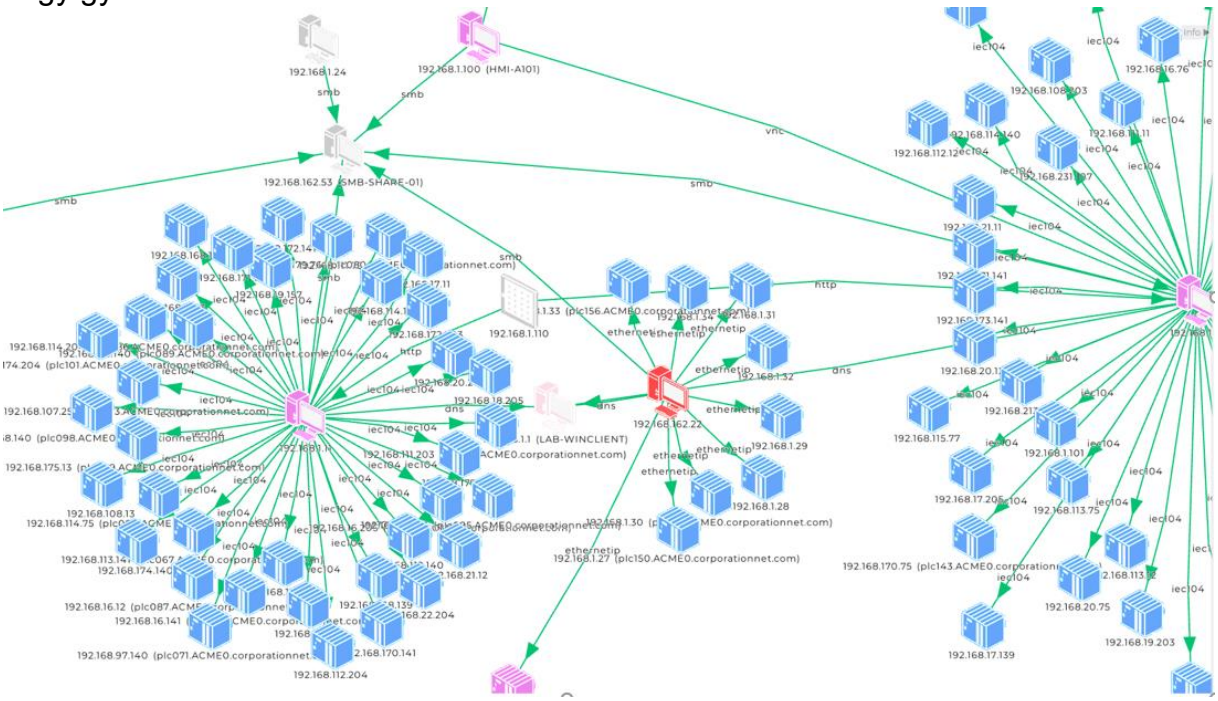
Botnet architektúra

4.2. Adatszivárgás és adatlopás

Az ipari rendszerek értékes és üzletileg kritikus adatokat tárolnak, mint például termelési ütemezések, minőségellenőrzési jelentések vagy szellemi tulajdonhoz kapcsolódó információk. Amennyiben ezek nem megfelelően védettek, a kibertámadók kiszivárogtathatják vagy ellophatják az adatokat, ezzel akár versenyelőnyhöz juttatva más szereplőket, vagy kárt okozva a márkának és a gyártási folyamat minőségének.

4.3. Fizikai hozzáférés és manipuláció

Az IoT rendszerek fizikai elérhetősége továbbra is jelentős kockázati tényező. Gyakran előfordul, hogy az eszközök kültéren vagy könnyen hozzáférhető területeken működnek (pl. ipari raktárak, gyártócsarnokok). Egy támadó fizikai hozzáféréssel képes lehet firmware-csere végrehajtására, konfigurációs adatok megszerzésére vagy új hálózati kapcsolat létesítésére is. Ez a fajta manipuláció különösen veszélyes lehet autonóm rendszerek, SCADA-vezérelt infrastruktúra vagy gyártórobotok esetén.



Fizikai hozzáférés

4.4. Szabályozási és jogi kihívások

A nemzetközi működésű ipari vállalatok számára kihívást jelent a különböző országok eltérő kiberbiztonsági szabályozása. A 2023-ban életbe lépett NIS2 irányelv célja éppen ezen szabályozások harmonizálása, ugyanakkor az alkalmazása még nem egységes. Sok vállalat nincs tisztában azzal, milyen jogi kötelezettségeik vannak incidensjelentés, adatvédelem vagy rendszer-audit terén. Ez a bizonytalanság késleltetett reakciókat és hibás döntéseket eredményezhet kibertámadások esetén.

NIS2

5. Védekezési lehetőségek ipari IoT rendszerekben

A biztonsági kihívásokkal szemben a védekezési lehetőségek többszintű megközelítést igényelnek, amelyek egyszerre kezelik a technikai, szervezeti és emberi tényezőket. Az alábbiakban a legfontosabb és leggyakrabban alkalmazott módszerekről lesz szó, ipari környezetre szabva.

5.1. Eszközök rendszeres frissítése

A szoftverek és firmware-ek naprakészen tartása rendkívül fontos. Az ipari környezetben ez kihívást jelenthet, mivel egyes eszközök nem támogatják az automatikus frissítéseket, vagy a gyártók ritkán biztosítanak hosszú távú támogatást. Érdemes olyan megoldásokat alkalmazni, amelyek lehetővé teszik a karbantartás időzítését a termelési ciklushoz igazodva, minimalizálva az állásidőt.

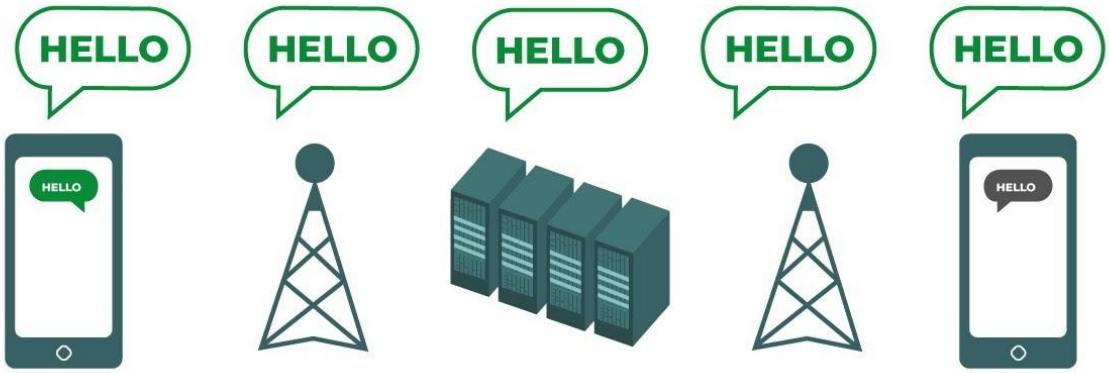
5.2. Erős jelszavak és többfaktoros hitelesítés

A sikeres támadások legfőbb okát a gyenge jelszavak jelentik. Ezek miatt érdemes minden eszközre erős jelszót állítani és figyelembe venni ahhoz a javaslatokat (kis- és nagybetűk, számok, speciális karakter(ek), stb.). Emellett a többfaktoros hitelesítés tovább növelheti a védelem szintjét.

Erős jelszavak fontossága

5.3. Adatok titkosítása és biztonságos kommunikáció

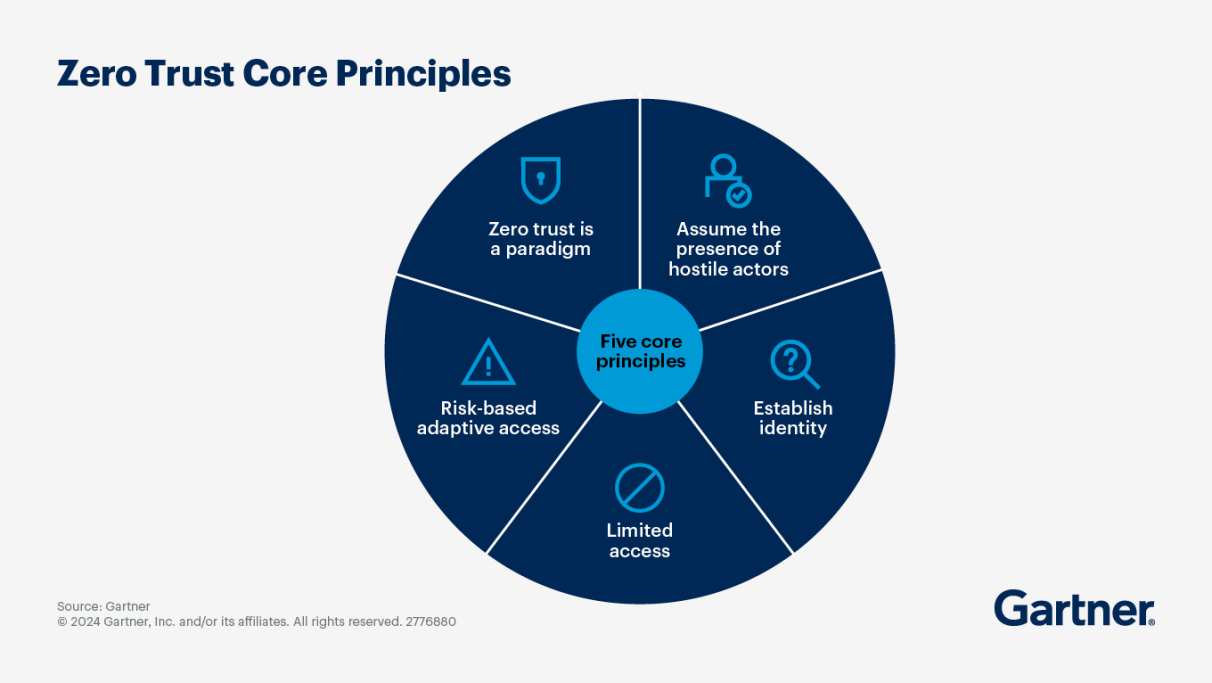
Az érzékeny adatok (pl. gyártási paraméterek, gépi visszajelzések) védelme kulcsfontosságú. Az ipari kommunikáció során titkosított adatcsatornák alkalmazása (TLS, VPN) segít megakadályozni a lehallgatást és az adatok módosítását. Emellett a helyi adattárolásra is célszerű titkosított fájlrendszert alkalmazni.



Titkosítatlan üzenetkküldés

5.4. Hálózati szegmentáció és hozzáférés-szabályozás

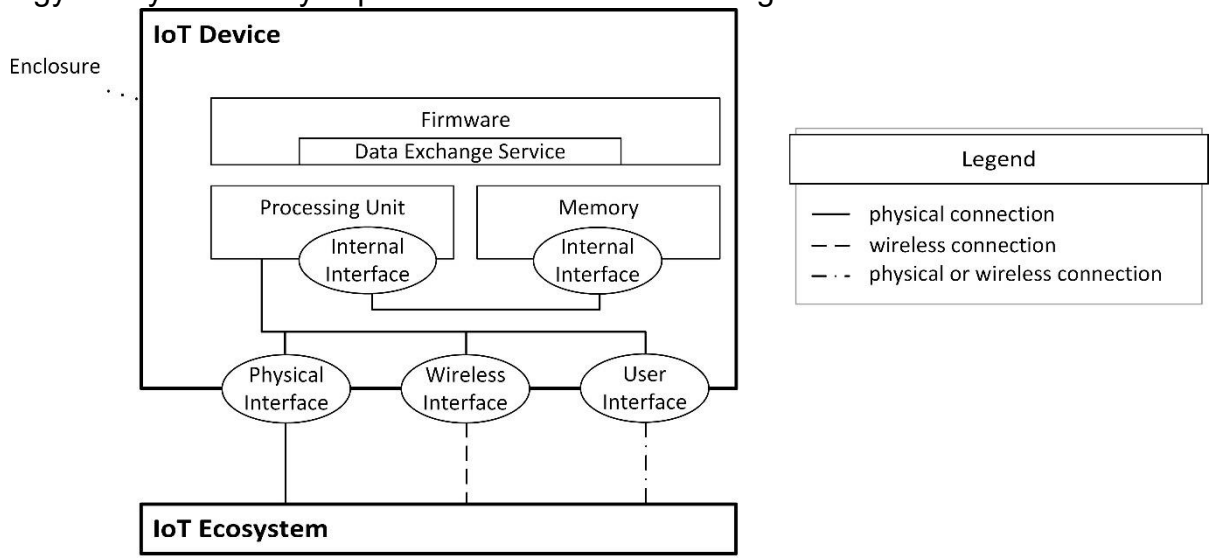
A hálózati szegmentáció célja, hogy elkülönítse az ipari eszközöket a vállalati vagy nyilvános hálózat többi részétől. Ezzel minimalizálható egy esetleges támadás hatóköre. Ennek eszközei lehetnek VLAN-ok, különálló SSID-k, tűzfalak, szerepkör-alapú hozzáférés-szabályozás, valamint Zero Trust alapú hálózatok kialakítása.



Zero Trust

5.5. Folyamatos monitorozás és anomália-észlelés

Az aktív megfigyelés lehetővé teszi, hogy az esetleges támadásokat már a korai szakaszban felismerjük. A logfájlok és hálózati forgalom automatikus elemzése, valamint az események valós idejű figyelése segíthet a gyanús tevékenységek gyors kiszűrésében. A mesterséges intelligencia alapú megoldások egyre népszerűbbek ezen a téren, mert olyan dolgokat is képesek kiszűrni, amelyek hagyományos szabályalapú rendszerekkel nem mindig azonosíthatók.



OWASP IoT Device Model

6. Szabályozási környezet ipari IoT rendszerekben

A jogi és szabályozási környezet kulcsszerepet játszik a kiberbiztonság ipari megvalósításában. Az elmúlt években az Európai Unió több lépést tett annak érdekében, hogy fokozza a kritikus infrastruktúrák védelmét.

6.1. A NIS2 irányelv hatása

A NIS2 (Network and Information Security) irányelv 2023-ban lépett hatályba, és célja, hogy egységes biztonsági minimumkövetelményeket írjon elő az Európai Unióban. Az ipari szereplők – például gyártóüzemek, logisztikai központok, energiaszolgáltatók – a kritikus ágazatok közé tartoznak, így a rendelet rájuk is kiterjed. A NIS2 előírja a megfelelő kockázatértékelést, biztonsági intézkedések bevezetését, valamint az incidensek bejelentését egy meghatározott időn belül.

NIS2 irányelv

6.2. Magyarországi megfelelés és kihívások

Magyarországon a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) és a Nemzeti Kibervédelmi Intézet (NKI) végzi a felügyeleti feladatokat. A vállalatok számára komoly kihívást jelent a pontosság biztosítása, különösen a kis- és középvállalkozások esetében. A dokumentált biztonsági eljárások, rendszeres auditok és incidens-jelentési protokollok bevezetése sokszor új működési kultúrát igényel.

SZTFH

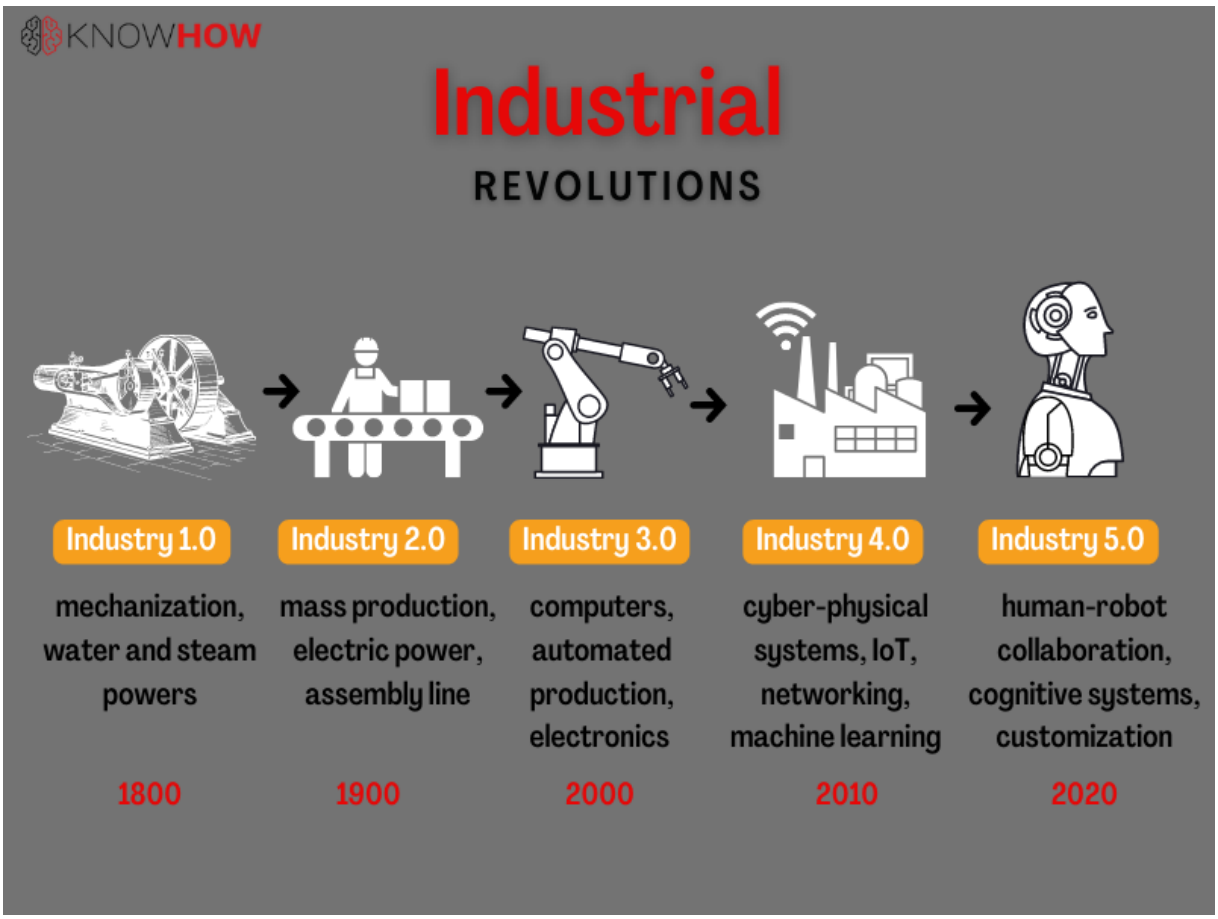
Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH)

NEMZETI KIBERVÉDELMI INTÉZET

Nemzeti Kibervédelmi Intézet (NKI)

7. Jövőbeli irányok az ipari IoT biztonságában

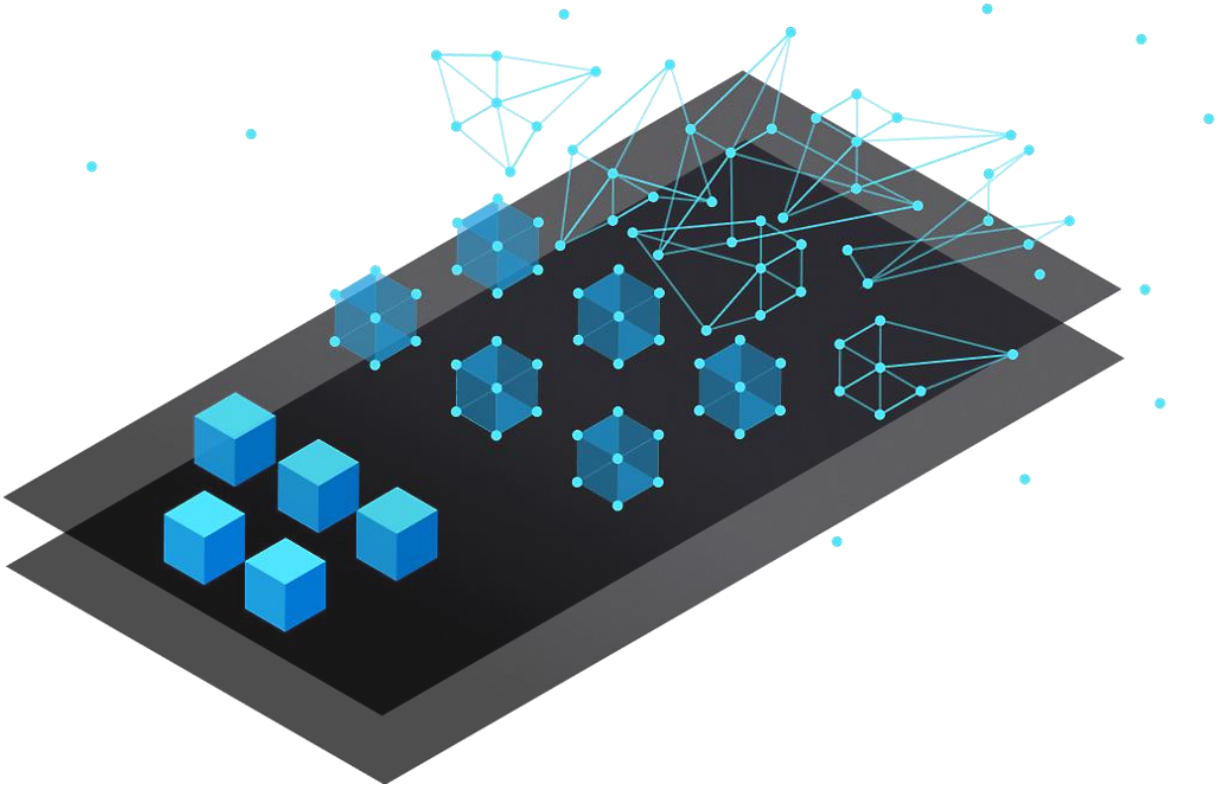
A biztonsági megközelítéseknek lépést kell tartaniuk a technológia fejlődésével. A következő évek kulcsfontosságú irányai a megelőző védekezésre, intelligens elemzésre és a biztonsági architektúrák átalakítására fókuszálnak majd.



Ipari fejlődés

7.1. Prediktív biztonság és gépi tanulás

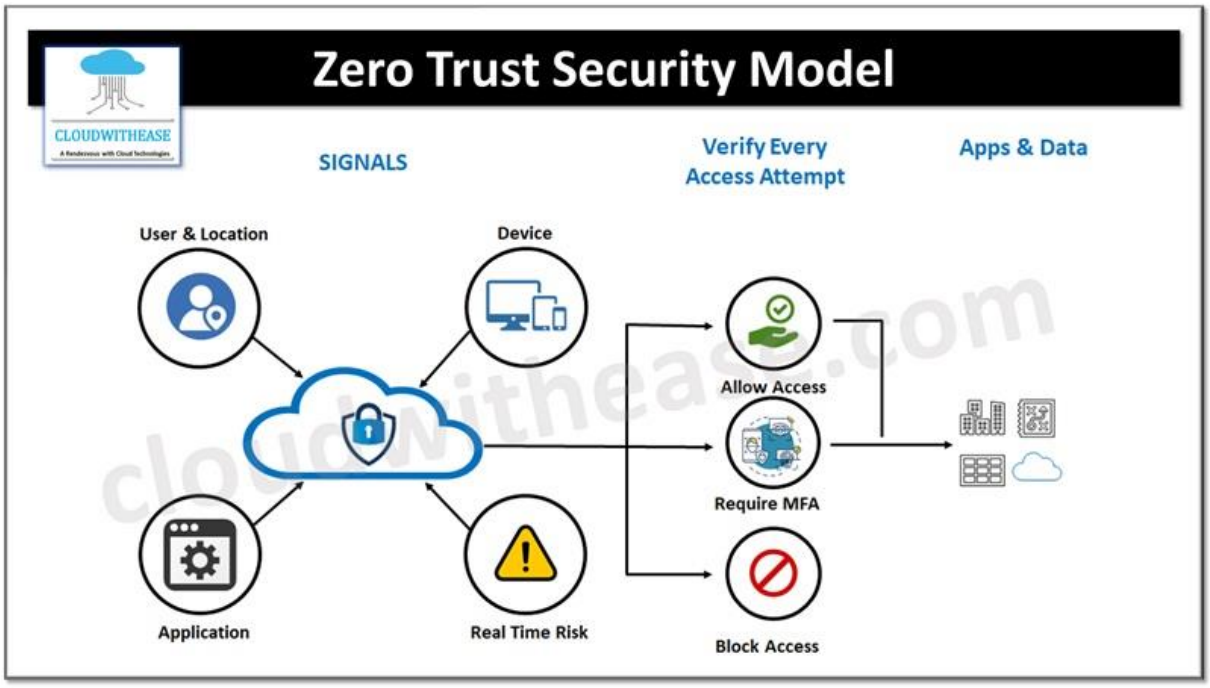
A gépi tanuláson alapuló anomáliadetektáló rendszerek képesek a viselkedésminták folyamatos tanulására és a rendellenes működés automatikus azonosítására. Az ipari rendszerekben ez különösen hasznos, mivel lehetővé teszi az ismeretlen támadások gyors felismerését. A prediktív karbantartással kombinálva a kiberbiztonság és az üzembiztonság egymást erősítő tényezőkké válhatnak.



Gépi tanulás

7.2. Zero Trust modell alkalmazása

A Zero Trust modell lényege, hogy soha nem feltételezzük egyetlen eszköz vagy felhasználó megbízhatóságát sem. Az ipari környezetben ez a megközelítés különösen hatékony lehet, például dinamikus szerepkörök vagy változó hálózati topológiák esetén. A Zero Trust architektúra bevezetése azonban jelentős infrastrukturális és szervezeti átalakítást igényel.



Zero Trust biztonsági modell

8. Következtetések

Az ipari IoT rendszerek térnyerésével a kiberbiztonság nem csupán informatika, hanem termelésbiztonsági kérdéssé is vált. A dolgozatban bemutatott sebezhetőségek, támadási felületek és kockázatok azt mutatják, hogy a IIoT-rendszerek különösen érzékenyek a célzott támadásokra. Az ipari környezetekre jellemző tényezők (például valós idejű működés, beágyazott rendszerek korlátai, fizikai hozzáférés) külön biztonsági megközelítést igényelnek.

A védekezési lehetőségek között szerepel a szoftverfrissítések rendszeres végrehajtása, a hozzáférések megfelelő szabályozása, a kommunikáció titkosítása, valamint az aktív monitorozás és gépi tanulás integrálása. A szabályozási háttér, élén a NIS2 irányelvvel, egyre szigorúbb elvárásokat támaszt, de ezzel párhuzamosan lehetőséget is nyújt a biztonsági szint növelésére.

A jövő ipari rendszereinek biztonsága olyan architektúrákra és folyamatokra épülhet, amelyek képesek dinamikusan alkalmazkodni a folyamatosan változó kiberfenyegetésekhez.

Források

[1] „Az IIoT támadási felülete: Fenyegetések és biztonsági megoldások | Trend Micro (USA)”. Elérés: 2025. május 24. [Online]. Elérhető: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions

[2] „Az IoT biztonságának első lépései - A támadási felület feltérképezése | Infosec”. Elérés: 2025. május 24. [Online]. Elérhető: https://www.infosecinstitute.com/resources/penetration-testing/getting-started-with-iot-security-mapping-the-attack-surface/?utm_source=chatgpt.com

[3] Péter, „Az IoT és az IT biztonság: kihívások és megoldások”, Panor. Elérés: 2025. május 24. [Online]. Elérhető: https://www.panor.hu/blog/az-iot-es-az-it-biztonsag-kihivasok-es-megoldasok/

[4] „Erős jelszavak fontossága, felépítése / Laptop hírek, laptop tesztek | Laptop.hu”. Elérés: 2025. május 24. [Online]. Elérhető: https://www.laptop.hu/hirek/eros-jelszavak-fontossaga-felepitese/

[5] J. Matuszak, „Felkészült vállalkozása az Ipar 5.0-ra?”, KnowHow. Elérés: 2025. május 24. [Online]. Elérhető: https://knowhow.distrelec.com/hu/gyartas-eloallitas/felkeszult-vallalkozasa-az-ipar-5-0-ra/

[6] barnstee, „Implement the Azure industrial IoT reference solution architecture - Azure IoT”. Elérés: 2025. május 24. [Online]. Elérhető: https://learn.microsoft.com/en-us/azure/iot/tutorial-iot-industrial-solution-architecture

[7] Garcia J., „Internet of Things”, Medium. Elérés: 2025. május 24. [Online]. Elérhető: https://medium.com/@1620/internet-of-things-7890793864af

[8] „IoT eszközmodell - OWASP IoT biztonsági tesztelési útmutató”. Elérés: 2025. május 24. [Online]. Elérhető: https://owasp.org/owasp-istg/02_framework/device_model.html?utm_source=chatgpt.com

[9] „Ipar 4.0 avagy beléptünk a jövőbe – 5 fogalom, ami segít az eligazodásban”, #Konzervtelefon. Elérés: 2025. május 24. [Online]. Elérhető: http://konzervtelefon.blog.hu/2017/07/12/ipar_4_0_avagy_beleptunk_a_jovobe_5_fogalom_ami_segit_az_eligazodasban

[10] „Ipari hálózatok a kibertámadók csemegéje”, Kontron. Elérés: 2025. május 24. [Online]. Elérhető: https://kontron.hu/blog/ipari-halozatok-a-kibertamadok-csemegeje/

[11] „Ipari hálózatok a kibertámadók csemegéje”, Kontron. Elérés: 2025. május 24. [Online]. Elérhető: https://kontron.hu/blog/ipari-halozatok-a-kibertamadok-csemegeje/

[12] „Kommunikáció és adatok megosztása | CyberSecurity Handbook”. Elérés: 2025. május 24. [Online]. Elérhető: https://cso.cyberhandbook.org/hu/topics/storing-data/kommunikacio-es-adatok-megosztasa

[13] „logo_nki_alpha”, Nemzeti Kibervédelmi Intézet. Elérés: 2025. május 24. [Online]. Elérhető: https://nki.gov.hu/szolgaltatasok/tartalom/incidenskivizsgalas/logo_nki_alpha/

[14] Zrt R. H., „NIS2 Irányelv, NIS2 tanácsadás - Termék | RSM Hungary”. Elérés: 2025. május 24. [Online]. Elérhető: https://www.rsm.hu/termek/nis2-tanacsadas

[15] D. L. A. Piper, „NIS2 irányelv: 2024. június 30. a nyilvántartásba vételi határidő az érintett szervezetek részére”, Advocatus. Elérés: 2025. május 24. [Online]. Elérhető: https://blogs.dlapiper.com/advocatus/2024/06/nis2-iranyelv-2024-junius-30-a-nyilvantartasba-veteli-hatarido-az-erintett-szervezetek-reszere/

[16] „Mi a gépi tanulás? | Microsoft Azure”. Elérés: 2025. május 24. [Online]. Elérhető: https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-machine-learning-platform

[17] „Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) - célja, tevékenysége és feladatai Magyarországon”. Elérés: 2025. május 24. [Online]. Elérhető: https://znaki.fm/hu/teams/sztfh/

[18] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, és N. Dragoni, „Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques”, *Sensors*, köt. 24, sz. 11, Art. sz. 11, jan. 2024, doi: 10.3390/s24113571.

[19] „Zéró bizalom biztonsági modell a felhőbiztonságban - Cloudwithease”. Elérés: 2025. május 24. [Online]. Elérhető: https://cloudwithease.com/zero-trust-security-model-in-cloud-security/
[20] „What is IIoT? (Industrial Internet of Things)”, Premio Inc. Elérés: 2025. május 24. [Online]. Elérhető: https://premioinc.com/blogs/blog/what-is-iiot-industrial-internet-of-things
[21] „Zero Trust Architecture: Strategies and Benefits”, Gartner. Elérés: 2025. május 24. [Online]. Elérhető: https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture

2.51. Kiberbiztonság a CPS-rendszerekben

Kiberbiztonság a CPS-rendszerekben

Hálózatbiztonság

Kalmár Patrik Bence

Mérnökinformatika, kalmaar.patrik@gmail.com

Absztrakt

A kiberfizikai rendszerek (CPS) hálózatbiztonsága napjainkban egyre kritikusabbá válik, tekintettel az ipari, pénzügyi és állami szektorokban betöltött központi szerepükre. A CPS-hálózatok összetettsége és a digitális infrastruktúrába való mély integrációjuk miatt különösen sérülékenyek a kibertámadásokkal szemben. Ez a dolgozat a CPS-hálózatok biztonsági kihívásait vizsgálja, kiemelve a hálózati infrastruktúra megvalósítását, a NIS2 előírásoknak való megfelelést, valamint a határvédelem és a kockázatelemzés terén tett lépéseket. A kutatás célja, hogy átfogó képet nyújtson a CPS-hálózatok védelmének aktuális állapotáról, és gyakorlati megoldásokat javasoljon a fenyegetések kezelésére. A dolgozat kitér a hálózati infrastruktúra megvalósítására, beleértve a védelmi zónák kialakítását és a hálózati szegmentáció fontosságát, amely csökkenti a támadási felületet és növeli a rendszer ellenállóképességét. A megfelelőségi követelmények elemzésén keresztül részletesen bemutatja a NIS2 irányelv technikai és adminisztratív intézkedéseit, amelyek elengedhetetlenek a kritikus infrastruktúrák védelmében. A határvédelem kulcsfontosságú elemei, például a tűzfalak, a behatolásérzékelő és megelőző rendszerek (IDS/IPS), valamint más modern határvédelmi technológiák alkalmazása is részletes bemutatásra kerül. A dolgozat foglalkozik az ipari protokollok (pl. Modbus, DNP3, MQTT) sebezhetőségeivel, valamint a Zero Trust modellek bevezetésének szükségességével, amely biztosítja, hogy minden eszköz és felhasználó folyamatos hitelesítési és jogosultságkezelési ellenőrzésen essen át. A referenciák és példák között valós CPS-támadások, például a Stuxnet (2010) és az ukrán áramhálózat elleni incidensek (2015/16) elemzése is szerepel, amelyek fontos tanulságokkal szolgálnak a kritikus infrastruktúrák biztonsági kockázatainak kezelésében. A CPS-hálózatok védelmének növelése érdekében számos technikai megoldás alkalmazható, többek között az erős hálózati szegmentáció, a védelmi zónák kialakítása, a titkosított kommunikációs protokollok (pl. TLS, VPN), valamint a biztonságos ipari protokollok (pl. OPC UA) használata, amelyek minimalizálják az adatszivárgás és manipuláció lehetőségét. A dolgozat záró részében összegzésként kiemeli a legfontosabb tanulságokat és ajánlásokat, amelyek segíthetnek a CPS-hálózatok biztonságának folyamatos fejlesztésében, figyelembe véve a hatályos szabályozásokat és a modern technológiai lehetőségeket.

Kulcsszavak: CPS, NIS2, Határvédelem, Zero Trust

Tartalomjegyzék

1 Bevezetés 4

2 A CPS-rendszerek jelentősége és a hálózatbiztonság kritikus szerepe 4

2.1 A kiberfizikai rendszerek (CPS) definíciója és szerepe 4

2.2 A CPS-rendszerek fejlődése és elterjedése (Ipar 4.0, IoT, AI integráció) 5

2.3 A hálózatbiztonság jelentősége a CPS-környezetben 5

2.4 Fenyegetések és kockázatok: sebezhetőségek, támadási vektorok, kritikus infrastruktúrák veszélyeztetettsége 5

2.5 Ipari, állami és katonai szektorok érintettsége a CPS-biztonságban 6

3 Hálózati infrastruktúra megvalósítása: A CPS-hálózatok felépítése, a védelmi zónák kialakítása és a hálózati szegmentáció fontossága 7

3.1 A CPS-hálózatok tipikus architektúrája (vezérlőrendszerek, érzékelők, aktorok, hálózati rétegek) 7

3.2 Védelmi zónák és biztonsági rétegek kialakítása (Purdue-modell alkalmazása) 7

3.3 Hálózati szegmentáció és forgalomszabályozás (VLAN, mikrosegmentáció, SDN-alapú biztonság) 11

3.4 Biztonságos kommunikációs csatornák (VPN, TLS, IPsec, SSH, MQTT-SN) 12

3.5 A fizikai hozzáférés elleni védelem (biztonságos helyiségek, fizikai behatolás elleni intézkedések) 13

3.6 Tipikus sérülékenységek és támadási pontok az infrastruktúrában 14

4 Megfelelőségi követelmények: A NIS2 előírások részletes elemzése, valamint a technikai és adminisztratív intézkedések bemutatása 16

4.1 A NIS2 irányelv célja és hatálya (EU-s és magyarországi jogi háttér) 16

4.2 Kritikus infrastruktúra védelmére vonatkozó előírások és kötelezettségek 17

4.3 Biztonsági incidensek kezelése és jelentési kötelezettségek 19

4.4 Technikai védelmi intézkedések (hálózati monitoring, behatolásmegelőzés, titkosítás, sandboxing) 21

4.5 Adminisztratív intézkedések (hozzáféréskezelés, kockázatelemzés, megfelelőségi auditok, kiberbiztonsági oktatás) 24

5 Határvédelem felépítése: Tűzfalak, IDS/IPS rendszerek és más határvédelmi technológiák alkalmazása 27

5.1 Tűzfalak és alkalmazásuk a CPS-hálózatokban (hagyományos tűzfalak vs. NGFW-k) 27

5.2 Intrusion Detection Systems (IDS) és Intrusion Prevention Systems (IPS) szerepe 30

5.3 SIEM (Security Information and Event Management) rendszerek és biztonsági eseményelemzés 32

5.4 Host-alapú védelmi mechanizmusok 34

5.5 Támadásészlelési és válaszmechanizmusok (SOC-k, SOAR rendszerek, AI-alapú anomáliadetektálás) 36

6 Általános hálózati kapcsolatok és kockázatelemzés: Az ipari protokollok (pl. Modbus, DNP3, MQTT) sebezhetőségeinek vizsgálata és a Zero Trust modellek bevezetése 37

6.1 Gyakran használt ipari protokollok és biztonsági kockázataik 37

6.2 Modbus, DNP3, MQTT és más protokollok sebezhetőségei 39

6.3 Zero Trust Architektúra (ZTA) alkalmazása a CPS-hálózatokban 40

6.4 Hitelesítés és hozzáférés-kezelés (pl. multi-factor authentication, RBAC, ABAC, PAM megoldások) 42
6.5 Biztonsági tesztelési és auditálási módszerek (penetrációs tesztelés, sebezhetőségvizsgálat) 44
6.6 Kibervédelmi megoldások (sandboxing, honeypotok, AI-alapú fenyegetésészlelés) 46
7 Referenciák és példák: Valós CPS-támadások elemzése és tanulságaik bemutatása 48
7.1 Stuxnet 2010 – Az első dokumentált ipari kiberfegyver elemzése 48
7.2 Ukrán áramhálózat elleni támadások (2015-2016) – Kritikus infrastruktúra elleni fenyegetések 49
7.3 TRITON (2017) – Biztonsági rendszerek elleni célzott támadás 51
7.4 Colonial Pipeline (2021) – Ransomware fenyegetések ipari rendszerek ellen 52
7.5 Újabb támadások és trendek (pl. AI-alapú fenyegetések, ellátási lánc elleni támadások) 54
8 Összegzés és javaslatok 56
8.1 Főbb megállapítások és kulcsfontosságú biztonsági kihívások 56
8.2 Jövőbeli trendek és kutatási lehetőségek a CPS-hálózatbiztonság terén 57
IRODALOMJEGYZÉK (Felhasznált/ajánlott irodalom) 58

1 BEVEZETÉS

A 21. század egyik legnagyobb technológiai vívmánya a kiberfizikai rendszerek (Cyber-Physical Systems, CPS) térnyerése, amely a fizikai világot és a digitális rendszereket egyesíti intelligens, valós idejű vezérlés és adatfeldolgozás segítségével. Ezek a rendszerek alapvető szerepet töltenek be az ipari automatizálásban, az energiahálózatok működésében, az egészségügyi eszközökben, a közlekedésirányításban és még számos más kritikus infrastruktúrában. Ahogy ezek a rendszerek egyre inkább hálózatba kapcsolódnak, úgy növekszik a kibertámadásokkal szembeni sebezhetőségük is.

A kiberbiztonság, különösen a hálózati biztonság, kulcsfontosságú tényezővé vált a CPS-rendszerek megbízhatóságának és működőképességének fenntartásában. A rosszindulatú támadások – legyenek azok ipari kémkedés, szabotázs vagy akár nemzetállami fenyegetések – komoly zavarokat okozhatnak a rendszer működésében, súlyos gazdasági és társadalmi következményekkel járva. A legismertebb példák, mint a Stuxnet vírus vagy az ukrán áramszolgáltatók elleni támadások, világosan rámutatnak arra, hogy a CPS-rendszerek nem csupán technológiai kihívást jelentenek, hanem nemzetbiztonsági kérdésekké is váltak.

Dolgozatom célja, hogy átfogó képet nyújtson a CPS-rendszerek hálózatbiztonságának kihívásairól, a lehetséges védekezési stratégiákról, valamint a kapcsolódó jogi és szabályozási környezetről. A dolgozat első részében bemutatom a CPS rendszerek felépítését és működését, majd a hálózati infrastruktúrák és védelmi zónák ismertetése következik. Külön fejezetet szentelek a NIS2 irányelvnek és annak megfelelőségi követelményeinek, valamint a határvédelmi mechanizmusok – mint a tűzfalak és behatolás-észlelő rendszerek – szerepének. Részletesen foglalkozom az ipari protokollok sebezhetőségeivel, a Zero Trust biztonsági modellel, valamint valódi, megtörtént támadások esettanulmányaival. A dolgozat zárásaként összegzem a legfontosabb tanulságokat, és ajánlásokat fogalmazok meg a CPS-hálózatok biztonságosabbá tételére.

Ez a dolgozat nemcsak technológiai és elméleti ismereteket kíván közvetíteni, hanem gyakorlati szempontból is rávilágít arra, miért elengedhetetlen a CPS-rendszerek célzott és rétegzett védelme a jövő fenntartható és biztonságos digitális infrastruktúráinak megóvása érdekében.

2 A CPS-RENDSZEREK JELENTŐSÉGE ÉS A HÁLÓZATBIZTONSÁG KRITIKUS SZEREPE

2.1 A kiberfizikai rendszerek (CPS) definíciója és szerepe

A **kiberfizikai rendszerek (Cyber-Physical Systems - CPS)** olyan fejlett technológiai megoldások, amelyek a fizikai és digitális világot egyesítik, lehetővé téve a valós idejű adatgyűjtést, elemzést és automatizált döntéshozatalt. Ezek a rendszerek szorosan kapcsolódnak az **IoT (Internet of Things), mesterséges intelligencia (AI) és big data technológiákhoz**, és számos iparágban meghatározó szerepet játszanak.

A CPS rendszerek főbb jellemzői:

- **Valós idejű adatgyűjtés és -feldolgozás**, amely lehetővé teszi a gyors reakciót a környezet változásaira.
- **Intelligens automatizálás**, amely csökkenti az emberi beavatkozás szükségességét és növeli a hatékonyságot.
- **Szenzorok és aktuátorok integrációja**, amelyek biztosítják a fizikai és digitális világ közötti kapcsolatot.

- **Önellenőrző és önjavító rendszerek**, amelyek képesek adaptálódni és optimalizálni a működésüket.

„Cyber-Physical Systems integrate computing and communication capabilities with monitoring and control of entities in the physical world."

— Rajkumar et al. (2009), *Cyber-Physical Systems: The Next Computing Revolution*

2.2 A CPS-rendszerek fejlődése és elterjedése (Ipar 4.0, IoT, AI integráció)

Az **Ipar 4.0 és a digitális transzformáció** egyik kulcseleme a CPS-rendszerek elterjedése, amelyek az ipari automatizálás és az intelligens rendszerek alapjait képezik. Az **5G és edge computing** technológiák fejlődése tovább növeli ezeknek a rendszereknek a hatékonyságát és megbízhatóságát.

Főbb alkalmazási területek:

- **Ipari automatizálás és robotika** (pl. okosgyárak, önálló gyártósorok)
- **Egészségügy** (pl. távdiagnosztika, sebészeti robotok, okosimplantátumok)
- **Energia** (pl. okoshálózatok, megújuló energiaforrások optimalizálása)
- **Kritikus infrastruktúrák** (pl. közlekedési hálózatok, víz- és gázellátás, intelligens városok)

2.3 A hálózatbiztonság jelentősége a CPS-környezetben

A CPS-rendszerek egyre növekvő szerepvállalása miatt a hálózatbiztonság kritikus jelentőségűvé válik. A fizikai és digitális elemek integrációja új típusú sebezhetőségeket eredményez, amelyek komoly fenyegetést jelentenek az adatbiztonságra, az üzletfolytonosságra és a fizikai infrastruktúrára.

Főbb kibertámadási fenyegetések:

- Adathalászat és jogosulatlan belépések, amelyek érzékeny információkhoz való hozzáférést eredményezhetnek.
- DDoS (Distributed Denial-of-Service) támadások, amelyek megbéníthatják a rendszer működését.
- Zsarolóprogramok (ransomware), amelyek titkosítják vagy törlik az adatokat.
- Sérülékeny ipari protokollok kihasználása (pl. Modbus, DNP3, MQTT).
- Belső fenyegetések és emberi mulasztások, amelyek komoly biztonsági kockázatokat jelenthetnek.

Alapvető biztonsági stratégiák a CPS-rendszerek védelmére:

- Hálózati szegmentáció – az egyes rendszerelemek elkülönítése biztonsági zónákba.
- Erős autentikáció és hozzáférés-kezelés – MFA (Multi-Factor Authentication), RBAC (Role-Based Access Control).
- Titkosított kommunikáció – VPN, TLS, IPsec használata az adatok védelmére.
- Fenyegetések monitorozása és incidenskezelés – IDS/IPS rendszerek, SIEM (Security Information and Event Management) alkalmazása.
- Zero Trust Architektúra (ZTA) – az elv, hogy semmilyen rendszerkomponensben nem szabad vakon megbízni.

2.4 Fenyegetések és kockázatok: sebezhetőségek, támadási vektorok, kritikus infrastruktúrák veszélyeztetettsége

A CPS-rendszerek sebezhetőségei **komoly gazdasági és biztonsági kockázatokat** jelentenek. Egy sikeres kibertámadás az alábbi következményekkel járhat:

- Kritikus infrastruktúrák leállása vagy meghibásodása (pl. áramszolgáltatás kiesése, közlekedési rendszerek leállása).
- Fizikai károk és üzemi balesetek (pl. ipari robotok meghibásodása, automatizált rendszerek túlterhelése).

- Adatszivárgás és ipari kémkedés, amely versenyhátrányt okozhat a vállalatok számára.

A CPS-rendszerek biztonságának garantálása tehát **nem csupán technikai, hanem nemzetbiztonsági és gazdasági kérdés is**. A megfelelő védekezési stratégiák kidolgozása elengedhetetlen az egyre növekvő fenyegetésekkel szemben.

2.5 Ipari, állami és katonai szektorok érintettsége a CPS-biztonságban

A **kiberfizikai rendszerek (CPS)** kulcsszerepet játszanak az ipari, állami és katonai szektorokban, mivel ezek az ágazatok nagymértékben támaszkodnak a digitális infrastruktúrára, az automatizált folyamatokra és a valós idejű adatfeldolgozásra. Az ilyen rendszerek biztonságának sérülékenysége közvetlen hatással lehet az ellátási láncokra, a nemzetbiztonságra és a társadalom működésére.

Ipari szektor:

Az ipari automatizáció és a **kritikus infrastruktúrák** digitalizációja jelentős előnyökkel jár, de egyben új biztonsági kockázatokat is felvet.

- **Okosgyárak és ipari robotok**: A gyártósorok automatizált vezérlése és az önállóan működő robotok hálózati kapcsolatban állnak egymással, így támadható felületek keletkeznek. Egy kibertámadás leállíthatja a termelést, súlyos gazdasági károkat okozva.
- **Energetikai rendszerek és okoshálózatok**: Az áramhálózatok, víz- és gázszolgáltató rendszerek CPS-technológiákkal működnek. Egy sikeres támadás, mint a 2015-ös ukrán áramszünetet okozó malware (BlackEnergy), akár milliók ellátását is veszélyeztetheti.
- **Autonóm járművek és szállítmányozás**: Az ipari logisztikai hálózatok és az önvezető járművek folyamatos hálózati kapcsolatot igényelnek, így támadhatóvá válhatnak a kommunikációs csatornák és az adatfeldolgozó rendszerek.

Állami szektor:

Az állami infrastruktúra és közigazgatás CPS-rendszerei szintén ki vannak téve a kiberfenyegetéseknek.

- **Közlekedési hálózatok és intelligens városok**: A forgalomirányító rendszerek, a tömegközlekedési hálózatok és az intelligens közvilágítási rendszerek mind CPS-alapúak. Egy támadás forgalmi káoszt, közlekedési baleseteket vagy akár teljes közlekedési leállást okozhat.
- **E-kormányzati rendszerek és közigazgatás**: Az elektronikus ügyintézés, adatbázisok és kritikus állami rendszerek támadása adatvesztést, rendszerek működésképtelenségét vagy kémkedési célokat szolgálhat.
- **Egészségügyi rendszerek**: Az orvosi berendezések, mint az okosimplantátumok és a távdiagnosztikai rendszerek, CPS-technológiát használnak. Egy sikeres támadás akár életeket is veszélyeztethet.

Katonai szektor:

A modern hadviselés egyre inkább támaszkodik a kiberfizikai rendszerekre, így azok védelme stratégiai jelentőségű.

- **Autonóm fegyverrendszerek és drónok**: A hálózatba kapcsolt fegyverrendszerek és katonai drónok meghackelése súlyos biztonsági fenyegetést jelenthet, mivel azok ellenőrzése illetéktelen kezekbe kerülhet.
- **Kommunikációs és hírszerzési infrastruktúra**: A katonai hálózatok, műholdak és titkosított kommunikációs csatornák CPS-alapú védelme elengedhetetlen a hadműveletek biztonságának fenntartásához.
- **Kiberhadviselés és kritikus infrastruktúra elleni támadások**: Egy ellenséges állam vagy csoport célzott támadásokat indíthat a katonai és polgári infrastruktúrák ellen, bénítva a működésüket.

A fenti szektorok védelmére **átfogó kibervédelmi stratégiákra, szigorú szabályozásokra és folyamatos biztonsági ellenőrzésekre van szükség**, hogy a CPS-rendszerek biztonságát és megbízhatóságát hosszú távon fenntartsák.

3 HÁLÓZATI INFRASTRUKTÚRA MEGVALÓSÍTÁSA: A CPS-HÁLÓZATOK FELÉPÍTÉSE, A VÉDELMI ZÓNÁK KIALAKÍTÁSA ÉS A HÁLÓZATI SZEGMENTÁCIÓ FONTOSSÁGA

3.1 A CPS-hálózatok tipikus architektúrája (vezérlőrendszerek, érzékelők, aktorok, hálózati rétegek)

Vezérlőrendszerek

- PLC-k (Programmable Logic Controller):
  - Példa: Siemens SIMATIC S7-1500 egy gyártósoron, ami a csomagoló gép sebességét szabályozza. Ha a hőmérséklet-érzékelő (pl. PT100) jelzi a túlmelegedést, a PLC leállítja a futószalagot.
  - Kommunikáció: PROFINET protokollon keresztül csatlakozik a SCADA rendszerhez.
- DCS (Distributed Control System):
  - Példa: Honeywell Experion PKS egy olajfinomítóban, ahol több ezer szenzor (pl. nyomásmérők) adatait integrálja, és optimalizálja a desztillációs folyamatot.

Érzékelők és aktorok

- Szenzorok:
  - Példa: LIDAR szenzor egy autonóm targoncán (AGV), ami a raktárban akadályokat érzékel. Hibás kalibrálás esetén a targonca falnak ütközik.
  - Protokoll: IO-Link (vezetékes) vagy LoRaWAN (vezeték nélküli).
- Aktorok:
  - Példa: Pneumatikus szelep egy sörgyárban, ami a PLC parancsára nyitja/zárja a csöveket. Ha hackelik a hálózatot, a szelep idő előtt nyithat, ami anyagvesztést okoz.

Hálózati rétegek

- Field szint: RS-485 vagy CAN busz (pl. egy autó gyári tesztpályáján a kerekek nyomatékát mérő szenzorok).
- Control szint: OPC UA szerver, ami összegyűjti a PLC-k adatait és továbbítja a SCADA-nak.
- Enterprise szint: SAP rendszer, ami a gyártási adatokat kapcsolja a beszerzési rendszerhez.

3.2 Védelmi zónák és biztonsági rétegek kialakítása (Purdue-modell alkalmazása)

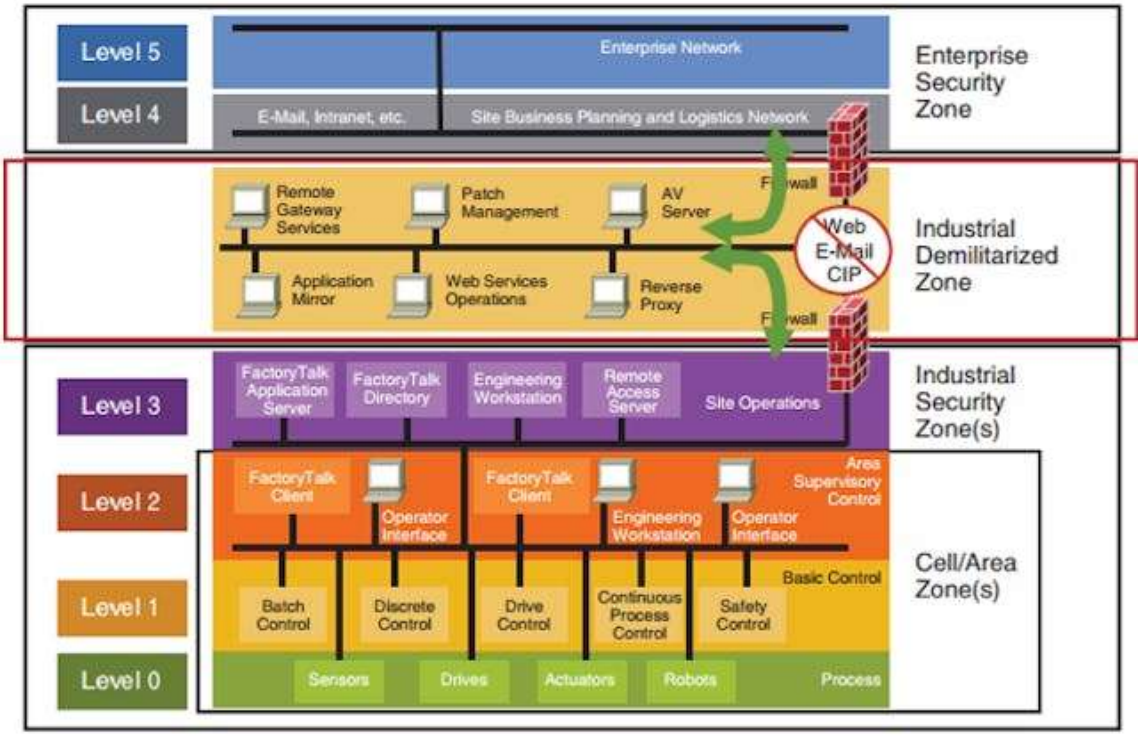
A Cyber-Fizikai Rendszerek (CPS) biztonsága alapvetően a **rétegezett védelmi modellre** épül, amely elkülöníti a kritikus ipari vezérlőrendszereket a vállalati hálózattól. A **Purdue-modell** (más néven ISA-95 standard) az ipari automatizálásban széles körben alkalmazott referencia-architektúra, amely logikai zónákra osztja a hálózatot, minimalizálva ezzel a kibertámadások terjedésének kockázatát.

A Purdue-modell rétegei és funkcionális felépítése

A modell 6 szintre tagolja a hálózati architektúrát, a vállalati informatikától (Enterprise) a fizikai folyamatokig (Process):

Szint	Funkció	Példa eszközök	Kommunikációs protokollok
Level 5 – Enterprise	Üzleti rendszerek, vállalati erőforrások	ERP (SAP), CRM, e-mail szerverek	HTTP(S), SQL, SMTP
Level 4 – Site Business	Helyi üzleti folyamatok, gyártásirányítás	MES (Manufacturing Execution System), adattárolók	OPC UA, REST API

Level 3 – Site Operations	SCADA, felügyeleti és adatgyűjtő rendszerek	SCADA (Ignition, WinCC), HMI (Human-Machine Interface)	Modbus TCP, DNP3, OPC Classic
Level 2 – Area Supervisory	PLC-k, lokális vezérlők, gyártási egységek	Siemens S7, Allen-Bradley ControlLogix, PAC (Programmable Automation Controller)	PROFINET, EtherCAT, DeviceNet
Level 1 – Basic Control	Mezőszintű eszközök, szenzorok és aktuátorok	I/O modulok, intelligens szenzorok (pH, hőmérséklet, nyomás)	IO-Link, CAN bus, HART
Level 0 – Process	Fizikai folyamatok (gépek, motorok, szelepek)	Elektromos motorok, pneumatikus rendszerek, szivattyúk	N/A (nem hálózati szint)



- https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant

<u>Zónák és konkrét védelmi intézkedések</u>

1. Enterprise & DMZ (Level 4-5) – Vállalati hálózat és demilitarizált zóna

- Feladata: Az üzleti rendszerek (pl. SAP, SharePoint) és a külső partnerek (pl. beszállítók, felhőszolgáltatók) kapcsolata.
- Kockázatok:

    - Adatkiszivárgás: Egy rosszindulatú e-mail melléklet (pl. phishing) veszélyeztetheti a vállalati hálózatot.
    - Lateral Movement: Ha egy támadó behatol a vállalati hálózatba, a DMZ-n keresztül próbálhat meg elérni az ipari rendszereket.
- Védelem:
    - Tűzfal (Next-Gen Firewall – NGFW):
        - A vállalati hálózat (Level 5) csak a DMZ-n (Level 4) keresztül kommunikálhat az SCADA-val (Level 3).
        - Példa szabály: Engedélyezett: Level 5 → DMZ (HTTPS, 443-es port), Tiltott: Level 5 → Level 3 (SCADA közvetlen elérése)
    - Proxy és forgalomellenőrzés: Minden külső kapcsolat (pl. felhőszolgáltató) a DMZ-n keresztül történik, titkosítva (TLS 1.3).

2. SCADA és Felügyeleti Réteg (Level 3) – A kritikus infrastruktúra magja

- Feladata: Valós idejű adatgyűjtés és felügyelet (pl. nyomás, hőmérséklet monitorozása).
- Kockázatok:
    - SCADA exploitok: Régi SCADA rendszerek (pl. Windows XP alapú WinCC) sebezhetők a WannaCry vagy Stuxnet-szerű támadásokkal szemben.
    - Man-in-the-Middle (MitM): Ha a kommunikáció nincs titkosítva (pl. régi Modbus TCP), egy támadó hamis parancsokat küldhet (pl. "állítsd le a szivattyút").
- Védelem:
    - Air-Gapped hálózat: Ideális esetben a SCADA fizikailag el van választva az internetről (nincs közvetlen kapcsolat).
    - OPC UA (titkosított OPC): A hagyományos OPC Classic (DCOM alapú) helyett OPC UA-t használni AES-256 titkosítással.
    - Jump Host / Bastion Host:
        - A karbantartók csak egy dedikált, erősen védett szerverről (Jump Host) léphetnek be a SCADA rendszerbe.
        - Példa: RDP gateway + kétfaktoros hitelesítés (YubiKey vagy Microsoft Authenticator)

3. Vezérlőszint (Level 2) – PLC-k és lokális automatizálás

- Feladata: A mezőeszközök (szenzorok, motorok) irányítása.
- Kockázatok:
    - PLC exploitok:
        - Példa: A Siemens S7-300/400-es PLC-k sebezhetők a S7Comm+-os támadásokkal, ahol egy rosszindulatú kód felülírja a PLC programot.
        - Valós eset: A TRITON/Trisis malware 2017-ben egy olajfinomító PLC-jét támadta meg, és veszélyes állapotba hozta a biztonsági rendszereket.
    - Default jelszavak: Sok PLC gyári jelszóval rendelkezik (pl. "admin:admin"), amelyet a támadók könnyen kitalálnak.
- Védelem:
    - PLC hardening:
        - Minden PLC-n változtassuk meg az alapértelmezett jelszavakat.

        - Tiltsuk le a felesleges szolgáltatásokat (pl. Telnet, HTTP felület).
    - Mikrosegmentáció:
        - Minden PLC saját hálózati szegmensben legyen (pl. VLAN 100 csak a PLC-knek).
        - Példa szabály: Engedélyezett: SCADA (Level 3) → PLC (Level 2) csak a 102/TCP (Siemens S7Comm), minden más forgalom tiltva

4. Mezőszint (Level 0-1) – Szenzorok és aktuátorok

- Feladata: A fizikai világ adatainak gyűjtése (pl. hőmérséklet, folyadékszint).
- Kockázatok:
    - Szenzor manipuláció:
        - Példa: Egy támadó GPS spoofinggal megtéveszthet egy autonóm targonca navigációs rendszerét.
        - Valós eset: 2016-ban hackerek rádiós jelekkel meghamisították egy hajó GPS-jét, és eltérítették azt.
    - Fizikai behatolás:
        - Ha egy támadó hozzáfér egy szenzorhoz (pl. egy gyárban), USB-n keresztül malware-t telepíthet (pl. USB Rubber Ducky).
- Védelem:
    - Szenzor hitelesítés:
        - Intelligens szenzorok (pl. IO-Link) digitális aláírással küldjenek adatokat.
    - Fizikai biztonság:
        - Szenzorok zárt helyen, riasztórendszerrel.
        - USB-portok letiltása PLC-kön és SCADA terminálokon.

Összefoglaló védelmi stratégia

Szint	Fő kockázatok	Védelmi intézkedések
Enterprise (5)	Phishing, adatelérési jogok visszaélése	NGFW, proxy, szigorú IAM (Identity & Access Management)
DMZ (4)	Külső támadások, adatszivárgás	Web Application Firewall (WAF), TLS titkosítás, szigorú API ellenőrzés
SCADA (3)	SCADA malware, MitM	Air-gapping, OPC UA, Jump Host + MFA
PLC (2)	PLC exploitok, ransomware	Mikrosegmentáció, PLC hardening, forgalomszűrés
Szenzorok (0-1)	Fizikai manipuláció, spoofing	Digitális aláírás, fizikai biztonság, USB-vezérlés

Következtetés

A Purdue-modell nem csupán elméleti keretrendszer, hanem **gyakorlatias biztonsági architektúra**, amely nélkülözhetetlen a kritikus infrastruktúrák védelmében. A rétegek közötti szigorú elkülönítés, a kommunikáció titkosítása és a fizikai védelem együttesen képezik a CPS-hálózatok ellenálló képességét. A valós veszélyek (pl. Stuxnet, TRITON, GPS spoofing) rámutatnak, hogy a hagyományos IT-biztonság nem elegendő az ipari környezetekben – a Purdue-modell alkalmazása létfontosságú.

3.3 Hálózati szegmentáció és forgalomszabályozás (VLAN, mikrosegmentáció, SDN-alapú biztonság)

A hálózati szegmentáció és forgalomszabályozás alapvető szerepet játszik a CPS-rendszerek biztonságának megőrzésében. A jól kialakított hálózati elkülönítés nemcsak csökkenti a támadási felületet, hanem korlátozza a potenciális károk terjedését is egy biztonsági incidens esetén.

VLAn-alapú szegmentáció ipari környezetben

Egy tipikus gyártóüzem hálózati architektúrájában a következő VLAN-okat érdemes kialakítani:

- **VLAN 10 (192.168.10.0/24):** PLC-k és SCADA rendszerek számára. Ez a VLAN tartalmazza az összes kritikus ipari vezérlőeszközt, és szigorúan elkülönített a többi hálózati szegmenstől.
- **VLAN 20 (192.168.20.0/24):** Felhasználói hálózat, ahol az operátorok és mérnökök munkaállomásai találhatók.
- **VLAN 30 (192.168.30.0/24):** Vendég WiFi hálózat, teljesen elkülönítve a termelési rendszerektől.

A VLAN-ok közötti forgalom szabályozása nélkülözhetetlen. Például, ha a VLAN 20 (felhasználói hálózat) és a VLAN 10 (PLC/SCADA) között nincs megfelelő forgalomszűrés, egy fertőzött laptop ARP spoofing támadással behatolhat a kritikus ipari rendszerek hálózatába. A 2014-es német acélművi incidens pontosan ezt demonstrálta, ahol egy spear phishing támadás révén a támadók a vállalati hálózatról a termelési rendszerekbe hatoltak be.

Mikrosegmentáció megvalósítása

A hagyományos VLAN-alapú szegmentációt kiegészíti a mikrosegmentáció, amely az egyes eszközök szintjére is kiterjeszti a hálózati elkülönítést. VMware NSX vagy Cisco ACI megoldások segítségével minden PLC saját virtuális tűzfallal rendelkezik. Például:

Egy Siemens S7-1200 PLC esetében csak a SCADA rendszer IP-címéről (pl. 192.168.10.50) engedélyezett a 102/TCP porton történő kommunikáció (S7Comm protokoll).

Minden más forgalom alapértelmezés szerint tiltott, beleértve a ping (ICMP) kéréseket is.

A szabályok dinamikusan frissülnek a hálózati topológia változásakor.

Ez a megközelítés jelentősen csökkenti a kártevők laterális mozgásának lehetőségét a hálózaton belül.

SDN-alapú biztonság (OpenFlow)

A Software Defined Networking (SDN) új lehetőségeket nyit meg a hálózati biztonság terén:

Reakció idő: Ha egy szenzor (pl. egy IP-kamera) gyanús forgalmat generál (pl. DDoS támadás részeként), az OpenFlow kontroller milliszekundumok alatt frissíti a switch-ek folyamatábláit, blokkolva a forráscímet.

Automatizált válasz: A hálózati eszközök képesek automatikusan elkülöníteni a fertőzött végpontokat anélkül, hogy emberi beavatkozásra lenne szükség.

Példa: Egy intelligens épületenergia-rendszerben a szenzorok hálózatán észlelt rendellenes forgalom esetén az SDN kontroller azonnal létrehoz egy quarantin VLAN-t a gyanús eszközök számára.

A hálózati szegmentáció és forgalomszabályozás hatékony megvalósítása nélkülözhetetlen a modern CPS-rendszerek biztonságához. A VLAN-ok, mikrosegmentáció és SDN technológiák kombinációja lehetővé teszi a rugalmas, de szigorúan szabályozott hozzáférési politikák kialakítását, miközben minimalizálja a biztonsági kockázatokat.

3.4 Biztonságos kommunikációs csatornák (VPN, TLS, IPsec, SSH, MQTT-SN)

A kiberfizikai rendszerekben a biztonságos kommunikáció megvalósítása alapvető követelmény, különösen a távoli hozzáférés és az eszközök közötti adatátvitel esetén. A modern titkosítási protokollok és hitelesítési mechanizmusok nélkülözhetetlenek a bizalmas adatok védelme és a rendszerek integritásának megőrzése érdekében.

IPsec VPN megvalósítás ipari környezetben

Egy bányavállalat esetében, ahol a geológusoknak távolról kell hozzáférniük a földrengés-érzékelők által gyűjtött adatokhoz, az IPsec VPN biztosítja a biztonságos kapcsolatot:

Protokoll konfiguráció: IKEv2 (Internet Key Exchange version 2) használata dinamikus kulcscsere érdekében
Titkosítási algoritmus: AES-256-GCM, amely biztosítja az adatok titkosságát és integritását
Hitelesítés: PSK (Pre-Shared Key) vagy digitális tanúsítványok alapján
Példa konfiguráció (Cisco eszközön):

```
crypto ikev2 proposal IKEv2-PROPOSAL
encryption aes-cbc-256
integrity sha512
group 19
crypto ipsec profile IPSEC-PROFILE
set ikev2-profile IKEv2-PROFILE
```

TLS védelmi réteg MQTT protokollhoz

Intelligens mezőgazdasági rendszerekben, ahol a talajnedvesség-szenzorok adatait felhő alapú rendszerbe továbbítják:
Protokoll verzió: TLS 1.3, amely kiküszöböli a régebbi verziók biztonsági hiányosságait
Tanúsítványkezelés: Let's Encrypt X.509 tanúsítványok automatikus megújítással
Algoritmusok: ECDHE-ECDSA-AES256-GCM-SHA384 kódcsomag
Példa konfiguráció (Mosquitto MQTT broker):

```
listener 8883
protocol mqtt
cafile /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
tls_version tlsv1.3
```

SSH alapú biztonságos távoli hozzáférés

SCADA rendszerek karbantartása esetén a jelszóalapú hitelesítés helyett:
Kulcs típusa: 4096 bites RSA vagy ED25519 kulcspár
Hitelesítés: Kizárólag nyilvános kulcsos hitelesítés (PasswordAuthentication no)

Jogosultság korlátozás: Sudo szerepkörök alapos delegálása
Példa konfiguráció (/etc/ssh/sshd_config):

```
Protocol 2
HostKey /etc/ssh/ssh_host_ed25519_key
KexAlgorithms curve25519-sha256
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com
MACs hmac-sha2-512-etm@openssh.com
AllowUsers maintuser@192.168.1.100
AuthenticationMethods publickey
```

Biztonsági szempontok és ajánlott gyakorlatok

- **Időzített kulcscsere:** Kriptográfiai kulcsok rendszeres (pl. évi) megújítása
- **Protokoll korlátozás:** Elavult SSL/TLS verziók és gyenge algoritmusok tiltása
- **Hálózati szegmentáció:** VPN végpontok elhelyezése DMZ zónában
- **Monitorozás:** Titkosított kapcsolatok aktív megfigyelése SIEM rendszerekkel
- **Folyamatos frissítés:** Biztonsági javítások időben történő alkalmazása

A biztonságos kommunikációs csatornák megvalósítása során különös figyelmet kell fordítani a kulcskezelésre, a protokoll konfigurációjára és a hozzáférés szigorú szabályozására. A fenti módszerek kombinációja jelentősen növeli a CPS rendszerek ellenálló képességét a kibertámadásokkal szemben, miközben megőrzi a rendelkezésre állást és az adatok integritását.

3.5 A fizikai hozzáférés elleni védelem (biztonságos helyiségek, fizikai behatolás elleni intézkedések)

A kiberfizikai rendszerek védelmében a fizikai biztonsági intézkedések ugyanolyan kritikus szerepet játszanak, mint a digitális védelem. A fizikai behatolás lehetőséget nyújt a támadóknak arra, hogy közvetlenül hozzáférjenek a kritikus infrastruktúrához, megkerülve ezzel a hálózati védelmi mechanizmusokat.

Atomenergia-üzemek példáján
Faraday-kalitka megvalósítása
A reaktorvezérlő terem speciális réz hálóval bevont falai teljesen blokkolják a külső rádiófrekvenciás jeleket (30 MHz - 40 GHz tartományban)
Kettős ajtórendszer (mantrap) biztosítja, hogy soha ne legyen egyidejűleg nyitva mindkét ajtó
Elektromágneses szűrők a kábelek bemeneténél megakadályozzák a TEMPEST támadásokat
Példa: A magyar Paksi Atomerőmű vezérlő terme 60 dB-es csillapítást biztosít a 2,4 GHz-es WiFi sávban

Rack szintű fizikai védelem
Biometrikus zárak (pl. HID Signo biometrikus olvasó) minden kritikus hálózati szekrényen
Súlyérzékelős rackek, amelyek riasztást adnak a jogosulatlan fizikai beavatkozás esetén

Rack beépített kamera minden szekrényben, amely a belépést követő 30 másodpercet rögzíti
Példa: A Siemens S7-1500 PLC-ket tartalmazó szekrényekhez csak 3 előjegyzett ujjlenyomat tárolás engedélyezett

Fokozott fizikai monitorozási rendszer
PIR mozgásérzékelők + hőmérséklet alapú lézeres érzékelők kombinációja
360 fokos PTZ kamerák (pl. Axis Q61) éjszakai látást biztosító infravörös megvilágítással
Hangalapú anomália detektálás (pl. a Schneider Electric EcoStruxure rendszere képes felismerni a szokatlan zajokat)
Példa: Egy német atomerőműben a fizikai biztonsági rendszer 150ms alatt képes riasztást generálni bármilyen szokatlan aktivitás esetén

Általános ajánlások CPS környezetekhez
Hozzáférési hierarchia:

- Zónákba osztás (nyilvános, korlátozott, magas biztonságú)
- Személyazonosító kártyák (NFC/PIV-II kompatibilis)
- Többtényezős hitelesítés fizikai belépéshez (kártya + biometria + PIN)

Környezeti védelem:

- Elektromágneses árnyékolás (EMSEC) minden kommunikációs eszköznél
- Faraday szekrények a tartalék kommunikációs eszközök tárolására
- Folyamatos légköri nyomás monitorozás a server termekben (lehetséges betörés észlelésére)

Karbantartói eljárások:

- Minden fizikai beavatkozás előzetes jóváhagyása
- Kísérő rendszer minden külsős szakember számára
- USB-portok fizikai letiltása epoxigyantával, kivéve a kijelölt audit pontokat

A fizikai és digitális biztonsági intézkedések integrált megvalósítása alapvető feltétele a valódi defense-in-depth stratégia kialakításának. A fenti módszerek alkalmazásával a kritikus infrastruktúrát képező CPS rendszerek jelentősen növelhetik ellenálló képességüket mind a fizikai, mind a digitális fenyegetésekkel szemben.

3.6 Tipikus sérülékenységek és támadási pontok az infrastruktúrában

A kiberfizikai rendszerekben számos kritikus sérülékenység jelenthet komoly biztonsági kockázatot. Ezek közül négy fő területet különösen fontos megemlíteni:

1. Elavult rendszerek és szoftverek

Probléma: A 2010-es Windows XP operációs rendszeren futó SCADA szerverek gyakran találhatók ipari környezetben, annak ellenére, hogy a Microsoft már 2014-ben megszüntette a támogatást. A WannaCry ransomware 2017-ben pontosan az ilyen rendszerek ellen irányult, kihasználva az EternalBlue exploitot.

Valós példa: A brit NHS (National Health Service) 2017-es kibertámadása során több mint 70.000 eszköz fertőződött meg, köztük MRI készülékek és műtői berendezések.

Megoldások:

- Air-gapped hálózat kialakítása a legkritikusabb rendszerek számára
- Virtuális javítás (Shield) alkalmazása, ha a frissítés nem lehetséges

- Virtualizált környezetbe migrálás (pl. VMware ESXi)

2. Gyenge hitelesítési mechanizmusok

Probléma: Az ipari eszközök gyakran alapértelmezett hitelesítő adatokkal kerülnek forgalomba. A Mitsubishi PLC-k esetében a "MELSEC" jelszó használata különösen veszélyes.

Statisztika: A Shodan kereső szerint 2023-ban több mint 1,200 nyilvánosan elérhető PLC található az interneten alapértelmezett bejelentkezési adatokkal.

Megoldások:

- Minden eszközön azonnali jelszóváltoztatás üzembe helyezéskor
- Többtényezős hitelesítés (MFA) bevezetése
- IP-alapú hozzáférési korlátozás (ACL)

3. Nem biztonságos ipari protokollok

Probléma: A Modbus TCP protokoll hiányosságai:

- Nincs beépített hitelesítés
- Nincs adatintegritás ellenőrzés
- Nincs titkosítás

Kockázat: A CVE-2020-14420 azonosítójú sebezhetőség lehetővé teszi, hogy a támadó hamis parancsokat küldjön a PLC-nek.

Megoldások:

- OPC UA használata a Modbus helyett
- Protokoll burkolás VPN vagy TLS segítségével
- Hálózati szegmentáció és mélypacket vizsgálat

4. Fizikai biztonsági réseken keresztüli támadások

Probléma: A USB Rubber Ducky eszköz képes emulálni egy billentyűzetet, és előre programozott parancsokat futtatni.

Támadási forgatókönyv:

- A támadó csatlakoztatja az eszközt
- A rendszer billentyűzetként ismeri fel
- Automatikusan végrehajtódik a rosszindulatú PowerShell szkript

Megoldások:

- USB-portok fizikai letiltása
- Csak aláírt szkriptek végrehajtásának engedélyezése
- Device Control szoftverek alkalmazása (pl. McAfee DLP)

Kiegészítő védelmi stratégiák:

- **Folyamatos sebezhetőség-értékelés:** Nessus vagy OpenVAS szkennelések havonta
- **Anomália detektálás:** AI-alapú megoldások a hálózati forgalom elemzésére
- **Incident Response terv:** Előre meghatározott válaszmechanizmusok
- **Szimulációs támadások:** Red Team gyakorlatok évente

A fenti sérülékenységek elleni védelem nélkülözhetetlen a kritikus infrastruktúra biztonságos működéséhez. A legfontosabb szempont a proaktív megközelítés - a problémák azonosítása és kezelése még azelőtt, hogy azok kompromittálhatnák a rendszert.

4 MEGFELELŐSÉGI KÖVETELMÉNYEK: A NIS2 ELŐÍRÁSOK RÉSZLETES ELEMZÉSE, VALAMINT A TECHNIKAI ÉS ADMINISZTRATÍV INTÉZKEDÉSEK BEMUTATÁSA

4.1 A NIS2 irányelv célja és hatálya (EU-s és magyarországi jogi háttér)

A **NIS2 irányelv** (Network and Information Security Directive 2), hivatalosan az **(EU) 2022/2555 irányelv**, az Európai Unió válasza a növekvő kiberbiztonsági kihívásokra, amely az előző, 2016-os NIS irányelvet váltja fel. Célja, hogy egységes és magas szintű kiberbiztonsági védelmet biztosítson a tagállamok kritikus infrastruktúrái és digitális szolgáltatói számára.

Célkitűzések:

- **Egységes kiberbiztonsági szabványok kialakítása:** A tagállamok közötti eltérések csökkentése érdekében az irányelv közös minimumkövetelményeket határoz meg.
- **Kockázatkezelési intézkedések bevezetése:** Az érintett szervezeteknek átfogó kockázatkezelési stratégiákat kell kidolgozniuk és alkalmazniuk.
- **Incidenskezelési és jelentési kötelezettségek meghatározása:** Az incidensek gyors felismerése és kezelése érdekében részletes jelentési protokollokat ír elő.

Hatály: A NIS2 irányelv kiterjed mind az **alapvető fontosságú** (essential), mind a **fontos** (important) entitásokra, amelyek a következő ágazatokban tevékenykednek:

Alapvető fontosságú ágazatok:

- Energia (villamosenergia, gáz, olaj)
- Közlekedés (légi, vasúti, vízi, közúti)
- Banki és pénzügyi piac infrastruktúrák
- Egészségügy
- Ivóvíz és szennyvíz
- Digitális infrastruktúra
- Közigazgatás
- Űrkutatás

Fontos ágazatok:

- Postai és futárszolgálatok
- Hulladékgazdálkodás
- Vegyipar
- Élelmiszeripar
- Gyártás (pl. gépjármű, elektronika)
- Digitális szolgáltatások (pl. online piacterek, keresőmotorok)

- Kutatás és fejlesztés

Magyarországi jogi háttér: Magyarországon a NIS2 irányelv átültetése érdekében 2024-ben elfogadták a **2024. évi LXIX. törvényt**, amely 2025. január 3-án lépett hatályba. Ez a törvény felváltotta a korábbi, 2023. évi XXIII. törvényt, és kibővítette annak rendelkezéseit. A törvény célja az elektronikus információs rendszerek védelmének fokozása, különös tekintettel az állami és közszolgáltatási infrastruktúrák védelmére a kibertámadásokkal szemben.

Főbb rendelkezések:

- **Elektronikus rendszerek védelme:** Az állami és közszolgáltatási infrastruktúrák elektronikus rendszereinek fokozott védelme.
- **Tanúsítási és megfelelőségértékelő szervezetek szerepe:** A tanúsító és megfelelőségértékelő szervezetek feladatainak és kötelezettségeinek meghatározása.
- **Adatkezelési és sérülékenységi vizsgálatok szabályozása:** Az adatkezelés és a sérülékenységi vizsgálatokra vonatkozó előírások részletezése.
- **Poszt-kvantum titkosítás alkalmazása:** A poszt-kvantum titkosítási technológiák bevezetésének előírása.
- **Telekommunikációs infrastruktúra kiépítése:** 2027-től kezdődően az új telekommunikációs infrastruktúrák városi területeken történő föld alatti elhelyezésének kötelezettsége.

Felügyeleti hatóság: A törvény végrehajtásáért a **Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH)** felelős, amely felügyeli a megfelelőséget, auditokat végez, és érvényesíti a szabályozásokat mind a köz-, mind a magánszektorban.

4.2 Kritikus infrastruktúra védelmére vonatkozó előírások és kötelezettségek

A NIS2 irányelv egyik kiemelt célterülete a **kritikus infrastruktúrák** védelme. Ezek olyan létesítmények, hálózatok, rendszerek vagy szolgáltatások, amelyek működése alapvetően befolyásolja a társadalom, a gazdaság, a közegészség és a nemzetbiztonság stabilitását. Bármely fennakadás ezek működésében katasztrofális következményekkel járhat, ezért az uniós és nemzeti jogalkotás különleges figyelmet fordít ezek biztonságára.

A kritikus infrastruktúra fogalma

Az Európai Unió az alábbi ágazatokat tekinti elsődleges kritikus infrastruktúráknak:

- **Energia** (villamosenergia, gáz, olaj)
- **Közlekedés** (vasúti, légi, vízi, közúti)
- **Vízgazdálkodás** (ivóvízellátás, szennyvízkezelés)
- **Egészségügy**
- **Digitális infrastruktúra** (adatközpontok, DNS-szolgáltatók, internet exchange-ek)
- **Pénzügyi szolgáltatások**
- **Élelmiszerlánc**

A kritikus infrastruktúrák meghatározása nemcsak uniós szinten történik, hanem **nemzeti szinten is**, hiszen az egyes tagállamok más-más stratégiai prioritásokkal rendelkezhetnek. Magyarországon a 2012. évi CLXVI. törvény és a 65/2013. (III. 8.) Korm. rendelet határozza meg a nemzeti létfontosságú rendszerelemeket és ágazatokat.

Kötelezettségek a kritikus infrastruktúrákat üzemeltető szervezetek számára

Követelmény	Leírás
Kockázatkezelési intézkedések	Minden szervezetnek kötelező a saját ágazati kockázataira szabott védelmi rendszer kiépítése.
Incidensjelentés	Súlyos incidensek esetén 24 órán belül előzetes, majd 72 órán belül részletes jelentés kötelező.
Műszaki és szervezeti védelem	Titkosítás, hálózati forgalom megfigyelése, tűzfalak, IDS/IPS rendszerek alkalmazása kötelező.
Audit és felügyelet	Rendszeres ellenőrzés és audit a kijelölt nemzeti hatóság (Magyarországon: SZTFH) részéről.
Ellenállóképesség fokozása	Vészhelyzeti tervek, üzletmenet-folytonosság biztosítása, rendszeres gyakorlatok.

Példa a megfelelésre: Energetikai szektor vs. Egészségügy

Jellemző	Energetikai szektor	Egészségügy
Védelmi rendszerek típusa	SCADA-tűzfalak, redundáns hálózatok	Kórházi informatikai rendszerek titkosítása
Gyakori támadástípusok	Ransomware, DDoS, állami támogatású támadások	Adatlopás, zsarolóvírus
Jogi megfelelőségi szint	Magas (fokozott ellenőrzés)	Közepes-magas (különösen járvány idején)
Kritikus következmény	Áramkimaradás, közellátási zavarok	Életek veszélyeztetése, bizalmi válság

Az EU-s és magyar felügyeleti mechanizmusok

A NIS2 előírja, hogy minden tagállam nevezze ki a kritikus infrastruktúrák biztonságáért felelős hatóságokat. Magyarországon ez a **Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH)**, amely az alábbiakat végzi:

- Kritikus szolgáltatók nyilvántartása
- Kockázatértékelési módszerek jóváhagyása
- Incidensek jelentésének fogadása és koordinálása
- Megfelelőségi auditok végrehajtása
- Bírság kiszabása (súlyos mulasztás esetén akár az éves forgalom 2%-a)

Kihívások és problémák

1. Szakember hiány:

2023-as ENISA jelentés szerint az EU-ban több mint **200.000 kiberbiztonsági szakember hiányzik**, ami különösen nehézzé teszi a kritikus szektorok védelmét.

2.Legacy rendszerek:

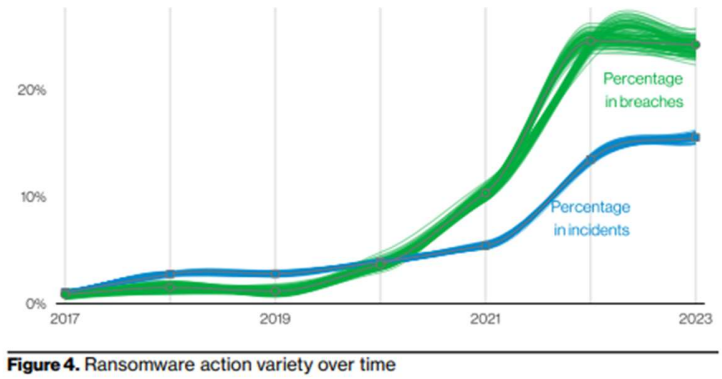
Sok kritikus infrastruktúra (pl. vízművek, kórházak) elavult, 10–15 éves rendszereket használ, amelyek nem kompatibilisek a modern védelemmel.

3. Határokon átnyúló incidensek:

Mivel az energiahálózatok és informatikai rendszerek szoros kapcsolatban állnak más országokkal, az egyik országban bekövetkező incidens másokat is érinthet. Erre példa a 2015-ös **ukrán áramszünet**, amely a teljes Nyugat-Európára figyelmeztető jel volt.

Statisztikai háttér (ENISA 2023 jelentés alapján):

Ágazat	Bejelentett incidensek száma (EU, 2022)	Leggyakoribb támadás	Átlagos helyreállási idő
Energia	183	Ransomware	3 nap
Egészségügy	245	Adatlopás	5 nap
Közlekedés	92	DDoS	1 nap
Digitális infrastruktúra	138	Exploit, Malware	2,5 nap



Ransomware remains a top action type.

Ransomware continues its reign as one of the top action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

Figure 4. Ransomware action variety over time

- DBIR 2023 Data Breach Investigations Report

A kritikus infrastruktúrák védelme nem csupán technikai kérdés, hanem stratégiai jelentőségű nemzetbiztonsági feladat. A NIS2 irányelv a jelenlegi legátfogóbb szabályozás, amely egységes követelményrendszert hoz létre az EU-ban. Magyarország jogi szabályozása összhangban van ezzel, de a gyakorlati megvalósítás számos kihívással szembesül: szakemberhiány, elavult rendszerek, pénzügyi források hiánya. A megfelelés azonban nem választható opció, hanem kulcseleme az állam és a társadalom biztonságának.

4.3 Biztonsági incidensek kezelése és jelentési kötelezettségek

A NIS2 irányelv egyik központi eleme a **kibertámadások és egyéb biztonsági incidensek kezelése és jelentése**. Az irányelv célja, hogy egységes európai protokollt hozzon létre a hálózat- és információbiztonság területén, különösen a kritikus szolgáltatók körében. Az incidensek időbeni felismerése, hatékony kezelése és a gyors bejelentés nélkülözhetetlen ahhoz, hogy megelőzhetővé váljanak a súlyos társadalmi és gazdasági következmények.

Mi minősül biztonsági incidensnek?

A NIS2 irányelv alapján biztonsági incidensnek tekinthető minden olyan esemény, amely:

- **Sérti az adatok integritását, rendelkezésre állását vagy bizalmasságát**
- **Zavart okoz az információs rendszerek működésében**
- **Hatással van a szolgáltatás folyamatosságára vagy minőségére**

Példák:

- Ransomware támadás egy kórházi rendszer ellen

- Szándékos adatszivárogtatás
- Kritikus frissítés hibás telepítése miatti leállás
- Szolgáltatásmegtagadási (DDoS) támadás

Jelentési kötelezettségek a NIS2 szerint

A NIS2 bevezeti az ún. **lépcsőzetes jelentési rendszert**, amely három szintű jelentést ír elő a kijelölt szervezetek számára.

Jelentés típusa	Határidő	Tartalom
Korai figyelmeztetés	Az incidens észlelésétől számított 24 órán belül	Rövid helyzetértékelés, előzetes következmények
Részletes jelentés	72 órán belül	Támadás jellege, terjedelme, hatása, technikai részletek, intézkedések
Zárójelentés	1 hónapon belül	Teljes körű eseményanalízis, helyreállítási lépések, tanulságok

A jelentéseket a nemzeti hatósághoz (Magyarországon az SZTFH-hoz) kell benyújtani, amely további intézkedéseket tehet (pl. figyelmeztetés kiadása, audit elrendelése).

Összehasonlító táblázat: NIS1 vs. NIS2 incidenskezelési elvárások

Szempont	NIS1 (2016)	NIS2 (2022)
Jelentés határideje	72 órán belül	24 órás előzetes, majd 72 órás részletes jelentés
Szankciók	Mérsékeltek (főként figyelmeztetés)	Súlyos bírság (max. 10 millió euró vagy az árbevétel 2%-a)
Elvárt kockázatelemzés	Nincs egységes szint	Részletes előírás a kockázatok felmérésére és kezelésére
Szabályozott ágazatok köre	Korlátozott	Jelentősen bővült (pl. postai, hulladék, gyártás is bekerült)

Incidensmenedzsment lépései a gyakorlatban (ENISA-ajánlás alapján)

1.Felderítés és észlelés

- Behatolásészlelő rendszerek (IDS), logok elemzése, SIEM-rendszerek használata

2.Értesítés és eszkaláció

- Incidenskoordinátor, belső és külső kommunikáció, felügyeleti szerv értesítése

3.Elemzés

- Támadási vektor meghatározása, érintett rendszerek és adatok azonosítása

4.Elhárítás

- Fertőzött gépek elszigetelése, szolgáltatások ideiglenes leállítása

5.Helyreállítás

- Biztonsági mentések visszatöltése, újraindítás kontrollált környezetben

6.Utóelemzés (post-mortem)

- Hibák feltárása, javaslatok dokumentálása, új védelmi szabályok bevezetése

Magyarországi gyakorlat és kihívások

Magyarországon a 2023-ban módosított **Kibertér-védelmi Törvény** beemelte a NIS2 előírásokat a hazai jogrendbe. A kijelölt szolgáltatóknak regisztrálniuk kell magukat az SZTFH-nál, és vészhelyzeti tervet kell kidolgozniuk.

Főbb kihívások:

- **Szakmai kapacitáshiány**: A kisebb szolgáltatóknál nincs dedikált IT biztonsági csapat.
- **Technikai elmaradottság**: Elavult eszközpark, korlátozott monitoring.
- **Jogi tudatosság hiánya**: Sok szervezet nem ismeri pontosan a jelentési kötelezettségeit.

Példák súlyos incidensekre és tanulságokra

1. Colonial Pipeline (USA, 2021)

Ransomware miatt 5 napra leállt az Egyesült Államok legnagyobb üzemanyagvezeték-hálózata. Az incidens megrázta az energiapiacot, és világszinten ösztönözte a kritikus infrastruktúrák védelmét.

2. HSE (Health Service Executive – Írország, 2021)

Az ír egészségügyi rendszer teljes informatikai rendszere megbénult egy zsarolóvírus-támadás miatt. Több mint 80.000 eszköz vált használhatatlanná. A helyreállítás költsége: 100 millió euró.

3. Ukrajnai energiahálózati támadás (2015)

Célzott, államilag támogatott támadás több város áramellátását is megbénította. Az incidens rávilágított arra, hogy **CPS-rendszerek** milyen sebezhetőek, ha nincs megfelelő incidenskezelési gyakorlat.

ENISA 2023 riport – incidensek megoszlása

Támadástípus	Előfordulási arány (%)	Átlagos észlelési idő	Költség/átlagos incidens (EUR)
Ransomware	38%	48 óra	250.000
Phishing & social eng.	25%	72 óra	150.000
DDoS	18%	12 óra	50.000
Zero-day exploit	9%	96 óra	300.000
Egyéb	10%	–	–

Az incidenskezelés nem csupán reagálás, hanem **proaktív kockázatmenedzsment** is. A NIS2 előírásai jelentősen megnövelik a szolgáltatók felelősségét és átláthatóságát. A jól működő incidensmenedzsment-rendszer nemcsak a kár minimalizálását, hanem a bizalom fenntartását is szolgálja. Ennek feltétele a technikai infrastruktúra, a szabályozott folyamatok és a képzett szakemberek hármas egysége.

„Cybersecurity is not just a technical issue, it is also a legal and strategic imperative."
— ENISA (European Union Agency for Cybersecurity)

4.4 Technikai védelmi intézkedések (hálózati monitoring, behatolásmegelőzés, titkosítás, sandboxing)

A technikai védelmi intézkedések a NIS2 irányelv és általában a hálózatbiztonság egyik alappillérét képezik. Céljuk a rendszerek és hálózatok integritásának, bizalmasságának és rendelkezésre állásának megőrzése az egyre kifinomultabb kibertámadásokkal szemben. A NIS2 nemcsak előírja ezen intézkedések meglétét, de elvárja azok rendszeres felülvizsgálatát, tesztelését és naprakészen tartását is.

Alapvető technikai intézkedések a NIS2 alapján

Intézkedés típusa	Konkrét példák	Cél és előny
Hozzáférés-szabályozás	Többlépcsős azonosítás (MFA), RBAC, jelszavak	Csökkenti az illetéktelen hozzáférések kockázatát
Titkosítás	TLS, AES-alapú adattárolás, VPN	Védi az adatok bizalmasságát, különösen átvitel során
Tűzfalak	Hálózati (periméter) és host-alapú tűzfalak	Határok védelme, nem kívánt kapcsolatok blokkolása
IDS/IPS rendszerek	Snort, Suricata, Zeek, Cisco Secure IPS	Gyanús tevékenységek észlelése és automatikus válaszadás
Naplózás és SIEM	Splunk, IBM QRadar, Elastic Stack	Események rögzítése és korrelálása, incidens észlelés és elemzés
Patch management	Automatikus frissítések, CVE-figyelés	Sérülékenységek gyors javítása, exploit megelőzése
Hozzáférési naplók	Admin tevékenységek, belépések, konfigurációk	Átláthatóság, utólagos ellenőrizhetőség

Tűzfalak: hálózati határvédelem

A tűzfalak a hálózati védelem első vonalát képezik. Két fő típusuk:

- **Statikus tűzfal (ACL alapú)** – csomagszűrés IP, port alapján
- **Alkalmazás-szintű tűzfal (Layer 7)** – képes HTTP, DNS, FTP forgalom elemzésére

Zero Trust modellek esetén a hálózati szegmentáció és **mikroperimeterek** tűzfalas védelme válik fontossá, így például a gyártósor egyik PLC-je nem kommunikálhat közvetlenül a könyvelési rendszerrel.

IDS/IPS rendszerek összehasonlítása

Rendszer	Működés	Előny	Hátrány
IDS	Észleli a támadásokat	Nem zavarja a forgalmat	Nem avatkozik be automatikusan
IPS	Észlel és be is avatkozik	Valós idejű védelem	Potenciális téves blokkolás

Gyakorlati példa: egy SCADA rendszerbe betörni próbáló IP-t az IDS észlel, az IPS pedig automatikusan tiltja azt a tűzfalon.

Titkosítás – adatvédelem az átvitel és tárolás során

A **titkosítás** ma már nem opció, hanem elvárás, különösen a kritikus szektorokban. A gyakorlatban a következő megoldások jellemzőek:

- **TLS 1.3** – biztonságos kommunikáció webes szolgáltatásoknál
- **AES-256** – fájlok, adatbázisok titkosítása
- **IPSec/VPN** – távoli hozzáférések titkosítása, például telepített mérnökök részére

Frissítések és sérülékenység-menedzsment

Az elavult szoftverek jelentik a támadók egyik kedvenc célpontját. A NIS2 értelmében minden szolgáltatónak rendelkeznie kell:

- **Sérülékenységi nyilvántartással** (CVE-figyelés)
- **Frissítési protokollal**
- **Rendszeres auditálással**

Példa: a WannaCry zsarolóvírus 2017-ben egy Windows SMB-sérülékenységet (CVE-2017-0144) használt ki, amelyet a Microsoft hónapokkal korábban már kijavított.

Naplózás és SIEM-rendszerek szerepe

A **Security Information and Event Management (SIEM)** rendszerek lehetővé teszik több adatforrás eseményeinek valós idejű korrelálását. Használatuk előnyei:

- Gyorsabb incidensészlelés
- Forensics támogatás (esemény-visszajátszás)
- Jogszabályi megfelelés biztosítása (pl. GDPR, NIS2)

Bevált megoldások:

- **Splunk** – nagyvállalati környezetek
- **Elastic Stack (ELK)** – nyílt forráskódú, testre szabható
- **Wazuh** – SIEM + HIDS megoldás, felhasználóbarát interfésszel

Példa: Gyártási hálózat védelme

Egy automatizált gyártósort védő rendszer jellemző technikai elemei:

- PLC eszközök leválasztása VLAN-onként
- Tűzfal és IPS közéjük és az IT-hálózat közé
- VPN-alapú hozzáférés a külső szervizpartnereknek
- Forrás IP-hez kötött hozzáférés, MFA minden adminhoz

Technikai védelmi hiányosságok (ENISA 2023)

Hiányosság típusa	Előfordulás a vizsgált cégek 54%-ánál
Frissítés hiánya	61%
Gyenge hozzáférés-kezelés	47%
Titkosítás hiánya	39%
Nem naplózott események	34%
Hiányzó IDS/IPS rendszer	29%

Nemzetközi standardok a technikai védelemben

A NIS2 irányelv mellett több szabvány is előírja a technikai kontrollokat:

Szabvány	Kulcsterületek
ISO/IEC 27001	Információbiztonsági menedzsment, kockázatalapú védekezés
IEC 62443	Ipari automatizálás védelme (SCADA, PLC)
NIST SP 800-53	Állami rendszerek részletes technikai kontrolllistája

A technikai védelmi intézkedések rendszerének kiépítése **nem egy statikus projekt, hanem egy dinamikus folyamat**. Az új fenyegetésekhez való alkalmazkodás, az automatizáció és a mesterséges intelligencia integrálása (pl. prediktív anomáliafelderítés SIEM-ben) jelenti a következő fejlődési szintet. A NIS2 előírásainak való megfelelés csak akkor érhető el, ha a védelem áthatja az egész hálózatot – a peremterületektől az alkalmazások szintjéig.

4.5 Adminisztratív intézkedések (hozzáféréskezelés, kockázatelemzés, megfelelőségi auditok, kiberbiztonsági oktatás)

A kiber-fizikai rendszerek (CPS) biztonsága nem épülhet kizárólag technikai megoldásokra, mint a tűzfalak, behatolásérzékelő rendszerek vagy szegmentáció. A **szabályozási és emberi tényezők** legalább ilyen meghatározó szerepet játszanak. Az adminisztratív intézkedések célja a **szervezeti szintű biztonsági tudatosság**, a **folyamatok átláthatósága** és a **kockázatok megelőzése**.

Hozzáféréskezelés (Access Control)

A jogosulatlan hozzáférés az egyik leggyakoribb biztonsági incidens forrása. A hozzáféréskezelés célja, hogy csak az arra jogosult személyek férhessenek hozzá a megfelelő adatokhoz vagy vezérlő rendszerekhez.

Alapelvek:

- **Legkisebb jogosultság elve (Principle of Least Privilege):** Minden felhasználónak csak annyi hozzáférést biztosítanak, amennyire a feladatai ellátásához feltétlenül szüksége van.
- **Szerepköralapú hozzáférés (Role-Based Access Control – RBAC):** Az egyének jogait szerepkörök határozzák meg (pl. mérnök, operátor, adminisztrátor).
- **Időalapú vagy ideiglenes jogosultság:** Kritikus rendszerekhez való hozzáférés csak meghatározott időtartamra vagy külön engedéllyel történhet.

Hozzáférés típusa	Példa
Fizikai hozzáférés	Szerverterem, vezérlőszoba belépési jogosultság
Logikai hozzáférés	PLC konfiguráció, SCADA bejelentkezés, fájlszerver
Távoli hozzáférés	VPN, SSH, RDP – többfaktoros hitelesítéssel

Támadási példa:

A 2021-es floridai vízmű támadás során a támadó távoli hozzáféréssel növelte a víz lúgosító anyagának szintjét. A probléma gyökere a távoli asztal (RDP) és az adminisztrátori jogok helytelen kezelése volt.

Kockázatelemzés (Risk Assessment)

A CPS rendszerek biztonságának alapja a **szisztematikus kockázatelemzés**. Ennek célja, hogy feltárja a sebezhetőségeket, és azok lehetséges következményeit.

Kockázatelemzés fő lépései:

- **Értékazonosítás** – Mely vagyonelemeket kell védeni? (pl. termelésirányító rendszer, szenzoradatok)
- **Fenyegetések azonosítása** – Külső (hacker, állami támadó), belső (elégedetlen dolgozó)
- **Sebezhetőségek feltérképezése** – Nem frissített firmware, nyílt portok, rossz jelszavak
- **Hatásvizsgálat** – Mi történik, ha egy komponens sérül?
- **Kockázatértékelés** – Valószínűség × hatás = kockázat szintje

- **Intézkedések tervezése** – Milyen kontrollokat kell bevezetni?

Példa kockázat	Valószínűség	Hatás	Összesített kockázat
PLC kompromittálása	Közepes	Nagy	**Magas**
SCADA jelszólopás	Magas	Nagy	**Kritikus**
Nem frissített eszköz	Magas	Közepes	**Magas**

Szabványos eszközök:

- ISO/IEC 31000 – Kockázatmenedzsment
- NIST SP 800-30 – IT kockázatelemzés útmutató
- IEC 62443-3-2 – Ipari rendszerek kockázatértékelése

Megfelelőségi auditok

A kiberbiztonság nem csak a védekezésről, hanem a **folyamatos megfelelésről** is szól. Az auditálás célja, hogy:

- Évente/negyedévente ellenőrizze a rendszer biztonságát
- Dokumentálja a hiányosságokat
- Elősegítse a jogszabályi és szabványi megfelelést (compliance)

Típusai:

- **Belső audit** – Saját szervezet végez (IT-biztonsági felelős vagy compliance officer)
- **Külső audit** – Független szakértő végzi (pl. tanúsítók, hatóságok)
- **Szabályozási audit** – NIS2, GDPR vagy egyéb irányelv szerint

Audit típusa	Példa célja
Technikai audit	Tűzfal, naplózás, patch management ellenőrzés
Folyamat audit	Hozzáférési szabályok, incidenskezelés
Fizikai biztonság	Szerverek, vezérlőhelyiségek, kártyaolvasók

NIS2 például előírja:

- Incidenskezelési eljárások meglétét
- Vészhelyzeti helyreállítási tervet
- Rendszeres biztonsági auditokat

Kiberbiztonsági oktatás

A humán tényező a leggyengébb láncszem a legtöbb kiberincidens során. Éppen ezért **kulcsfontosságú a rendszeres oktatás és tudatosítás**.

Főbb célcsoportok:

- **Mérnökök és karbantartók:** Eszközfrissítések, hozzáférések, jelszavak helyes használata
- **Operátorok:** Gyanús viselkedés felismerése, alapvető incidensjelentés
- **Vezetők:** Kockázattudatosság, döntéshozatali támogatás
- **Új belépők:** Alapképzés minden új alkalmazottnak

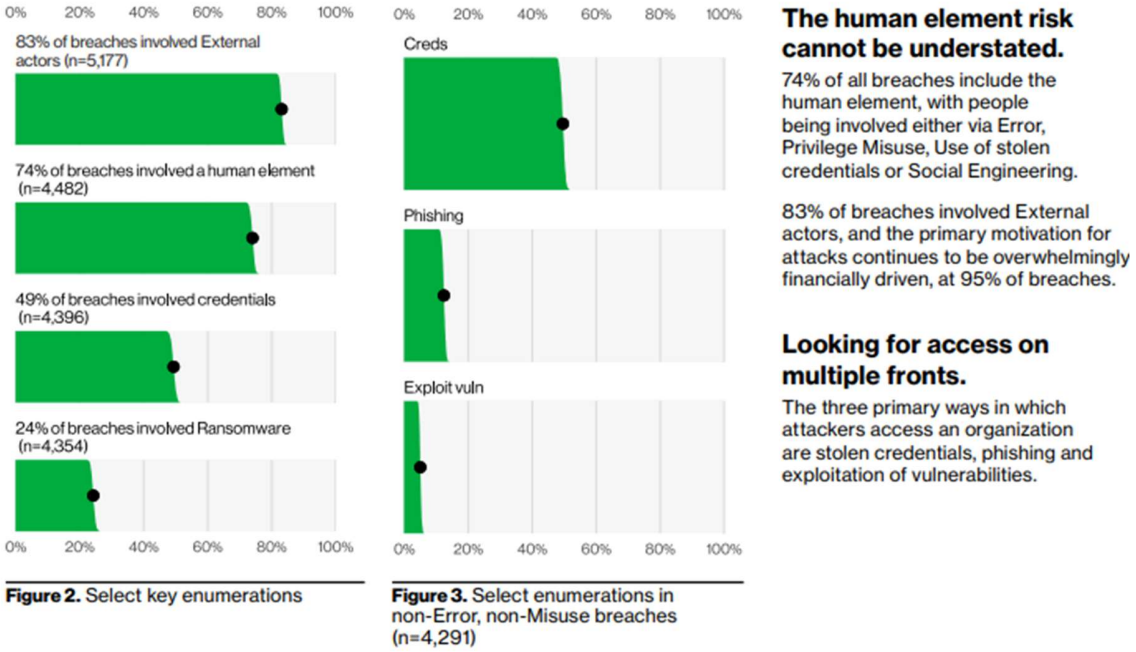
Témakörök:

- Adathalászat felismerése

- Hozzáférési szabályok
- Gyanús fájlok/USB eszközök kezelése
- Social engineering példák

Oktatás típusa	Rendszeresség	Módszer
Alapképzés	Belépéskor	Prezentáció + teszt
Éves frissítő	Évente 1×	Online kurzus, kvíz
Rendszerspecifikus	Új technológia bevezetésekor	Workshop, gyakorlat

A *SANS Institute* 2023-as kutatása szerint a cégek 65%-a tapasztalt biztonsági incidenst, amely egy **emberi hibából** – például rossz linkre kattintásból – indult ki. Az oktatás bevezetése után ezek 45%-kal csökkentek.



- DBIR 2023 Data Breach Investigations Report

Az adminisztratív intézkedések **keretet adnak a technikai védekezésnek**, és biztosítják, hogy a rendszerek nemcsak működnek, hanem **biztonságosan és fenntarthatóan működnek**. A hozzáféréskezelés, kockázatelemzés, auditálás és oktatás együttesen képezik a **kiberbiztonsági kultúra** alapjait, ami elengedhetetlen a CPS rendszerek megbízható üzemeltetéséhez – különösen a kritikus infrastruktúrák világában.

5 HATÁRVÉDELEM FELÉPÍTÉSE: TŰZFALAK, IDS/IPS RENDSZEREK ÉS MÁS HATÁRVÉDELMI TECHNOLÓGIÁK ALKALMAZÁSA

5.1 Tűzfalak és alkalmazásuk a CPS-hálózatokban (hagyományos tűzfalak vs. NGFW-k)

A **kiber-fizikai rendszerek (Cyber-Physical Systems – CPS)** védelmében kulcsszerepet játszanak a **tűzfalak**, melyek a hálózati forgalmat ellenőrizve szabályozzák az adatáramlást az egyes rendszerek és szegmensek között. A **klasszikus IT-tűzfalak** alkalmazása az ipari rendszerekben azonban számos kihívással jár, ezért egyre inkább előtérbe kerülnek a **Next Generation Firewall-ok (NGFW-k)**, melyek képesek alkalmazásszintű és protokollspecifikus vizsgálatokat is végezni.

A tűzfalak szerepe a CPS-hálózatokban

A CPS hálózatok többszintű architektúrája – ahol IT- és OT-rendszerek (Operational Technology) működnek együtt – különösen sérülékeny a külső és belső fenyegetésekkel szemben. A tűzfalak elsődleges célja itt a **szegmentáció** biztosítása, az **engedélyezett kommunikáció szabályozása**, valamint a **gátként való működés** az illetéktelen hozzáférések ellen.

Tűzfalalkalmazási helyek a CPS-ben:

- **IT-OT határ** (pl. vállalati hálózat és SCADA központ között)
- **DMZ zóna** létrehozása a külső hozzáférések izolálására
- **PLC-k és vezérlők védelme** a vezetékezett hálózatokban
- **Távoli hozzáférések (VPN, RDP)** monitorozása

Hagyományos tűzfalak (Packet Filtering, Stateful Inspection)

A **hagyományos tűzfalak** a forgalmat alapesetben a következő paraméterek alapján vizsgálják:

- IP-cím
- Portszám
- Protokoll (TCP, UDP, ICMP)
- Kapcsolati állapot (Stateful Inspection)

Előnyök:

- Egyszerű beállítás
- Alacsony erőforrásigény
- Megfelelő alapszintű szegmentációra

Hátrányok:

- Nem képesek megkülönböztetni alkalmazásszintű forgalmat (pl. Modbus vs. HTTP)
- Nem képesek detektálni anomáliákat vagy alkalmazásréteg támadásokat
- Nincs mély csomagvizsgálat (Deep Packet Inspection – DPI)

Jellemző	Hagyományos tűzfal
IP/Port szűrés	✓
Protokollalapú döntés	✓
DPI / alkalmazásszint	✗
ICS-protokoll támogatás	✗
Fenyegetésdetekció	✗

Gyakorlati példa: Egy klasszikus ipari SCADA rendszer, amelyet egy routeren keresztül védenek IP-alapú szűréssel – nem fogja kiszűrni, ha például valaki egy Modbus TCP parancson keresztül próbálja manipulálni a PLC-t, mivel az engedélyezett IP-címről érkezik a kérés.

NGFW – Next Generation Firewall-ok

- https://www.linkedin.com/pulse/what-next-generation-firewall-ngfw-stephen-deal-cissp/

Az NGFW-k (új generációs tűzfalak) a hagyományos funkciók mellett **intelligens, alkalmazásalapú szűrést**, **vírus- és támadásdetekciót**, valamint **forgalomelemzést** is végeznek. Kifejezetten hasznosak ipari környezetben, ahol az **ICS/SCADA protokollokat ismerniük kell** (pl. DNP3, Modbus, OPC UA).

Funkciók:

- Alkalmazásszintű DPI (Layer 7)
- ICS-specifikus protokollfelismerés
- Anomália-érzékelés
- Integrált IDS/IPS (Intrusion Detection/Prevention System)
- Felhasználói és gépi viselkedéselemzés (UBA/UEBA)

Jellemző	NGFW
DPI – Deep Packet Inspection	✓
ICS-protokollok ismerete	✓
Támadásminta felismerés (signature-based)	✓
Gépi tanulásos anomáliadetekció	✓
Felhasználóalapú szabályozás	✓

Példa – Palo Alto, Fortinet, Cisco Firepower, Check Point:

Ezek a gyártók mind kínálnak olyan megoldásokat, amelyek képesek ipari protokollok kezelésére, például egy Modbus-parancs szintaktikai hibáinak felismerésére, vagy egy OPC UA csatorna manipulációjára figyelmeztetni.

Összehasonlítás: Hagyományos tűzfal vs. NGFW CPS környezetben

Kritérium	Hagyományos tűzfal	NGFW
IP/Port szűrés	✓	✓
DPI / Layer 7 felismerés	✗	✓
ICS protokoll támogatás	✗	✓
IDS/IPS integráció	✗	✓
Zero Trust támogatás	✗	✓
Felhasználó- és alkalmazáskontroll	✗	✓
Támadásszignatúrák kezelése	✗	✓

Következtetés:

A **hagyományos tűzfalak** elegendők lehetnek kisebb, zárt rendszerekben, vagy csak alapszintű szeparációra, de **a korszerű CPS hálózatokban NGFW-re van szükség**, mivel ezek képesek értelmezni az ipari protokollokat, figyelni a viselkedési mintákat és reagálni a finom támadásokra is.

Ajánlások CPS környezetekben

- **Szegmentálj zónákra és vezess be szabályalapú NGFW-t minden határra** (IT/OT, OT/vezérlők).
- **Használj DPI-t képes eszközt**, amely érti az adott ipari protokollokat (pl. Siemens S7, EtherCAT).
- **Állíts be riasztásokat és naplózást minden tiltott eseményre** – NGFW-k integrálhatók SIEM rendszerekbe.
- **Ne csak peremvédelmet alkalmazz**: alkalmazz NGFW-t belső szegmensek között is (pl. PLC és HMI között).
- **Rendszeresen frissítsd a tűzfal szignatúrákat**, mert az ICS támadások is fejlődnek (pl. TRITON, Industroyer2).

„There are only two types of companies: those that have been hacked, and those that will be."
— Robert Mueller, FBI igazgató (RSA Conference, 2012)

5.2 Intrusion Detection Systems (IDS) és Intrusion Prevention Systems (IPS) szerepe

A **kiber-fizikai rendszerek (CPS)** működésének védelme nem korlátozódhat csupán a peremvédelmi (pl. tűzfal) intézkedésekre. Az **Intrusion Detection Systems (IDS)** és **Intrusion Prevention Systems (IPS)** kritikus réteget képeznek a mélyebb hálózati forgalom elemzésében, és különösen fontosak az **anomáliák, ismeretlen fenyegetések vagy belső támadások észlelésében/megelőzésében**.

IDS és IPS: fogalmi alapok

Tulajdonság	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Funkció	Betörési kísérletek észlelése	Betörések aktív megelőzése
Működés	Forgalom figyelése, riasztás	Forgalom figyelése és blokkolás
Intervenció	Passzív – riasztást küld	Aktív – megszakítja a kapcsolatot
Elhelyezés	Jellemzően hálózati tükörporton	Átmenő forgalomban (inline)
Kockázat	Alacsony (nem avatkozik be)	Magasabb (téves pozitív esetén blokkolhat)

Az IDS fő célja tehát **riasztani**, az IPS viszont **megelőzni** is képes a támadást.

IDS/IPS típusok CPS környezetben

A CPS rendszerek sajátos igényei miatt az IDS/IPS rendszereket is testreszabottan kell alkalmazni:

a) Signature-based IDS/IPS (aláírás-alapú)

- Ismert támadási minták alapján dolgozik (pl. Snort szabályok).
- Hatékony ismert fenyegetések ellen.
- Gyors és pontos, de nem képes új, ismeretlen támadásokat felismerni.

b) Anomaly-based IDS/IPS (anomália-alapú)

- Tanulás vagy statisztikai modellezés alapján figyeli az „átlagos” viselkedést.
- Képes ismeretlen támadások felismerésére (zero-day).
- Viszont hajlamos lehet téves riasztásokra.

c) Hybrid IDS/IPS

- Kombinálja a signature- és anomaly-alapú elemzést.
- A leginkább javasolt ipari környezetekben, ahol fontos az egyensúly a védelem és a stabilitás között.

IDS és IPS alkalmazása CPS hálózatokban

A CPS rendszerek – különösen a SCADA, vezérlő, PLC-k és HMI-k közötti kommunikáció – különleges protokollokat (pl. Modbus, DNP3, S7) használnak, amelyekhez az IDS/IPS rendszereknek **specifikusan igazodniuk kell**.

Helyszín	Védelem típusa	Példa IDS/IPS használatra
IT–OT határ	IPS	Tiltott kapcsolat blokkolása
SCADA szerver védelme	IDS + SIEM	Anomália-észlelés (pl. szabálytalan lekérdezés)
HMI–PLC közötti kapcsolat	Anomaly-based IDS	Nem szokásos parancssorozat riasztása
Távoli elérés (VPN, RDP)	Signature-based IPS	Exploit kísérlet blokkolása

ICS-specifikus IDS/IPS megoldások

A klasszikus Snort vagy Suricata IDS motorokon túl mára már **ipari környezetre optimalizált** IDS/IPS rendszerek is elérhetőek, például:

Rendszer	Specializáció	Megjegyzés
Dragos	ICS/SCADA-specifikus, anomáliaérzékelés	Kiemelkedő protokollismeret
Nozomi Networks	OT-hálózatok elemzése és eszkalációja	Támogatja Modbus, S7, DNP3 stb.
Claroty	Teljes OT-eszközfeltérképezés + IDS	Integrálható SIEM-be
Cisco Secure IPS	Hybrid IPS, NGFW integrációval	Alkalmazásszintű vizsgálat
Snort / Suricata	Nyílt forráskódú, általános megoldások	Ipari szabályokkal bővíthetők

Példák támadások detektálására

- **Stuxnet (2010)** – Az IPS nem tudta volna megállítani, de egy anomáliaalapú IDS (amely figyeli a centrifugák parancsait) riaszthatott volna, hogy a vezérlési logika megváltozott.
- **Industroyer (2016)** – ICS protokollokat célzott (IEC-104). Egy signature-alapú IDS, amely ismeri az IEC-104 parancsok szerkezetét, képes lehetett volna a szokatlan vezérlési parancsokat azonosítani.
- **TRITON (2017)** – A biztonsági vezérlőket célozta. A megfelelő IPS blokkolhatta volna a változtatási kísérletet, míg egy IDS előre jelezhette volna a manipulációs kísérletet.

IDS/IPS integráció más rendszerekkel

A hatékony kiberbiztonsági stratégia részeként az IDS/IPS rendszereket gyakran **SIEM-ekkel**, **tűzfalakkal** és **hálózati monitorozó eszközökkel** integrálják:

- **SIEM (Security Information and Event Management)** – elemzi a riasztásokat, összefüggéseket keres és automatizálja az incidensválaszt.
- **Tűzfal + IPS** – sok NGFW már integrált IPS modullal működik.
- **Asset Inventory** – ha az IDS felismeri a hálózatba kerülő új, nem dokumentált eszközt, azt jelenteni kell.

Kihívások és ajánlások

Kihívás	Ajánlás
ICS protokollok felismerésének hiánya	Használj ipari IDS-t (pl. Nozomi)
Sok téves riasztás (false positive)	Finomhangolt szabályrendszer, tanulási idő
Integráció komplexitása	Előre tesztelt, modularizált megoldások
Vezérlési hálózat érzékenysége	IDS inkább megfigyelésre, ne IPS legyen elsőként

Összefoglalás és szerepük a CPS-védelemben

Az IDS/IPS rendszerek a **"második védelmi vonalat"** képezik, különösen akkor, ha a tűzfal már nem tudja kiszűrni a finomabb vagy belső támadásokat. Míg az IDS a forgalom elemzésével és riasztással támogatja a kiberbiztonsági elemzőket, az IPS képes **proaktívan blokkolni támadásokat**, így csökkentve az üzemzavarok kockázatát.

A megfelelő, ipari környezetre szabott IDS/IPS rendszer kiválasztása és integrálása **elengedhetetlen a CPS rendszerek biztonságos működéséhez**, különösen a kritikus infrastruktúrák és ipari automatizálási rendszerek esetében.

5.3 SIEM (Security Information and Event Management) rendszerek és biztonsági eseményelemzés

A CPS-rendszerekben keletkező adatok és események hatékony, valós idejű feldolgozása és elemzése kulcsfontosságú a kiberbiztonság fenntartása szempontjából. A **SIEM rendszerek** pontosan ezt a célt szolgálják: integrálják a hálózat és az eszközök naplóit (logokat), elemzik a gyanús viselkedést, és **riasztásokat vagy automatikus válaszokat generálnak**, ezzel segítve a biztonsági incidensek felismerését és kezelését.

A SIEM rendszerek alapfunkciói

A SIEM rendszerek két fő funkciót egyesítenek:

Funkció	Leírás
Security Information Management (SIM)	Történelmi logadatok tárolása, keresése, jelentéskészítés.
Security Event Management (SEM)	Valós idejű eseményfigyelés, korreláció, riasztás.

Egy modern SIEM rendszer képes az IT és OT környezet **teljes biztonsági képének** integrálására, és alkalmas arra, hogy a **CPS infrastruktúrában is hatékonyan működjön**.

SIEM működése CPS-rendszerben

Egy CPS-hálózatban különösen fontos a **heterogén rendszerekből** származó események összehangolt kezelése. A SIEM:

- gyűjti a **hálózati eszközök (switch, router, tűzfal)**,
- **IDS/IPS**,
- **vezérlőrendszerek (PLC, SCADA)**,
- **felhasználói tevékenység**,
- valamint **alkalmazások (VPN, Active Directory)** logjait.

Ezeket a logokat egy központi platformon tárolja, **összefüggéseket keres (korreláció)**, és lehetővé teszi a **gyors reagálást egy támadás esetén**.

SIEM előnyei CPS környezetben

Előny	Részletezés
Valós idejű riasztások	Gyanús események automatikus felismerése és eszkalálása.
Összefüggések keresése	Több logforrásból származó események összekapcsolása (pl. IP cím, eszköz neve, időbélyeg).
Történeti elemzés	Incidens után rekonstruálható az események láncolata.
Megfelelőségi riportok	Támogatja a NIS2, ISO/IEC 27001, IEC 62443 auditokat.
Automatizálható válaszok (SOAR)	Automatizált védekezés a gyors válaszadás érdekében.

Gyakori CPS-kompatibilis SIEM rendszerek

SIEM rendszer	Specialitás	Megjegyzés
IBM QRadar	Nagyvállalati, erős analitika	Integrálható OT környezetekbe is.
Splunk Enterprise Security	Testreszabható, vizualizációs képességek	Különösen hasznos ipari logok elemzéséhez.
LogRhythm	Automatizált korreláció, SOAR integráció	Jó választás OT rendszerekhez.
ArcSight (Micro Focus)	Komplex szabályrendszer, skálázható	Katonai és pénzügyi CPS-ekben gyakori.
OSSIM (nyílt forráskódú)	Alapvető SIEM funkciók, kis rendszerekhez	Oktatási célra is kiváló.

Tipikus CPS-események, amelyeket SIEM-mel észlelhetünk

Eseménytípus	Példa	Lehetséges válasz
Ismeretlen eszköz csatlakozása	Egy új IP cím megjelenik a vezérlőhálózaton	Riasztás, hálózati karantén
Vezérlési parancsok szokatlan időben	Éjjel 2-kor vezérlőparancs érkezik egy HMI-ről	Riasztás, forgalom megszakítása
Többszöri sikertelen belépés	Felhasználó próbálkozik a SCADA bejelentkezéssel	Fiók zárolása, figyelmeztetés
Adatátviteli mennyiség anomália	PLC kommunikációs forgalma megduplázódik	IDS/IPS aktiválás
Konfigurációs fájl módosítása	SCADA rendszer .ini fájlja módosul	Incidens vizsgálat indítása

SIEM integráció más védelmi rendszerekkel

A SIEM önmagában nem végzi el a védelmi intézkedéseket, de:

- együttműködik az **IDS/IPS rendszerekkel**, amelyek biztosítják a riasztási forrásokat,
- kapcsolódik a **firewall logokhoz**, amelyek alapján észleli a tiltott hozzáféréseket,
- integrálható **SOAR (Security Orchestration, Automation and Response)** rendszerekkel a **reakció automatizálásához**.

Kihívások a SIEM CPS-alkalmazásában

Kihívás	Megoldási javaslat
Logforrások eltérő formátuma	Normalizeálási szabályok használata
Nagy mennyiségű adat generálódása	Tárolási és feldolgozási skálázás, archiválás
ICS protokollok felismerésének hiánya	Ipari SIEM vagy integrált ICS-elemző modul
Késleltetett reagálás	SOAR integráció a gyors reakció érdekében
Komplex szabályrendszer kezelése	Előre konfigurált template-ek alkalmazása

Ukrajnai áramszolgáltató elleni támadás (2015):

A támadók hónapokon át gyűjtöttek adatokat a hálózatról. Egy SIEM rendszer korábban észlelhette volna:

- a **furcsa bejelentkezési mintákat**,

- a **VPN-szerver túlterheltségét**,
- és a **vezérlőrendszer éjszakai parancsait**.

Stuxnet támadás (2010):
Bár a támadás célzott és kifinomult volt, egy jól beállított SIEM rendszer:

- korrelálhatta volna a **rendszermódosításokat a HMI-ről**,
- és a **centrifugák sebességének szokatlan változását**,
- ezzel riasztva a biztonsági csapatot.

A SIEM rendszerek képezik a CPS-hálózatok **biztonsági megfigyelő központját**. Képességük az **események összefüggésbe helyezésére, azonnali riasztások küldésére és szabályozott válaszlépések elindítására** létfontosságú a modern ipari és kritikus infrastruktúrák számára. Hatékony működésükhöz azonban **pontos konfigurációra, protokollismeretre és folyamatos karbantartásra** van szükség.

5.4 Host-alapú védelmi mechanizmusok

A kiberfizikai rendszerek (CPS) biztonságának egyik alapvető pillére az **eszközszintű (host-alapú) védelem**, amely célzottan a végponti berendezéseket – mint a PLC-k, HMI-k, ipari szerverek és vezérlők – hivatott megóvni a jogosulatlan hozzáféréstől, rosszindulatú kódoktól, hibás konfigurációtól vagy belső fenyegetésektől. Mivel ezek az eszközök gyakran elavult, korlátozott operációs rendszereken futnak, és hosszú élettartamra tervezettek, különösen sérülékenyek lehetnek a célzott támadásokkal szemben.

Host-alapú védelem jelentősége a CPS környezetben

A CPS rendszerek hostjai kritikus feladatokat látnak el: szenzoradatokat gyűjtenek, döntéseket hoznak, vezérlési parancsokat továbbítanak. Egy ilyen komponens kompromittálása az egész ipari folyamatra hatással lehet – ezért kiemelten fontos a megbízhatóságuk, sértetlenségük biztosítása.

Host-alapú védelmi megoldások

Védelmi technológia	Leírás	Alkalmazási lehetőség CPS-ben
Host Intrusion Detection System (HIDS)	Naplófájlok, fájlrendszer-változások és rendszeresemények monitorozása	HMI-k és SCADA szerverek változásfigyelése
Endpoint Detection and Response (EDR)	Viselkedéselemzésen alapuló fenyegetésdetekció, automatizált válaszmechanizmusokkal	PLC-k vagy operátorállomások végponti védelme
Whitelisting (Allowlisting)	Csak engedélyezett alkalmazások és folyamatok futtatása	PLC-re és vezérlőre csak valid szoftver tölthető fel
Fájlrendszer-integritás ellenőrzés	Kulcsfontosságú fájlok (pl. konfigurációs állományok) hash-értékeinek monitorozása	SCADA rendszerbeállítások jogosulatlan módosításának felismerése
Malware-védelem / Antivirus	Vírusok, trójaiak, rootkitek keresése és eltávolítása	Főként Windows-alapú HMI-ken és szervereken
Hardening / OS-zárás	A rendszer konfigurációjának szigorítása: felesleges szolgáltatások tiltása, jogosultságkezelés	Régi Windows vagy Linux operációs rendszerek biztonságossá tétele

Védelmi technológia	Leírás	Alkalmazási lehetőség CPS-ben
Secure Boot / Trusted Boot	Csak hitelesített szoftverindítás engedélyezett a bootolás során	Beágyazott vezérlők és edge-eszközök indítási integritásának védelme

Működési példa: HIDS alkalmazása SCADA szerveren

Egy SCADA szerverre HIDS-t telepítenek, amely figyeli:

- új futtatható fájlok megjelenését
- rendszernaplók változásait (pl. új felhasználó létrehozása)
- kritikus konfigurációs fájlok módosítását

Ha például egy új program kerül a rendszer indítási listájára (pl. `C:\ProgramData\startup.exe`), a HIDS azonnal riasztást küld az adminisztrátornak, aki megelőző intézkedést tehet, mielőtt a kártékony szoftver aktiválódna.

Előnyök és kihívások

Előny	Magyarázat
Pontosabb detekció	Mély rendszerismerettel bíró megoldások
Független a hálózati forgalomtól	Belső változásokat akkor is lát, ha nem tükröződnek hálózaton
Folyamat-integráció	Automatikus válaszadás (futtatás leállítása, felhasználó zárolása)

Kihívás	Megoldási javaslat
CPU/memória korlátok az eszközökön	Könnyített HIDS vagy whitelist alkalmazása
Elavult operációs rendszerek inkompatibilitása	Alternatív: fájlintegritás-ellenőrzés + manuális auditálás
Hamis pozitív riasztások	Rendszer finomhangolása, szabályrendszerek testreszabása

Szabványi megfelelés

A host-alapú védelmi mechanizmusokat több szabályozás is kiemelten kezeli:

- **IEC 62443-3-3**: megköveteli az eszközszintű védelem alkalmazását (SR 2.1 – Host-based malware protection, SR 7.6 – Least functionality).
- **ISO/IEC 27001**: előírja a végpontvédelmet, naplózást, jogosultságkezelést.
- **NIS2**: hangsúlyozza a végponti incidensészlelés és reakcióképesség fontosságát.

A host-alapú védelmi mechanizmusok nélkülözhetetlenek a CPS rendszerek biztonságának fenntartásához. Ezek az eszközök lehetővé teszik az **eszközszintű kontrollt**, amely megakadályozza a jogosulatlan hozzáférést, riaszt az anomáliákra, és fokozza a rendszer biztonsági rezilienciáját. Az ipari környezetekben különösen fontos, hogy a védelmi eszközök erőforrás-takarékosak és stabilak legyenek, alkalmazkodva a meglévő infrastruktúrához.

5.5 Támadásészlelési és válaszmechanizmusok (SOC-k, SOAR rendszerek, AI-alapú anomáliadetektálás)

(**Security Operation Center-ek, SOAR rendszerek, mesterséges intelligencián alapuló anomáliadetektálás**)

A kiberfizikai rendszerek (CPS-ek) védelme ma már nem képzelhető el csupán megelőző intézkedésekkel. Mivel az ipari rendszereket gyakran célzott, kifinomult és kitartó (APT – Advanced Persistent Threat) támadások érhetik, elengedhetetlen a **proaktív észlelés** és a **gyors reagálás** képessége. Ennek kulcselemei a **biztonsági műveleti központok (SOC)**, a **SOAR (Security Orchestration, Automation and Response)** platformok, valamint az **AI-alapú anomáliadetektálás**.

Security Operation Center (SOC)

A SOC (biztonsági műveleti központ) egy központosított egység, ahol szakértők és eszközök együttműködve végzik a szervezet informatikai és ipari rendszereinek valós idejű megfigyelését, elemzését és incidensre adott válaszait.

Főbb funkciók:

- **24/7 megfigyelés:** CPS rendszerek folyamatos megfigyelése SIEM-en vagy egyéb forrásokon keresztül.
- **Incidensfelismerés:** Szabály- és viselkedésalapú figyelmeztetések kezelése.
- **Korai riasztások:** Zero-day támadások vagy belső fenyegetések időben történő felismerése.
- **Eseménykorreláció:** Különböző forrásokból érkező események összekapcsolása (pl. PLC log + VPN belépés).
- **Forenzikai elemzés:** Támadási láncok visszafejtése, bizonyítékgyűjtés.

Példa CPS környezetben: Ha egy SCADA szerveren ismeretlen szoftver futását észlelik, a SOC azonnal elemzi, hogy:

- ki futtatta le,
- milyen kommunikációt próbál indítani (pl. PLC irányába),
- szükséges-e beavatkozni (futás leállítása, izolálás).

SOAR rendszerek (Security Orchestration, Automation and Response)

A SOAR platformok a SOC munkáját támogatják azáltal, hogy **automatizálják az észlelés utáni válaszlépéseket**, és integrálják a különböző biztonsági rendszereket.

Kulcsfunkciók:

- **Automatizált válaszadás:** pl. gyanús IP automatikus tiltása tűzfalon.
- **Eseménykezelési playbook-ok:** előre definiált forgatókönyvek aktiválása riasztás esetén.
- **Workflow-menedzsment:** a válaszfolyamat lépéseinek nyomon követése.
- **Integráció:** SIEM, EDR, tűzfal, ticketing rendszerek összekapcsolása.

Példa: Incidens típusa	SOAR válaszlépés
SCADA login Kínából	IP cím tiltása tűzfalon, user account zárolás
PLC firmware megváltozik	Bejelentés nyitása, műszaki csapat riasztása
Fájl hash eltérés	Eszköz izolálása, hash visszaellenőrzése

Előny a CPS-ben:

- Automatizált válasz lehetővé teszi, hogy a rendszer gyorsan és emberi beavatkozás nélkül csökkentse a támadás hatását – különösen fontos, ha fizikai károk is bekövetkezhetnek.

Mesterséges intelligencián alapuló anomália detektálás

A hagyományos szabályalapú biztonsági rendszerek (pl. IDS, SIEM) gyakran nem képesek felismerni az új típusú, célzott támadásokat. Ezzel szemben a **gépi tanulási (ML)** és **mesterséges intelligencia (AI)** megoldások képesek a **normál viselkedési minták megtanulására**, és **anomáliák** detektálására, amelyek rejtett támadásokra utalhatnak.

Alkalmazási módok CPS rendszerekben:

- **Kommunikációs mintázatok monitorozása:** Ha egy HMI hirtelen elkezd gyakran kommunikálni nem megszokott PLC-kkel.
- **Felhasználói viselkedéselemzés (UEBA):** például, ha egy mérnök szokatlan időpontban tölt le firmware-t.
- **Fizikai paraméterek változása:** Hőmérséklet vagy nyomás eltér a tanult normától, miközben minden más működés jónak tűnik.

AI-megoldás típusa	Példa alkalmazás
Supervised learning (felügyelt tanulás)	Ismert támadások detektálása tanítóadat alapján
Unsupervised learning	Normálistól való eltérések, pl. új porthasználat
Reinforcement learning	Rendszer válaszainak optimalizálása tapasztalat alapján

Példa: Egy AI-rendszer észleli, hogy egy edge-eszköz egyre nagyobb gyakorisággal próbál HTTP-n keresztül kapcsolatot létesíteni egy külső szerverrel – amit eddig sosem tett. Bár nem szerepel ismert feketelistán, ez egy "slow exfiltration" próbálkozás lehet. Az AI értesíti a SOC-ot vagy SOAR rendszert.

Technológiai összehasonlítás

Megoldás	Erősség	Gyengeség	CPS-hez való illeszkedés
SOC	Széleskörű felügyelet, manuális elemzés	Emberi erőforrás igényes	Magas szintű felügyelet
SOAR	Gyors válasz, automatizálás	Beállítása komplex	Kritikus válaszidők csökkentése
AI-anomália	Ismeretlen támadások észlelése	Hamis pozitív lehetőség	Ritka, kifinomult támadások kivédése

A CPS rendszerek biztonságának jövője a **valós idejű, intelligens válaszképességen alapul**. A SOC-ok biztosítják a központosított elemzést, a SOAR platformok lehetővé teszik az **automatizált és konzisztens válaszokat**, míg az **AI-alapú megoldások** felismerik a szabályalapúan láthatatlan fenyegetéseket is. Ezek integrált alkalmazása teszi lehetővé, hogy a kritikus infrastruktúrák ne csak reagáljanak, hanem előre jelezzék és megelőzzék a kibertámadásokat – csökkentve az üzemszüneteket, gazdasági veszteségeket és fizikai kockázatokat.

6 ÁLTALÁNOS HÁLÓZATI KAPCSOLATOK ÉS KOCKÁZATELEMZÉS: AZ IPARI PROTOKOLLOK (PL. MODBUS, DNP3, MQTT) SEBEZHETŐSÉGEINEK VIZSGÁLATA ÉS A ZERO TRUST MODELLEK BEVEZETÉSE

6.1 Gyakran használt ipari protokollok és biztonsági kockázataik

A kiberfizikai rendszerek (Cyber-Physical Systems, CPS) biztonságának egyik alapvető összetevője a használt ipari kommunikációs protokollok megbízhatósága és védettsége. A CPS-hálózatokban használt protokollok gyakran több évtizedes múltra tekintenek vissza, és nem az internetre kötött rendszerekhez vagy a mai fenyegetési környezethez lettek

tervezve. Ennek következtében számos sebezhetőséggel rendelkeznek, amelyek potenciálisan kihasználhatók egy támadó által a rendszer leállítására, manipulálására vagy adatlopásra.

Gyakran használt ipari protokollok rövid áttekintése

Protokoll	Használati terület	Kiemelt jellemzők
Modbus	SCADA rendszerek, PLC-k	Egyszerű master/slave architektúra, nyílt protokoll
DNP3	Energiaipari rendszerek	Széles körben használt, részleges biztonsági kiegészítésekkel
PROFINET	Automatizálás, gyártás	Ethernet alapú, valós idejű kommunikáció
EtherCAT	Precíziós gyártás, robotika	Nagy sebesség, determinisztikus adatátvitel
MQTT	IoT, szenzorhálózatok	Könnyű, üzenet-alapú, publish/subscribe modell

Ezek a protokollok kulcsszerepet játszanak a vezérlőrendszerek és mezőszintű eszközök közti kommunikációban. Biztonságuk tehát kritikus a teljes infrastruktúra szempontjából.

Főbb biztonsági kockázatok

- **Hitelesítés hiánya**
  - A legtöbb ipari protokoll (különösen Modbus és a klasszikus DNP3) nem alkalmaz semmilyen beépített hitelesítési mechanizmust.
  - Ez lehetővé teszi, hogy egy támadó egy egyszerűen csatlakozó eszközként utasításokat küldjön a vezérlőrendszernek.
- **Titkosítás hiánya**
  - A legtöbb protokoll **plaintext** formátumban küldi az adatokat.
  - Ez támadási lehetőségeket biztosít: pl. **Man-in-the-Middle (MitM)** támadás során a forgalom lehallgatható vagy módosítható.
- **Üzenetmanipuláció és parancs-visszajátszás**
  - Az üzenetek gyakran nem tartalmaznak **digitális aláírást vagy időbélyeget**, így a támadó újra elküldheti a korábban elfogott parancsokat ("replay attack").
- **Hamis adatok injektálása**
  - Mivel nincs ellenőrzés, a támadó **hamis szenzoradatokat** küldhet, amelyek téves riasztást vagy rendszerműködést válthatnak ki.
- **Szolgáltatásmegtagadás (DoS) támadások**
  - A protokollok nincsenek felkészítve erőforrás-túlterhelésre: egy túl sok kérésből álló támadással **leállítható a kommunikáció**

Statisztikák és kutatási adatok

A *Dragos Inc.* 2023-as ipari kiberbiztonsági jelentése szerint:

Protokoll	Észlelt sebezhetőségek száma 2022-ben	Leggyakoribb probléma
Modbus	48	Nincs hitelesítés
DNP3	36	Nincs titkosítás, replay támadások

Protokoll	Észlelt sebezhetőségek száma 2022-ben	Leggyakoribb probléma
MQTT	21	Alacsony hozzáférés-kezelés
PROFINET	17	Adatmanipuláció

„Az ipari protokollok 68%-a nem használ semmilyen formájú titkosítást a gyártói alapbeállításokban.” – SANS ICS Survey, 2022

6.2 Modbus, DNP3, MQTT és más protokollok sebezhetőségei

Modbus TCP

Modbus az egyik legrégebbi, legismertebb nyílt ipari protokoll, széles körben használják SCADA rendszerekben és PLC-k vezérlésére. Különösen a **Modbus TCP/IP** implementáció vált a támadók célpontjává.

Fő sebezhetőségek:

- **Nincs hitelesítés**: bármely eszköz küldhet utasításokat egy Modbus-slave-nek, akár káros parancsokat is.
- **Nincs titkosítás**: minden adat plaintext formátumban utazik, így lehallgatható vagy módosítható.
- **Replay támadás lehetősége**: a protokoll nem tartalmaz időbélyeget vagy szekvencia-azonosítót, így korábban elfogott parancs újra elküldhető.
- **Funkciókód sebezhetőségek**: bizonyos funkciókódok (pl. 0x08 – *Diagnostics*) kihasználhatók DoS támadásokra.

Példa:

- **CVE-2018-10630**: egyes Modbus-eszközök hibásan kezelik az érvénytelen funkciókódokat, ami szolgáltatásmegtagadáshoz vezethet.

Distributed Network Protocol v3

A DNP3 protokoll főként az energiaiparban használatos, különösen távvezérlés és mérési adatok továbbítása céljából. Bár fejlettebb, mint a Modbus, a klasszikus DNP3 sem volt felkészülve az internetes fenyegetésekre.

Fő sebezhetőségek:

- **Alapverzióban nincs titkosítás**: a DNP3 nem használ TLS-t vagy más rejtjelezési módszert.
- **Replay és spoofing támadások**: az üzenetek nem tartalmaznak integritásvédelmet, így könnyen manipulálhatók.
- **Outstation túlterhelés**: túl sok válaszüzenet küldésével leterhelhető az állomás (DoS).
- **TCP vs. serial megközelítés**: a TCP-alapú változat fokozottan sebezhető, mivel kívülről is elérhető lehet.

Példa:

- **CVE-2012-1803**: hibás DNP3 implementációval rendelkező rendszerek DoS támadással megbéníthatók voltak rosszul formázott üzenetek révén.

MQTT (Message Queuing Telemetry Transport)

Az MQTT protokoll egy könnyű, publish-subscribe architektúrán alapuló rendszer, amelyet kifejezetten alacsony erőforrás-igényű IoT és CPS-eszközökre terveztek. Míg hatékony, a biztonság szempontjából több problémával küzd.

Fő sebezhetőségek:

- **Alapértelmezetten nincs titkosítás vagy hitelesítés**: a kapcsolatok nem használják kötelezően a TLS-t.

- **Topic hijacking**: ha nincs megfelelő hozzáférés-szabályozás, támadók publikálhatnak/olvashatnak tetszőleges témákban.
- **Broker túlterhelés (DoS)**: szándékosan generált túl sok publish/subscriber kapcsolat megakaszthatja a szolgáltatást.
- **Üzenetmanipuláció**: az MQTT nem biztosít üzenet integritást vagy digitális aláírást.

Példa:

- **CVE-2020-13849**: a Mosquitto MQTT brokerben felfedezett hiba DoS támadáshoz vezethetett, ha egy kliens rosszul formázott CONNECT üzenetet küldött.

PROFINET, EtherNet/IP, BACnet – Egyéb gyakori protokollok

PROFINET

- Ethernet-alapú, determinisztikus kommunikáció ipari környezetben.
- **Sebezhetőség**: hibás adatkeret-kezelés miatt túlterhelhetők a résztvevők.
- **Biztonsági bővítések hiányos implementálása** egyes gyártóknál.

BACnet

- Épületautomatizálási rendszerekben elterjedt.
- **Nem kér hitelesítést**, a legtöbb BACnet implementáció lehetővé teszi a teljes irányítás átvételét egy támadó számára.
- **CVE-2020-6967**: egyes BACnet stackek lehetővé tették távoli kódfuttatást.

Összehasonlító táblázat a sebezhetőségekről

Protokoll	Titkosítás	Hitelesítés	Replay elleni védelem	Ismert CVE-k (2024-ig)
Modbus	✗	✗	✗	50+
DNP3	✗ / részlegesen ✓	✗	✗	40+
MQTT	✗ (de támogatja TLS-t)	✗ (opcionális)	✗	30+
PROFINET	✓ (opcionális)	✓ (gyártófüggő)	✓	20+
BACnet	✗	✗	✗	25+

6.3 Zero Trust Architektúra (ZTA) alkalmazása a CPS-hálózatokban

Bevezetés a Zero Trust szemléletbe

A **Zero Trust Architektúra (ZTA)** egy olyan kiberbiztonsági paradigma, amely a klasszikus, periméteralapú védelem elavultságát felismerve abból indul ki, hogy **semmilyen felhasználó, eszköz vagy hálózati kapcsolat nem tekinthető automatikusan megbízhatónak** – még akkor sem, ha az a szervezet belső hálózatában található. Mottója: **„Soha ne bízz, mindig ellenőrizz”** („Never trust, always verify”).

A kiberfizikai rendszerek (CPS-ek) – különösen az ipari vezérlőrendszerek (ICS), SCADA rendszerek, vagy IoT-ökoszisztémák – egyre inkább ki vannak téve külső és belső fenyegetéseknek, így a **Zero Trust alkalmazása** ezekben a rendszerekben különösen időszerű és szükségszerű.

A klasszikus modell problémái CPS környezetben

A hagyományos hálózati védelem a **perimeterre (tűzfal, VPN, DMZ)** koncentrál, és a hálózatba belépő entitásokat megbízhatónak tekinti. A CPS-hálózatokra jellemző:

- Hosszú életciklusú eszközök (20+ év), gyakran elavult operációs rendszerek
- Internetkapcsolattal rendelkező alrendszerek (pl. távfelügyelet)
- Gyenge vagy hiányzó hitelesítés az eszközök között
- Korlátozott naplózás és átláthatóság

Egy támadó, ha egyszer bejutott, szabadon mozoghat a rendszerben („**lateral movement**”), amit a ZTA koncepció **explicit módon tiltani** kíván.

A ZTA alapelvei a CPS-hálózatokban

A Zero Trust megvalósítása CPS környezetben a következő alapelvekre épül:

Alapelv	Leírás
Minimális jogosultság (least privilege)	Minden entitás csak azokat az erőforrásokat éri el, amelyekre feltétlenül szüksége van.
Kötelező azonosítás és hitelesítés	Minden kommunikációs kapcsolat, felhasználói és gépi hozzáférés többfaktoros azonosításon és hitelesítésen keresztül történik.
Kontekstuális hozzáférés-kezelés	Az engedélyezés a felhasználó, eszköz típusa, helye, viselkedési mintái alapján dinamikusan változik.
Folyamatos ellenőrzés és naplózás	Az összes hálózati és eszközhöz kapcsolódó esemény folyamatos monitorozása és elemzése.
Szegmentálás és mikroperimeterek	A rendszer zónákra bontása, melyek között szabályozott, naplózott és védett a kommunikáció.

Zero Trust elemek alkalmazása a CPS-ekben

Komponens	CPS-specifikus implementáció
Identitáskezelés (IAM)	Eszközök, gépi folyamatok és felhasználók azonosítása (pl. RBAC, ABAC, PAM)
MFA és cert-alapú hitelesítés	Pl. PLC-khez csak aláírt tanúsítványú mérnök férhet hozzá
Szegmentált hálózat	A HMI, PLC és SCADA közötti forgalom szigorúan szabályozott zónákon megy keresztül
Policy-alapú hozzáférés	„Policy Engine” dönt a hozzáférésről – idő, eszközállapot, geolokáció alapján
NAPLÓZÁS (SIEM)	Teljes eseménynaplózás, riasztás gyanús viselkedés esetén
SOAR és válaszmechanizmusok	Gyanús tevékenység esetén automatikus izolálás, riasztás vagy beavatkozás

ZTA és ipari rendszerek együttélése – kihívások

Bár a ZTA hatékony megoldást kínál, a **CPS-hálózatokban történő implementációja nem triviális**:

- **Kompatibilitás**: a régi PLC-k és RTU-k nem támogatják a modern hitelesítési szabványokat.
- **Valós idejű követelmények**: egyes Zero Trust elemek (pl. dinamikus policy-ellenőrzés) késleltetést okozhatnak, ami elfogadhatatlan vezérlési rendszerek esetén.
- **Erőforrás-korlátok**: kis fogyasztású, beágyazott IoT-eszközök nem képesek erős kriptográfiai számításokra.
- **Költség és komplexitás**: ZTA teljes implementációja komoly beruházást igényel mind technológiailag, mind szervezetileg.

ZTA bevezetésének javasolt lépései CPS-ben

Eszköz- és adatfolyam-felderítés

- Mely eszközök kommunikálnak, milyen adatokat továbbítanak?

Identitás- és hozzáférés-kezelés kialakítása

- Egyedi azonosítók eszközöknek, RBAC/ABAC alkalmazása.

Hálózati szegmentáció megvalósítása

- Logikai vagy fizikai szintekre bontott mikroperimeterek.

Szoftveres ügynökök telepítése

- Host-alapú viselkedésfigyelők és policy enforcement agentek.

Naplózás és forgalomelemzés (SIEM)

- Anomáliaészlelés, hosszútávú viselkedési minták feltárása.

Automatizált válaszmechanizmusok bevezetése (SOAR)

- Gyanús viselkedés esetén automatikus reakció (pl. eszköz karanténozása).

ZTA és NIS2 kapcsolata

Az **EU NIS2 irányelv** szintén megköveteli a hozzáférések kontrollálását, naplózását, incidenskezelést – ezek szinte mind a Zero Trust elveire épülnek. A ZTA alkalmazása segíthet a NIS2 megfelelőség elérésében is.

A **Zero Trust Architektúra** nem pusztán egy újabb biztonsági modell, hanem egy **paradigmaváltás**: a feltétel nélküli bizalom megszűnt, és helyét a folyamatos ellenőrzés és validálás veszi át. CPS rendszerek esetén a ZTA segíthet a szegmentáció, azonosítás, naplózás és dinamikus válaszmechanizmusok révén **csökkenteni a kockázatokat és növelni a kiberbiztonsági érettséget**.

„Never trust, always verify – this is the core principle of Zero Trust security.” — John Kindervag, a Zero Trust modell kidolgozója (Forrester Research)

6.4 Hitelesítés és hozzáférés-kezelés (pl. multi-factor authentication, RBAC, ABAC, PAM megoldások)

A **hitelesítés** (authentication) és a **hozzáférés-kezelés** (authorization) a kiberbiztonság két alapköve. A kiberfizikai rendszerek (CPS) – különösen az ipari környezetek – különösen érzékenyek az illetéktelen hozzáférésekre, mivel az eszközök közvetlenül befolyásolhatják a fizikai világot. Egy kompromittált PLC, HMI vagy szenzor nemcsak adatvesztéshez, hanem **üzemzavarhoz vagy életveszélyes helyzethez is vezethet**.

A megfelelő hitelesítési és hozzáférés-kezelési megoldások bevezetése tehát **elkerülhetetlen** a CPS rendszerek biztonságos működtetéséhez.

Hitelesítési eljárások

A hitelesítés célja, hogy egy rendszer meggyőződjön arról, hogy egy adott entitás (felhasználó, alkalmazás vagy eszköz) **valóban az, akinek mondja magát**.

- **Egylépcsős hitelesítés (Single-Factor Authentication – SFA)**
  - Általában **felhasználónév és jelszó** páros.
  - CPS környezetben gyakori, de **önmagában nem elegendő** a magas kockázatok miatt.

- **Többfaktoros hitelesítés (Multi-Factor Authentication – MFA)**
  A hitelesítés több, egymástól független tényezőre épül:
  - **Tudás**: pl. jelszó, PIN
  - **Birtoklás**: pl. okostelefon, token
  - **Biometria**: ujjlenyomat, arcfelismerés

Példa: Egy mérnök csak úgy tud belépni a SCADA felügyeleti rendszerbe, ha beírja jelszavát, majd megerősíti belépését egy mobiltelefonos alkalmazáson keresztül.

- **Gépek közötti hitelesítés**
  - Pl. **tanúsítvány-alapú** hitelesítés (X.509)
  - Különösen fontos, amikor eszközök automatikusan kommunikálnak egymással (pl. PLC ↔ RTU)

Hozzáférés-kezelési modellek

A hitelesítést követően az engedélyezés (authorization) dönti el, hogy az adott entitás **mit tehet a rendszerben**. Az engedélyek strukturált kezelése különösen fontos CPS-ben, ahol **minden művelet fizikai hatással járhat**.

RBAC – Role-Based Access Control

- A jogosultságokat **szerepkörökhöz** (pl. adminisztrátor, operátor, mérnök) rendelik.
- Könnyen kezelhető, de kevésbé rugalmas finomhangolt igények esetén.

Példa: Egy „mérnök" szerepkörrel rendelkező felhasználó módosíthat PLC konfigurációt, míg az „operátor" csak megfigyelhet.

ABAC – Attribute-Based Access Control

- Az engedélyezés **attribútumok** alapján történik:
  - Felhasználói: szerepkör, műszak, jogosultsági szint
  - Erőforrás: típus, érzékenység
  - Környezet: időpont, helyszín, hálózati zóna

Példa: Egy felhasználó csak munkaidőben, a telephelyi hálózatról férhet hozzá a HMI-hez.

PAM – Privileged Access Management

- A **kiemelt jogosultságú fiókok** (pl. admin, root) kontrollálása és naplózása.
- Felhasználói tevékenységek rögzítése, hozzáférések időalapú szabályozása.
- „Just-in-time access" (JIT) – ideiglenes admin jog biztosítása ellenőrzött módon.

Példa: Egy külsős szakember csak 2 órára kap hozzáférést egy meghatározott HMI panelhez, minden tevékenysége rögzítésre kerül.

CPS-specifikus kihívások

Kihívás	Leírás
Örökölt rendszerek	Régi vezérlők és szoftverek gyakran nem támogatják az MFA-t vagy modern IAM megoldásokat
Offline működés	Hálózati problémák esetén a hitelesítés nem függhet külső központi rendszerektől
Folyamatkontinuitás	Egy túl szigorú szabály vagy hibás azonosítás leállíthat egy kritikus folyamatot

Kihívás	Leírás
Erőforrás-korlátok	Beágyazott eszközök nem bírják a komplex hitelesítési protokollokat vagy titkosítást

Jó gyakorlatok CPS környezetben

- **Erőteljes jelszavak + MFA mindenhol**, ahol lehetséges
- **RBAC + ABAC kombinált alkalmazása** finomhangolt jogosultságkezeléshez
- **Privilegizált hozzáférések auditálása** (PAM) – különösen távoli karbantartók esetén
- **Automatizált belépési és jogosultsági vizsgálatok**: pl. SOAR vagy SIEM rendszer integráció
- **Zero Trust modell integrálása**: minden hozzáférést újra és újra ellenőrizni

A CPS-rendszerek biztonsága csak akkor lehet teljes, ha **a hitelesítés és a hozzáférés-kezelés szigorúan szabályozott**, naplózott és dinamikusan alkalmazkodik a környezet változásaihoz. A hagyományos modellek (RBAC) ma már nem elegendőek – szükség van **intelligens, kontextusérzékeny megoldásokra (ABAC)** és a **kiemelt fiókok kontrolljára (PAM)**. A többfaktoros hitelesítés pedig ma már nem extra lehetőség, hanem **alapkövetelmény** minden kritikus rendszer esetében.

6.5 Biztonsági tesztelési és auditálási módszerek (penetrációs tesztelés, sebezhetőségvizsgálat)

Sebezhetőségvizsgálat (Vulnerability Assessment)

A sebezhetőségvizsgálat célja, hogy automatizált vagy félautomatikus eszközökkel **feltérképezze a rendszer gyenge pontjait**, anélkül hogy kihasználná azokat.

Jellemzői:

- Automatikus szkennelők (pl. **Nessus**, **OpenVAS**, **Qualys**)
- Szabály- és aláírásalapú keresés (CVE-k, CVSS értékek alapján)
- Tipikus vizsgálati területek: nyitott portok, frissítetlen szoftverek, elavult protokollok

Példa CPS környezetben:

Egy vizsgálat során a SCADA szerver elavult Apache verziója kerül azonosításra, amely ismert távoli kódfuttatási sebezhetőséget tartalmaz.

Megjegyzés:

- **Nem jár szolgáltatáskimaradással**, ezért gyakrabban végezhető
- Általában az **első lépés** a biztonsági tesztelési ciklusban

Penetrációs tesztelés (Penetration Testing / Ethical Hacking)

A penetrációs tesztelés során a biztonsági szakértők – az etikus hackerek – megpróbálják **valóban kihasználni a felfedezett sebezhetőségeket**, hogy felmérjék azok valós kockázatát.

Típusai:

- **Black box**: Tesztelő nem kap előzetes információt

- **White box**: Teljes dokumentáció és hozzáférés biztosított
- **Gray box**: Korlátozott információval dolgoznak

Tesztelési célpontok:

- HMI és SCADA rendszerek
- IP-alapú érzékelők és vezérlők (pl. PLC-k)
- Felügyeleti protokollok (pl. Modbus TCP, DNP3)

Fontos:

- **Szimulált támadás valós környezetben**
- Részletes engedélyek és üzemeltetői együttműködés szükséges
- Előfordulhatnak **üzemzavarok**, ezért kontrollált környezetben (pl. teszthálózatban) javasolt

Eredmény:

- Részletes jelentés: kihasználható sebezhetőségek, támadási láncok, javasolt javítási lépések

Biztonsági auditálás

A biztonsági audit **formális vizsgálat**, amely során az információbiztonsági irányelvek, szabályzatok és gyakorlatok betartását ellenőrzik.

Vizsgálati területek:

- Jogosultságkezelés és hitelesítési folyamatok
- Naplózás, eseményfigyelés és reagálás
- Patch management és rendszerfrissítések
- Hozzáférési naplók és behatolásjelző rendszerek működése

Irányelvek és szabványok:

- **IEC 62443** – ipari automatizálási és vezérlőrendszerek biztonsága
- **ISO/IEC 27001** – információbiztonság irányítási rendszerek
- **NIST SP 800-82** – ICS rendszerek biztonságának útmutatója

Egy audit során kiderülhet például, hogy egy mérnöki fiók inaktív, de még mindig aktív hozzáférése van a vezérlőrendszerhez.

Tesztelési és auditálási integráció CPS-ben

Szempont	Sebezhetőségvizsgálat	Penetrációs tesztelés	Auditálás
Fókusz	Ismert sebezhetőségek azonosítása	Valós támadási útvonalak feltárása	Szabályzatok és kontrollok betartása
Eszközök	Nessus, OpenVAS	Metasploit, Kali Linux	Manuális + riport alapú
Időzítés	Rendszeresen, pl. havonta	Évente vagy projektzáráskor	Évente, megfelelőségi szempontból
Kockázat	Alacsony	Közepes–magas (ha éles környezetben)	Alacsony

Ajánlások CPS rendszerek esetén

- **Tesztelési tervek és protokollok kialakítása**, figyelembe véve a működési sajátosságokat (pl. real-time rendszerek)
- **Tesztek elvégzése teszthálózatban**, nem éles gyártási rendszeren
- **Automatizált és rendszeres sebezhetőségvizsgálat**
- **Független penetrációs tesztelők** bevonása évente
- **Auditnyomok és naplófájlok folyamatos elemzése**, SIEM rendszerekkel kiegészítve

A CPS rendszerek védelme nem lehet teljes átfogó tesztelés és auditálás nélkül. A sebezhetőségvizsgálatok gyors és automatizált áttekintést adnak, míg a penetrációs tesztek valós támadási forgatókönyveket tárnak fel. A biztonsági auditálás segít biztosítani a megfelelőséget és hosszú távú fenntarthatóságot. A három módszer **együtt alkalmazva biztosítja a legnagyobb védelmet** a CPS hálózatok számára.

6.6 Kibervédelmi megoldások (sandboxing, honeypotok, AI-alapú fenyegetésészlelés)

Sandboxing – Elkülönített futtatási környezetek

A **sandboxing** olyan biztonsági technika, amely lehetővé teszi, hogy gyanús fájlokat, kódokat vagy alkalmazásokat **elszigetelten futtassanak**, ezáltal megelőzve, hogy azok kárt tegyenek a fő rendszerben.

Működési elv:

- A program egy virtuális környezetben fut
- A rendszer figyeli a viselkedését (pl. hálózati kapcsolatokat, fájlműveleteket)
- Gyanús aktivitás esetén riasztást generál vagy automatikusan blokkol

Használat CPS rendszerekben:

- SCADA-fájlok és firmware frissítések **ellenőrzése telepítés előtt**
- Ipari e-mail rendszerekbe érkező mellékletek tesztelése
- Kártevők dinamikus elemzése (pl. ICS-malware)

Példák:

- **FireEye**, **Cuckoo Sandbox**, **CrowdStrike Falcon Sandbox**

Honeypotok – Csapdák a támadók számára

A **honeypot** egy tudatosan sebezhető vagy érdekes célpontnak tűnő rendszer, amelyet arra használnak, hogy **csalétekként viselkedjen** a támadók számára, miközben figyeli azok tevékenységét.

Típusai:

- **Low-interaction honeypot**: csak limitált válaszokat ad (pl. portnyitogatás figyelése)
- **High-interaction honeypot**: teljes operációs rendszert szimulál a támadók számára
- **Honeynet**: több honeypotból álló szimulált hálózat

Előnyök:

- Valós idejű információkat nyújt a támadókról (IP-címek, eszközök, támadási módszerek)
- Segít a 0-day támadások mintáinak korai felismerésében
- **Eltéríti a támadót** az éles rendszerektől

Ipari környezetben:

- PLC-honeypotok (pl. **Conpot** – nyílt forráskódú ICS-honeypot)
- HMI-szimulátorok, melyek a támadóknak úgy tűnnek, mint valódi SCADA rendszerek

AI-alapú fenyegetésészlelés – Tanuló rendszerek a támadások ellen

A hagyományos aláírásalapú detektálással ellentétben a mesterséges intelligencián (AI) és gépi tanuláson (ML) alapuló megközelítések **képesek ismeretlen, új támadások azonosítására is**, anomáliák vagy viselkedésminták alapján.

Alkalmazott technikák:

- **Folyamatos forgalomelemzés**: eltérés a normál hálózati mintázatoktól
- **Felhasználói viselkedéselemzés** (UEBA): például egy mérnök szokatlan időpontban fér hozzá rendszerhez
- **Eszközprofilozás**: ha egy PLC másként viselkedik, mint a tanult profil alapján elvárható

Előnyök:

- **Zero-day támadások felismerése** aláírás nélkül
- Skálázhatóság és automatizált reagálás lehetősége (pl. AI + SOAR integráció)
- Folyamatos tanulás új fenyegetésekről

Megoldások:

- **Darktrace**, **Vectra AI**, **Microsoft Defender for IoT**, **Cisco Secure Analytics**

Összehasonlító áttekintés

Módszer	Célja	Előnyei	Használat CPS-ben
Sandboxing	Gyanús kódok biztonságos futtatása	Dinamikus elemzés, megelőzés	Firmware ellenőrzés, e-mailek
Honeypot	Támadók csalogatása és elemzése	Támadó technikák azonosítása	ICS-hálózatok megfigyelése
AI-alapú észlelés	Ismeretlen fenyegetések felismerése	Zero-day felismerés, tanulóképesség	Anomália alapú észlelés

Ajánlások

- **Kombinált védekezés**: sandbox + honeypot + AI-modul együtt alkalmazva hatékonyabb
- Honeypotokat mindig **elszigetelten** futtassuk, ne legyen kapcsolatuk a belső rendszerekkel
- AI-alapú rendszerek esetén **folyamatos tanítás és finomhangolás szükséges** a téves riasztások elkerülésére
- Sandboxing rendszerek frissítése a legújabb malware technikák felismerésére

7 REFERENCIÁK ÉS PÉLDÁK: VALÓS CPS-TÁMADÁSOK ELEMZÉSE ÉS TANULSÁGAIK BEMUTATÁSA

7.1 Stuxnet 2010 – Az első dokumentált ipari kiberfegyver elemzése

2010 júniusában a világ szemtanúja lehetett a kiberhadviselés új korszakának, amikor felfedezték a **Stuxnet** nevű számítógépes férget. Bár kezdetben csak egy technikai érdekességnek tűnt, hamarosan kiderült, hogy a kártevő **egy rendkívül fejlett, célzott kiberfegyver**, amely az iráni **natanzi urándúsító üzemet** célozta meg. A támadás célja nem információszerzés vagy kémkedés volt, hanem **fizikai rombolás**, ami egyértelműen elválasztotta a Stuxnetet a korábbi kártékony programoktól.

A Stuxnet jelentősége nem csupán technikai komplexitásában rejlik, hanem abban, hogy **egy kormányzati szintű kibertámadás első ismert példájaként** vonult be a történelembe. A támadás **CPS-rendszert** – konkrétan Siemens PLC-ket – vett célba, és **hibátlanul integrálódott** az ipari irányítástechnikai környezetbe, hogy aztán észrevétlenül tönkretegye a berendezéseket.

A Stuxnet technikai működése röviden

A Stuxnet komplexitása több szinten is megmutatkozott. A féreg **négy 0-day sebezhetőséget** használt ki, és **digitálisan aláírt** drivereket alkalmazott, hogy hiteles szoftverként tűnjön fel. A kártékony kód a Microsoft Windows operációs rendszeren keresztül terjedt, de végső célja az volt, hogy olyan **Siemens Step7 szoftverrel programozott PLC-ket fertőzzön meg**, amelyek a centrifugák sebességét szabályozzák.

Miután bekerült a rendszerbe, a Stuxnet **hamis adatokat** továbbított a HMI-rendszerek felé, így az operátorok nem érzékelték, hogy a centrifugák túl gyorsan vagy túl lassan forognak – mindez a gépek fokozatos meghibásodásához vezetett.

A támadás hatása és mértéke

A támadás konkrét célpontja az iráni nukleáris program volt, de a Stuxnet később **több mint 100 országban** megjelent, ami mutatja a kontrollálatlan terjedés kockázatát.

Támadással kapcsolatos adat	Érték / Megjegyzés
Első észlelés ideje	2010. június
Felhasznált 0-day sebezhetőségek száma	4
Digitálisan aláírt driverek száma	2
Érintett országok száma	>100
Célpont	Natanz, Irán – urándúsító létesítmény
Fizikai károsodás	~1000 centrifuga vált működésképtelenné

A becslések szerint a támadás **közel két évvel vetette vissza** az iráni nukleáris programot. Bár az Egyesült Államok és Izrael szerepe hivatalosan sosem került megerősítésre, a legtöbb szakértő a **"Operation Olympic Games"** fedőnév alatt futó közös művelethez köti a fejlesztést.

Stuxnet jelentősége a kiberbiztonságban

A Stuxnet új korszakot nyitott a **kiberhadviselésben**. Míg a korábbi támadások főként adatlopásra vagy rendszerek megbénítására irányultak, itt egyértelmű **fizikai rombolás** történt szoftveres úton. Ez volt az első bizonyíték arra, hogy **egy állam által támogatott kibertámadás képes ipari berendezéseket megsemmisíteni**, anélkül, hogy fizikai behatolás történt volna.

A támadás nyomán világszerte megnőtt az érdeklődés az **ICS/SCADA biztonság** iránt. Egy 2021-es IBM X-Force jelentés szerint a kritikus infrastruktúrák elleni támadások száma az elmúlt években **évi 20–30%-kal növekszik**, részben a Stuxnet által inspirált újabb kiberfegyverek miatt (pl. Duqu, Flame, Triton).

Tanulságok és javaslatok CPS-védelmi szempontból

A Stuxnet eset tanulságai ma is relevánsak. A legfontosabb következtetések a következők:

- **Elszigetelt rendszerek is sebezhetők**: A fizikai levegőrés (air-gap) nem jelent teljes védelmet, ha a támadó célzottan juttatja be a kódot (pl. USB-n keresztül).
- **Zero Trust szemlélet szükséges**: Minden eszköz és felhasználó bizalmatlansági alapon kezelendő, különösen kritikus környezetekben.
- **Aktív felügyelet és anomáliadetektálás**: AI-alapú megoldások segíthetnek a rendellenes viselkedések korai felismerésében.
- **Firmware integritás-ellenőrzés**: Minden ipari vezérlőberendezés esetében rendszeres firmware audit és aláírás-ellenőrzés szükséges.

A Stuxnet nem csupán egy kiberbiztonsági mérföldkő, hanem egy globális figyelmeztetés is. Megmutatta, hogy a szoftveres világ már képes **fizikai károkozásra is**, és hogy a kiberfegyverkezés nem sci-fi, hanem napjaink realitása. A Stuxnet öröksége az, hogy minden nemzet és ipari szereplő számára világossá vált: **a CPS-rendszerek védelme stratégiai kérdéssé vált** a 21. században.

7.2 Ukrán áramhálózat elleni támadások (2015-2016) – Kritikus infrastruktúra elleni fenyegetések

A 2015 decemberében Ukrajnában bekövetkezett áramkimaradás sokáig példa nélküli esemény volt a kibertámadások történetében. Ekkor vált világossá a szakértők számára, hogy nemcsak elméleti lehetőség, hanem *valóságos, jól koordinált* veszély is lehet egy kiberincidens, amely közvetlen hatással van egy ország lakosságára és kritikus infrastruktúrájára. Az **Ivano-Frankivszk** régióban több mint **230 000 fogyasztó** maradt áram nélkül néhány órára, miután ismeretlen (de vélhetően orosz hátterű) hackerek bejutottak az elektromos hálózat irányító rendszereibe.

A támadást követően alig egy évvel, 2016 decemberében újabb célzott támadás érte Kijev körzetét. A módszertan tovább finomodott, és már nemcsak a SCADA rendszereket vették célba, hanem *automatizált malware-ekkel* is operáltak. A támadások jelentősége túlmutat az azonnali hatáson: **először történt meg, hogy egy digitális támadás fizikailag megbénított egy városi elektromos hálózatot** – nem egy távoli elmélet, hanem kézzelfogható valóság.

Milyen módszereket használtak a támadók?

A 2015-ös támadás során a hackerek **spear phishing e-maileken keresztül** szerezték meg a belépési adatokat, majd **távoli hozzáférésű trójaiakat** (pl. BlackEnergy) alkalmaztak az irányító rendszerek kompromittálására. A támadás három energetikai szolgáltatót ért szinte egyszerre, és a támadók képesek voltak:

- belépni a HMI-felületekre,
- manuálisan lekapcsolni alállomásokat,

- blokkolni a helyreállítást (firmware-törlés, fájlrendszer rombolás),
- és **DoS-támadással** megbénítani az ügyfélszolgálati rendszereket is.

A 2016-os támadás során a **Industroyer/CrashOverride** malware-t alkalmazták, amely egy **moduláris, ipari protokollokra specializálódott malware**, képes például az IEC 101/104 vagy az OPC rendszerek kezelésére.

A támadások hatása számokban

Jellemző	2015	2016
Érintett város/régió	Ivano-Frankivszk	Kijev
Érintett fogyasztók száma	~230 000 fő	~200 000 fő
Áramkimaradás időtartama	1–6 óra	1 óra
Használt malware	BlackEnergy, KillDisk	Industroyer / CrashOverride
Irányítástechnikai célpont	SCADA, HMI	Alállomások, vezérlők

Miért volt különösen veszélyes a támadás?

A támadások jól mutatják, hogy a **kritikus infrastruktúrák sebezhetőek**, különösen, ha hagyományos IT-védelmi modellekre építenek, és nem különítik el kellően az OT (Operational Technology) rendszereket. A 2015-ös támadás idején az ukrán hálózatok **gyenge szegmentálással** rendelkeztek, a **felhasználói fiókok túl nagy jogosultságokkal** bírtak, és hiányzott a **Zero Trust-alapú hozzáférés-kezelés**.

Az is világossá vált, hogy **az emberi tényező – például egy jól megírt phishing e-mail – elegendő lehet egy ország energiahálózatának megbénításához**.

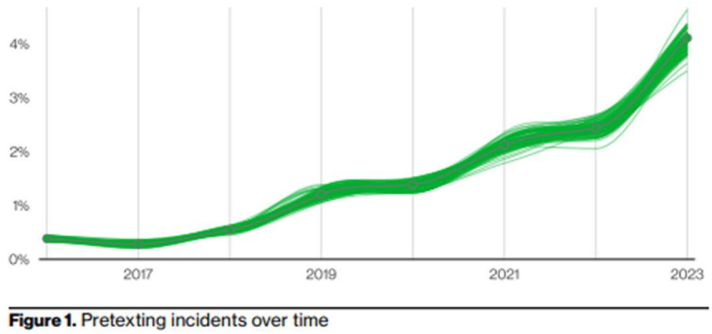


Figure 1. Pretexting incidents over time

Business Email Compromise is a key issue.

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 1, and now represent more than 50% of incidents within the Social Engineering pattern.

- DBIR 2023 Data Breach Investigations Report

Tanulságok és válaszintézkedések

Az ukrán tapasztalatok hatására világszerte felértékelődött a kritikus infrastruktúrák védelme. Az alábbi intézkedések váltak kiemelten fontossá:

- **Hálózati szegmentáció**: Az IT és OT hálózatok éles elválasztása fizikai és logikai szinten.
- **Képzések és szimulációk**: A személyzet felkészítése phishing, insider threat és vészhelyzeti eljárások kapcsán.
- **Anomáliadetektálás bevezetése**: AI-alapú IDS/IPS rendszerek, amelyek a rendellenes viselkedést időben felismerik.

- **Zero Trust és hozzáférés-kezelés**: Minimális jogosultság elve, RBAC/ABAC alkalmazása minden eszközre és felhasználóra.

A 2015–2016-os ukrán áramszolgáltatás elleni kibertámadások rámutattak arra, hogy **a kritikus infrastruktúrák nem csupán elméleti célpontok, hanem a kiberhadviselés aktív terepei**. Az ilyen támadások következményei nem csupán technikai, hanem társadalmi, gazdasági és politikai szinten is érzékelhetők. Ma már az energetikai és ipari szektor védelme nem csak IT-probléma, hanem **nemzetbiztonsági kérdés**, és ezt a legtöbb fejlett ország – a NATO-tól az EU-ig – stratégiai dokumentumokban is rögzíti.

7.3 TRITON (2017) – Biztonsági rendszerek elleni célzott támadás

A 2017-ben felfedezett **TRITON** (más néven TRISIS vagy HatMan) támadás nemcsak új szintre emelte a kiberfegyverek kifinomultságát, hanem példátlan veszélyt is jelentett a **fizikai biztonságra**. Ellentétben korábbi támadásokkal – amelyek termelési folyamatokat, adatokat vagy SCADA rendszereket céloztak –, a TRITON közvetlenül **ipari biztonsági vezérlőrendszerek (SIS – Safety Instrumented Systems)** ellen irányult. Ez a támadás volt az első, amely kimondottan egy **biztonsági redundanciát biztosító rendszer semlegesítésére** irányult – vagyis egy olyan rendszert próbált meg kikapcsolni, amely **emberek életét és berendezések épségét** hivatott védeni.

Mi is az SIS, és miért fontos?

A **Safety Instrumented System (SIS)** olyan biztonsági rendszer, amely az üzemekben – például vegyi üzemekben, olajfinomítókban vagy gázerőművekben – automatikusan beavatkozik, ha veszélyes körülményeket érzékel. Például ha a nyomás vagy a hőmérséklet meghalad egy kritikus értéket, a SIS leállítja a folyamatot, mielőtt robbanás vagy mérgező anyag kibocsátása történhetne.

A TRITON támadás célja az volt, hogy **ezeket a védelmi mechanizmusokat hatástalanítsa**, ezáltal lehetővé téve egy későbbi – akár robbanással járó – támadást a fő folyamatirányítási rendszeren keresztül. A támadás tehát **életveszélyes kimenetellel** is járhatott volna.

A támadás menete és működése

A támadók célpontja egy közel-keleti (valószínűsíthetően szaúd-arábiai) **petrokémiai üzem** volt, amely a **Triconex** nevű SIS rendszert használta (gyártó: Schneider Electric). A támadás során a következő lépések történtek:

1. **Támadók bejutása az IT-hálózaton keresztül** az OT-rendszerbe, valószínűleg adathalászat vagy hibás konfiguráció révén.
2. A támadók **hozzáfértek a Triconex SIS vezérlőkhöz**, és feltöltöttek egy módosított firmware-t, amely nemcsak manipulálta a védelmi logikát, hanem lehetővé tette a későbbi távoli parancsvégrehajtást is.
3. A támadás során hiba történt: a módosított SIS firmware összeomlást okozott, és ez automatikusan **leállította az üzemet**, így a támadást felfedezték.

A TRITON rosszindulatú komponensei **Python-alapú scripteket**, Windows DLL fájlokat és **különlegesen célzott exploitokat** használtak a Triconex SIS-kontroller specifikus szoftverének manipulálására.

A TRITON támadás fő jellemzői

Tulajdonság	Érték / Megjegyzés
Felfedezés ideje	2017. december

Tulajdonság	Érték / Megjegyzés
Célpont	Közel-keleti petrokémiai üzem
Célrendszer	Schneider Electric Triconex SIS
Használt technikák	SIS firmware módosítás, OT hozzáférés manipulálása
Potenciális következmény	Robbanás, mérgező anyag kibocsátás, emberélet-kockázat
Malware nevei	TRITON, TRISIS, HatMan

Miért volt ez a támadás történelmi jelentőségű?

A TRITON több okból is különösen veszélyes volt:

- **Célzottan a fizikai biztonság ellen irányult** – nem adatlopás vagy zsarolás volt a cél, hanem emberi élet veszélyeztetése.
- A támadók **nagyon magas OT-tudással rendelkeztek** – ismerték a Triconex rendszert, a memóriacímzéseket, a szoftverarchitektúrát.
- **Csak egy technikai hiba** miatt nem következett be súlyosabb katasztrófa – ha a manipulált SIS logika nem omlik össze, a támadók akár teljesen kikapcsolhatták volna a biztonsági rendszert.

Az esetet követően több kiberbiztonsági vállalat – például a FireEye és a Dragos – jelentéseikben hangsúlyozták, hogy **valós idejű, fizikai hatású támadás valószínűleg államilag támogatott csoport műve volt**, és hogy **az ilyen szintű támadások a jövőben is várhatók** kritikus infrastruktúrák ellen.

A TRITON tanulságai CPS rendszerek számára

1. **A biztonsági rendszerek is támadási célpontok** – nem szabad megelégedni a SCADA vagy PLC védelmével.
2. **SIS rendszerek firmware-je szigorúan kontrollált legyen** – hitelesítés, aláírás, naplózás szükséges.
3. **Megbízhatósági és biztonsági kontrollokat külön kell kezelni** – ne legyen összemosva az irányítási és védelmi logika.
4. **Végponti védelem az OT-ben is szükséges** – EDR/HIDS használata SIS programozási munkaállomásokon.
5. **Fizikai elválasztás és szegmentáció** – ne lehessen távolról elérni a SIS vezérlőket közvetlenül.

A TRITON támadás világosan jelezte, hogy a jövő kibertámadásai **nem csupán adatokat, hanem emberéleteket is veszélyeztethetnek**. A támadók nem egyszerű zsarolóvírussal vagy adathalászattal dolgoztak, hanem egy kritikus biztonsági rendszert próbáltak meg semlegesíteni, hogy később egy potenciális fizikai katasztrófát idézzenek elő. A támadás mérföldkő volt a kiberbiztonság történetében, és azt mutatja: a biztonsági rendszerek **nem „érinthetetlenek" többé**. Az ilyen fenyegetések ellen csak többrétegű, naprakész, aktív védelem biztosíthat valódi védelmet.

7.4 Colonial Pipeline (2021) – Ransomware fenyegetések ipari rendszerek ellen

A **Colonial Pipeline** elleni 2021-es ransomware-támadás az egyik legismertebb és legnagyobb hatású incidenssé vált az Egyesült Államok történetében, amely közvetlenül érintette a **kritikus energiaellátási infrastruktúrát**. A támadás kiemelte, hogy az **informatikai rendszerek sebezhetőségei** hogyan eredményezhetnek **valós, fizikai hatásokat** – például üzemanyaghiányt, áremelkedést vagy közlekedési zavarokat –, még akkor is, ha az **operatív technológiát (OT)** közvetlenül nem éri támadás.

Mi az a Colonial Pipeline, és miért volt ez fontos célpont?

A **Colonial Pipeline Company** Észak-Amerika legnagyobb kőolajvezeték-rendszerét üzemelteti, amely több mint **8,850 km** hosszan szállít üzemanyagokat – benzin, dízel, kerozin – a mexikói-öbölbeli finomítóktól egészen New Jersey-ig. A rendszer a keleti part **üzemanyagellátásának kb. 45%-át** biztosítja, ami napi több **millió gallon** szállított mennyiséget jelent.

A támadás részletei

2021. május 7-én a **DarkSide** nevű ransomware csoport sikeresen kompromittálta a Colonial Pipeline vállalat **IT-rendszereit**, különösen a **számlázási és üzleti adminisztrációs hálózatot**. Bár az OT-rendszert közvetlenül nem támadták meg, a vállalat **megelőző céllal leállította** az üzemanyag-szállító vezetékrendszer működését, mivel nem tudta garantálni, hogy a kártékony kód nem terjedt át a kritikus vezérlő rendszerekre is.

A támadás következményei számokban

Jellemző	Érték / Hatás
Érintett rendszer	Colonial Pipeline IT-hálózata
Támadás típusa	Ransomware (DarkSide csoport)
Kifizetett váltságdíj	4.4 millió USD bitcoinban (részben visszaszerezve)
Leállás időtartama	5 nap (2021. május 7 – május 12)
Ellátási hatás	11.000+ benzinkútnál ellátási zavar, pánikvásárlás, üzemanyaghiány
Üzemanyagár-emelkedés	Átlagosan +6-10% az USA keleti partján
FBI nyomozás eredménye	Több DarkSide tag azonosítása, 2.3 millió USD visszaszerzése

A támadás rövid távú következményei között szerepelt a **pánikvásárlás**, különösen az USA délkeleti államaiban, mint Georgia, Észak-Karolina és Florida. Több államban szükségállapotot hirdettek, mivel az üzemanyaghiány közlekedési fennakadásokat és gazdasági leállásokat is eredményezett.

A ransomware támadás technikai és szervezeti aspektusai

A DarkSide csoport professzionálisan működő **Ransomware-as-a-Service (RaaS)** modellt használt. Ez lehetővé tette, hogy más kiberbűnözők is béreljék a szoftverüket. A támadók hozzáférést szereztek a Colonial Pipeline belső hálózatához – valószínűleg **ellopott VPN hitelesítő adatok** révén, amelyek **MFA (többlépcsős azonosítás) hiányában** védtelenek voltak.

A kártékony szoftver titkosította a céges fájlokat, és zsaroló üzenetet helyezett el, amely fizetési utasításokat tartalmazott. Érdekesség, hogy a támadás után a DarkSide csoport nyilatkozatban próbálta csökkenteni a politikai nyomást, kijelentve: „nem állami támogatásúak, és csak pénzt akartak keresni, nem zavarni a társadalmat."

Tanulságok és következtetések

1. **Az IT és OT közötti határvonal elmosódik**: bár a támadás kizárólag az IT-hálózatot érintette, az OT-rendszer leállítása elkerülhetetlenné vált a biztonság érdekében.

2. **Kritikus a hozzáférés-kezelés**: a támadók egy elavult, MFA nélküli VPN-hozzáférés révén jutottak be – ez elkerülhető lett volna.
3. **A váltságdíj kifizetése nem old meg mindent**: noha a vállalat fizetett, a helyreállítás így is napokat vett igénybe, és a reputációs károk jelentősek maradtak.
4. **Állami és szabályozói reakciók gyorsak voltak**: az eset után az Egyesült Államok kormánya új kiberbiztonsági rendeleteket adott ki az üzemanyag-infrastruktúra védelmére.

Védekezési lehetőségek és javaslatok

A Colonial Pipeline incidens rávilágított arra, hogy a **kritikus infrastruktúrák védelmét nem lehet kizárólag technológiai oldalról kezelni**. Szükség van:

- **Többlépcsős hitelesítés** (MFA) minden hozzáférési ponton
- **Szegmentált hálózati architektúra**, IT-OT elválasztás erősítése
- **Zero Trust elv** alkalmazása, ahol minden kapcsolat gyanúsnak tekinthető
- **Rendszeres mentések**, offline is elérhető módon
- **Kiberbiztonsági tudatosság növelése**, különösen az IT-személyzet körében

A Colonial Pipeline ransomware-támadás mérföldkőnek számít a kritikus infrastruktúrák elleni fenyegetések történetében. Egy korábban főként pénzügyi vagy adatlopási célú eszköz, a **ransomware**, egy csapásra **stratégiai fenyegetéssé** vált, amely képes megbénítani nemzetgazdaságokat is. A támadás rávilágított, hogy **a kritikus szolgáltatásoknak nemcsak technológiai, hanem operatív rugalmasságra és átláthatóságra is szükségük van**, ha hosszú távon biztonságban akarnak működni a digitális térben.

7.5 Újabb támadások és trendek (pl. AI-alapú fenyegetések, ellátási lánc elleni támadások)

A kiberfizikai rendszerek (CPS) biztonsági környezete napjainkban gyorsan és kiszámíthatatlanul változik. A klasszikus támadási módszereken túl egyre nagyobb teret kapnak **új generációs fenyegetések**, mint például az **AI-alapú támadások**, valamint az **ellátási lánc mentén történő kompromittálás**, amelyek már nemcsak egy-egy rendszert, hanem **komplett infrastruktúrákat** képesek célba venni. A digitalizáció térhódításával és az IT–OT konvergencia fokozódásával ezek a támadások **egyre nehezebben észlelhetők, gyorsabban terjednek**, és sokszor **megbízható alrendszerekbe ágyazva** érkeznek.

AI-alapú fenyegetések: a gépi tanulás fegyverré válik

Miközben a mesterséges intelligencia (AI) és a gépi tanulás hasznos eszközök a védelemben (pl. fenyegetésészlelés, anomáliafigyelés), **a támadók is elkezdték alkalmazni ezeket a technológiákat**. Az AI lehetővé teszi számukra, hogy:

- **Automatizált sérülékenység-felderítést** végezzenek (AI-alapú exploit generálás)
- **Adathalász kampányokat személyre szabjanak** (pl. deepfake hangalapú hívások, social engineering chatbotok)
- **Elkerüljék a detekciót** azáltal, hogy a rosszindulatú kódok viselkedése dinamikusan módosul a védekezési mechanizmusokhoz igazodva

Egy 2024-es IBM X-Force jelentés szerint a kibertámadások során használt mesterséges intelligencia technológiák aránya **18%-ról 31%-ra nőtt két év alatt**, és a növekedés üteme gyorsul.

Példa:

2023-ban az egyik nagyobb európai energiaipari vállalatot **deepfake videóval csalták csapdába**, amelyen a vezérigazgató arcát és hangját utánozva utasították a pénzügyi osztályt nagy összegű átutalásra. Az AI-vezérelt támadás órák alatt történt, és csak napokkal később derült ki, hogy nem az igazgató volt a képen.

Ellátási lánc elleni támadások: a leggyengébb láncszem célkeresztben

Az **ellátási lánc (supply chain) támadások** lényege, hogy a célrendszerbe egy harmadik fél – tipikusan megbízható beszállító vagy szoftverpartner – rendszerén keresztül jut be a támadó. Ez a stratégia különösen veszélyes CPS-eknél, mivel **az ipari rendszerek jellemzően sok gyártó és külső szolgáltató komponenseit integrálják**, így a támadási felület jelentősen megnő.

Statisztika:

A 2022-es ENISA jelentés szerint az **ellátási lánc-alapú támadások 62%-a szoftverfrissítésen vagy konfigurációs csatornán keresztül történt**, míg 16%-uk fizikai eszközökön keresztül érkezett (pl. fertőzött USB, okoseszközök). A SolarWinds támadás (2020) rávilágított, hogy egy népszerű IT-menedzsment platform frissítésébe ágyazott kóddal **több mint 18 ezer szervezetet** sikerült kompromittálni – köztük kormányzati és kritikus infrastruktúrákat is.

Újabb fenyegetési trendek 2023–2025 között

Trend	Leírás
AI-generált malware	Olyan kódok, melyek viselkedését a védelmi rendszerekhez igazítják
Ellátási lánc backdoor-ok	Megbízható szoftverbe ágyazott hátsó kapuk
Firmware-szintű támadások	Alacsonyszintű BIOS/UEFI kompromittálás ipari eszközökön
IoT-botnetek és ICS zombihálózatok	Nagyszámú eszköz összehangolt támadásra való használata (pl. Mirai ICS-variáns)
Quantum-hack előkészítés	Adatok „gyűjtése jövőbeli feltöréshez”, amikor kvantumszámítógép elérhető lesz

Védekezési irányelvek az új típusú fenyegetésekkel szemben

1. **Beszállítói biztonság értékelése (Third-Party Risk Management)**
   Minden külső partner, hardver- és szoftverszállító biztonsági átvilágítása legyen alapkövetelmény (pl. NIS2 előírások szerint).
2. **Digitális aláírás és forrásellenőrzés szoftvereknél**
   Csak hitelesített és digitálisan aláírt frissítéseket szabad elfogadni.
3. **Zero Trust alkalmazása partnereknél is**
   Ne bízzunk semmilyen kapcsolatban implicit módon, még partnerek esetén sem – minimális jogosultság, mikro-szegmentáció.
4. **AI-alapú védekezés erősítése**
   Olyan rendszerek telepítése, amelyek nemcsak AI-alapú támadásokat képesek detektálni, hanem maguk is **gépi tanulással javulnak** (pl. Darktrace, SentinelOne).
5. **Firmware-szintű ellenőrzések**
   Rendszeres BMC, BIOS/UEFI auditálás, valamint write-protection alkalmazása ipari eszközökön.

Az ipari rendszerek elleni támadások új korszaka kezdődött – egy olyan korszak, ahol a **fenyegetések intelligensebbek, célzottabbak és nehezebben észlelhetők**, mint valaha. A védelem nem lehet statikus: **dinamikusan alkalmazkodnia kell**

a fenyegetések változásához. A mesterséges intelligencia kettős szerepet játszik: miközben a támadók egyre ügyesebben használják, a védekezők is egyre hatékonyabb eszközöket fejlesztenek ellene. A jövő CPS-védelme tehát a proaktivitáson, a bizalommentes hozzáálláson és a technológiai szinergiák kiaknázásán múlik.

8 ÖSSZEGZÉS ÉS JAVASLATOK

8.1 Főbb megállapítások és kulcsfontosságú biztonsági kihívások

A dolgozat célja az volt, hogy átfogó képet adjon a **kiberbiztonság helyzetéről a kiberfizikai rendszerek (CPS)** világában, különös tekintettel a hálózatbiztonság kihívásaira, szabályozási környezetére, támadási trendjeire és a védekezési lehetőségekre. A vizsgálatok során számos **fontos megállapítás és kritikus biztonsági probléma** került felszínre.

Főbb megállapítások:

1. **CPS-rendszerek komplexitása és sebezhetősége** A kiberfizikai rendszerek egyre összetettebbé válnak, miközben az IT és OT rendszerek integrációja új támadási felületeket nyit. A klasszikus IT-védelem nem alkalmazható egy az egyben az ipari környezetekre, ahol a rendelkezésre állás és a fizikai biztonság prioritást élvez.
2. **A hálózati zónák szerepe kritikus** A biztonsági zónák és szegmentáció elengedhetetlenek ahhoz, hogy egy-egy támadás ne tudjon gyorsan szétterjedni a teljes infrastruktúrában. A zónák közötti **tűzfalak, IDS/IPS rendszerek**, és az erős hitelesítés a biztonság alapját képezik.
3. **NIS2 irányelv erős szabályozási keretet ad** A NIS2 irányelv bevezetésével az európai vállalatok és infrastruktúrák számára kötelezővé válik a **kockázatalapú biztonságmenedzsment**, az incidenskezelési képesség és a beszállítói biztonság kezelése – ami eddig sok helyen hiányzott.
4. **Zero Trust modell és a hozzáférés-szabályozás szerepe** Az implicit bizalomra épülő hálózatmodellek már nem védhetők megfelelően. A Zero Trust alapelvek – a minimális jogosultság, a folyamatos hitelesítés és a mikro-szegmentáció – alkalmazása jelentős biztonsági előnyt jelent.
5. **AI-alapú és ellátási lánc fenyegetések előretörése** Az új típusú támadások – például az **AI-alapú malware-ek**, vagy az ellátási láncon keresztüli beszivárgás – arra utalnak, hogy a támadók nemcsak technikailag fejlettek, de gyakran **stratégiai gondolkodással** célozzák meg a leggyengébb pontokat.

Kulcsfontosságú biztonsági kihívások:

- **Elavult ipari rendszerek (legacy systems)** továbbra is széles körben működnek, amelyek nem frissíthetők és nem kompatibilisek a modern biztonsági megoldásokkal.
- **Tudáshiány és emberi tényező**: A CPS-biztonság szaktudást igényel, ám a képzett szakemberek hiánya továbbra is kritikus probléma, ahogy az emberi hibákból eredő sebezhetőségek is.
- **Késleltetett incidens-észlelés és reakcióidő**: A legtöbb támadást nem percek alatt detektálják, hanem napokkal, hetekkel később – ez idő alatt pedig a támadó már komoly károkat okozhat.
- **Fenyegetések gyors fejlődése**: A támadási módszerek sokkal gyorsabban fejlődnek, mint a védekezés, különösen az **AI-t, gépi tanulást** vagy **kvantumrezisztens titkosítás hiányát** kihasználó támadások esetén.
- **Ellátási lánc átláthatatlansága**: A beszállítói rendszerek gyakran nincsenek megfelelően monitorozva, pedig ezek a támadók kedvenc célpontjai, mivel megbízhatónak tűnnek a célrendszer szemszögéből.

A fentiek alapján egyértelmű, hogy a **CPS rendszerek védelme nem csupán technológiai kérdés**, hanem **szervezeti, szabályozási és humán kihívás** is egyben. A jövő biztonságos infrastruktúrája csak akkor valósítható meg, ha ezekre a kihívásokra **proaktív és több szintű válaszokat adunk**.

8.2 Jövőbeli trendek és kutatási lehetőségek a CPS-hálózatbiztonság terén

A kiberfizikai rendszerek (CPS) biztonsága az elkövetkező évtizedek egyik legdinamikusabban fejlődő és leginkább fókuszált kutatási területévé válik. Ahogy az ipari automatizálás, a mesterséges intelligencia, a gépi kommunikáció és az IoT-technológiák egyre mélyebben integrálódnak a kritikus infrastruktúrákba, úgy nő azoknak a sebezhetőségeknek a száma is, amelyeket a támadók kihasználhatnak. Ennek megfelelően a jövőben nemcsak új technikai megoldásokra lesz szükség, hanem szemléletváltásra is a védekezés filozófiájában és gyakorlati alkalmazásában.

Az egyik legjelentősebb trend az AI-alapú fenyegetésészlelés és prediktív biztonság térnyerése. A kutatások jelenleg is arra irányulnak, hogy a gépi tanulás különböző ágaival – például neurális hálózatokkal vagy deep learning technikákkal – hogyan lehet már a támadási próbálkozás legelső jeleiből következtetni a lehetséges incidensre. A prediktív modellek képesek lehetnek a normálistól való eltérések automatikus felismerésére, így nemcsak észlelés, hanem megelőzés szintjén is kulcsszerepet játszanak. Az ilyen rendszerek különösen fontosak lehetnek a gyártósorokon, energetikai hálózatokban vagy közlekedési irányításban, ahol a válaszidő kulcsfontosságú.

Ezzel párhuzamosan egyre nagyobb figyelmet kap az automatizált válaszmechanizmusok fejlesztése, különösen a SOAR (Security Orchestration, Automation and Response) rendszerek evolúciója. A kutatás célja, hogy a riasztások értelmezése és a válaszintézkedések kiválasztása egyre kevesebb emberi beavatkozást igényeljen, ezáltal gyorsabb és következetesebb reakciókat lehessen végrehajtani – akár valós időben.

A Zero Trust modell alkalmazása sem áll meg a jelenlegi formájában: a kutatások abba az irányba mutatnak, hogy a ZTA-t kiterjesszék a felhőalapú, elosztott és 5G-alapú CPS-ök kontextusára. A decentralizált rendszerek hitelesítésének és hozzáférés-kezelésének új formái – például blokklánc-alapú hitelesítés vagy decentralizált azonosító rendszerek – szintén aktív kutatási témakörök. E technológiák célja, hogy a biztonságot a rendszer minden szintjén garantálják, még akkor is, ha az adatforgalom több különálló ökoszisztémán halad keresztül.

Egy másik feltörekvő irány a kvantumkiberbiztonság kérdésköre. Noha a kvantumtechnológia még gyerekcipőben jár, a szakértők már most keresik azokat a kriptográfiai megoldásokat, amelyek képesek lesznek ellenállni a kvantumszámítógépek által jelentett veszélyeknek. A CPS-rendszerek hosszú élettartama és frissítési nehézségei miatt már most elengedhetetlen elkezdeni az ún. „post-quantum” algoritmusok bevezetését és alkalmazását.

A humán tényező továbbra is kulcsfontosságú marad. A jövőbeli kutatások nemcsak a technológiai, hanem a viselkedési kockázatok mérséklésére is összpontosítanak. A szimulált támadásokkal támogatott biztonságtudatossági tréningek, a pszichológiai manipuláció (pl. social engineering) elleni programok, valamint a viselkedéselemzésre épülő belső fenyegetésészlelés szintén a kutatás kiemelt területei közé tartoznak.

Végezetül a szabályozói és jogi környezet fejlődése sem elhanyagolható. A kutatás egyre inkább multidiszciplináris irányt vesz, ahol a kiberbiztonsági technológiák összehangolása a jogi, etikai és társadalmi szempontokkal elengedhetetlen.

Az olyan előírások, mint a NIS2 irányelv vagy az ENSZ kiberdiplomáciai egyezményei új kutatási irányokat nyitnak meg a megfelelőség automatizálása és a nemzetközi adatvédelmi együttműködések terén is.

Összefoglalva: a CPS-hálózatbiztonság jövője nemcsak a támadásokkal szembeni védekezés tökéletesítéséről szól, hanem a rendszerek megbízhatóságának, rugalmasságának és adaptivitásának növeléséről is. A kutatás és innováció közös célja, hogy a digitális és fizikai világ összefonódása ellenére a biztonság sose váljon másodlagos szemponttá – hanem minden ipari és szolgáltatási rendszer integráns részévé váljon.

IRODALOMJEGYZÉK (FELHASZNÁLT/AJÁNLOTT IRODALOM)

Könyvek és tanulmányok

Krutz, R. L. (2005). *Industrial Control Systems Security and Resiliency*. John Wiley & Sons.

Kim, K. D., & Kumar, P. R. (2012). Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue), 1287–1308.

Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier*. Symantec Security Response.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA Security in the Light of Cyber-Warfare. *Computers & Security*, 31(4), 418–436.

Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats*. Momentum Press.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207.

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security Issues in SCADA Networks. *Computers & Security*, 25(7), 498–506.

Weboldalak és online cikkek

CISA. (2022). *Industrial Control Systems*. https://www.cisa.gov/ics

Dragos. (2018–2024). *Threat Intelligence Reports*. https://www.dragos.com

cybersecuritydive (2021) *Colonial Pipeline attack embodies security risk to nation's critical infrastructure* - https://www.cybersecuritydive.com/news/colonial-pipeline-ransomware-attack/599885/

SANS Institute. (n.d.). *ICS Security White Papers*. - https://www.sans.org/blog/industrial-control-systems-library/

Hírek, riportok, esettanulmányok

ICS-CERT. (2016). *Incident Reports: Ukraine 2015 Power Outage*. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

SANS Institute. (2016). *Confirmation of a Coordinated Attack on the Ukrainian Power Grid* - https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/

CISA. (2021). *DarkSide Ransomware: Best Practices for Prevention and Response*. - https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

Wired. (2017). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. - https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

The New York Times. (2012). *Obama Order Sped Up Wave of Cyberattacks Against Iran*. - https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

BBC News. (2021). *Colonial hack: How did cyber-attackers shut off pipeline? - https://www.bbc.com/news/technology-57063636*

Jogszabályok, irányelvek, szabványok

Európai Parlament és Tanács. (2022). *Directive (EU) 2022/2555 (NIS2 Irányelv)*. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022L2555

Magyarország. (2024). *2024. évi LXIX. törvény az elektronikus információs rendszerek védelméről*. - https://njt.hu/jogszabaly/2024-69-00-00

GDPR – *General Data Protection Regulation (EU) 2016/679*. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679

ISO/IEC 27001:2022 – *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

IEC 62443 – *INDUSTRIAL NETWORK AND SYSTEM SECURITY - https://www.isa.org/getmedia/b75b5611-1fa8-4807-99e5-d8707b7cff18/Phinneydone.pdf*

Statisztikák és jelentések

IBM X-Force. (2023). *ICS/SCADA Cyber Threat Report*. - https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf

IBM X-Force Threat Intelligence Index 2024 - https://www.ibm.com/reports/threat-intelligence

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. - https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf

ENISA. (2023). *Incidents in Critical Sectors: Energy, Transport, and Healthcare*. - https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors

Kaspersky ICS CERT Publications - https://ics-cert.kaspersky.com/publications/reports/?t=industrial-cybersecurity

ENISA. (2023). *Threat Landscape for Industrial Automation Systems*. - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Technológiai dokumentációk és javaslatok

Splunk. SIEM: Security Information & Event Management Explained (2025) - https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

MITRE ATT&CK. (2023). *ICS Tactics, Techniques, and Procedures (TTPs)*. - https://attack.mitre.org/techniques/ics/

NIST. (2023). *Guidelines for Using TLS in Industrial Control Systems*. - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Konferenciák és szakmai testületek

Black Hat USA. (2023). *Zero Trust in Critical Infrastructure*.
DEF CON. (2023). *ICS Village: Hands-on Industrial Security*.
Nemzetközi Elektrotechnikai Bizottság (IEC)
Magyar Szabványügyi Testület (MSZT)

2.52. Okosvárosok és beágyazott rendszerek: Technológiai megoldások és alkalmazások az

A

Széchenyi István Egyetem

Gépészmérnöki, Informatikai és Villamosmérnöki Kar

Informatika Tanszék

Okosvárosok és beágyazott rendszerek:
Technológiai megoldások és alkalmazások az intelligens városi infrastruktúrába

Rugonfalvi-Ress Barnabás

[redacted]

Gazdaságinformatikus BSc

2024/2025/2

Tartalomjegyzék

Tartalom

Tartalomjegyzék....2
Bevezetés....4
1. Okosváros fogalma és jelentősége....5
1.1 Egy okosváros alapvetően három pilléren nyugszik:....5
1.2 Az okosvárosoknak számos célja van:....5
2. Beágyazott rendszerek technológiai alapjai....6
2.1. A beágyazott rendszerek meghatározása....6
2.2. Főbb összetevők....6
2.2.1 Mikrokontroller vagy mikroprocesszor:....7
2.2.2 Érzékelők (szenzorok):....7
2.2.3 Aktuátorok:....7
2.2.4 Kommunikációs interfészek:....7
2.2.5 Energiaforrás:....7
2.3. Operációs rendszerek és szoftverplatformok....7
2.4. Beágyazott rendszerek és valós idejű kommunikáció....7
2.5. Példák beágyazott rendszerekre az okosvárosban....8
2.6. Előnyök és jelentőség....8
3. Kommunikációs technológiák okosvárosokban....8
3.1 Az IoT (Internet of Things) hálózat jelentősége....9
3.1.1 IoT topológiák (csillag, mesh)....9
3.1.2 Eszközorientált kommunikáció....9
3.1.3 Adatforgalom és sávszélesség dimenziói....9
3.2 LPWAN-technológiák....9
3.2.1 LoRaWAN (Long Range Wide Area Network):....10
3.2.2 NB-IoT (Narrowband IoT):....10
3.3. 5G hálózat az okosvárosban....11
3.4. Mesh hálózatok és helyi kommunikáció....11
3.5. Kommunikációs protokollok....12
3.6. Kihívások a kommunikációban....12
4. Alkalmazási területek és megoldások az okosvárosokban....12
4.1. Intelligens közlekedési irányítás és mobilitás....13

4.1.1. Okos közlekedési fények és időzítők 14
4.1.2. A V2X kommunikáció kulcsfontosságú 14
4.2. Okos parkolás 14
4.3. Energiahatékonyság és intelligens közvilágítás 15
4.4. Hulladékgazdálkodás 15
4.5. Környezeti monitoring 16
4.6. Közbiztonság és térfigyelés 16
4.7. Egészségügyi és szociális rendszerek támogatása 17
5. Esettanulmány: Barcelona Smart City 17
5.1. A projekt célkitűzései 17
5.2. Kiemelt fejlesztési területek 18
5.2.1 Intelligens közlekedés 18
5.2.2 Okos parkolási rendszer 18
5.2.3 Okos közvilágítás 18
5.2.4 Hulladékgazdálkodás 18
5.2.5 Környezeti monitoring 18
5.3. Műszaki infrastruktúra 19
5.4. Társadalmi dimenzió 19
5.5. Eredmények és tanulságok 19
6. Technológiai és társadalmi kihívások 20
6.1. Az interoperabilitás és a szabványosítás hiánya 20
6.1.1 Az interoperabilitás hiánya többféle problémát okozhat: 20
6.1.2 A megoldás: 20
6.2. Adatvédelem és biztonság 20
6.3. Finanszírozás és hosszú távú fenntarthatóság 21
6.4. Technológiai egyenlőtlenségek 21
6.5. Lakossági elfogadottság és bizalom 22
6.6. Etikai dilemmák és szabályozási kérdések 22
7. Jövőbeli irányok és az Ipar 5.0 szerepe az okosvárosokban 22
7.1. Az 5.0 iparvezérelvei 23
7.2. Digitális ikerpárok 24
7.3. Mesterséges értelem és adaptív városirányítás 25
7.4. Ember és technológia együttműködése 25
7.5. A városi életminőség újradefiniálása 26
7.6. Összegzés a jövőről 26
8. Összefoglalás és következtetések 27

Irodalomjegyzék 28

Bevezetés

A huszonegyedik század sorsdöntő kihívása a városiasodás: az ENSZ becslései szerint 2050-re a bolygó népességének körülbelül 70%-a városi területeken fog élni. Ez a tendencia komoly nyomást gyakorol a közlekedésre, energiaellátásra, vízellátásra, egészségügyi szolgáltatásokra, valamint a közbiztonságra. A hagyományos városüzemeltetési módszerek egyre kevésbé képesek hatékony megoldást kínálni ezekre az összetett problémákra. Ennek eredményeként egyre nagyobb hangsúlyt kap az "okosváros" koncepciója, amely a technológiai innovációk felhasználásával egyidejűleg kívánja javítani a városi életminőséget, a fenntarthatóságot és a szolgáltatások hatékonyságát.

Az **okosváros** egy olyan városi rendszer, amely beágyazott rendszerek, érzékelő hálózatok, kommunikációs protokollok, mesterséges intelligencia és adatvezérelt döntéshozatal segítségével optimalizálja a működését. Az intelligens infrastruktúra **nem csupán adatokat gyűjt**, hanem **képes azokat elemezni és hasznosítani** is, lehetővé téve az **önálló működést és a proaktív városi szolgáltatásokat.** A városiasodás globális növekedése és az infrastruktúra túlterheltsége új, technológiai alapú városirányítási modelleket követel meg [1].

Például a forgalomirányítás már nem csak statikus tervek alapján működik: a valós idejű közlekedési adatok és a V2X (járművek közötti) kommunikáció révén a város rugalmasan tudja szabályozni a forgalmat. Hasonló elv érvényesül a közvilágításban, ahol a mozgás- és fényérzékelők segítségével optimalizálható a világítás teljesítménye, csökkentve az energiafogyasztást és a fényszennyezést.

Az okosváros technológiai alapjait az Ipar 4.0 eredményei adják**: IoT (dolgok internete), felhőszolgáltatások, edge computing, adatelemzés és valós idejű kommunikáció**. Az okosváros azonban nem pusztán technológiai kérdés, hanem egy társadalmi változás is, amely az együttműködésre, az átláthatóságra és az emberközpontú megoldásokra épül.

A piaci prognózisok szerint a smart city szektor értéke 2024-ben meghaladta a 340 milliárd USD-t, és 2033-ra várhatóan eléri a 830 milliárd USD-t (IMARC Group, 2024). Az IoT eszközök száma a városi környezetben 2025-re elérheti a 17 milliárd darabot, az adatforgalom pedig a 2016-os szinthez képest tízszeresére nőhet (Cisco VNI, Ericsson Mobility Report, 2023).

A beadandó célja, hogy **átfogó képet adjon az okosváros technológiai felépítéséről, a beágyazott rendszerek szerepéről, valamint a megvalósítás kihívásairól és a jövőbeli trendekről**. Az elemzés kiterjed a gyakorlati példákra is – kiemelt figyelmet fordítva a barcelonai Smart City projekt tapasztalataira – valamint bemutatja az Ipar 5.0 emberközpontú megközelítésének lehetséges hatásait.

1. Okosváros fogalma és jelentősége

Az **"intelligens városok"** koncepciója az elmúlt években a technológiai diskurzusok sűrűn hangoztatott témájává vált, ám meghatározása még napjainkban is sokféleképpen értelmezhető. Az Európai Unió "Smart Cities" kezdeményezése szerint az okosváros olyan városi környezet, amely az **infokommunikációs technológiák és az adatokon alapuló döntéshozatal segítségével fenntarthatóbbá, befogadóbbá és élhetőbbé tehető**. A cél az, hogy a város képes legyen optimalizálni saját működését, miközben gyorsan és hatékonyan reagál a lakosság igényeire, valamint a környezeti és gazdasági kihívásokra. A digitális ikerpár és valós idejű adatfeldolgozás lehetővé teszi az adaptív, proaktív döntéshozatalt. [2]

1.1 Egy okosváros alapvetően három pilléren nyugszik:

Érzékelés és adatgyűjtés: Különféle szenzorok és beágyazott eszközök (pl. közlekedési kamerák, levegőminőség-mérők, parkolóérzékelők) révén valós időben gyűjt adatokat a város különböző pontjairól.

Adatfeldolgozás és elemzés: A összegyűjtött adatokat intelligens algoritmusok és mesterséges intelligencia segítségével dolgozzák fel, ami lehetővé teszi a város működésének optimalizálását.

Reakció és automatizáció: A rendszer képes önállóan reagálni, például a közlekedési lámpák átállításával, energiaelosztás szabályozásával vagy a közszolgáltatások optimalizálásával.

1.2 Az okosvárosoknak számos célja van:

- *Fenntarthatóság:* Energiatakarékos működés, megújuló energiaforrások integrálása, a szén-dioxid-kibocsátás csökkentése.
- *Hatékonyság:* Az erőforrások okos elosztása, a szolgáltatások működésének optimalizálása.
- *Átláthatóság és részvétel:* A lakosság aktív részvétele az adatmegosztásban és a döntéshozatalban.
- *Rugalmasság és ellenállóképesség:* Váratlan események, természeti katasztrófák

vagy válsághelyzetek esetén gyors reagálásra képes infrastruktúra kialakítása.

Az okosvárosok koncepcióját támogató technológiai réteg a szenzorhálózatoktól kezdve a hálózati kommunikációs eszközökön (pl. 5G, NB-IoT) át egészen a felhőalapú és edge computing rendszerekig terjed. Mindegyik elemnek saját, gyakran beágyazott rendszere van, mely helyben képes adatfeldolgozásra és döntéshozatalra. Ezek adják a város intelligens működésének az alapját.

Az okosvárosok jelentősége túlmutat a technológiai újításokon: társadalmi, gazdasági és környezeti szempontból is kiemelkedőek. Segítenek csökkenteni az egyenlőtlenségeket, javítják a szolgáltatásokhoz való hozzáférést, és elősegítik a digitális társadalom fejlődését. Nem véletlen, hogy a világ számos vezető városa – például Barcelona, Szingapúr, Helsinki vagy Bécs – már elindította saját okos város stratégiáját.

2. Beágyazott rendszerek technológiai alapjai

Az okosvárosok működését a beágyazott rendszerek alapozzák meg, amik a technológiai alapot biztosítják. Ezek specifikus, egy adott feladatra tervezett számítógépes egységek, egy nagyobb hálózat részét képezik, és előre meghatározott funkciókat látnak el. A beágyazott rendszerek nem önállóan tevékenykedő számítógépek, hanem integráltan működnek, például közlekedési **lámpákban**, **energiamérőkben**, **térfigyelő kamerákban** vagy épp egy teljes **épületautomatizálási rendszer részeként**.

2.1. A beágyazott rendszerek meghatározása

A beágyazott rendszer hardver és szoftver kombinációja, ami képes a környezetéből érkező adatokat érzékelni, feldolgozni, és ennek megfelelően cselekedni. Ezek a rendszerek gyakran valós idejű működésre optimalizáltak, azaz adott eseményekre meghatározott időn belül reagálniuk kell. Ez kritikus fontosságú olyan területeken, mint a forgalomszabályozás, a biztonsági rendszerek, vagy az energiaelosztás.

2.2. Főbb összetevők

A beágyazott rendszerek felépítése általában a következő elemekből áll:

2.2.1 Mikrokontroller vagy mikroprocesszor:

A rendszer "agyaként" szolgál, feldolgozza az érzékelőktől érkező információkat, futtatja az algoritmusokat és vezérli az aktuátorokat.

2.2.2 Érzékelők (szenzorok):

Környezeti adatok (pl. hőmérséklet, fény, mozgás, légszennyezettség) és események detektálására.

2.2.3 Aktuátorok:

Válaszreakciók kivitelezésére alkalmas eszközök, mint például elektromos motorok, kijelzők, fényjelzések.

2.2.4 Kommunikációs interfészek:

A rendszer hálózati kapcsolatait biztosítják, pl. Wi-Fi, ZigBee, LoRa, Bluetooth, NB-IoT vagy 5G modulok.

2.2.5 Energiaforrás:

Bizonyos rendszerek önálló energiaellátással rendelkeznek, akkumulátorral vagy napelemmodullal.

2.3. Operációs rendszerek és szoftverplatformok

A beágyazott rendszerek gyakran speciális operációs rendszert (RTOS – Real-Time Operating System) használnak, ami garantálja a kiszámítható reakcióidőt. Ilyenek a FreeRTOS, Zephyr, Contiki vagy az ARM Mbed OS. Ezek az operációs rendszerek többnyire nyílt forráskódúak, és kifejezetten IoT-alkalmazásokra optimalizáltak.

A fejlesztői környezetek (IDE-k) szintén kulcsfontosságúak. Az Arduino és Raspberry Pi alapú rendszerek egyszerű prototípusok fejlesztésére alkalmasak, míg ipari alkalmazásoknál a STMicroelectronics, Texas Instruments vagy Renesas fejlesztői platformjai dominálnak.

2.4. Beágyazott rendszerek és valós idejű kommunikáció

Az okosvárosi környezet egyik alapvető kihívása, hogy a különböző alrendszerek – például a közlekedés, a vízkezelés, a közbiztonság – zökkenőmentesen és összehangoltan működjenek. Ehhez elengedhetetlen a valós idejű adatfeldolgozás és kommunikáció, amit a beágyazott rendszerek tesznek lehetővé.

Például: egy V2X (vehicle-to-everything) kommunikációs rendszerben a járművek, a közlekedési lámpák és az útszéleken elhelyezett érzékelők között másodpercenként több száz adatcsomag cserélődik. A beágyazott rendszerek ezeket nemcsak gyorsan, hanem biztonságosan és megbízhatóan is kell, hogy feldolgozzák.

2.5. Példák beágyazott rendszerekre az okosvárosban

Okos közvilágítás: Az egyes lámpatestekbe integrált mikrokontrollerek lehetővé teszik a mozgásérzékelést, fényerőszabályozást és távvezérlést.

Forgalomfigyelő rendszerek: Kamerákhoz és érzékelőkhöz kapcsolt eszközök, melyek képfeldolgozással detektálják a torlódásokat vagy baleseteket.

Okos parkolás: Ultrahangos vagy mágneses érzékelőkkel ellátott, beágyazott rendszerek figyelik a parkolóhelyek foglaltságát.

Légszennyezettség-monitorozó eszközök: Gázérzékelőket és kommunikációs modulokat tartalmazó kompakt rendszerek, melyek folyamatosan küldik az adatokat a város üzemeltetőinek.

2.6. Előnyök és jelentőség

A beágyazott rendszerek előnyei a kis méret, az alacsony energiafogyasztás, a megbízhatóság, a lokális intelligencia (edge computing) és a moduláris bővíthetőség. Ezek a rendszerek alkotják az intelligens városi infrastruktúra "idegrendszerét", mely képes érzékelni, feldolgozni és reagálni – akár emberi beavatkozás nélkül.

3. Kommunikációs technológiák okosvárosokban

A hatékony okosvárosok alapvető feltétele a stabil, gyors, és energiatakarékos kommunikációs hálózat megléte. Az okos városok alapvető jellemzője, hogy a különböző alrendszereik, mint a közlekedés, közvilágítás, energiagazdálkodás, vagy a hulladékkezelés valós időben osztanak meg adatokat egymással. Ezáltal integráltan képesek reagálni az aktuális eseményekre. Ezt a rendszerszintű kapcsolódást kommunikációs protokollok és hálózati struktúrák biztosítják. A decentralizált, szenzor-alapú IoT rendszerek gyors fejlődése új kommunikációs kihívásokat szült, különösen az adatok megbízhatóságával és időzítési késleltetésekkel kapcsolatban [11].

3.1 Az IoT (Internet of Things) hálózat jelentősége

3.1.1 IoT topológiák (csillag, mesh)

Az IoT-rendszerek kommunikációs felépítésének meghatározása kritikus a megbízhatóság, az energiafelhasználás és az adatmozgás szempontjából. A **csillag topológiánál** minden berendezés közvetlenül egy központi egységhez csatlakozik. Ez egyszerűsíti a rendszert, viszont sebezhetővé is teszi, hiszen a központi csomópont hibája az egész hálózatot leállíthatja. Ezzel szemben a **Mesh** topológia decentralizált, az eszközök több más egységhez is kapcsolódnak, így az adatok alternatív útvonalakon is eljuthatnak a célba. Ez ideális nagyméretű, városi környezetekben, ahol a robusztus, öngyógyító kommunikáció létfontosságú. A szenzoros hálózatok és edge computing révén a beágyazott rendszerek decentralizált döntéshozatalt is lehetővé tesznek [3].

3.1.2 Eszközorientált kommunikáció

Az eszközorientált (device-centric) kommunikáció lényege, hogy az IoT-eszközök nem csak egy központi rendszerhez kapcsolódnak, hanem közvetlenül egymással is kommunikálnak. Ez elengedhetetlen például **a járművek közötti (V2V)** rendszerekben, ahol a járművek valós időben cserélnek információt a balesetek elkerülése érdekében. Hasonló elven működik az okos közvilágítás, ahol a lámpák mozgásérzékelés alapján továbbítják a jelet a következő egységnek.

3.1.3 Adatforgalom és sávszélesség dimenziói

Az IoT rendszerek skálázhatóságát nagymértékben befolyásolja az adatforgalom kezelése. A nagy adatsebességet igénylő alkalmazások (pl. videóalapú biztonsági rendszerek) esetében **nagy sávszélességű megoldásokra**, mint amilyen az 5G vagy az optikai hálózatok, van szükség. Ugyanakkor az alacsony frekvencián működő érzékelők – például hőmérséklet- vagy páratartalom-mérők – **LPWAN hálózatokon** is kiválóan teljesítenek (például LoRaWAN, NB-IoT). Az intelligens városmenedzsmenthez adaptív hálózati architektúra szükséges, ami dinamikusan képes elosztani a rendelkezésre álló sávszélességet a prioritás függvényében.

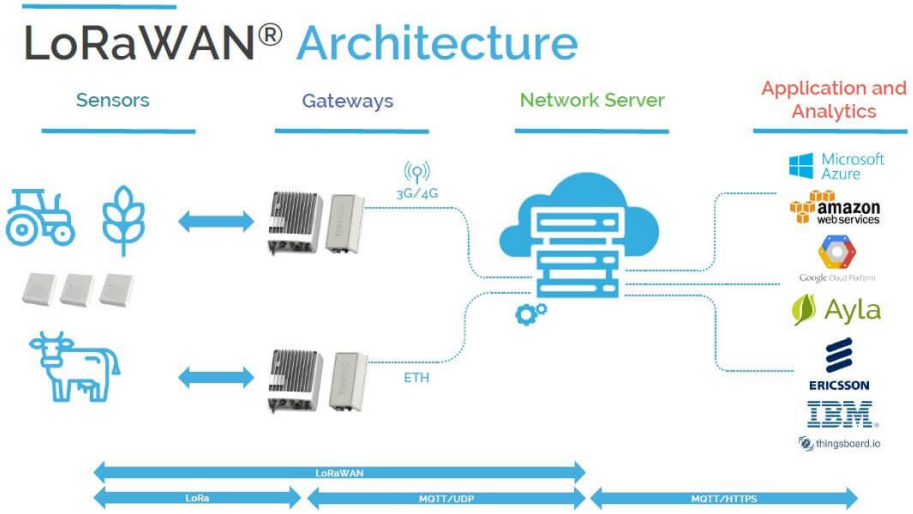
3.2 LPWAN-technológiák

Az LPWAN (Low-Power Wide-Area Network) technológiákat kifejezetten az olyan IoT-alkalmazásokhoz fejlesztették, ahol alacsony energiafelhasználás mellett nagy távolságokat

kell áthidalni, miközben az adatmennyiség alacsony. Két fő LPWAN technológia elterjedt az okosvárosokban:

3.2.1 LoRaWAN (Long Range Wide Area Network):

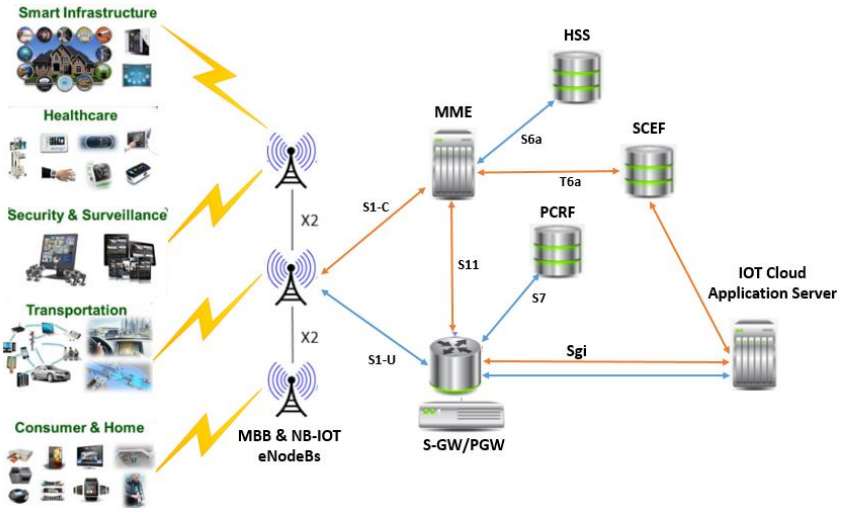
A LoRaWAN a legnépszerűbb, nyílt protokollal rendelkező LPWAN megoldások egyike. A LoRa technológia ideálisan használható például intelligens parkolórendszerekben, okos vízórákban vagy a levegőminőség-érzékelőkben. Az eszközök akár éveken át működhetnek elemről, és vidéken akár 10-15 km-es távolságot is áthidalhatnak, míg városi környezetben 1-3 km-t. Előnye a nagy hatótávolság, az alacsony energiafogyasztás és a decentralizálható infrastruktúra. 1. ábrán a LoRaWAN architektúra komponenseinek kapcsolódása.



1. ábra LoRaWAN architektúrája

3.2.2 NB-IoT (Narrowband IoT):

Az NB-IoT egy mobilhálózaton (általában 4G/LTE) alapuló technológia, amelyet a kis sávszélességű, de megbízható és biztonságos adatátvitelre terveztek. Az előnye, hogy a meglévő mobilhálózatokba integrálható, így nincs szükség külön infrastruktúra kiépítésére. Tipikusan okos mérőórákban, távfelügyeleti eszközökben és okos épületek szenzoraiban használják. 2. ábrán látható a Narrowband IoT működésének bemutatása.



2. ábra Narrowband IoT architektúrája

3.3. 5G hálózat az okosvárosban

Az 5G technológia forradalmi változást hoz az okosvárosi kommunikációban. Az alacsony késleltetés (latency), a nagy adatátviteli sebesség és a megnövelt eszközsűrűség-kezelési képesség révén az 5G lehetővé teszi a valós idejű alkalmazások megbízható működését.

Az 5G előnyei:

- <10 ms késleltetés
- Több millió eszköz/km² támogatása
- Dinamikus hálózatszeletelés (network slicing)
- Valós idejű videófeldolgozás támogatása (pl. biztonsági kamerák)

Az 5G különösen fontos az olyan időérzékeny alkalmazások esetében, mint az önvezető járművek, a forgalomirányítás, vagy a közbiztonsági események valós idejű követése és kezelése.

3.4. Mesh hálózatok és helyi kommunikáció

Az okosvárosokban gyakran használnak mesh hálózatokat, ahol az eszközök egymással közvetlenül is tudnak kommunikálni, és a hálózat dinamikusan átalakul, ha egyes eszközök kiesnek vagy mozognak. Ez a megközelítés robosztusabb és rugalmasabb, különösen parkolásvezérlésnél vagy közvilágítási rendszerekben.

3.5. Kommunikációs protokollok

Az okosvárosok kommunikációs rendszerei a különböző alkalmazások jellegétől és a műszaki feltételektől függően különféle protokollokat használnak:

Protokoll	Használati terület	Előnyök
MQTT	Szenzorhálózatok, időjárás, vízórák	Könnyű, nyílt szabvány, kis adatterhelés
CoAP	Erőforrásszegény eszközök	REST-szerű, UDP alapú, kis sávszélesség
HTTP/HTTPS	Webes interfészek	Széles körben támogatott, emberi interfészeknél hasznos
ZigBee	Épületautomatizálás	Mesh támogatás, alacsony energiaigény

3.6. Kihívások a kommunikációban

Bár a technológiák gyorsan fejlődnek, több kihívás továbbra is fennáll:

Interoperabilitás: Különböző eszközök és protokollok összehangolt működése

Adatbiztonság: A nyílt hálózatokban az adatátvitel sérülékeny lehet, különösen az önkormányzati vagy közbiztonsági adatok esetében

Késleltetés és megbízhatóság: Kritikus rendszerek esetén (pl. V2X) nem megengedhető az adatvesztés vagy a késleltetett válasz

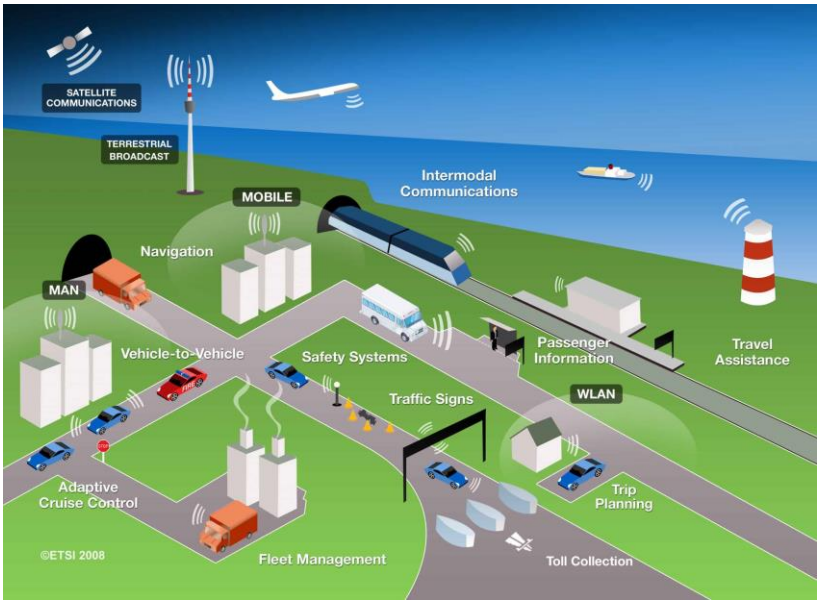
4. Alkalmazási területek és megoldások az okosvárosokban

Az okos városok akkor öltenek formát, amikor a technológiai alappillérek – beépített rendszerek, hálózatok, szenzor hálók és adatközpontok – meghatározott, behatárolt felhasználási területeken egyesülnek. Ezek azok a területek, ahol az "okos város" előnyei a lakók számára láthatóak és érzékelhetőek. A következőkben az okosvárosok legfontosabb

alkalmazási területeit vázoljuk.

4.1. Intelligens közlekedési irányítás és mobilitás

A legelterjedtebb és leggyakrabban fejlesztett okosvárosi alkalmazás a közlekedési rendszerek intelligens kezelése (ITS – Intelligent Transportation System). 3. ábrán látható ennek a bemutatása. A cél a közutak optimális kihasználtságának elérése, a torlódások csökkentése, a közlekedési balesetek számának mérséklése, továbbá az utazási idők kiszámíthatóságának növelése. A mesterséges inteligencián alapuló közlekedési szabályozás előre jelezhetővé teszi a városi forgalmat [5].



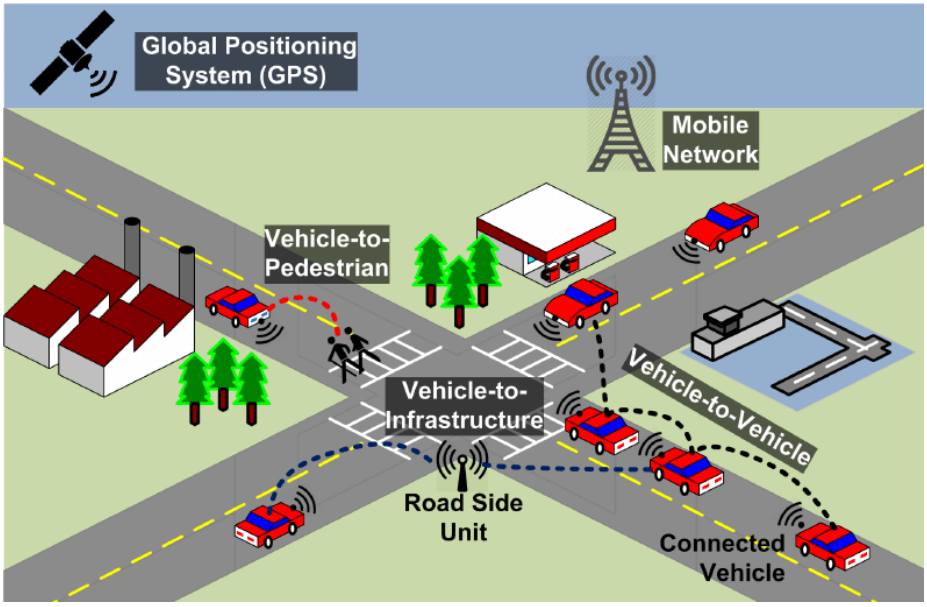
3. ábra ITS bemutatása

Ezen rendszerek alapját a beépített érzékelők és kamerák adják, amelyek képesek a járműforgalmat, a gyalogosmozgást és a sebességet valós időben monitorozni, továbbá a dugókat vagy baleseteket detektálni. Ezek az adatok a központi forgalomirányító rendszerekhez érkeznek, amelyek képesek:

- adaptív módon szabályozni a közlekedési lámpákat,
- valós időben átirányítani a forgalmat,
- informálni a közlekedőket közlekedési táblák és digitális kijelzők segítségével.

Ezekhez a rendszerekhez hatékony kiegészítő a V2X kommunikáció (vehicle-to-everything), amely a járművek közötti közvetlen kommunikációt (V2V), az infrastruktúrával (V2I), a gyalogosokkal (V2P) és a hálózatokkal (V2N) teszi lehetővé. A cél a közlekedés

előre jelezhetővé tétele, nem csupán reagálóvá formálása.



4. ábra V2X kommunikáció bemutatása

4.1.1. Okos közlekedési fények és időzítők

Az intelligens lámpák függetlenül képesek a döntéshozatalra. Érzékelők és a hálózati összeköttetésük révén folyamatosan figyelik a gyalogosok áthaladását, a közlekedési dugókat, és a kapcsolódó utak forgalmát. Ez a rendszer nem csupán a forgalmat teszi hatékonyabbá, hanem a környezetet is óvja, csökkentve az állásidőt és a kipufogógázok mennyiségét.

4.1.2. A V2X kommunikáció kulcsfontosságú

A Vehicle-to-Everything (V2X) technológia lehetővé teszi, hogy a járművek kommunikáljanak egymással, az úthálózattal (V2I), a gyalogosokkal (V2P), valamint a hálózati szolgáltatókkal (V2N) is. Ennek révén csökkenthető a balesetek esélye, gyorsul a közlekedési reakcióidő, és ritkul a torlódások előfordulása. A V2X rendszerek elengedhetetlenek az önvezető autók városi közlekedésbe történő bevezetésénél. Az intelligens forgalomirányítás az MI és V2X alapú adaptív rendszerekre épül [5].

4.2. Okos parkolás

A parkolóhelyek keresése a nagyvárosokban időigényes és stresszes feladat. Az okos parkolási rendszerek érzékelők (pl. mágneses vagy ultrahangos) segítségével jelzik a szabad

parkolóhelyeket. Ezek az információk egy központi adatbázisba kerülnek, a sofőrök pedig mobilalkalmazásokon keresztül valós időben értesülhetnek a lehetőségekről.

Ez nemcsak kényelmi szempontból jelent előnyt, hanem csökkenti a felesleges körözést, a károsanyag-kibocsátást és a városi zajterhelést is.

4.3. Energiahatékonyság és intelligens közvilágítás

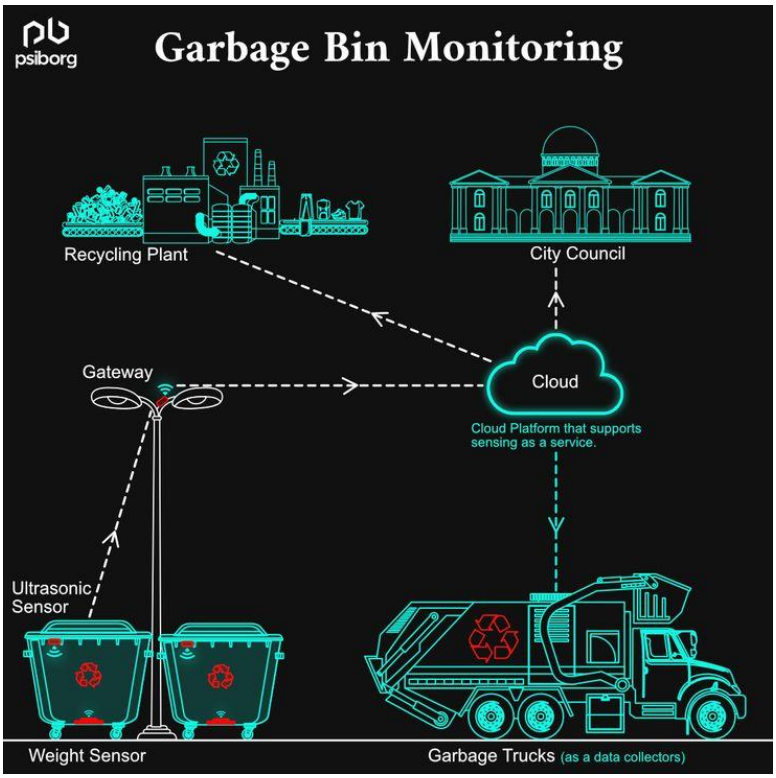
Az energiafogyasztás optimalizálása és a fenntarthatóság az okosvárosok egyik legfontosabb célkitűzése. Ennek leglátványosabb példája az intelligens közvilágítás, ahol a lámpatestekbe épített fény- és mozgásérzékelők, valamint kommunikációs modulok automatikusan szabályozzák a fényerőt az aktuális igények szerint.

Például a gyalogos- vagy autóforgalom alacsony intenzitása esetén csökkenthető a fényerő, majd a mozgásérzékeléskor automatikusan világosabb lesz a terület. Ezek a rendszerek akár 50-70%-kal is csökkenthetik az energiafelhasználást, miközben javítják a közbiztonságot.

Az energiahatékonyság másik területe az épületfelügyelet, ahol az okos mérők (smart meters) és az energiamenedzsment rendszerek figyelik és szabályozzák a fogyasztást. Ezen adatok felhasználásával személyre szabott energiaprofilok alakíthatók ki, valamint optimalizálható a fűtés, a világítás és a hűtés.

4.4. Hulladékgazdálkodás

A hulladékgyűjtés optimalizálása érdekében az okosvárosokban szenzoros kukákat helyeznek ki, amelyek jelzik a telítettségi szintjüket. A hulladékszállító járművek ennek megfelelően tervezik meg útvonalaikat, amivel csökken az üzemanyag-felhasználás, a költségek, valamint elkerülhető a túlcsordulás. 5. ábrán látható, hogy ennek mi is a megvalósulási folyamata.



5. ábra IoT eszközökkel támogatott hulladékgyűjtési folyamat

Ezen rendszerek IoT-eszközökkel, GPS-alapú útvonaltervezéssel és felhőalapú adatelemzéssel kombinálva rendkívül hatékonnyá tehetők.

4.5. Környezeti monitoring

Az okosvárosoknak nemcsak a közlekedést és az energiafelhasználást kell optimalizálniuk, hanem a környezetvédelmi szempontokat is figyelembe kell venniük. A levegőminőség-ellenőrzés, a zajmérés, a hőmérséklet és a páratartalom figyelése mind hozzájárulhatnak ahhoz, hogy a város megalapozott döntéseket hozzon – például forgalomkorlátozást léptessen életbe a rossz levegőminőség esetén.

Kis méretű beépített szenzoregységek kihelyezésével ezek az adatok sűrű térbeli lefedettséggel gyűjthetők, majd az önkormányzati adatplatformon keresztül értelmezhetők és publikálhatók.

4.6. Közbiztonság és térfigyelés

A közbiztonság szintén kulcsfontosságú terület, ahol az okosvárosi rendszerek jelentős

hatást gyakorolhatnak. A modern térfigyelő rendszerek nemcsak rögzítik a videót, hanem valós idejű képfeldolgozással (pl. rendszámfelismerés, arcfelismerés) is dolgoznak. Ezek a rendszerek képesek automatikusan észlelni gyanús viselkedést, tömeges eseményeket vagy biztonsági fenyegetéseket, és ezekről értesítést küldenek az illetékes hatóságoknak.

Ez különösen hasznos közlekedési balesetek, rendkívüli időjárási események vagy akár bűncselekmények megelőzésénél.

4.7. Egészségügyi és szociális rendszerek támogatása

A járványhelyzetekben az egészségügyi rendszerbe integrált IoT-eszközök (pl. hőmérő kapuk, szenzoros lázmérők, fertőtlenítő automatikák) gyorsabb reagálást tettek lehetővé. A telemedicina, a mobil egészségügyi egységek és a távoli betegmonitorozás egyre inkább elérhetővé válik városi szinten is.

Az okosvárosi megközelítés itt nemcsak az infrastruktúra hatékonyságát növeli, hanem aktívan hozzájárul a lakosság jóllétéhez és egészségi állapotának fenntartásához.

5. Esettanulmány: Barcelona Smart City

Barcelona, a világ egyik mérvadó képviselője az okosvárosok megvalósításában. Az európai metropolisz már 2011 óta folyamatosan fejleszti digitális infrastruktúráját, s így nem csupán technológiai értelemben jelent követendő példát, de a társadalmi és környezeti vonatkozásban is. A Barcelona Smart City projekt integrált, intelligens rendszerek együttesét öleli fel, melyek a város szinte valamennyi területén aktívak. A modellben a valós idejű adatgyűjtés és feldolgozás integrált rendszerként működik [6], [9].

5.1. A projekt célkitűzései

Barcelona nem csupán technológiai újításra törekszik. A városvezetés hosszú távú célokat fogalmazott meg:

- A lakosság életszínvonalának javítása
- A városi szolgáltatások hatékonyságának növelése
- Az energiafelhasználás és a környezeti terhelés csökkentése
- Nyílt adathozzáférés a polgárok és a fejlesztők számára
- A társadalmi részvétel erősítése a döntéshozatalban

A fenti célokat technológiai eszközökkel kívánják elérni, amihez modern kommunikációs rendszerekre, érzékelőhálózatokra és a beágyazott rendszerek széles körű alkalmazására van szükség.

5.2. Kiemelt fejlesztési területek

5.2.1 Intelligens közlekedés

A város útjain több mint 500 intelligens közlekedési lámpa működik, melyek valós időben alkalmazkodnak a forgalom mértékéhez. Ezeket szenzoros hálózatok és központi adatfeldolgozó rendszerek irányítják. A tömegközlekedési eszközök (buszok, villamosok) valós idejű követése mobilalkalmazáson keresztül is megoldott, ami nagyban javítja az utazók kényelmét.

5.2.2 Okos parkolási rendszer

Barcelona bevezette az „AreaDUM” rendszert, mely érzékelőkkel méri a parkolóhelyek foglaltságát. Az autósok mobilapplikációval kereshetnek szabad parkolóhelyeket, s azonnal fizethetnek is a parkolásért. Ez nemcsak kényelmes, de csökkenti a felesleges közlekedést, s ezáltal a környezeti terhelést is mérsékli.

5.2.3 Okos közvilágítás

A város LED-es lámpatesteket helyezett üzembe, melyek beágyazott rendszerekkel és mozgásérzékelőkkel vannak ellátva. Ezek a gyalogos- és gépjármű forgalom nagyságától függően automatikusan szabályozzák a fényerőt. Az energiafelhasználás optimalizálásával évi szinten akár 30%-os megtakarítást is sikerült elérniük.

5.2.4 Hulladékgazdálkodás

A szeméttárolókba szenzorokat szereltek, melyek jelzik a telítettséget. A gyűjtés optimalizált útvonalakon történik, ezzel elkerülik a felesleges üzemanyag-felhasználást és a CO_2-kibocsátást. Ez a rendszer a forgalmas belvárosi zónákban kiemelkedően hatékony.

5.2.5 Környezeti monitoring

A város számos pontján vannak érzékelők, melyek a légszennyezést, zajszintet, hőmérsékletet, páratartalmat, illetve a városi hősziget-hatás nagyságát mérik. Az adatok

nyilvánosan elérhetőek, s a várospolitikai döntések alapját képezik – például zöldövezetek kijelölése, vagy kerékpárosbarát zónák kialakítása.

5.3. Műszaki infrastruktúra

Barcelona városa kiemelt figyelmet fordít az IoT-platformok központi integrációjára. Minden adat – parkolás, közlekedés, energia vagy környezet – egy közös városi adatplatformra érkezik be. Ez a platform teszi lehetővé:

- **a valós idejű megfigyelést,**
- **a prediktív elemzést,**
- **a fejlesztők számára nyitott API-k használatát (pl. Open Data BCN portál).**

A kommunikációt LPWAN és Wi-Fi mesh hálózatok kombinációja biztosítja. A város több mint 500 km-es optikai kábelhálózattal bír, ami a gyors és stabil adatáramlás alapja. Barcelona fejlesztéseiben a digitális ikerpárok alapú városmodellezés és adatvizualizáció is megjelenik [6].

5.4. Társadalmi dimenzió

Barcelona különösen fontosnak tartja a polgárok bevonását. A „Decidim” nevű digitális platformon a lakosok javaslatokat tehetnek, szavazhatnak, és visszajelzést adhatnak a városi döntéshozatalról. Ez a digitális részvétel példaértékűen illeszkedik az okosváros emberközpontú megközelítésébe, mely a jövőbeli Ipar 5.0 alapelvével is összhangban van.

5.5. Eredmények és tanulságok

A Smart City Barcelona projekt több mint egy évtizedes tapasztalata azt mutatja, hogy az okosvárosi rendszerek nemcsak technológiailag, hanem társadalmilag és gazdaságilag is fenntarthatók. Az intelligens rendszerek révén:

- **33%-kal csökkent az energiafogyasztás a közvilágításban,**
- **a parkolási idő 25%-kal csökkent,**
- **a forgalom optimalizálása 21%-kal mérsékelte az utazási időket,**
- **a lakossági elégedettségi mutatók is emelkedtek.**

A legfontosabb tanulság az, hogy egy város digitális átalakulása nem csupán technológiai kérdés, hanem egy komplex társadalmi folyamat, amely hosszú távú stratégiai gondolkodást, nyitottságot és a közösség részvételét igényli.

6. Technológiai és társadalmi kihívások

A felhőkarcolók mintájára tervezett, ám a gyakorlatban számtalan akadályba ütköző okosváros koncepciója. Ezen nehézségek technikai természetűek, de emellett gazdasági, jogi és társadalmi természetűek is lehetnek. A következőkben részletezem, hogy a legfontosabb kihívások melyek, melyekkel szembesülnek az okosvárosi rendszerek tervezése, megvalósítása és üzemeltetése során.

6.1. Az interoperabilitás és a szabványosítás hiánya

Egy okosváros esetében elengedhetetlen, hogy a külön-külön fejlesztett rendszerek és eszközök képesek legyenek együttműködni. Ez a gyakorlatban azonban korántsem mindig gördülékeny. A gyártók gyakran különböző protokollokat, adatstruktúrákat és kommunikációs normákat alkalmaznak, amelyek nem feltétlenül kompatibilisek egymással.

6.1.1 Az interoperabilitás hiánya többféle problémát okozhat:

- az adatok megosztásának és újrafelhasználásának nehézségeit,
- a különböző rendszerek közötti integráció magas költségeit,
- az informatikai sebezhetőségek növekedését.

6.1.2 A megoldás:

A nyílt szabványok és API-k (Application Programming Interface) alkalmazása, melyekkel az adatok és szolgáltatások közötti átjárhatóság biztosítható. Nemzetközi kezdeményezések, mint az ETSI, az Open & Agile Smart Cities (OASC) vagy a FIWARE nyílt platformja, nagymértékben segíthetik a technológiai egységesítést. A társadalmi befogadás és a lakosság digitális kompetenciája elengedhetetlen az okosvárosi megoldások sikeréhez [8].

6.2. Adatvédelem és biztonság

Az okosvárosok egyik legnagyobb kihívása a hatalmas mennyiségben képződő személyes és érzékeny adatok védelme. A szenzorhálózatok, kamerák, mobilalkalmazások és intelligens szolgáltatások folyamatosan adatokat gyűjtenek a lakókról: tartózkodási hely, közlekedési szokások, energiafogyasztás, egészségügyi adatok stb.

A GDPR (General Data Protection Regulation) és más adatvédelmi szabályozások egyértelműen kimondják, hogy az adatgyűjtés átláthatóan, jogszerűen és csak a

meghatározott célok érdekében történhet. A technológiai megvalósítás azonban nem mindig képes megfelelni ezeknek a követelményeknek.

Továbbá az adatok tárolása és feldolgozása során számos sebezhetőség alakulhat ki:

- **adatlopás** (pl. érzékeny állampolgári adatok),
- **rendszerbe hatolás** (pl. közlekedésirányítás megbénítása),
- **hamis adatbevitellel történő rendszerzavarás**.

A kiberbiztonság ezért elengedhetetlen: kriptográfiai protokollok, biztonságos autentikációs rendszerek, tűzfalak, hálózatszeparáció és decentralizált (blockchain-alapú) megoldások válhatnak szükségessé.

6.3. Finanszírozás és hosszú távú fenntarthatóság

Az okosvárosok kiépítése komoly pénzügyi befektetést igényel. A szenzorhálózatok, adatközpontok, hálózati infrastruktúra, alkalmazások fejlesztése, üzemeltetése és karbantartása is jelentős költségekkel jár.

Különösen a kis- és közepes méretű önkormányzatoknak okoz kihívást a megfelelő finanszírozási struktúra kialakítása. A városvezetés gyakran külső – állami, uniós vagy magán – forrásokra szorul, melyhez átlátható és meggyőző üzleti modellek szükségesek.

A fenntarthatóság kérdése szintén kritikus: a pilot projektek után a működtetés költségei gyakran váratlanul megemelkednek. Ezért a projekt hosszú távú gazdasági modelljét már a kezdetektől alaposan át kell gondolni.

6.4. Technológiai egyenlőtlenségek

Nem minden város, és nem minden városrészen belül élők részesülhetnek egyenlő mértékben az okosvárosi technológiák előnyeiből. A digitális szakadék fogalma ma már nemcsak országos, hanem településen belüli szinten is értelmezhető: bizonyos városrészek kimaradhatnak a fejlesztésekből, vagy a lakosság nem tudja megfelelően használni az elérhető szolgáltatásokat.

Az okosvárosi rendszerek tervezésekor a társadalmi befogadást is figyelembe kell venni:

- *a lakosság digitális kompetenciájának fejlesztését,*
- *akadálymentes felhasználói interfészek kialakítását,*
- *idősek, mozgáskorlátozottak vagy hátrányos helyzetű csoportok bevonását.*

6.5. Lakossági elfogadottság és bizalom

Hiába a legfejlettebb technológia, ha a lakosság nem bízik a rendszerben, nem fogja használni. A bizalom kialakítása alapvető:

- *az adatkezelés átláthatósága,*
- *nyílt forráskódú rendszerek preferálása,*
- *közérthető kommunikáció,*
- *közösségi részvétel (pl. közösségi tervezés, szavazás, visszajelzés lehetősége).*

A társadalmi elfogadottság hiánya megbéníthatja a legjobb technológiai projekteket is – ezt láttuk például a torontói „Sidewalk Labs" projekt kudarcánál, ahol a Google leányvállalata adatvédelmi aggályok miatt visszalépett a től.

6.6. Etikai dilemmák és szabályozási kérdések

Az okosvárosok működése olyan mennyiségű és érzékenységű adatot generál, hogy új típusú etikai kérdések is felmerülnek:

- meddig terjed az állam megfigyelési joga?
- kik férhetnek hozzá az adatokhoz?
- használhatók-e ezek az információk üzleti célokra?
- hogyan kezeljük az algoritmikus döntéshozatal hibáit?

A szabályozás ebben a tekintetben még mindig kezdeti stádiumban van. A „technológia gyorsabban fejlődik, mint a törvények" közhelye sajnos igaz. Ezért is fontos, hogy a jogalkotók, etikusok, informatikusok és polgárok együttesen alakítsák ki az okosvárosok etikai és jogi keretrendszerét.

7. Jövőbeli irányok és az Ipar 5.0 szerepe az okosvárosokban

A XXI. század okos városai új megoldások tömegével büszkélkedhetnek, melyek a 4.0 ipari forradalom technológiai pilléreire épülnek: a **dolgok internete (IoT), a mesterséges intelligencia, a felhőalapú rendszerek, az élfeldolgozás, a nagymennyiségű adat elemzése, az 5G hálózatok**, továbbá a beágyazott rendszerek kulcsszerepe mind ezt szolgálják. Ez lehetővé teszi a valós világ digitális másolatának, elemzésének, és a vezérlés automatizálásának megvalósítását. Ezzel egy időben a gazdaság és a technológia az 5.0 ipar irányába tart, ami nem csak az automatizálásra, hanem az ember és a gépek közötti szimbiózisra is fókuszál.

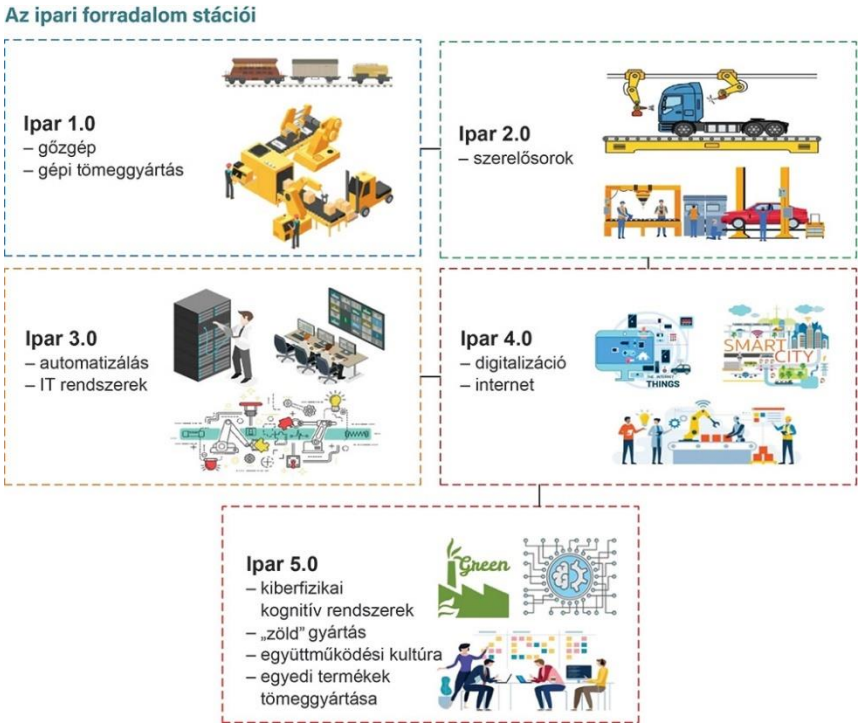
Ez a szemlélet gyökeres változást hozhat a jövő okos városaiban, mivel a következő évek intelligens városai nem csak hatékonyabbak és okosabbak lesznek, de empatikusabbak, befogadóbbak és proaktívabbak is.

7.1. Az 5.0 iparvezérelvei

Az Európai Bizottság 2021-es felmérése szerint az 5.0-s ipar alapkövei a következők:

- **Emberközpontúság**: Az emberi jólét, a jogok és a méltóság áll a technológiai döntéshozatal középpontjában.
- **Fenntarthatóság**: A környezetterhelés minimalizálása, a megújuló energiaforrások és a körforgásos gazdaság előnyben részesítése.
- **Rugalmasság és ellenállóképesség**: A válsághelyzetekre történő gyors és hatékony válaszadás képessége.

Az 5.0-s ipar nem a gépekre, hanem az emberre összpontosít, a technológiai fejlődést ehhez igazítva. Ennek az alapelvnek az okos városokban történő alkalmazása forradalmasíthatja a városok polgárokat szolgáló módját.



6. ábra Az ipari forradalmak

7.2. Digitális ikerpárok

Az egyik leginnovatívabb megközelítés a digitális ikerpárok (Digital Twin) technológiájának alkalmazása az okos városokban. Ez a valós városi környezet, épület, kerület vagy közlekedési hálózat pontos, folyamatosan frissített digitális másolata. Az okosvárosi rendszerek alapját a digitális ikerpárok adják [2].

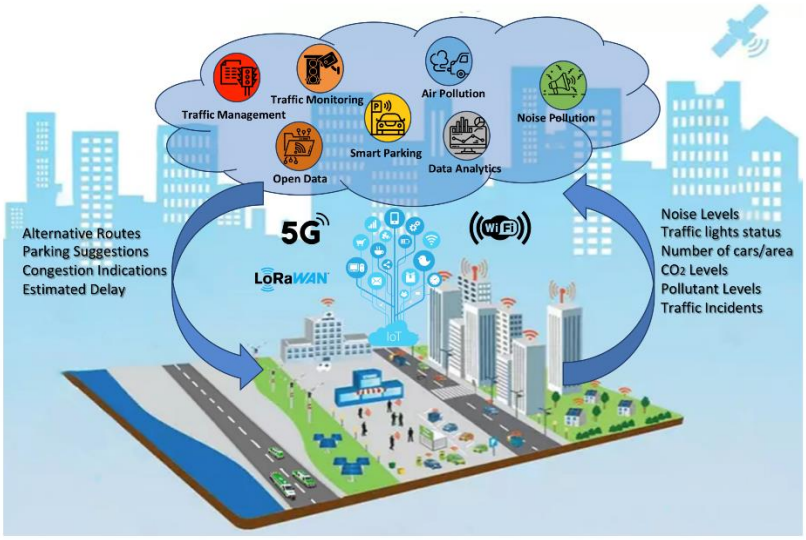
A digitális ikerpár a városvezetés és -tervezés számára:

- Valós időben figyeli az infrastruktúra állapotát.
- Előre modellezheti a természeti katasztrófákat vagy a közlekedési helyzeteket.
- Különböző forgatókönyveket tesztelhet a valós környezet veszélyeztetése nélkül.

Ez a technológia lehetővé teszi, hogy a városok proaktívan működjenek: ne csak reagáljanak a történésekre, hanem előre lássák azokat, és megelőzzék a problémákat.

7.ábrán bemutatása kerül a Digitális ikerpár adat körforgása a városon belül.

Az új generációs digitális ikerpár architektúrák egyre több mesterséges intelligencia réteget tartalmaznak, amelyek prediktív karbantartásra és városi szimulációkra is alkalmazhatók [12].



7. ábra Digitális ikerpár adat körforgása

7.3. Mesterséges értelem és adaptív városirányítás

A jövőbeli intelligens városok "agyát" a mesterséges értelem adja. Az MI nem csak adatok elemzésére és mintázatok felismerésére képes, hanem önálló döntésekre is.

Példák:

- *A közlekedési lámpák önálló tanulása a forgalmi adatokból.*
- *Egészségügyi járványügyi előrejelzések a lakosok mozgásából.*
- *Energiahálózatok adaptív szabályozása a fogyasztási előrejelzések alapján.*

Az ilyen adaptív rendszerek hatékonyabbá teszik az erőforrások felhasználását, gyorsabban reagálnak a rendkívüli eseményekre, és folyamatosan képesek tanulni a környezetükből.

7.4. Ember és technológia együttműködése

Az 5.0-s ipar és az intelligens városok összefonódása nem csupán technológiai kérdés. **A jövő városaiban nem az a cél, hogy az embert helyettesítsék, hanem hogy támogassák**. Ez megvalósulhat például:

- *Kiterjesztett valóság (AR) és virtuális valóság (VR) eszközökkel támogatott várostervezésben.*
- *Emberközpontú kezelőfelületekben (pl. látás- vagy hallássérültek számára optimalizált rendszerek).*
- *Robotikus segédekben, melyek az idősek vagy a mozgáskorlátozottak életét könnyíthetik meg.*

A robotok (cobotok), a csevegésre képes mesterséges intelligencia (chatbotok) és a felhasználóbarát (UX/UI) interfészek révén az okos város valóban a lakók igényeihez igazodik, nem fordítva.

7.5. A városi életminőség újradefiniálása

Az intelligens város végső célja nem az, hogy több adatot gyűjtsön vagy gyorsabban működjön, hanem az, hogy jobb életminőséget teremtsen az emberek számára. A jövő városa:

- *Egészséges, zöld és szennyezésmentes.*
- *Akadálymentes és befogadó.*
- *Biztonságos, ugyanakkor szabad.*
- *Demokratikus, a lakók bevonásán alapuló, és nyitott.*

Az olyan kezdeményezések, mint a 15 perces város koncepciója (ahol minden alapvető szolgáltatás 15 percen belül elérhető gyalog vagy kerékpárral), vagy a zöld infrastruktúra tervezése (urban jungle), kiválóan példázzák ezt az irányt.

7.6. Összegzés a jövőről

Az **5.0-s ipar** elvein alapuló **intelligens városok** túlmutatnak a technológiai bemutatón: **céljuk az emberi jólét szolgálata a technológia eszközeivel**. A digitális ikerpárok, a MI-alapú predikció, a decentralizált rendszerek és az emberközpontú tervezés együttesen hozzák létre a holnap városait. Az Ipar 5.0 technológiák új generációja a digitális ikerpárok emberközpontú alkalmazását helyezi előtérbe [10].

Ezekben a városokban az emberek nem csupán lakók, hanem aktív résztvevők és alkotótársak, a jövő nemcsak épül, hanem velük együtt formálódik.

8. Összefoglalás és következtetések

A huszonegyedik század települései soha nem látott kihívásokkal néznek szembe. A városiasodás üteme, a környezeti problémák egyre súlyosabbak, a közszolgáltatások iránti igény folyamatosan nő, és az energiafelhasználás fenntarthatósága mind olyan szempontok, amelyek új megoldásokat követelnek. Az okosvárosok koncepciója ezekre a komplex problémákra ad választ – technológiai, társadalmi és gazdasági szinteken egyaránt.

Jelen írás célja annak bemutatása volt, hogy a beágyazott rendszerek és az Ipar 4.0 technológiák hogyan járulnak hozzá az intelligens városi infrastruktúrák működéséhez.

A kommunikációs technológiák, mint a LoRaWAN, NB-IoT vagy 5G, lehetővé teszik a különböző rendszerek közötti valós idejű adatcserét és összehangolt működést. Ezek a hálózatok elengedhetetlenek a dinamikus és autonóm városi szolgáltatásokhoz. A digitális ikerpárok, az edge computing, és a mesterséges intelligencia további lehetőségeket nyújtanak az okosvárosok fejlődésében – nem csupán a városi környezet eseményeire reagálnak, hanem előre is jeleznek, illetve proaktívan döntenek.

A barcelonai példaanyag jól szemlélteti, hogyan lehet egy európai nagyvárosban az intelligens megoldásokat integráltan, hosszú távú stratégiával bevezetni, és a lakosságot aktívan bevonni. Ez a gyakorlat kiváló példa más települések, köztük a magyar városok számára is.

Ugyanakkor nem szabad elfelejtenünk az akadályokat és kockázatokat:

- Az interoperabilitás hiánya nehezítheti a különböző rendszerek integrálását.
- Az adatvédelem kérdése központi etikai dilemmává vált.
- A finanszírozási nehézségek és a fenntartható üzleti modellek hiánya veszélyeztetheti a projektek hosszú távú működését.
- A társadalmi befogadás, a digitális kompetencia szintje és az egyenlő hozzáférés kérdései szintén fontosak.

A beadandó végén bemutatott Ipar 5.0 koncepció és az emberközpontú technológia új távlatokat nyit: az okosváros nem csupán a gépek és algoritmusok világa lesz, hanem az embereké, akik aktívan alakítják és élvezik a városi digitális ökoszisztéma előnyeit.

Irodalomjegyzék

[1] *P. Patel and V. Sharma, "Global perspectives on digital twin smart cities," Sustainable Cities and Society, vol. 101, 2025. [Online]. Available:*

[2] Lorenzo Adreani et al.: *Smart City Digital Twin Framework for Real-Time Multi-Data Integration and Wide Public Distribution*

[3] Aidan Fuller et al.: *Digital Twin: Enabling Technologies, Challenges and Open Research*

[4] S. Aslam & H. Sami Ullah: *A Comprehensive Review of Smart Cities Components, Applications, and Technologies Based on Internet of Things*

[5] M. K. Ali, "AI-Powered Digital Twins and IoT for Smart Cities and Sustainable Building Environments," *Applied Sciences*, vol. 14, no. 24, Article 12056, 2024.

[6] Eduardo Felipe Zambom Santana et al.: *Software Platforms for Smart Cities: Concepts, Requirements, Challenges, and a Unified Reference Architecture*

[7] MDPI: *Virtual Reality and Internet of Things Based Digital Twin for Smart City*

[8] Emerald Insight: *Smart City Digital Twins: Overview of Implementation Challenges and Recommendations for Citizens Training*

[9] L. Adreani et al., "Smart City Digital Twin Framework for Real-Time Multi-Data Integration and Wide Public Distribution," *arXiv*, Sep. 2023.

[10] OAEPublish: *Developments of digital twin technologies in industrial, smart city, and healthcare applications*

[11] MDPI: *AI-Powered Digital Twins and Internet of Things for Smart Cities and Sustainable Building Environments*

[12] S. R. Rauf, "Trends in Digital Twin Framework Architectures for Smart Cities," *Sensors*, vol. 23, no. 5, Article 10934255, 2024.

[13] Reuters: *How AI is arming cities in the battle for climate resilience*

[14] ACM Digital Library: *Opportunistic Digital Twin: an Edge Intelligence enabler for Smart City*

2.53. Okosvárosok és beágyazott rendszerek: Technológiai megoldások és alkalmazások az

Széchenyi István Egyetem

Gépészmérnöki, Informatikai és Villamosmérnöki Kar

Informatika Tanszék

Okosvárosok és beágyazott rendszerek:
Technológiai megoldások és alkalmazások az intelligens városi infrastruktúrába

Rugonfalvi-Ress Barnabás

[redacted]

Gazdaságinformatikus BSc

2024/2025/2

Tartalomjegyzék

Tartalom

Tartalomjegyzék....2
1. Bevezetés....4
2. Okosváros fogalma és jelentősége....5
3. Beágyazott rendszerek technológiai alapjai....7
3.1. A beágyazott rendszerek meghatározása....7
3.2. Főbb összetevők....7
3.3. Operációs rendszerek és szoftverplatformok....8
3.4. Beágyazott rendszerek és valós idejű kommunikáció....8
3.5. Példák beágyazott rendszerekre az okosvárosban....8
3.6. Előnyök és jelentőség....8
4. Kommunikációs technológiák okosvárosokban....10
4.1. Az IoT (Internet of Things) hálózat jelentősége....10
4.2. LPWAN-technológiák....10
4.3. 5G hálózat az okosvárosban....12
4.4. Mesh hálózatok és helyi kommunikáció....12
4.5. Kommunikációs protokollok....12
4.6. Kihívások a kommunikációban....13
5. Alkalmazási területek és megoldások az okosvárosokban....14
5.1. Intelligens közlekedési irányítás és mobilitás....14
5.2. Okos parkolás....15
5.3. Energiahatékonyság és intelligens közvilágítás....15
5.4. Hulladékgazdálkodás....16
5.5. Környezeti monitoring....16
5.6. Közbiztonság és térfigyelés....16
5.7. Egészségügyi és szociális rendszerek támogatása....17
Esettanulmány: Barcelona Smart City....18
6.1. A projekt célkitűzései....18
6.2. Kiemelt fejlesztési területek....18
6.3. Műszaki infrastruktúra....19
6.4. Társadalmi dimenzió....19
6.5. Eredmények és tanulságok....20

Technológiai és társadalmi kihívások 21
7.1. Az interoperabilitás és a szabványosítás hiánya 21
7.2. Adatvédelem és biztonság 21
7.3. Finanszírozás és hosszú távú fenntarthatóság 22
7.4. Technológiai egyenlőtlenségek 22
7.5. Lakossági elfogadottság és bizalom 23
7.6. Etikai dilemmák és szabályozási kérdések 23
Jövőbeli irányok és az Ipar 5.0 szerepe az okosvárosokban 24
8.1. Az 5.0 iparvezérelvei 24
8.2. Digitális ikerpárok 25
8.3. Mesterséges értelem és adaptív városirányítás 25
8.4. Ember és technológia együttműködése 26
8.5. A városi életminőség újradefiniálása 26
8.6. Összegzés a jövőről 27
Összefoglalás és következtetések 28
Irodalomjegyzék 29

1. Bevezetés

A huszonegyedik század sorsdöntő kihívása a városiasodás: az ENSZ becslései szerint 2050-re a bolygó népességének körülbelül 70%-a városi területeken fog élni. Ez a tendencia komoly nyomást gyakorol a közlekedésre, energiaellátásra, vízellátásra, egészségügyi szolgáltatásokra, valamint a közbiztonságra. A hagyományos városüzemeltetési módszerek egyre kevésbé képesek hatékony megoldást kínálni ezekre az összetett problémákra. Ennek eredményeként egyre nagyobb hangsúlyt kap az "okosváros" koncepciója, amely a technológiai innovációk felhasználásával egyidejűleg kívánja javítani a városi életminőséget, a fenntarthatóságot és a szolgáltatások hatékonyságát.

Az **okosváros** egy olyan városi rendszer, amely beágyazott rendszerek, érzékelő hálózatok, kommunikációs protokollok, mesterséges intelligencia és adatvezérelt döntéshozatal segítségével optimalizálja a működését. Az intelligens infrastruktúra **nem csupán adatokat gyűjt**, hanem **képes azokat elemezni és hasznosítani** is, lehetővé téve az **önálló működést és a proaktív városi szolgáltatásokat**.

Például a forgalomirányítás már nem csak statikus tervek alapján működik: a valós idejű közlekedési adatok és a V2X (járművek közötti) kommunikáció révén a város rugalmasan tudja szabályozni a forgalmat. Hasonló elv érvényesül a közvilágításban, ahol a mozgás- és fényérzékelők segítségével optimalizálható a világítás teljesítménye, csökkentve az energiafogyasztást és a fényszennyezést.

Az okosváros technológiai alapjait az Ipar 4.0 eredményei adják: IoT (dolgok internete), felhőszolgáltatások, edge computing, adatelemzés és valós idejű kommunikáció. Az okosváros azonban nem pusztán technológiai kérdés, hanem egy társadalmi változás is, amely az együttműködésre, az átláthatóságra és az emberközpontú megoldásokra épül.

A piaci prognózisok szerint a smart city szektor értéke 2024-ben meghaladta a 340 milliárd USD-t, és 2033-ra várhatóan eléri a 830 milliárd USD-t (IMARC Group, 2024). Az IoT eszközök száma a városi környezetben 2025-re elérheti a 17 milliárd darabot, az adatforgalom pedig a 2016-os szinthez képest tízszeresére nőhet (Cisco VNI, Ericsson Mobility Report, 2023).

A beadandó célja, hogy átfogó képet adjon az okosváros technológiai felépítéséről, a beágyazott rendszerek szerepéről, valamint a megvalósítás kihívásairól és a jövőbeli trendekről. Az elemzés kiterjed a gyakorlati példákra is – kiemelt figyelmet fordítva a barcelonai Smart City projekt tapasztalataira – valamint bemutatja az Ipar 5.0 emberközpontú megközelítésének lehetséges hatásait.

2. Okosváros fogalma és jelentősége

Az "intelligens városok" koncepciója az elmúlt években a technológiai diskurzusok sűrűn hangoztatott témájává vált, ám meghatározása még napjainkban is sokféleképpen értelmezhető. Az Európai Unió "Smart Cities" kezdeményezése szerint az okosváros olyan városi környezet, amely az infokommunikációs technológiák és az adatokon alapuló döntéshozatal segítségével fenntarthatóbbá, befogadóbbá és élhetőbbé tehető. A cél az, hogy a város képes legyen optimalizálni saját működését, miközben gyorsan és hatékonyan reagál a lakosság igényeire, valamint a környezeti és gazdasági kihívásokra.

Egy okosváros alapvetően három pilléren nyugszik:

Érzékelés és adatgyűjtés: Különféle szenzorok és beágyazott eszközök (pl. közlekedési kamerák, levegőminőség-mérők, parkolóérzékelők) révén valós időben gyűjt adatokat a város különböző pontjairól.

Adatfeldolgozás és elemzés: A összegyűjtött adatokat intelligens algoritmusok és mesterséges intelligencia segítségével dolgozzák fel, ami lehetővé teszi a város működésének optimalizálását.

Reakció és automatizáció: A rendszer képes önállóan reagálni, például a közlekedési lámpák átállításával, energiaelosztás szabályozásával vagy a közszolgáltatások optimalizálásával.

Az okosvárosoknak számos célja van:

- *Fenntarthatóság:* Energiatakarékos működés, megújuló energiaforrások integrálása, a szén-dioxid-kibocsátás csökkentése.
- *Hatékonyság:* Az erőforrások okos elosztása, a szolgáltatások működésének optimalizálása.
- *Átláthatóság és részvétel:* A lakosság aktív részvétele az adatmegosztásban és a döntéshozatalban.
- *Rugalmasság és ellenállóképesség:* Váratlan események, természeti katasztrófák vagy válsághelyzetek esetén gyors reagálásra képes infrastruktúra kialakítása.

Az okosvárosok koncepcióját támogató technológiai réteg a szenzorhálózatoktól kezdve a hálózati kommunikációs eszközökön (pl. 5G, NB-IoT) át egészen a felhőalapú és edge computing rendszerekig terjed. Mindegyik elemnek saját, gyakran beágyazott rendszere van,

mely helyben képes adatfeldolgozásra és döntéshozatalra. Ezek adják a város intelligens működésének az alapját.

Az okosvárosok jelentősége túlmutat a technológiai újításokon: társadalmi, gazdasági és környezeti szempontból is kiemelkedőek. Segítenek csökkenteni az egyenlőtlenségeket, javítják a szolgáltatásokhoz való hozzáférést, és elősegítik a digitális társadalom fejlődését. Nem véletlen, hogy a világ számos vezető városa – például Barcelona, Szingapúr, Helsinki vagy Bécs – már elindította saját okos város stratégiáját.

3. Beágyazott rendszerek technológiai alapjai

Az okosvárosok működését a beágyazott rendszerek alapozzák meg, amik a technológiai alapot biztosítják. Ezek specifikus, egy adott feladatra tervezett számítógépes egységek, egy nagyobb hálózat részét képezik, és előre meghatározott funkciókat látnak el. A beágyazott rendszerek nem önállóan tevékenykedő számítógépek, hanem integráltan működnek, például közlekedési **lámpákban**, **energiamérőkben**, **térfigyelő kamerákban** vagy épp egy teljes **épületautomatizálási rendszer részeként**.

3.1. A beágyazott rendszerek meghatározása

A beágyazott rendszer hardver és szoftver kombinációja, ami képes a környezetéből érkező adatokat érzékelni, feldolgozni, és ennek megfelelően cselekedni. Ezek a rendszerek gyakran valós idejű működésre optimalizáltak, azaz adott eseményekre meghatározott időn belül reagálniuk kell. Ez kritikus fontosságú olyan területeken, mint a forgalomszabályozás, a biztonsági rendszerek, vagy az energiaelosztás.

3.2. Főbb összetevők

A beágyazott rendszerek felépítése általában a következő elemekből áll:

- Mikrokontroller vagy mikroprocesszor: A rendszer "agyaként" szolgál, feldolgozza az érzékelőktől érkező információkat, futtatja az algoritmusokat és vezérli az aktuátorokat.
- Érzékelők (szenzorok): Környezeti adatok (pl. hőmérséklet, fény, mozgás, légszennyezettség) és események detektálására.
- Aktuátorok: Válaszreakciók kivitelezésére alkalmas eszközök, mint például elektromos motorok, kijelzők, fényjelzések.
- Kommunikációs interfészek: A rendszer hálózati kapcsolatait biztosítják, pl. Wi-Fi, ZigBee, LoRa, Bluetooth, NB-IoT vagy 5G modulok.
- Energiaforrás: Bizonyos rendszerek önálló energiaellátással rendelkeznek, akkumulátorral vagy napelemmodullal.

3.3. Operációs rendszerek és szoftverplatformok

A beágyazott rendszerek gyakran speciális operációs rendszert (RTOS – Real-Time Operating System) használnak, ami garantálja a kiszámítható reakcióidőt. Ilyenek a FreeRTOS, Zephyr, Contiki vagy az ARM Mbed OS. Ezek az operációs rendszerek többnyire nyílt forráskódúak, és kifejezetten IoT-alkalmazásokra optimalizáltak.

A fejlesztői környezetek (IDE-k) szintén kulcsfontosságúak. Az Arduino és Raspberry Pi alapú rendszerek egyszerű prototípusok fejlesztésére alkalmasak, míg ipari alkalmazásoknál a STMicroelectronics, Texas Instruments vagy Renesas fejlesztői platformjai dominálnak.

3.4. Beágyazott rendszerek és valós idejű kommunikáció

Az okosvárosi környezet egyik alapvető kihívása, hogy a különböző alrendszerek – például a közlekedés, a vízkezelés, a közbiztonság – zökkenőmentesen és összehangoltan működjenek. Ehhez elengedhetetlen a valós idejű adatfeldolgozás és kommunikáció, amit a beágyazott rendszerek tesznek lehetővé.

Például: egy V2X (vehicle-to-everything) kommunikációs rendszerben a járművek, a közlekedési lámpák és az útszéleken elhelyezett érzékelők között másodpercenként több száz adatcsomag cserélődik. A beágyazott rendszerek ezeket nemcsak gyorsan, hanem biztonságosan és megbízhatóan is kell, hogy feldolgozzák.

3.5. Példák beágyazott rendszerekre az okosvárosban

Okos közvilágítás: Az egyes lámpatestekbe integrált mikrokontrollerek lehetővé teszik a mozgásérzékelést, fényerőszabályozást és távvezérlést.

Forgalomfigyelő rendszerek: Kamerákhoz és érzékelőkhöz kapcsolt eszközök, melyek képfeldolgozással detektálják a torlódásokat vagy baleseteket.

Okos parkolás: Ultrahangos vagy mágneses érzékelőkkel ellátott, beágyazott rendszerek figyelik a parkolóhelyek foglaltságát.

Légszennyezettség-monitorozó eszközök: Gázérzékelőket és kommunikációs modulokat tartalmazó kompakt rendszerek, melyek folyamatosan küldik az adatokat a város üzemeltetőinek.

3.6. Előnyök és jelentőség

A beágyazott rendszerek előnyei a kis méret, az alacsony energiafogyasztás, a megbízhatóság, a lokális intelligencia (edge computing) és a moduláris bővíthetőség. Ezek

a rendszerek alkotják az intelligens városi infrastruktúra "idegrendszerét", mely képes érzékelni, feldolgozni és reagálni – akár emberi beavatkozás nélkül.

4. Kommunikációs technológiák okosvárosokban

A hatékony okosvárosok alapvető feltétele a stabil, gyors, és energiatakarékos kommunikációs hálózat megléte. Az okos városok alapvető jellemzője, hogy a különböző alrendszereik, mint a közlekedés, közvilágítás, energiagazdálkodás, vagy a hulladékkezelés valós időben osztanak meg adatokat egymással. Ezáltal integráltan képesek reagálni az aktuális eseményekre. Ezt a rendszerszintű kapcsolódást kommunikációs protokollok és hálózati struktúrák biztosítják.

4.1. Az IoT (Internet of Things) hálózat jelentősége

Az okosvárosok kommunikációs gerincét az IoT, vagyis a Dolgok Internete képezi, amely lehetővé teszi az eszközök, mint például az érzékelők, vezérlők, aktuátorok, közötti és a központi rendszerekkel való kapcsolatot. Az IoT hálózatok tervezésekor a méretezhetőség, energiahatékonyság, biztonság, és a lefedettség a legfontosabb szempontok.

Az IoT-eszközök általában kis mennyiségű adatot küldenek, de gyakran, és nagyszámú eszközzel egy időben. Ezért speciális vezeték nélküli technológiákra van szükség, amelyek kezelni tudják az eszközsűrűséget, az alacsony sávszélességet és a hosszú akkumulátor-élettartamot.

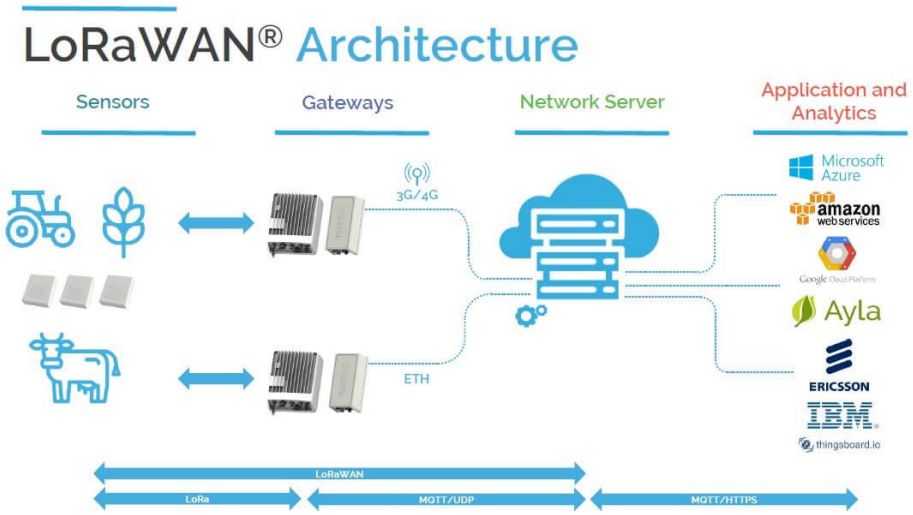
4.2. LPWAN-technológiák

Az LPWAN (Low-Power Wide-Area Network) technológiákat kifejezetten az olyan IoT-alkalmazásokhoz fejlesztették, ahol alacsony energiafelhasználás mellett nagy távolságokat kell áthidalni, miközben az adatmennyiség alacsony. Két fő LPWAN technológia elterjedt az okosvárosokban:

LoRaWAN (Long Range Wide Area Network):

A LoRaWAN a legnépszerűbb, nyílt protokollal rendelkező LPWAN megoldások egyike. A LoRa technológia ideálisan használható például intelligens parkolórendszerekben, okos

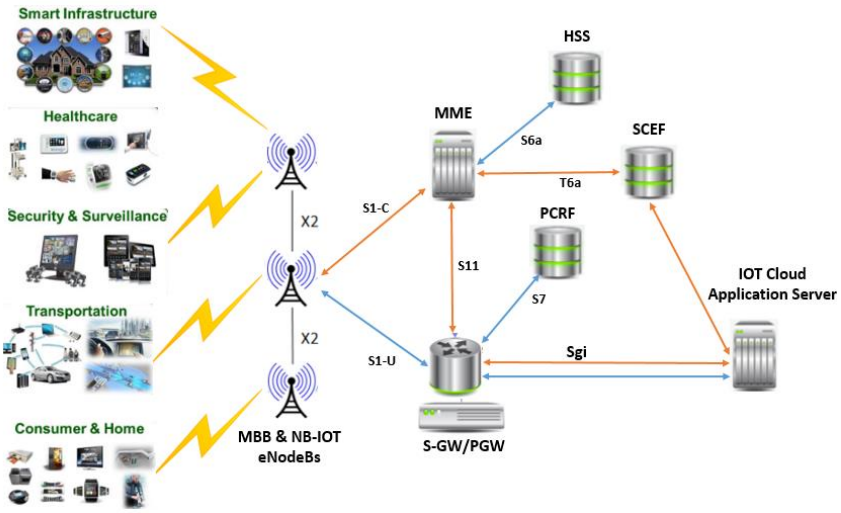
vízórákban vagy a levegőminőség-érzékelőkben. Az eszközök akár éveken át működhetnek elemről, és vidéken akár 10-15 km-es távolságot is áthidalhatnak, míg városi környezetben 1-3 km-t. Előnye a nagy hatótávolság, az alacsony energiafogyasztás és a decentralizálható infrastruktúra.



1. ábra LoRaWAN architektúrája

NB-IoT (Narrowband IoT):

Az NB-IoT egy mobilhálózaton (általában 4G/LTE) alapuló technológia, amelyet a kis sávszélességű, de megbízható és biztonságos adatátvitelre terveztek. Az előnye, hogy a meglévő mobilhálózatokba integrálható, így nincs szükség külön infrastruktúra kiépítésére. Tipikusan okos mérőórákban, távfelügyeleti eszközökben és okos épületek szenzoraiban használják.



2. ábra Narrowband IoT architektúrája

4.3. 5G hálózat az okosvárosban

Az 5G technológia forradalmi változást hoz az okosvárosi kommunikációban. Az alacsony késleltetés (latency), a nagy adatátviteli sebesség és a megnövelt eszközsűrűség-kezelési képesség révén az 5G lehetővé teszi a valós idejű alkalmazások megbízható működését.

Az 5G előnyei:

- <10 ms késleltetés
- Több millió eszköz/km² támogatása
- Dinamikus hálózatszeletelés (network slicing)
- Valós idejű videófeldolgozás támogatása (pl. biztonsági kamerák)

Az 5G különösen fontos az olyan időérzékeny alkalmazások esetében, mint az önvezető járművek, a forgalomirányítás, vagy a közbiztonsági események valós idejű követése és kezelése.

4.4. Mesh hálózatok és helyi kommunikáció

Az okosvárosokban gyakran használnak mesh hálózatokat, ahol az eszközök egymással közvetlenül is tudnak kommunikálni, és a hálózat dinamikusan átalakul, ha egyes eszközök kiesnek vagy mozognak. Ez a megközelítés robosztusabb és rugalmasabb, különösen parkolásvezérlésnél vagy közvilágítási rendszerekben.

4.5. Kommunikációs protokollok

Az okosvárosok kommunikációs rendszerei a különböző alkalmazások jellegétől és a műszaki feltételektől függően különféle protokollokat használnak:

Protokoll	Használati terület	Előnyök
MQTT	Szenzorhálózatok, időjárás, vízórák	Könnyű, nyílt szabvány, kis adatterhelés
CoAP	Erőforrásszegény eszközök	REST-szerű, UDP alapú,

		kis sávszélesség
HTTP/HTTPS	Webes interfészek	Széles körben támogatott, emberi interfészeknél hasznos
ZigBee	Épületautomatizálás	Mesh támogatás, alacsony energiaigény

4.6. Kihívások a kommunikációban

Bár a technológiák gyorsan fejlődnek, több kihívás továbbra is fennáll:

Interoperabilitás: Különböző eszközök és protokollok összehangolt működése

Adatbiztonság: A nyílt hálózatokban az adatátvitel sérülékeny lehet, különösen az önkormányzati vagy közbiztonsági adatok esetében

Késleltetés és megbízhatóság: Kritikus rendszerek esetén (pl. V2X) nem megengedhető az adatvesztés vagy a késleltetett válasz

5. Alkalmazási területek és megoldások az okosvárosokban

Az okos városok akkor öltenek formát, amikor a technológiai alappillérek – beépített rendszerek, hálózatok, szenzor hálók és adatközpontok – meghatározott, behatárolt felhasználási területeken egyesülnek. Ezek azok a területek, ahol az "okos város" előnyei a lakók számára láthatóak és érzékelhetőek. A következőkben az okosvárosok legfontosabb alkalmazási területeit vázoljuk.

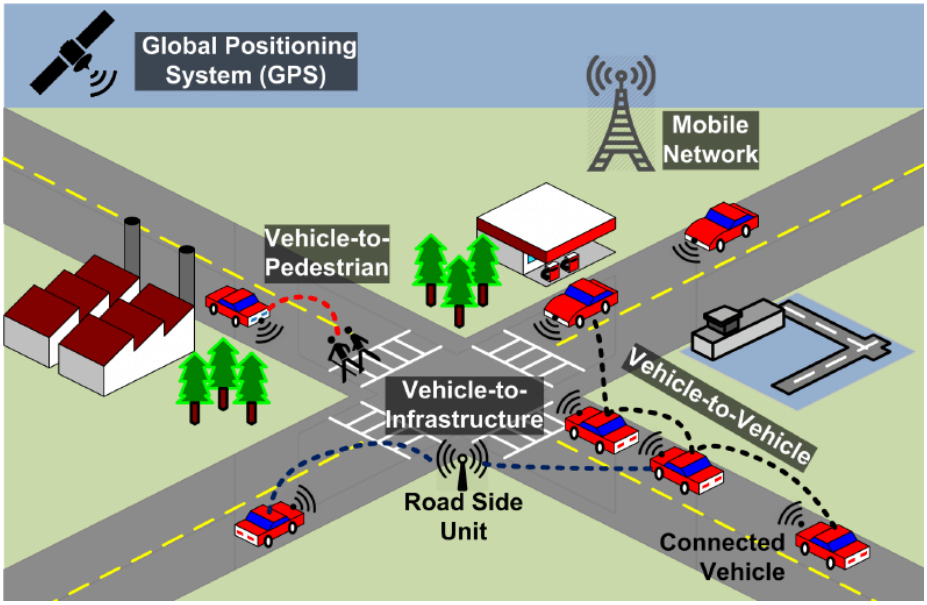
5.1. Intelligens közlekedési irányítás és mobilitás

A legelterjedtebb és leggyakrabban fejlesztett okosvárosi alkalmazás a közlekedési rendszerek intelligens kezelése (ITS – Intelligent Transportation System). A cél a közutak optimális kihasználtságának elérése, a torlódások csökkentése, a közlekedési balesetek számának mérséklése, továbbá az utazási idők kiszámíthatóságának növelése.

Ezen rendszerek alapját a beépített érzékelők és kamerák adják, amelyek képesek a járműforgalmat, a gyalogosmozgást és a sebességet valós időben monitorozni, továbbá a dugókat vagy baleseteket detektálni. Ezek az adatok a központi forgalomirányító rendszerekhez érkeznek, amelyek képesek:

- adaptív módon szabályozni a közlekedési lámpákat,
- valós időben átirányítani a forgalmat,
- informálni a közlekedőket közlekedési táblák és digitális kijelzők segítségével.

Ezekhez a rendszerekhez hatékony kiegészítő a V2X kommunikáció (vehicle-to-everything), amely a járművek közötti közvetlen kommunikációt (V2V), az infrastruktúrával (V2I), a gyalogosokkal (V2P) és a hálózatokkal (V2N) teszi lehetővé. A cél a közlekedés előre jelezhetővé tétele, nem csupán reagálóvá formálása.



3. ábra V2X kommunikáció bemutatása

5.2. Okos parkolás

A parkolóhelyek keresése a nagyvárosokban időigényes és stresszes feladat. Az okos parkolási rendszerek érzékelők (pl. mágneses vagy ultrahangos) segítségével jelzik a szabad parkolóhelyeket. Ezek az információk egy központi adatbázisba kerülnek, a sofőrök pedig mobilalkalmazásokon keresztül valós időben értesülhetnek a lehetőségekről.

Ez nemcsak kényelmi szempontból jelent előnyt, hanem csökkenti a felesleges körözést, a károsanyag-kibocsátást és a városi zajterhelést is.

5.3. Energiahatékonyság és intelligens közvilágítás

Az energiafogyasztás optimalizálása és a fenntarthatóság az okosvárosok egyik legfontosabb célkitűzése. Ennek leglátványosabb példája az intelligens közvilágítás, ahol a lámpatestekbe épített fény- és mozgásérzékelők, valamint kommunikációs modulok automatikusan szabályozzák a fényerőt az aktuális igények szerint.

Például a gyalogos- vagy autóforgalom alacsony intenzitása esetén csökkenthető a fényerő, majd a mozgásérzékeléskor automatikusan világosabb lesz a terület. Ezek a rendszerek akár 50-70%-kal is csökkenthetik az energiafelhasználást, miközben javítják a közbiztonságot.

Az energiahatékonyság másik területe az épületfelügyelet, ahol az okos mérők (smart meters) és az energiamenedzsment rendszerek figyelik és szabályozzák a fogyasztást. Ezen adatok felhasználásával személyre szabott energiaprofilok alakíthatók ki, valamint optimalizálható a fűtés, a világítás és a hűtés.

5.4. Hulladékgazdálkodás

A hulladékgyűjtés optimalizálása érdekében az okosvárosokban szenzoros kukákat helyeznek ki, amelyek jelzik a telítettségi szintjüket. A hulladékszállító járművek ennek megfelelően tervezik meg útvonalaikat, amivel csökken az üzemanyag-felhasználás, a költségek, valamint elkerülhető a túlcsordulás.

Ezen rendszerek IoT-eszközökkel, GPS-alapú útvonaltervezéssel és felhőalapú adatelemzéssel kombinálva rendkívül hatékonnyá tehetők.

5.5. Környezeti monitoring

Az okosvárosoknak nemcsak a közlekedést és az energiafelhasználást kell optimalizálniuk, hanem a környezetvédelmi szempontokat is figyelembe kell venniük. A levegőminőség-ellenőrzés, a zajmérés, a hőmérséklet és a páratartalom figyelése mind hozzájárulhatnak ahhoz, hogy a város megalapozott döntéseket hozzon – például forgalomkorlátozást léptessen életbe a rossz levegőminőség esetén.

Kis méretű beépített szenzoregységek kihelyezésével ezek az adatok sűrű térbeli lefedettséggel gyűjthetők, majd az önkormányzati adatplatformon keresztül értelmezhetők és publikálhatók.

5.6. Közbiztonság és térfigyelés

A közbiztonság szintén kulcsfontosságú terület, ahol az okosvárosi rendszerek jelentős hatást gyakorolhatnak. A modern térfigyelő rendszerek nemcsak rögzítik a videót, hanem valós idejű képfeldolgozással (pl. rendszámfelismerés, arcfelismerés) is dolgoznak. Ezek a rendszerek képesek automatikusan észlelni gyanús viselkedést, tömeges eseményeket vagy biztonsági fenyegetéseket, és ezekről értesítést küldenek az illetékes hatóságoknak.

Ez különösen hasznos közlekedési balesetek, rendkívüli időjárási események vagy akár bűncselekmények megelőzésénél.

5.7. Egészségügyi és szociális rendszerek támogatása

A járványhelyzetekben az egészségügyi rendszerbe integrált IoT-eszközök (pl. hőmérő kapuk, szenzoros lázmérők, fertőtlenítő automatikák) gyorsabb reagálást tettek lehetővé. A telemedicina, a mobil egészségügyi egységek és a távoli betegmonitorozás egyre inkább elérhetővé válik városi szinten is.

Az okosvárosi megközelítés itt nemcsak az infrastruktúra hatékonyságát növeli, hanem aktívan hozzájárul a lakosság jóllétéhez és egészségi állapotának fenntartásához.

Esettanulmány: Barcelona Smart City

Barcelona, a világ egyik mérvadó képviselője az okosvárosok megvalósításában. Az európai metropolisz már 2011 óta folyamatosan fejleszti digitális infrastruktúráját, s így nem csupán technológiai értelemben jelent követendő példát, de a társadalmi és környezeti vonatkozásban is. A Barcelona Smart City projekt integrált, intelligens rendszerek együttesét öleli fel, melyek a város szinte valamennyi területén aktívak.

6.1. A projekt célkitűzései

Barcelona nem csupán technológiai újításra törekszik. A városvezetés hosszú távú célokat fogalmazott meg:

- A lakosság életszínvonalának javítása
- A városi szolgáltatások hatékonyságának növelése
- Az energiafelhasználás és a környezeti terhelés csökkentése
- Nyílt adathozzáférés a polgárok és a fejlesztők számára
- A társadalmi részvétel erősítése a döntéshozatalban

A fenti célokat technológiai eszközökkel kívánják elérni, amihez modern kommunikációs rendszerekre, érzékelőhálózatokra és a beágyazott rendszerek széles körű alkalmazására van szükség.

6.2. Kiemelt fejlesztési területek

1. *Intelligens közlekedés*

A város útjain több mint 500 intelligens közlekedési lámpa működik, melyek valós időben alkalmazkodnak a forgalom mértékéhez. Ezeket szenzoros hálózatok és központi adatfeldolgozó rendszerek irányítják. A tömegközlekedési eszközök (buszok, villamosok) valós idejű követése mobilalkalmazáson keresztül is megoldott, ami nagyban javítja az utazók kényelmét.

2. *Okos parkolási rendszer*

Barcelona bevezette az „AreaDUM” rendszert, mely érzékelőkkel méri a parkolóhelyek foglaltságát. Az autósok mobilapplikációval kereshetnek szabad parkolóhelyeket, s azonnal fizethetnek is a parkolásért. Ez nemcsak kényelmes, de csökkenti a felesleges közlekedést, s ezáltal a környezeti terhelést is mérsékli.

3. *Okos közvilágítás*

A város LED-es lámpatesteket helyezett üzembe, melyek beágyazott rendszerekkel és mozgásérzékelőkkel vannak ellátva. Ezek a gyalogos- és gépjármű forgalom nagyságától függően automatikusan szabályozzák a fényerőt. Az energiafelhasználás optimalizálásával évi szinten akár 30%-os megtakarítást is sikerült elérniük.

4. *Hulladékgazdálkodás*

A szeméttárolókba szenzorokat szereltek, melyek jelzik a telítettséget. A gyűjtés optimalizált útvonalakon történik, ezzel elkerülik a felesleges üzemanyag-felhasználást és a CO_2-kibocsátást. Ez a rendszer a forgalmas belvárosi zónákban kiemelkedően hatékony.

5. *Környezeti monitoring*

A város számos pontján vannak érzékelők, melyek a légszennyezést, zajszintet, hőmérsékletet, páratartalmat, illetve a városi hősziget-hatás nagyságát mérik. Az adatok nyilvánosan elérhetőek, s a várospolitikai döntések alapját képezik – például zöldövezetek kijelölése, vagy kerékpárosbarát zónák kialakítása.

6.3. Műszaki infrastruktúra

Barcelona városa kiemelt figyelmet fordít az IoT-platformok központi integrációjára. Minden adat – parkolás, közlekedés, energia vagy környezet – egy közös városi adatplatformra érkezik be. Ez a platform teszi lehetővé:

- **a valós idejű megfigyelést,**
- **a prediktív elemzést,**
- **a fejlesztők számára nyitott API-k használatát (pl. Open Data BCN portál).**

A kommunikációt LPWAN és Wi-Fi mesh hálózatok kombinációja biztosítja. A város több mint 500 km-es optikai kábelhálózattal bír, ami a gyors és stabil adatáramlás alapja.

6.4. Társadalmi dimenzió

Barcelona különösen fontosnak tartja a polgárok bevonását. A „Decidim” nevű digitális platformon a lakosok javaslatokat tehetnek, szavazhatnak, és visszajelzést adhatnak a városi döntéshozatalról. Ez a digitális részvétel példaértékűen illeszkedik az okosváros emberközpontú megközelítésébe, mely a jövőbeli Ipar 5.0 alapelvével is összhangban van.

6.5. Eredmények és tanulságok

A Smart City Barcelona projekt több mint egy évtizedes tapasztalata azt mutatja, hogy az okosvárosi rendszerek nemcsak technológiailag, hanem társadalmilag és gazdaságilag is fenntarthatók. Az intelligens rendszerek révén:

- **33%-kal csökkent az energiafogyasztás a közvilágításban,**
- **a parkolási idő 25%-kal csökkent,**
- **a forgalom optimalizálása 21%-kal mérsékelte az utazási időket,**
- **a lakossági elégedettségi mutatók is emelkedtek.**

A legfontosabb tanulság az, hogy egy város digitális átalakulása nem csupán technológiai kérdés, hanem egy komplex társadalmi folyamat, amely hosszú távú stratégiai gondolkodást, nyitottságot és a közösség részvételét igényli.

Technológiai és társadalmi kihívások

A felhőkarcolók mintájára tervezett, ám a gyakorlatban számtalan akadályba ütköző okosváros koncepciója. Ezen nehézségek technikai természetűek, de emellett gazdasági, jogi és társadalmi természetűek is lehetnek. A következőkben részletezem, hogy a legfontosabb kihívások melyek, melyekkel szembesülnek az okosvárosi rendszerek tervezése, megvalósítása és üzemeltetése során.

7.1. Az interoperabilitás és a szabványosítás hiánya

Egy okosváros esetében elengedhetetlen, hogy a külön-külön fejlesztett rendszerek és eszközök képesek legyenek együttműködni. Ez a gyakorlatban azonban korántsem mindig gördülékeny. A gyártók gyakran különböző protokollokat, adatstruktúrákat és kommunikációs normákat alkalmaznak, amelyek nem feltétlenül kompatibilisek egymással.

Az interoperabilitás hiánya többféle problémát okozhat:

- az adatok megosztásának és újrafelhasználásának nehézségeit,
- a különböző rendszerek közötti integráció magas költségeit,
- az informatikai sebezhetőségek növekedését.

A megoldás a nyílt szabványok és API-k (Application Programming Interface) alkalmazása, melyekkel az adatok és szolgáltatások közötti átjárhatóság biztosítható. Nemzetközi kezdeményezések, mint az ETSI, az Open & Agile Smart Cities (OASC) vagy a FIWARE nyílt platformja, nagymértékben segíthetik a technológiai egységesítést.

7.2. Adatvédelem és biztonság

Az okosvárosok egyik legnagyobb kihívása a hatalmas mennyiségben képződő személyes és érzékeny adatok védelme. A szenzorhálózatok, kamerák, mobilalkalmazások és intelligens szolgáltatások folyamatosan adatokat gyűjtenek a lakókról: tartózkodási hely, közlekedési szokások, energiafogyasztás, egészségügyi adatok stb.

A GDPR (General Data Protection Regulation) és más adatvédelmi szabályozások egyértelműen kimondják, hogy az adatgyűjtés átláthatóan, jogszerűen és csak a meghatározott célok érdekében történhet. A technológiai megvalósítás azonban nem mindig képes megfelelni ezeknek a követelményeknek.

Továbbá az adatok tárolása és feldolgozása során számos sebezhetőség alakulhat ki:

- adatlopás (pl. érzékeny állampolgári adatok),
- rendszerbe hatolás (pl. közlekedésirányítás megbénítása),
- hamis adatbevitellel történő rendszerzavarás.

A kiberbiztonság ezért elengedhetetlen: kriptográfiai protokollok, biztonságos autentikációs rendszerek, tűzfalak, hálózatszeparáció és decentralizált (blockchain-alapú) megoldások válhatnak szükségessé.

7.3. Finanszírozás és hosszú távú fenntarthatóság

Az okosvárosok kiépítése komoly pénzügyi befektetést igényel. A szenzorhálózatok, adatközpontok, hálózati infrastruktúra, alkalmazások fejlesztése, üzemeltetése és karbantartása is jelentős költségekkel jár.

Különösen a kis- és közepes méretű önkormányzatoknak okoz kihívást a megfelelő finanszírozási struktúra kialakítása. A városvezetés gyakran külső – állami, uniós vagy magán – forrásokra szorul, melyhez átlátható és meggyőző üzleti modellek szükségesek.

A fenntarthatóság kérdése szintén kritikus: a pilot projektek után a működtetés költségei gyakran váratlanul megemelkednek. Ezért a projekt hosszú távú gazdasági modelljét már a kezdetektől alaposan át kell gondolni.

7.4. Technológiai egyenlőtlenségek

Nem minden város, és nem minden városrészen belül élők részesülhetnek egyenlő mértékben az okosvárosi technológiák előnyeiből. A digitális szakadék fogalma ma már nemcsak országos, hanem településen belüli szinten is értelmezhető: bizonyos városrészek kimaradhatnak a fejlesztésekből, vagy a lakosság nem tudja megfelelően használni az elérhető szolgáltatásokat.

Az okosvárosi rendszerek tervezésekor a társadalmi befogadást is figyelembe kell venni:

- *a lakosság digitális kompetenciájának fejlesztését,*
- *akadálymentes felhasználói interfészek kialakítását,*

- *idősek, mozgáskorlátozottak vagy hátrányos helyzetű csoportok bevonását.*

7.5. Lakossági elfogadottság és bizalom

Hiába a legfejlettebb technológia, ha a lakosság nem bízik a rendszerben, nem fogja használni. A bizalom kialakítása alapvető:

- *az adatkezelés átláthatósága,*
- *nyílt forráskódú rendszerek preferálása,*
- *közérthető kommunikáció,*
- *közösségi részvétel (pl. közösségi tervezés, szavazás, visszajelzés lehetősége).*

A társadalmi elfogadottság hiánya megbéníthatja a legjobb technológiai projekteket is – ezt láttuk például a torontói „Sidewalk Labs" projekt kudarcánál, ahol a Google leányvállalata adatvédelmi aggályok miatt visszalépett a fejlesztéstől.

7.6. Etikai dilemmák és szabályozási kérdések

Az okosvárosok működése olyan mennyiségű és érzékenységű adatot generál, hogy új típusú etikai kérdések is felmerülnek:

- meddig terjed az állam megfigyelési joga?
- kik férhetnek hozzá az adatokhoz?
- használhatók-e ezek az információk üzleti célokra?
- hogyan kezeljük az algoritmikus döntéshozatal hibáit?

A szabályozás ebben a tekintetben még mindig kezdeti stádiumban van. A „technológia gyorsabban fejlődik, mint a törvények" közhelye sajnos igaz. Ezért is fontos, hogy a jogalkotók, etikusok, informatikusok és polgárok együttesen alakítsák ki az okosvárosok etikai és jogi keretrendszerét.

Jövőbeli irányok és az Ipar 5.0 szerepe az okosvárosokban

A XXI. század okos városai új megoldások tömegével büszkélkedhetnek, melyek a 4.0 ipari forradalom technológiai pilléreire épülnek: a **dolgok internete (IoT), a mesterséges intelligencia, a felhőalapú rendszerek, az élfeldolgozás, a nagymennyiségű adat elemzése, az 5G hálózatok**, továbbá a beágyazott rendszerek kulcsszerepe mind ezt szolgálják. Ez lehetővé teszi a valós világ digitális másolatának, elemzésének, és a vezérlés automatizálásának megvalósítását. Ezzel egy időben a gazdaság és a technológia az 5.0 ipar irányába tart, ami nem csak az automatizálásra, hanem az ember és a gépek közötti szimbiózisra is fókuszál.

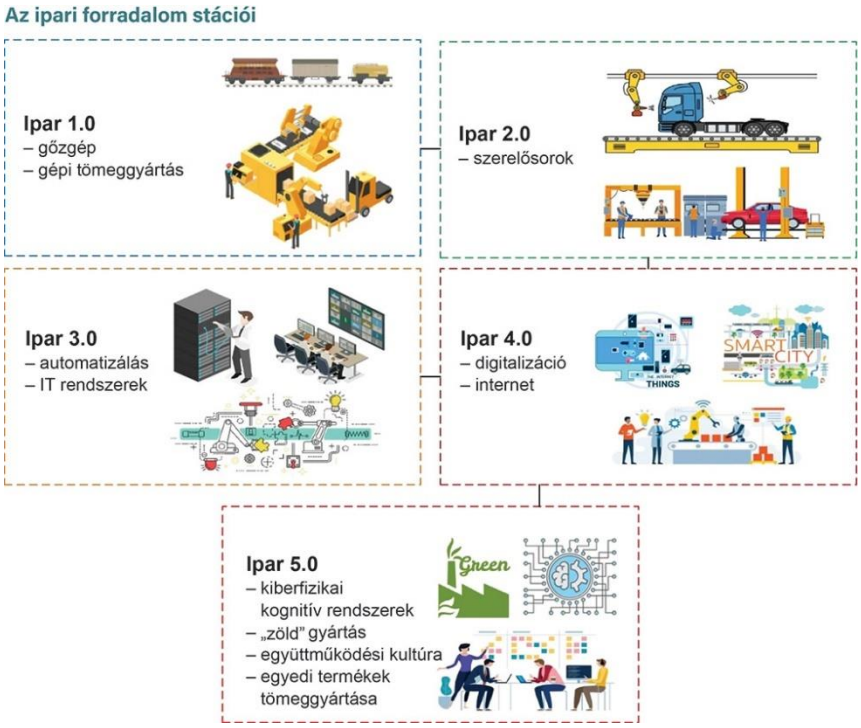
Ez a szemlélet gyökeres változást hozhat a jövő okos városaiban, mivel a következő évek intelligens városai nem csak hatékonyabbak és okosabbak lesznek, de empatikusabbak, befogadóbbak és proaktívabbak is.

8.1. Az 5.0 iparvezérelvei

Az Európai Bizottság 2021-es felmérése szerint az 5.0-s ipar alapkövei a következők:

- **Emberközpontúság**: Az emberi jólét, a jogok és a méltóság áll a technológiai döntéshozatal középpontjában.
- **Fenntarthatóság**: A környezetterhelés minimalizálása, a megújuló energiaforrások és a körforgásos gazdaság előnyben részesítése.
- **Rugalmasság és ellenállóképesség**: A válsághelyzetekre történő gyors és hatékony válaszadás képessége.

Az 5.0-s ipar nem a gépekre, hanem az emberre összpontosít, a technológiai fejlődést ehhez igazítva. Ennek az alapelvnek az okos városokban történő alkalmazása forradalmasíthatja a városok polgárokat szolgáló módját.



4. ábra Az ipari forradalmak

8.2. Digitális ikerpárok

Az egyik leginnovatívabb megközelítés a digitális ikerpárok (Digital Twin) technológiájának alkalmazása az okos városokban. Ez a valós városi környezet, épület, kerület vagy közlekedési hálózat pontos, folyamatosan frissített digitális másolata.

A digitális ikerpár a városvezetés és -tervezés számára:

- Valós időben figyeli az infrastruktúra állapotát.
- Előre modellezheti a természeti katasztrófákat vagy a közlekedési helyzeteket.
- Különböző forgatókönyveket tesztelhet a valós környezet veszélyeztetése nélkül.

Ez a technológia lehetővé teszi, hogy a városok proaktívan működjenek: ne csak reagáljanak a történésekre, hanem előre lássák azokat, és megelőzzék a problémákat.

8.3. Mesterséges értelem és adaptív városirányítás

A jövőbeli intelligens városok "agyát" a mesterséges értelem adja. Az MI nem csak adatok elemzésére és mintázatok felismerésére képes, hanem önálló döntésekre is.

Példák:

- *A közlekedési lámpák önálló tanulása a forgalmi adatokból.*
- *Egészségügyi járványügyi előrejelzések a lakosok mozgásából.*
- *Energiahálózatok adaptív szabályozása a fogyasztási előrejelzések alapján.*

Az ilyen adaptív rendszerek hatékonyabbá teszik az erőforrások felhasználását, gyorsabban reagálnak a rendkívüli eseményekre, és folyamatosan képesek tanulni a környezetükből.

8.4. Ember és technológia együttműködése

Az 5.0-s ipar és az intelligens városok összefonódása nem csupán technológiai kérdés. A jövő városaiban nem az a cél, hogy az embert helyettesítsék, hanem hogy támogassák. Ez megvalósulhat például:

- *Kiterjesztett valóság (AR) és virtuális valóság (VR) eszközökkel támogatott várostervezésben.*
- *Emberközpontú kezelőfelületekben (pl. látás- vagy hallássérültek számára optimalizált rendszerek).*
- *Robotikus segédekben, melyek az idősek vagy a mozgáskorlátozottak életét könnyíthetik meg.*

A robotok (cobotok), a csevegésre képes mesterséges intelligencia (chatbotok) és a felhasználóbarát (UX/UI) interfészek révén az okos város valóban a lakók igényeihez igazodik, nem fordítva.

8.5. A városi életminőség újradefiniálása

Az intelligens város végső célja nem az, hogy több adatot gyűjtsön vagy gyorsabban működjön, hanem az, hogy jobb életminőséget teremtsen az emberek számára. A jövő városa:

- *Egészséges, zöld és szennyezésmentes.*
- *Akadálymentes és befogadó.*
- *Biztonságos, ugyanakkor szabad.*
- *Demokratikus, a lakók bevonásán alapuló, és nyitott.*

Az olyan kezdeményezések, mint a 15 perces város koncepciója (ahol minden alapvető szolgáltatás 15 percen belül elérhető gyalog vagy kerékpárral), vagy a zöld infrastruktúra tervezése (urban jungle), kiválóan példázzák ezt az irányt.

8.6. Összegzés a jövőről

Az 5.0-s ipar elvein alapuló intelligens városok túlmutatnak a technológiai bemutatón: céljuk az emberi jólét szolgálata a technológia eszközeivel. A digitális ikerpárok, a MI-alapú predikció, a decentralizált rendszerek és az emberközpontú tervezés együttesen hozzák létre a holnap városait.

Ezekben a városokban az emberek nem csupán lakók, hanem aktív résztvevők és alkotótársak, a jövő nemcsak épül, hanem velük együtt formálódik.

Összefoglalás és következtetések

A huszonegyedik század települései soha nem látott kihívásokkal néznek szembe. A városiasodás üteme, a környezeti problémák egyre súlyosabbak, a közszolgáltatások iránti igény folyamatosan nő, és az energiafelhasználás fenntarthatósága mind olyan szempontok, amelyek új megoldásokat követelnek. Az okosvárosok koncepciója ezekre a komplex problémákra ad választ – technológiai, társadalmi és gazdasági szinteken egyaránt.

Jelen írás célja annak bemutatása volt, hogy a beágyazott rendszerek és az Ipar 4.0 technológiák hogyan járulnak hozzá az intelligens városi infrastruktúrák működéséhez.

A kommunikációs technológiák, mint a LoRaWAN, NB-IoT vagy 5G, lehetővé teszik a különböző rendszerek közötti valós idejű adatcserét és összehangolt működést. Ezek a hálózatok elengedhetetlenek a dinamikus és autonóm városi szolgáltatásokhoz. A digitális ikerpárok, az edge computing, és a mesterséges intelligencia további lehetőségeket nyújtanak az okosvárosok fejlődésében – nem csupán a városi környezet eseményeire reagálnak, hanem előre is jeleznek, illetve proaktívan döntenek.

A barcelonai példaanyag jól szemlélteti, hogyan lehet egy európai nagyvárosban az intelligens megoldásokat integráltan, hosszú távú stratégiával bevezetni, és a lakosságot aktívan bevonni. Ez a gyakorlat kiváló példa más települések, köztük a magyar városok számára is.

Ugyanakkor nem szabad elfelejtenünk az akadályokat és kockázatokat:

- Az interoperabilitás hiánya nehezítheti a különböző rendszerek integrálását.
- Az adatvédelem kérdése központi etikai dilemmává vált.
- A finanszírozási nehézségek és a fenntartható üzleti modellek hiánya veszélyeztetheti a projektek hosszú távú működését.
- A társadalmi befogadás, a digitális kompetencia szintje és az egyenlő hozzáférés kérdései szintén fontosak.

A beadandó végén bemutatott Ipar 5.0 koncepció és az emberközpontú technológia új távlatokat nyit: az okosváros nem csupán a gépek és algoritmusok világa lesz, hanem az embereké, akik aktívan alakítják és élvezik a városi digitális ökoszisztéma előnyeit.

Irodalomjegyzék

[1] *P. Patel and V. Sharma, "Global perspectives on digital twin smart cities," Sustainable Cities and Society, vol. 101, 2025. [Online]. Available:*

[2] Lorenzo Adreani et al.: *Smart City Digital Twin Framework for Real-Time Multi-Data Integration and Wide Public Distribution*

[3] Aidan Fuller et al.: *Digital Twin: Enabling Technologies, Challenges and Open Research*

[4] S. Aslam & H. Sami Ullah: *A Comprehensive Review of Smart Cities Components, Applications, and Technologies Based on Internet of Things*

[5] M. K. Ali, "AI-Powered Digital Twins and IoT for Smart Cities and Sustainable Building Environments," *Applied Sciences*, vol. 14, no. 24, Article 12056, 2024.

[6] Eduardo Felipe Zambom Santana et al.: *Software Platforms for Smart Cities: Concepts, Requirements, Challenges, and a Unified Reference Architecture*

[7] MDPI: *Virtual Reality and Internet of Things Based Digital Twin for Smart City*

[8] Emerald Insight: *Smart City Digital Twins: Overview of Implementation Challenges and Recommendations for Citizens Training*

[9] L. Adreani et al., "Smart City Digital Twin Framework for Real-Time Multi-Data Integration and Wide Public Distribution," *arXiv*, Sep. 2023.

[10] OAEPublish: *Developments of digital twin technologies in industrial, smart city, and healthcare applications*

[11] MDPI: *AI-Powered Digital Twins and Internet of Things for Smart Cities and Sustainable Building Environments*

[12] S. R. Rauf, "Trends in Digital Twin Framework Architectures for Smart Cities," *Sensors*, vol. 23, no. 5, Article 10934255, 2024.

[13] Reuters: *How AI is arming cities in the battle for climate resilience*

[14] ACM Digital Library: *Opportunistic Digital Twin: an Edge Intelligence enabler for Smart City*

2.54. Mesterséges Intelligencia és alkalmazásai CPS keretrendszerekben Orvosi diagnosztika, személyre szabott gyógyászat

Mesterséges Intelligencia és alkalmazásai CPS keretrendszerekben

Orvosi diagnosztika, személyre szabott gyógyászat

Horváth Márk

Mérnökinformatikus, horvathm4rk0420@gmail.com

A dolgozat a mesterséges intelligencia és a kiberfizikai rendszerek (CPS) integrációját vizsgálja az orvosi diagnosztika és a személyre szabott gyógyászat területén. A negyedik ipari forradalom vívmányainak köszönhetően egyre több olyan intelligens rendszer jelenik meg, amely képes a betegek valós idejű monitorozására, az egészségügyi adatok elemzésére és prediktív döntések meghozatalára. A dolgozat bemutatja az MI különböző formáit – például a gépi tanulást, a mélytanulást és a természetes nyelvfeldolgozást (NLP) –, valamint azok alkalmazási lehetőségeit a képalkotó diagnosztikában, az orvosi dokumentációk feldolgozásában és a prediktív analitikában. Kitér a CPS rendszerek technikai felépítésére, a szenzoros adatgyűjtés, edge computing és felhőalapú technológiák szerepére, valamint a személyre szabott orvoslás kialakulására genetikai és klinikai adatok felhasználásával. A dolgozat továbbá tárgyalja az adatvédelemmel, anonimitással, etikai kérdésekkel és algoritmikus torzításokkal kapcsolatos kihívásokat is, amelyek az MI egészségügyi alkalmazását kísérik. Az összefoglalásban a jelenlegi trendek mellett jövőbeli kilátásokat is vázol, hangsúlyozva a technológiai megoldások emberközpontú fejlesztésének fontosságát.

Kulcsszavak: CPS, MI, NLP

1 BEVEZETÉS

A negyedik ipari forradalom, vagyis az Ipar 4.0 új korszakot hozott az ipari és technológiai fejlődésben, amelyet az intelligens, hálózatba kapcsolt rendszerek integrációja jellemez. A kiberfizikai rendszerek (Cyber-Physical Systems – CPS) és a mesterséges intelligencia (MI) alkalmazása alapjaiban alakítja át a különböző iparágakat, köztük az egészségügyet

is. E fejlett technológiák összekapcsolják a fizikai környezetet a digitális világgal, lehetővé téve a valós idejű adatgyűjtést, feldolgozást és döntéshozatalt.

A modern egészségügyi ellátásban egyre nagyobb hangsúlyt kap a prediktív, megelőző és személyre szabott gyógyászat, amelynek alapját a nagymennyiségű, strukturált és strukturálatlan adat elemzése képezi. Az MI-alapú megoldások képessé váltak arra, hogy diagnosztikai eszközként támogassák az orvosokat a pontosabb, gyorsabb és költséghatékonyabb döntések meghozatalában. A kiberfizikai rendszerek és az intelligens szenzorok lehetővé teszik a páciensek állapotának folyamatos monitorozását, a kezelések dinamikus testreszabását, valamint az egészségügyi adatok biztonságos és hatékony kezelését.

A dolgozat célja annak vizsgálata, hogy a mesterséges intelligencia hogyan alkalmazható a kiberfizikai rendszerek keretében az orvosi diagnosztika és a személyre szabott gyógyászat területén. Ennek keretében bemutatásra kerülnek az MI legfontosabb algoritmusai, a képfeldolgozás és a természetes nyelvfeldolgozás szerepe, az adatfeldolgozási módszerek, valamint a rendszerbe integrált eszközök és keretrendszerek. A dolgozat külön figyelmet fordít az etikai és

adatvédelmi kérdésekre, amelyek kulcsszerepet játszanak a digitális egészségügyi rendszerek elfogadottságában és megbízhatóságában.

A dolgozat szakirodalmi forrásokra, esettanulmányokra és konkrét példákra támaszkodva törekszik teljes képet adni a mesterséges intelligencia egészségügyi alkalmazásainak jelenlegi állásáról, lehetőségeiről és kihívásairól a CPS keretrendszerek kontextusában.

2 AZ MI SZEREPE A MODERN ORVOSI DIAGNOSZTIKÁBAN

2.1 Gépi tanulás és mélytanulás

A gépi tanulás (Machine Learning – ML) az MI egyik olyan ága, amely lehetővé teszi, hogy algoritmusok tanuljanak korábban gyűjtött adatokból, és ezen ismeretek alapján előrejelzéseket vagy döntéseket hozzanak új adatokra vonatkozóan. Az egészségügyben ez az alkalmazási forma különösen értékes, mivel lehetővé teszi a betegségek korai felismerését, a diagnózis automatizálását, valamint a terápiás döntések támogatását.

A felügyelt tanuláson alapuló módszerek – mint például a logisztikus regresszió, döntési fák, támogatott vektorgépek (Support Vector Machines – SVM), valamint a k-nn (knearest neighbors) algoritmus – sikerrel alkalmazhatók diagnosztikai osztályozási problémák megoldására. Ezek az algoritmusok képesek például különbséget tenni egészséges és beteg szövetek között orvosi képeken, vagy előre jelezni egy adott betegség kialakulásának valószínűségét a beteg korábbi adatai alapján.

A mélytanulás (Deep Learning – DL), amely a mesterséges neurális hálózatok egy speciális típusa, különösen nagy potenciállal bír az orvosi kép- és hangadatok feldolgozásában. A konvolúciós neurális hálózatok (Convolutional Neural Networks – CNN) jól alkalmazhatók orvosi képek, például MRI-, CT- és röntgenfelvételek automatikus elemzésére, mivel képesek felismerni a finom morfológiai eltéréseket a képi adatokban.[1]

Egy másik elterjedt mélytanulási architektúra az ismétlődő neurális hálózat (Recurrent Neural Network – RNN), amely időbeli adatsorokat (pl. EKG-jel, betegmonitor adatok) képes feldolgozni. Az RNN-ek különösen hatékonyak a hosszú távú összefüggések felismerésében, így például a beteg állapotának előrejelzésében egy intenzív osztályos környezetben.

A mesterséges intelligencia ezen formáinak sikeressége azonban nagymértékben függ az adatok mennyiségétől, minőségétől és a felhasznált tanítóhalmaz reprezentativitásától. Az orvosi MI-algoritmusok fejlesztésében ezért alapvető fontosságú a jól strukturált, megfelelően címkézett adatbázisok használata, valamint a gondos előfeldolgozás és validálás.

2.2 Képalkotó diagnosztika és konvolúciós neurális hálók (CNN) működése

A modern orvosi diagnosztika egyik kulcsterülete a képalkotó eljárásokra épül, mint például a röntgen, a komputertomográfia (CT), a mágneses rezonancia képalkotás (MRI) vagy az ultrahang. Ezek a technológiák hatalmas mennyiségű képi adatot generálnak, amelyek értelmezése időigényes és szakértelmet igénylő folyamat. A konvolúciós neurális hálózatok (CNN) lehetőséget kínálnak e képek automatizált és pontos elemzésére.

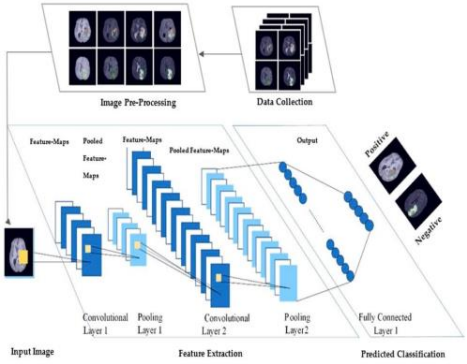
A CNN-ek az emberi látórendszer működését utánzó mélytanulási architektúrák, amelyek képesek felismerni és osztályozni vizuális mintázatokat a képek különböző rétegein keresztül. A hálózat rétegei – például konvolúciós, aktivációs (ReLU), pooling és teljesen összekapcsolt (fully connected) rétegek – hierarchikusan dolgozzák fel a bemeneti képet, egyre absztraktabb jellemzőket kinyerve belőle. Ez a rétegzett struktúra lehetővé teszi, hogy a CNN-ek

automatikusan tanulják meg az orvosi képeken jellemző elváltozásokat, például daganatok, gyulladások, vagy strukturális rendellenességek felismerését.

A képalkotó diagnosztikában a CNN-eket számos területen alkalmazzák, például:

1. Tüdőrák detektálása mellkasi CT-felvételeken
2. Bőrrák osztályozása dermatoszkópos képek alapján
3. Agyi elváltozások felismerése MRI-felvételeken (pl. Alzheimer-kór){1}
4. Szemfenéki képek elemzése diabéteszes retinopátia detektálásához

A tanítás során gyakran alkalmazzák a transfer learning módszert, amely során előre betanított hálózatokat (pl. VGGNet, ResNet, EfficientNet) finomhangolnak orvosi célra. Ez különösen hasznos, mivel az orvosi adatok gyakran szűkösen állnak rendelkezésre, és az annotáció költséges, időigényes folyamat.



{1} CNN használata az emberi agy vizsgálatára [18]

A CNN-alapú rendszerek teljesítményét rendszerint standard metrikák segítségével értékelik, mint például pontosság, érzékenység, specificitás, és az ROC-görbe alatti terület (AUC). Emellett fontos a hálózatok interpretálhatósága is, amelyre a saliency map, GradCAM vagy más XAI (Explainable AI) módszerek szolgálnak. Ezek vizualizálni képesek, hogy a hálózat mely képterületekre fókuszál döntéshozatal során, ezzel növelve az orvosok bizalmát az MI-rendszerekben.

2.3 NLP az orvosi dokumentációkban és chatbotokban

A természetes nyelvfeldolgozás (Natural Language Processing – NLP) az MI egyik olyan területe, amely a humán nyelv számítógépes értelmezésével, feldolgozásával és generálásával foglalkozik. Az egészségügyi informatika világában az NLP különösen fontos szerepet tölt be, mivel az orvosi dokumentumok jelentős része strukturálatlan szöveges formában áll rendelkezésre – például kórlapok, műtéti jegyzőkönyvek, orvosi vélemények, zárójelentések vagy laborleletek.

Az NLP algoritmusok segítségével ezek a szöveges adatok strukturálttá tehetők, lehetővé téve a hatékonyabb keresést, automatikus kódolást, kockázatelemzést és döntéstámogatást. Tipikus feladatok közé tartozik az entitásfelismerés (Named Entity Recognition – NER), a szövegosztályozás, a szentimentelemzés, valamint a kulcsinformációk kinyerése.

A legfejlettebb NLP-rendszerek ma már nagyméretű nyelvi modelleken (Large Language Models – LLM) alapulnak, mint például a BERT, BioBERT, ClinicalBERT vagy GPT. Ezek a modellek képesek kontextusfüggő szövegértelmezésre, így pontosabban képesek feldolgozni az orvosi terminológiát és nyelvi sajátosságokat.

2.3.1 *Példák orvosi NLP alkalmazásokra {2}:*

1. Kórlapok automatikus kódolása: pl. SNOMED CT vagy ICD-10 szerinti besorolás
2. Leletértékelés: kulcsdiagnózisok azonosítása radiológiai vagy patológiai szövegekből
3. Rizikófaktor azonosítás: pl. dohányzás, cukorbetegség említése szöveges dokumentumban
4. Orvosi chatbotok: tünetalapú kérdőívek, beteg-tájékoztatás, utánkövetés automatizálása

Az orvosi chatbotok területén az NLP-re épülő megoldások lehetővé teszik, hogy a betegek emberi nyelven kommunikáljanak a rendszerekkel, kérdéseket tegyenek fel, vagy akár tüneteket írjanak le. A válaszadó rendszerek a háttérben strukturált adatokat, betegtörténetet és orvosi protokollokat használnak a válasz generálásához, gyakran kombinálva döntéstámogató rendszerekkel mint például a CDSS. [2]

{2} NLP alkalmazása az egészségügyben [19]

Az NLP-alapú orvosi rendszerek használata azonban komoly kihívásokkal is jár, elsősorban az adatvédelmi követelmények, a nyelvi komplexitás, valamint a kontextusfüggő jelentések miatt. A helytelenül értelmezett szöveg komoly orvosi következményekkel járhat, ezért ezekben az alkalmazásokban a magas pontosság és magyarázhatóság elengedhetetlen.

2.4 **Benchmark adathalmazok és kiértékelési módszerek**

A mesterséges intelligencián alapuló orvosi rendszerek fejlesztése során kulcsfontosságú szerepet kap a modellek teljesítményének pontos és objektív mérése. Ehhez elengedhetetlenek a benchmark adathalmazok, amelyek standardizált környezetet biztosítanak az algoritmusok összehasonlítására, valamint a kiértékelési metrikák, amelyek alapján meghatározható a modellek diagnosztikai hatékonysága.

2.4.1 *Benchmark adathalmazok*

A kutatásban és fejlesztésben gyakran használt nyílt forráskódú orvosi adathalmazok közé tartoznak:

1. MIMIC-III / MIMIC-IV: Elektronikus egészségügyi adatok intenzív osztályos betegek esetén, több ezer beteg élettani jeleit, gyógyszereit, diagnózisait és jegyzeteit tartalmazza .

2. ChestX-ray14: A NIH által kiadott, több mint 100 000 mellkasi röntgenfelvételt tartalmazó adathalmaz, 14 különféle tüdőbetegség annotációjával.
3. MedMNIST: Egy sokféle modalitást (kézi bőrrák, retina, mellkas, emlő, stb.) tartalmazó mini benchmark, mely kifejezetten oktatási és gyors prototípusfejlesztési célokra készült.
4. TCGA (The Cancer Genome Atlas): Genomikai adathalmaz, amelyet gyakran alkalmaznak prediktív modellezési kutatásokhoz onkológiai kontextusban.

Ezen benchmarkok biztosítják az adatok konzisztenciáját, annotációját és reprezentativitását, ezáltal lehetővé téve a modellek érdemi összehasonlítását és reprodukálhatóságát.

2.4.2 *Kiértékelési metrikák*

A diagnosztikai MI-algoritmusok értékelése során a klasszikus osztályozási metrikák mellett figyelembe kell venni az orvosi környezetre jellemző sajátosságokat (pl. a hamis negatív döntések veszélyességét). A leggyakrabban használt metrikák:

1. Pontosság (Accuracy): A helyes előrejelzések aránya az összes előrejelzéshez képest.
2. Érzékenység (Sensitivity / Recall): A ténylegesen beteg páciensek közül hányat ismer fel a modell (valódi pozitív arány).
3. Specificitás (Specificity): A ténylegesen egészséges páciensek közül hányat azonosít helyesen a modell (valódi negatív arány).
4. F1-mérték: A precision (pozitív predikciós érték) és a recall harmonikus átlaga, különösen hasznos kiegyensúlyozatlan adatoknál.
5. AUC-ROC: Az osztályozó teljesítményének átfogó mutatója, amely a szenzitivitás és a téves riasztási arány (false positive rate) kapcsolatát ábrázolja.

A megfelelő metrikák kiválasztása az alkalmazás céljától függ. Például egy életveszélyes betegség felismerése esetén a magas érzékenység elengedhetetlen, míg szűrővizsgálatok esetében a specificity is nagy hangsúlyt kaphat. Az orvosi kontextusban tehát a metrikák súlyozott elemzése és értelmezése kulcsfontosságú a rendszer megbízhatóságának értékeléséhez.[3][4]

3 CPS ÉS EGÉSZSÉGÜGYI ADATKEZELÉS

3.1 Kiberfizikai rendszerek felépítése és egészségügyi szerepük

A kiberfizikai rendszerek olyan összetett rendszerek, amelyek szoros integrációban működtetik együtt a fizikai és a digitális világ elemeit. Ezek a rendszerek szenzorok, beavatkozók, beágyazott számítástechnikai egységek és kommunikációs hálózatok révén képesek valós idejű adatgyűjtésre, -feldolgozásra és automatizált döntéshozatalra.

Az egészségügyben a CPS rendszerek alkalmazása lehetővé teszi a betegek állapotának folyamatos monitorozását, a kezelések személyre szabását, valamint a diagnosztikai döntések támogatását. A CPS technológia különösen hasznos az intenzív osztályokon, krónikus betegségkezelésben, otthoni egészségügyi felügyelet során, vagy akár a rehabilitációs folyamatokban.

A kiberfizikai rendszerek alapvető elemei az alábbiak:

1. Szenzorok: Fiziológiai adatok gyűjtésére szolgálnak (pl. pulzus, vérnyomás, testhőmérséklet, EKG, vércukorszint).
2. Beavatkozók (aktuátorok): Automatikus terápiás beavatkozásokat tesznek lehetővé (pl. inzulinpumpa vezérlése, pacemaker).
3. Beágyazott számítástechnikai egységek: Az adatok feldolgozásáért és lokális döntéshozatalért felelnek (pl. microcontroller, edge device).
4. Kommunikációs interfészek: Adatok továbbítása felhőalapú rendszerekhez, orvosi döntéstámogató rendszerekhez vagy mobilalkalmazásokhoz.
5. Felhasználói interfész: A páciensek, orvosok vagy ápolók számára visszacsatolást biztosít.

{3} Egészségügyi CPS felépítése [20]

Egy egészségügyi CPS rendszer működése például így nézhet ki:

1. Egy viselhető eszköz (pl. okosóra) EKG-adatokat gyűjt.
2. Az adatot egy edge device előfeldolgozza és kiszűri az artefaktumokat.
3. A megtisztított adat felkerül a felhőbe, ahol egy gépi tanulási modell osztályozza a szívritmust.
4. Az eredményt a rendszer továbbítja az orvosnak, és riasztást küld, ha szükséges.{3}

Az ilyen rendszerek előnyei közé tartozik a valós idejű reagálás, a megelőző jellegű beavatkozás, valamint a nagy mennyiségű adat alapján történő döntéshozatal, amelyek együttesen jelentős mértékben javíthatják a betegellátás minőségét és hatékonyságát.

Ugyanakkor a CPS rendszerek orvosi alkalmazása komoly követelményeket támaszt a megbízhatóság, adatbiztonság, valamint az interoperabilitás terén. A különféle eszközök és szoftverek integrációjához szabványos protokollokra van szükség, mint például az HL7, FHIR vagy DICOM.[5]

3.2 **Szenzorok, IoT és valós idejű adatgyűjtés**

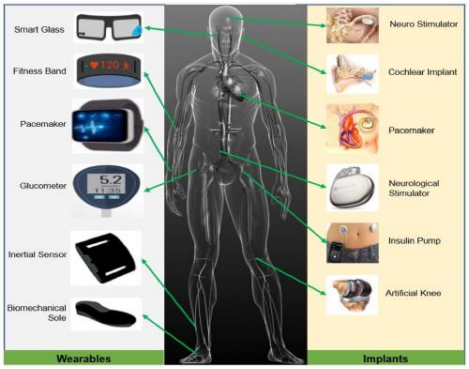
A valós idejű adatgyűjtés kulcsfontosságú a kiberfizikai rendszerek hatékony működésében, különösen az egészségügyi alkalmazásokban, ahol az időérzékeny döntések és beavatkozások közvetlen hatással vannak a beteg állapotára. Az adatok gyűjtését és továbbítását elsősorban szenzorokkal és IoT (Internet of Things) eszközökkel végzik, amelyek képesek folyamatosan monitorozni a páciens fiziológiai paramétereit.

3.2.1 *Szenzorok típusai és funkciói az orvosi CPS rendszerekben*

Az orvosi célú szenzorok különféle típusokba sorolhatók az általuk mért paraméterek alapján. Néhány gyakran alkalmazott szenzor:

1. EKG szenzorok: A szív elektromos aktivitásának mérésére (pl. szívritmuszavarok detektálása).
2. SpO_2 szenzorok: Vér oxigénszaturációját mérik, különösen fontos légzőszervi betegségeknél.
3. Vércukor szenzorok: Folyamatos glükózmonitorozás (CGM) diabéteszes betegek számára.
4. Vérnyomásmérők: Otthoni és kórházi használatra egyaránt.
5. Hőmérséklet- és mozgásérzékelők: Fertőzés- vagy elesésdetektálás céljára.{4}

Ezeket a szenzorokat gyakran integrálják viselhető eszközökbe (wearables), például okosórákba, okospólókba vagy tapaszokba (pl. BioPatch). Az adatok rögzítése tipikusan percenként vagy másodpercenként történik, amit az eszköz vagy azonnal, vagy előfeldolgozás után továbbít egy központi rendszerbe.



{4} Viselhető/hordható eszközök amik segítik az adatgyűjtést az egészségügyben [21]

3.2.2 *IoT-eszközök szerepe az adatkommunikációban*

Az IoT-eszközök (pl. beágyazott mikrovezérlők, Bluetooth/WiFi/GSM kommunikációs modulok) közvetítik a szenzoradatokat a hálózaton keresztül. Ezek az eszközök kulcsszerepet játszanak az adatok előfeldolgozásában, tömörítésében és az adatbiztonság biztosításában.[6]

A valós idejű adatgyűjtés és -továbbítás követelményei:

1. Alacsony késleltetés (latency)
2. Nagy megbízhatóság
3. Energiahatékonyság
4. Biztonságos adatátvitel (titkosítás, hitelesítés)

A szenzoradatokat gyakran edge computing eszközök dolgozzák fel lokálisan, mielőtt azok a felhőbe kerülnének – ezzel csökkenthető a válaszidő, és a sávszélesség-használat is optimalizálható.

3.2.2.1 *Alkalmazási példák*

1. Okos intenzív osztály: ahol minden beteg monitorozása szenzorokkal és edge eszközökkel történik, azonnali riasztással az ápolószemélyzet számára.
2. Otthoni távmonitorozás: pl. krónikus betegek állapotának követése okoseszközökön keresztül.
3. Mobil egészségügyi alkalmazások: ahol a beteg okostelefonja közvetíti az adatokat a kórházi rendszerekhez.

3.3 **Big Data, Cloud és Edge Computing**

Az orvosi kiberfizikai rendszerek működése során keletkező adatok mennyisége, sebessége és változatossága jelentős kihívásokat támaszt a feldolgozásukkal szemben. A különféle forrásokból – például szenzorokból, viselhető eszközökből, képalkotó rendszerekből vagy elektronikus egészségügyi nyilvántartásokból (EHR) – származó adatok hatékony kezelése csak korszerű, méretezhető technológiai megoldások alkalmazásával valósítható meg. Ilyenek a Big Data analitika, a felhőalapú számítástechnika és az edge computing.

3.3.1 *Big Data az egészségügyben*

A „Big Data" azokat az adatállományokat jelöli, amelyek túl nagyok vagy komplexek ahhoz, hogy hagyományos adatfeldolgozó eszközökkel hatékonyan kezelhetők legyenek. Az egészségügyben ez az adatok térbeli, időbeli és formátumbeli sokféleségét is magában foglalja. A Big Data technológiák (pl. Apache Hadoop, Apache Spark) lehetővé teszik az ilyen adatok párhuzamos feldolgozását, klaszteres környezetben történő elemzését, valamint prediktív modellek képzését és kiértékelését nagy léptékben.

Például egy teljes kórház EHR-rendszeréből származó több tízezer páciens adata használható fel a szív-érrendszeri kockázat előrejelzésére, vagy akár új biomarkerek azonosítására gépi tanulás segítségével.

3.3.2 *Felhőalapú számítástechnika (Cloud Computing)*

A felhőalapú rendszerek – mint az Amazon Web Services (AWS), Google Cloud Platform (GCP) vagy Microsoft Azure – lehetővé teszik az adatok távoli tárolását, skálázható feldolgozását és biztonságos elérését. A felhőalapú környezetek támogatják az MI modellek betanítását és beágyazását (deployment), lehetővé téve a valós idejű döntéstámogatást akár mobil eszközökön is.

Egészségügyi alkalmazásban a felhő előnyei:

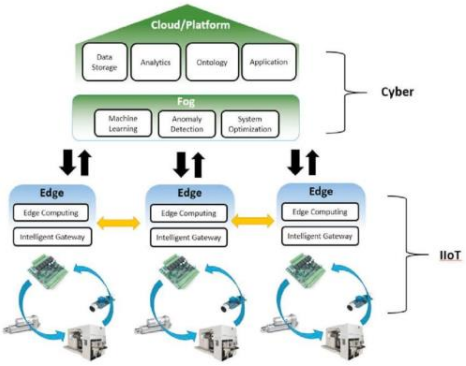
1. Skálázhatóság: gyors bővítés/növelés betegelőzmény-elemzéshez
2. Magas rendelkezésre állás: 24/7 adatelérés sürgősségi esetekhez
3. Távdiagnosztika támogatása: orvos és beteg eltérő földrajzi helyzetből is kapcsolatba léphet

A biztonsági követelmények ugyanakkor fokozott figyelmet igényelnek. A PHI (Protected Health Information) kezelése során a titkosítás, autentikáció és megfelelőség (pl. GDPR, HIPAA) elsődleges szempontok.

3.3.3 *Edge és Fog Computing{5}*

Az edge computing lényege, hogy az adatok feldolgozása a hálózati „peremen", vagyis az adatforrás (pl. szenzor, eszköz) közelében történik, nem pedig távoli felhőben. Ez jelentősen csökkenti a válaszidőt (latency), és lehetővé teszi a lokális döntéshozatalt kritikus helyzetekben – például egy pacemaker azonnali beavatkozása.

A fog computing hasonló koncepció, de még egy közbenső réteget iktat be (pl. helyi gateway vagy kórházi szerver), amely aggregálja és előfeldolgozza az adatokat a felhőbe küldés előtt. Ez különösen előnyös nagy adatforgalom esetén, vagy ha a hálózati kapcsolat nem megbízható.



{5} Edge-fog-cloud modell - egy adatfeldolgozási architektúra a CPS rendszerekben [22]

A három technológia – Big Data, Cloud és Edge/Fog – egymást kiegészítve alkotják a modern orvosi CPS rendszerek alapját, lehetővé téve a nagy teljesítményű, gyors és megbízható MI-alapú diagnosztikát. A megfelelő architektúra kiválasztása mindig az adott alkalmazási környezet igényeitől, költségkeretétől és biztonsági követelményeitől függ. [7]

3.4 **Diagnosztikai hibák csökkentése intelligens rendszerekkel**

Az orvosi diagnosztika egyik legnagyobb kihívása a diagnosztikai hibák előfordulása, amelyek közé tartozik a hamis pozitív (false positive, FP) és hamis negatív (false negative, FN) döntések aránya. A hamis pozitív eredmények felesleges beavatkozásokhoz, stresszhez és költségekhez vezethetnek, míg a hamis negatív esetek különösen veszélyesek, mivel a betegség rejtve maradhat, elmarad a kezelés, és a beteg állapota romlik.

A mesterséges intelligenciával támogatott kiberfizikai rendszerek képesek jelentős mértékben csökkenteni ezen hibák előfordulását, az alábbi fő mechanizmusokon keresztül:

3.4.1 *Nagyobb pontosságú mintázatfelismerés*

A mélytanulási modellek – különösen a konvolúciós neurális hálózatok (CNN-ek) – kiválóan teljesítenek komplex és nem nyilvánvaló vizuális mintázatok felismerésében. Ez segíti a ritka vagy atipikus kórképek azonosítását is, amelyeket az orvosok esetleg figyelmen kívül hagynának.

3.4.2 *Ensemble modellek használata*

Több modell kombinálása – például bagging, boosting, stacking – jelentősen javíthatja a predikciós teljesítményt. Az ilyen ensemble rendszerek általában robosztusabbak és kevésbé hajlamosak túltanulásra (overlearning), ami különösen hasznos heterogén orvosi adathalmazok esetén.

3.4.3 *Kalibrált előrejelzések*

A prediktív modellek gyakran valószínűségi kimeneteket adnak. Az output értékek kalibrálása (pl. Platt-skalázás, isotonic regression) segíti a bizonytalanság megfelelő értelmezését, így az orvos mérlegelheti, mikor szükséges további vizsgálat, vagy épp mikor bízhat meg teljes mértékben az MI ajánlásában.

3.4.4 *Valós idejű monitorozás és trendanalízis*

A CPS rendszerek képesek időben észlelni a fiziológiai változásokat, még mielőtt azok tünetek formájában jelentkeznének. Az adatok hosszú távú elemzése – például EKG-jelek vagy vércukorszint időbeli változása – lehetőséget ad korai beavatkozásra, így megelőzhető a súlyos állapot kialakulása.

3.4.5 *Kognitív torzítások kompenzálása*

A humán diagnosztikai hibák gyakran kognitív torzításokon alapulnak (pl. megerősítési torzítás, horgonyzás, túlzott tapasztalat-alapúság). Az MI-rendszerek – ha jól tervezettek és validáltak – képesek objektív és standardizált kiértékelést nyújtani, ezzel csökkentve az emberi döntéshozatalból eredő hibák számát.

3.4.6 *Alkalmazási példa*

Egy 2020-as kutatásban [8] mellkasi röntgenek automatikus osztályozására fejlesztettek ki CNN-alapú modellt, amely 15%-kal csökkentette a hamis negatív arányt az emberi radiológushoz képest, miközben a hamis pozitív arányt is optimalizálta. A modell kimenetét egy interpretálható Grad-CAM hőtérkép is kiegészítette, ami növelte a klinikai felhasználhatóságot.

4 SZEMÉLYRE SZABOTT GYÓGYÁSZAT ÉS PREDIKTÍV MODELLEZÉS

4.1 **Betegspecifikus kezelési tervek kialakítása**

A hagyományos orvoslásban a terápiás döntések jellemzően statikus irányelveken és populációs átlagokon alapulnak. Ezzel szemben a személyre szabott orvoslás (personalized medicine) célja, hogy az adott beteg egyedi jellemzői – genetikai profilja, életmódja, környezeti tényezői és korábbi kórtörténete – alapján optimalizálja a diagnosztikai és terápiás döntéseket. A mesterséges intelligencia (MI) ebben a kontextusban kulcsfontosságú szerepet játszik, mivel képes az összetett adathalmazokból releváns mintázatokat azonosítani, és ezek alapján egyénre szabott kezelési javaslatokat generálni.

Adatforrások a személyre szabott döntésekhez

A betegspecifikus döntéstámogatáshoz különböző adatforrásokat szükséges integrálni:

1. Elektronikus egészségügyi nyilvántartások (EHR) – kórtörténet, laborleletek, gyógyszerelés
2. Genetikai profilok – SNP-k, génexpresszió, genomszekvenálás
3. Képalkotó adatok – pl. MRI, CT, PET eredmények
4. Viselkedési és életmódbeli adatok – alvás, aktivitás, étrend, dohányzás
5. Környezeti hatások – lakókörnyezet, szennyeződések, társadalmi tényezők{6}

A mesterséges intelligencia algoritmusai ezeket az adatokat kombinálva képesek felismerni a betegségkockázatokat, terápiás válaszreakciókat, valamint előre jelezni a kezelési eredmények sikerességét.

4.1.1 *Ajánlórendszerek az orvoslásban*

Az MI egyik kiemelkedő alkalmazási formája az orvosi ajánlórendszerek (recommendation systems) kialakítása, amelyek hasonló betegprofilok alapján javaslatot tesznek kezelési stratégiákra, gyógyszeradagolásra vagy életmódváltoztatásokra. Ezeket gyakran kollaboratív szűrés (collaborative filtering), tartalomalapú szűrés (content-based filtering) vagy ezek hibrid kombinációja alapján működtetik – hasonló módon, ahogyan például a streaming platformok vagy webshopok működnek.

4.1.2 *Orvos-MI együttműködés*

Fontos kiemelni, hogy a mesterséges intelligencia nem helyettesíti az orvost, hanem kiegészíti azt. A betegspecifikus ajánlásokkal az MI segíti a klinikai döntések megalapozását, különösen komplex, többtényezős helyzetekben. A jól kalibrált rendszerek képesek figyelembe venni az egyedi kockázati tényezőket, mellékhatásokat, illetve a betegpreferenciákat is – ezzel támogatva a precíziós orvoslás megvalósítását.[9]

{6} Személyre szabott orvoslás adatforrásai appok alapján [23]

4.1.3 *Esettanulmány*

Egy ismert példa az IBM Watson for Oncology rendszere, amely különböző onkológiai esetekben személyre szabott kezelési javaslatokat kínál a beteg EHR és genetikai profilja alapján. A rendszer a szakirodalom elemzésére is képes, így az aktuálisan elérhető legfrissebb terápiás lehetőségek is beépülnek az ajánlásokba.

4.2 **Prediktív analitika a betegségek korai felismerésére**

A prediktív analitika célja, hogy a meglévő adatok alapján előrejelzéseket készítsen a jövőbeni események valószínűségéről. Az egészségügyben ez a megközelítés különösen hasznos lehet a betegségek korai felismerésében, a kockázatelemzésben, valamint a személyre szabott terápiás döntések meghozatalában. A mesterséges intelligencia és a gépi tanulási algoritmusok alkalmazásával ezek a predikciók egyre pontosabbá, megbízhatóbbá és klinikailag relevánssá válnak.

4.2.1 *Alkalmazott prediktív módszerek*

A prediktív modellek a statisztikai és gépi tanulási technikák széles skáláját alkalmazzák. A legismertebb módszerek közé tartoznak:

1. Logisztikus regresszió: bináris kimenetek előrejelzésére, pl. egy betegség megléte vagy hiánya.
2. Döntési fák és random forest: jól értelmezhető, átlátható modellek, amelyek strukturált egészségügyi adatbázisokra jól alkalmazhatók.
3. Gradient boosting (pl. XGBoost, LightGBM): kiemelkedően jó teljesítményt nyújt osztályozási és regressziós feladatokban.

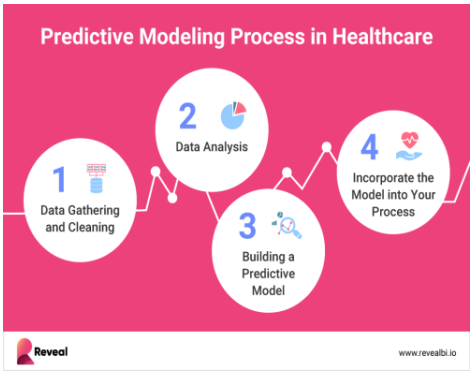
4. Neurális hálózatok: különösen hasznosak komplex, nemlineáris összefüggések feltárására, időfüggő adatok feldolgozására (pl. RNN, LSTM).

4.2.2 *Korai felismerés és megelőzés*

A prediktív modellek képesek felismerni a betegségek kialakulására utaló korai jeleket még a tünetek megjelenése előtt. Például:

1. Kardiovaszkuláris betegségek: EKG-idősorokból szívritmuszavarok vagy infarktuskockázat előrejelzése.
2. Diabétesz: életmódi, genetikai és metabolikus adatok alapján történő kockázatbecslés.
3. Onkológiai kórképek: képalkotó vagy genomikai adatokból kiindulva daganatok prediktív azonosítása.

Az MI-alapú prediktív rendszerek nemcsak a betegségek jelenlétére képesek előrejelzést adni, hanem az egyéni terápiás válaszreakciókra is. Ez lehetővé teszi, hogy egy adott gyógyszer vagy beavatkozás csak azon betegeknél kerüljön alkalmazásra, akiknél várhatóan hatásos.[10]{7}



{7} Prediktív analitikai modellezés orvosi környezetben

4.2.2.1 *Példák a gyakorlatból*

1. A Mount Sinai Health System prediktív analitikai rendszert használ az EHRadatokból való korai COVID-19 detektálásra [10].
2. A DeepMind egy vesebetegség-előrejelző modellt fejlesztett ki, amely 48 órával a veseelégtelenség bekövetkezte előtt képes jelezni a kockázatot.
3. A Tempus nevű amerikai cég genomikai és klinikai adatok alapján prediktív modelleket kínál a rákos betegek egyénre szabott kezelésére.

4.3 **Genetikai alapú prediktív modellek**

A precíziós orvoslás (precision medicine) alapelve, hogy a terápiás döntéseket a beteg genetikai, környezeti és életmódbeli jellemzőinek figyelembevételével hozzák meg. A genetikai információk értelmezése és alkalmazása azonban csak megfelelő adatelemzési eszközökkel és prediktív modellezési technikákkal lehetséges. Ebben a folyamatban a mesterséges intelligencia – különösen a mélytanulás és a bioinformatikai eszköztár – kiemelt szerepet játszik.

4.3.1 *Genetikai adatok típusai és forrásai*

A genetikai adatok típusa szerint lehetnek:

1. SNP-k (single nucleotide polymorphisms): pontmutációk, melyek gyakran összefüggésbe hozhatók bizonyos betegségekkel vagy gyógyszer-reakciókkal.
2. Génexpressziós adatok: egyes gének aktivitásának szintjét mutatják, jellemző például tumorok szövettani típusának meghatározására.
3. Teljes genomszekvenálás (WGS) / exomszekvenálás (WES): komplex öröklődési mintázatok feltérképezésére.

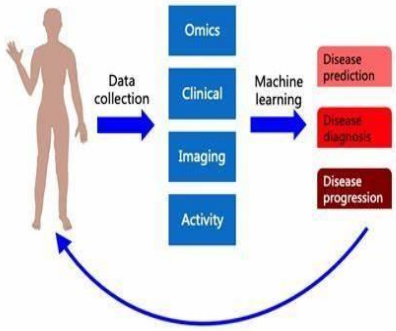
A biobankok és nyílt hozzáférésű genomikai adatbázisok (pl. TCGA – The Cancer Genome Atlas, 1000 Genomes Project) lehetővé teszik nagyléptékű prediktív modellek fejlesztését.

4.3.2 *MI-alapú prediktív modellek genetikai adatokra*

A genetikai információk elemzése különleges feldolgozást igényel: a bemeneti adatok magas dimenziószámúak, zajosak és gyakran nemlineáris kapcsolatokat tartalmaznak. Az MI-eszközök – például a mély neurális hálózatok, autoencoderek, vagy graph neural networks (GNN-ek) – képesek ezeket a komplex mintázatokat felismerni és előrejelezni:

1. Betegségkockázat becslése (pl. BRCA1/BRCA2 mutációk és mellrák)
2. Gyógyszerhatékonyság előrejelzése (pharmacogenomics)
3. Terápiás válaszreakciók predikciója (pl. immunterápia vs kemoterápia){8}

Ezek az algoritmusok lehetővé teszik az individualizált kezelés tervezését, csökkentve a sikertelen terápiák és mellékhatások arányát.[11]



{8} Genetikai adatok feldolgozása MI-alapú prediktív modellel [25]

4.3.3 *Kihívások és lehetőségek*

Bár a genetikai adatokra épülő predikciók ígéretesek, számos kihívással is járnak:

1. Adatvédelmi aggályok: a genetikai adatok érzékeny, azonosításra alkalmas információt tartalmaznak.
2. Minta-méret problémák: a magas dimenzióhoz képest gyakran alacsony a betegszám.
3. Interpretálhatóság: az MI-modellek "fekete doboz" jellege akadályozhatja a klinikai elfogadottságot.

4. Biológiai validáció szükségessége: az algoritmusok predikcióit kísérleti vagy klinikai úton is igazolni kell.

4.3.4 *Példaalkalmazás*

A Tempus és a Foundation Medicine nevű cégek fejlesztettek olyan rendszereket, amelyek tumorok genetikai profilja alapján javasolnak terápiás lehetőségeket. Egyes onkológiai MImodellek például képesek megjósolni, hogy egy adott beteg jobban reagál-e PD-1 gátlóra, mint kemoterápiára, így segítve a terápiás döntés személyre szabását.

4.4 **Szoftveres eszközök és keretrendszerek**

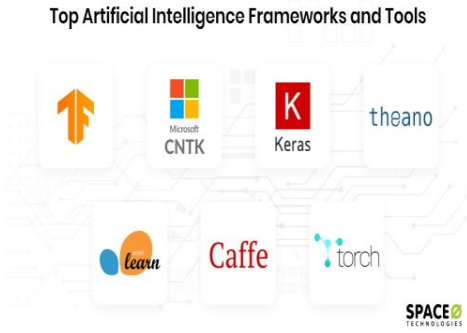
A mesterséges intelligencia egészségügyi alkalmazásaihoz szükséges modellek fejlesztéséhez és beágyazásához a kutatók és fejlesztők különféle szoftveres keretrendszerekre és eszközökre támaszkodnak. Ezek az eszközök lehetővé teszik a gépi tanulási modellek hatékony létrehozását, tanítását, validálását, valamint integrálását az egészségügyi rendszerekbe – mindezt különböző adatmodalitások (szöveg, kép, genom, időbeli jelek) mentén.

4.4.1 *Általános gépi tanulási keretrendszerek*

1. TensorFlow(Google):
   Nyílt forráskódú, széles körben használt DL/ML keretrendszer. Kiválóan alkalmas képfeldolgozásra, idősor-elemzésre és modellek beágyazására (TensorFlow Lite). Orvosi alkalmazás: pl. retina-képek osztályozása diabéteszes retinopátia szűrésére [12].
2. PyTorch(Meta)
   Dinamikus számítási gráfjának köszönhetően rugalmasabb modellfejlesztést tesz lehetővé. Kedvelt kutatási környezet, számos orvosi publikáció használja. Elérhetőek egészségügy-specifikus moduljai, mint a MONAI (Medical Open Network for AI).
3. Keras
   Magas szintű API, ami egyszerűsíti a TensorFlow használatát. Ideális kezdőknek és prototípusok gyors elkészítéséhez. Széleskörű támogatás képfeldolgozó feladatokra (pl. CNN-ek építése MRI képekhez).

4.4.2 *Kifejezetten orvosi célra fejlesztett keretrendszerek*

4. MONAI (Medical Open Network for AI)
   A PyTorch-alapú orvosi képfeldolgozó keretrendszer, amely támogatja a DICOM fájlformátumot, augmentálási és pre-processing lehetőségeket. Tipikus alkalmazás: szervszegmentálás MRI vagy CT képeken.
5. NiftyNet
   Orvosi képfeldolgozásra tervezett TensorFlow-alapú eszköz, különösen 3D képadatok kezelésére. Kiemelt terület: daganat- vagy elváltozás-szegmentálás.
6. BioPython/scikit-bio
   Biológiai és genetikai adatok kezelésére specializált könyvtárak. Genomszekvenálás, fehérjeszerkezet-elemzés, phylogenetic modellezés.
7. Snorkel
   Gyenge tanítással (weak supervision) működő eszköz, amely hasznos orvosi NLP alkalmazásokban – különösen, ha kevés címkézett adat áll rendelkezésre.
8. Apache cTAKES (clinical Text Analysis and Knowledge Extraction System)
   Természetes nyelvfeldolgozó keretrendszer, kifejezetten orvosi szövegek (pl. EHR) feldolgozására. Entitásfelismerés, ICD-kódolás, információkinyerés.



{9} Szoftver keretrendszerek, amiket az AI alapú orvosi feladatokban használnak [13]

4.4.3 *Fejlesztői eszközök és kiegészítők*

1. Jupyter Notebook: interaktív fejlesztés, vizualizáció, dokumentáció egyben.
2. Zotero / Mendeley: irodalomkezelés, automatikus IEEE-hivatkozás generálás.
3. GitHub / GitLab: kódverzió-kezelés és csapatmunka.

A megfelelő eszköz kiválasztása mindig az adott projekt típusától, az adatok típusától és a fejlesztési környezettől függ. A modern orvosi adatfeldolgozásban azonban szinte elengedhetetlen legalább egy mélytanulási keretrendszer ismerete, valamint annak integrálása kórházi rendszerekbe vagy felhőalapú infrastruktúrákba.{9}

5 ETIKAI ÉS ADATVÉDELMI KIHÍVÁSOK

5.1 Adatvédelmi kockázatok

A mesterséges intelligenciát alkalmazó egészségügyi rendszerek – különösen a kiberfizikai rendszerekkel integrált megoldások – egyre nagyobb mennyiségű, érzékeny személyes egészségügyi adatot dolgoznak fel. Ezen rendszerek használata számos adatvédelmi kockázatot hordoz, amelyek megfelelő kezelése nélkül a betegek bizalma és a rendszerek megbízhatósága jelentősen csökkenhet.

5.1.1 *Különösen érzékeny adatok jellege*

Az MI-alapú diagnosztikai rendszerek és döntéstámogató eszközök olyan adatokat használnak, mint:

1. Elektronikus egészségügyi nyilvántartások (EHR)
2. Genetikai profilok (DNS-adatok)
3. Képalkotó vizsgálatok eredményei (pl. MRI, CT)
4. Szenzoros és viselkedési adatok (pl. alvásmonitorozás, aktivitás)
5. Pszichológiai vagy mentális egészségügyi információk

Ezek az adatok nemcsak a páciens egészségi állapotát fedik fel, hanem közvetetten hozzájárulhatnak diszkriminációhoz (pl. biztosítási elutasítás), identitáslopáshoz, vagy jogosulatlan profilalkotáshoz.

5.1.2 *Tipikus adatvédelmi kockázatok*

1. Jogosulatlan hozzáférés: Hackerek vagy rosszindulatú szereplők hozzáférhetnek érzékeny orvosi adatokhoz.

2. Adatszivárgás: A felhőben vagy edge eszközökön tárolt adatok szivárgása harmadik félhez.
3. Nem megfelelő anonimizálás: Sok esetben a „névtelenített” adatok újraazonosíthatók (reidentifikáció).
4. Túlzott adatgyűjtés: A rendszer több adatot gyűjt, mint ami feltétlenül szükséges lenne a cél érdekében (data minimization elvének megsértése).
5. Profilalkotás és predikciós visszaélések: A prediktív modellek alapján történő előítéletes vagy hátrányos döntések (pl. biztosítási kockázatok becslése alapján történő kizárás).

5.1.3 *Gyakorlati példák és incidensek*

1. 2019-ben a Google és az Ascension közötti „Project Nightingale” adatmegosztási projekt komoly adatvédelmi vitát váltott ki az adatok betegbeleegyezés nélküli megosztása miatt.
2. Egyes kutatások szerint a genetikai adatokhoz elég néhány SNP alapján az egyén újraazonosítása, még akkor is, ha az adatokat anonimként tárolják [14].

5.1.4 *Megelőző technikai megoldások*

1. Adattitkosítás (encryption): Tárolás és átvitel során egyaránt elengedhetetlen (pl. TLS, AES).
2. Hozzáférés-szabályozás: Szerepkör alapú hozzáférések (RBAC), auditálható logok.
3. Differenciális privát adatok: Az MI modellek tanítása során a valódi adatok helyett szintetikus vagy „zajos” adatok használata.
4. Federated learning (szövetségi tanulás): Az adatot nem mozgatják, hanem a modell kerül kiküldésre a helyi gépekre tanulás céljából. [14]

5.2 **Anonimitás és adatintegritás**

A kiberfizikai rendszerek az orvosi gyakorlatban olyan érzékeny adatokkal dolgoznak, amelyek egyértelműen azonosíthatják az egyént – legyen szó genetikai profilról, EKGidősorról vagy akár mozgásmintázatról. Emiatt nemcsak az adatvédelmi incidensek elkerülése, hanem az adatok anonimizálása és integritásuk biztosítása is kiemelt jelentőségű.

5.2.1 *Anonimitás és újraazonosítás problémája*

Az adatok anonimizálása célja, hogy a személyazonosság visszafejtése lehetetlenné váljon. Azonban több kutatás is kimutatta, hogy a különféle adathalmazok – akár nyilvánosan is elérhető adatokkal kombinálva – alkalmasak lehetnek az egyének újraazonosítására.

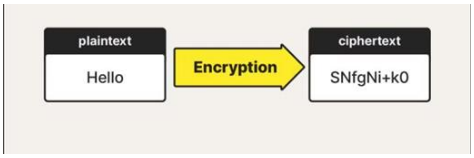
Tipikus példák:

1. Genetikai adatokhoz társított demográfiai információk alapján történő visszakövetés.
2. Páciensek mozgásmintáinak összevetése közösségi médiából származó GPSadatokkal.
3. Szöveges orvosi dokumentumokban megmaradt nevek, időpontok, helyszínek.

5.2.2 *Anonimitás biztosítására alkalmazott technikák*

1. Pszeudonimizálás: A személyes azonosítók (pl. név, TAJ-szám) helyettesítése kóddal. Előnye, hogy a visszakövethetőség megmarad, de a közvetlen azonosítás megszűnik.{10}
2. Differenciális privát adatvédelem: Statikus zajt ad az adatokhoz, így azok aggregálva hasznosak maradnak, de egyedi szinten nem visszafejthetők.

3. K-anonimitás, l-diverzitás, t-closeness: Ezek statisztikai módszerek, amelyek biztosítják, hogy egy adott egyén legalább "k" másikkal legyen megkülönböztethetetlen a mintában.



{10} Az anonimitás egyik fajtája: pszeudonomizálás avagy titkosítás [26]

5.2.3 *Adatintegritás fontossága a CPS rendszerekben*

A valós idejű diagnosztikai döntések alapját képező adatok torzulása, elvesztése vagy manipulálása súlyos következményekkel járhat. Az adatintegritás azt biztosítja, hogy az adatok teljesek, pontosak és megbízható forrásból származnak – tehát nem módosultak jogosulatlanul a rendszer egyetlen pontján sem.

Megvalósítási lehetőségek:

1. Kriptográfiai ellenőrzések: Digitális aláírás, hash-értékek (pl. SHA-256) alkalmazása minden adatcsomagra.
2. Blockchain-technológia: A tranzakciók vagy egészségügyi naplók megváltoztathatatlan tárolása elosztott főkönyvben.
3. Audit trail és naplózás: Minden hozzáférés és módosítás naplózása, időbélyeggel és jogosultsági információkkal.
4. Redundancia és hibadetektálás: Több szenzoregység párhuzamos működtetése és keresztellenőrzés az adatmegbízhatóság érdekében.

Példák az egészségügyből

1. Estonia (Észtország) e-Health rendszer: blockchain-alapú tárolás, teljes auditálhatósággal.
2. MedRec projekt (MIT): decentralizált, Ethereum-alapú EHR rendszer, amely biztosítja a betegek adatainak integritását és kontrollját. [15]

5.3 **Jogi és etikai szabályozás**

Az MI-alapú egészségügyi megoldások fejlődése jelentős előnyökkel jár, ugyanakkor komoly jogi és etikai kérdéseket is felvet – különösen a felelősség, a betegjogok, az átláthatóság és a szabályozás területén. A kiberfizikai rendszerek sajátossága, hogy összetett, sokszereplős architektúrában működnek, ahol nem mindig egyértelmű, ki felel a döntésekért: a fejlesztő, a szolgáltató, az orvos, vagy maga az MI-rendszer?

Jogi szabályozási környezet

5.3.1 *Európai Unió – AI Act*

Az Európai Unió 2021-ben nyújtotta be a Mesterséges Intelligencia Rendelettervezetet, amely az első átfogó szabályozási keretrendszer a mesterséges intelligenciára. Az egészségügyi alkalmazások többsége magas kockázatú kategóriába esik, így szigorúbb követelményeket kell teljesíteni:

1. Átláthatóság és dokumentációs kötelezettség
2. Emberi felügyelet biztosítása
3. Adatminőség és reprezentativitás

4. Nyomon követhetőség és auditálhatóság
5. Pontosság, robusztusság és kiberbiztonság

5.3.2 *Általános Adatvédelmi Rendelet (GDPR)*

Az EU GDPR külön figyelmet szentel a személyes egészségügyi adatok feldolgozásának. Az MI rendszereknek meg kell felelniük az alábbi elveknek:

1. Célhoz kötöttség
2. Adatminimalizálás
3. Jogalap és hozzájárulás
4. Átláthatóság a döntéshozatalban
5. Tiltakozáshoz és emberi beavatkozáshoz való jog (pl. automatikus döntéshozatallal szemben – GDPR 22. cikk)

5.3.3 *Egyesült Államok – HIPAA*

Az USA-ban a Health Insurance Portability and Accountability Act szabályozza az egészségügyi információk kezelését, amely szintén alkalmazandó MI rendszerek esetében, különös tekintettel az adatvédelmi és információbiztonsági előírásokra.

5.3.4 *Etikai elvek és dilemmák*

Az MI-alapú diagnosztika alkalmazása során nemcsak a jogi megfelelés, hanem az etikai szempontok is elengedhetetlenek. Ezek közé tartozik:

1. Igazságosság (fairness): az algoritmusok ne diszkrimináljanak sem életkor, nem, etnikum vagy társadalmi háttér alapján.
2. Átláthatóság és magyarázhatóság (explainability): az orvos és a beteg is értse a döntés indoklását.
3. Felelősség (accountability): világosan meghatározott legyen, ki viseli a felelősséget egy hibás döntés esetén.
4. Autonómia: a betegnek joga van dönteni saját adatai és kezelése felett.
5. Bizalom: az MI-rendszerek használata csak akkor fenntartható, ha a betegek megbíznak azok működésében.

A **bioetikai alapelvek** (Beauchamp és Childress):

1. Ártalomkerülés (non-maleficence)
2. Jótékonyság (beneficence)
3. Autonómia tiszteletben tartása
4. Igazságos elosztás (justice)

Ezek mind érvényesíthetők az MI-rendszerek tervezése és alkalmazása során.

Gyakorlati példa – Etikai kódexek

1. WHO: „Ethics and Governance of Artificial Intelligence for Health” (2021) – 6 alapelv az egészségügyi MI alkalmazásához
2. OECD AI Principles
3. IEEE Ethically Aligned Design [16]

5.4 Algoritmikus torzítások és azok kezelése

A mesterséges intelligencia egészségügyi alkalmazásainak egyik legkomolyabb kihívása az algoritmikus torzítás. Ez azt jelenti, hogy az MI-rendszerek döntései szisztematikusan kedveznek vagy hátrányosan megkülönböztetnek bizonyos egyéneket vagy csoportokat – gyakran nem szándékosan, hanem az eddig használt adatok vagy modellek strukturális hibái miatt.

A torzítások forrásai

1. Adatkészletek torzítottsága: ha a tréningadatok 80%-a fehér bőrszínű férfiaktól származik, az MI rosszabbul fog teljesíteni más demográfiai csoportokon. Különösen problémás az alulreprezentált kisebbségek, ritka betegségek, vagy nem tipikus kórképek esetén.
2. Címkézési hibák és emberi elfogultság: Ha a címkézést végző orvosok szubjektív döntéseket hoznak, az MI ezeket a mintákat is megtanulhatja.
3. Modellarchitektúra és tanulási célok: A modell gyakran csak az „átlagos" esetek optimalizálására törekszik, a marginális esetek rovására.
4. Külső tényezők figyelmen kívül hagyása, azaz hanyagolása: Szociális, gazdasági vagy környezeti tényezők, amelyek nem jelennek meg az adatokban, de hatással lehetnek a diagnózisra vagy a kezelésre.

5.4.1 *Következmények az egészségügyben*

1. Diagnosztikai egyenlőtlenség: bizonyos csoportok esetén alacsonyabb érzékenységű MI-modellek.
2. Diszkrimináció a kezelésben: predikciók alapján eltérő hozzáférés kezelésekhez vagy erőforrásokhoz.
3. Bizalomhiány a rendszer iránt: a betegek, orvosok bizalma csökken, ha érzékelik a rendszer elfogultságát.

Torzításkezelési módszerek

1. Adatkészlet-kiegyensúlyozás: Több adatgyűjtés marginalizált csoportoktól. Data augmentation technikák alkalmazása.
2. Fairness-tudatos modellépítés: Fairness regularizáció (pl. Demographic Parity, Equalized Odds). Konfúziós mátrixok elemzése szegmensenként
3. Torzításdetektáló eszközök: IBM AI Fairness 360, Google What-If Tool
4. XAI – Explainable AI: A döntések magyarázhatósága segíti a torz viselkedés felismerését. Grad-CAM, SHAP, LIME – modellek „megnyitása" .
5. Folyamatos audit és visszacsatolás: A modellek teljesítményét rendszeresen újra kell értékelni új adatokon. Emberi beavatkozás lehetősége kritikus esetekben.

5.4.2 *Etikai reflektálás*

Az algoritmikus igazságosság nemcsak technikai, hanem filozófiai kérdés is: mit tekintünk méltányosnak? A teljes pontosság mindenkinél egyformán fontos? Vagy azokat segítsük többet, akik a legnagyobb kockázatnak vannak kitéve? E kérdésekre nincs egyetlen jó válasz, de a technikai fejlesztésnek ezeket az elveket is figyelembe kell vennie. [17]

6 ÖSSZEFOGLALÁS

A dolgozat célja annak vizsgálata volt, hogyan járul hozzá a mesterséges intelligencia (MI) a kiberfizikai rendszerek keretében az orvosi diagnosztika és a személyre szabott gyógyászat fejlődéséhez. A feldolgozott szakirodalom, technológiai áttekintések és esettanulmányok alapján egyértelműen megállapítható, hogy az MI-alapú CPS rendszerek már ma is meghatározó szerepet töltenek be a modern egészségügy digitalizációjában.

A dolgozatban bemutatott elemzések alapján az alábbi főbb következtetések vonhatók le:

1. A mesterséges intelligencia – különösen a mélytanulás és a természetes nyelvfeldolgozás – képes jelentősen javítani a diagnosztikai pontosságot, csökkentve a hibás döntések (hamis pozitív / negatív) arányát.
2. A CPS rendszerek, valós idejű szenzoros adatgyűjtéssel és döntéstámogatással, lehetővé teszik a folyamatos betegmonitorozást és gyors beavatkozást, ami kulcsfontosságú a sürgősségi és krónikus ellátásban.
3. A prediktív analitikai modellek és a genetikai adatfeldolgozás lehetőséget teremtenek az egyre pontosabb, személyre szabott kezelések kidolgozására, támogatva ezzel a precíziós orvoslást.
4. A technológiai fejlődés mellett azonban számos adatvédelmi, etikai és jogi kihívás is megjelenik, amelyek csak szigorú szabályozás, átláthatóság és magyarázhatóság mellett kezelhetők fenntartható módon.

A dolgozatban tárgyalt eszközök (TensorFlow, MONAI, cTAKES stb.) és módszerek (CNN, NLP, federated learning) már jelenleg is rendelkezésre állnak a gyakorlati implementációhoz, és folyamatosan fejlődnek, hogy még inkább megfeleljenek az orvosi alkalmazások kritikus elvárásainak.

Jövőbeli kilátások

A technológiai lehetőségek és az MI-rendszerek érettsége alapján a következő években várható:

1. Az MI-alapú diagnosztikai rendszerek rutin klinikai eszközzé válnak.
2. A federált tanulás és az edge computing térnyerése révén biztonságosabb adatkezelés válik lehetővé.
3. Az interoperábilis, nyílt forrású rendszerek elterjedése támogatja a globális kutatási együttműködéseket.
4. Az algoritmikus átláthatóság (XAI) és az etikai megfelelés új módszereinek fejlődése erősítheti a betegbizalmat.

Ugyanakkor fontos, hogy a technológiai fejlődést ne csak mérnöki, hanem társadalmi és humán oldalról is kísérjük, és az orvos-beteg-MI kapcsolatban mindig az emberi döntés és empátia maradjon középpontban.

IRODALOMJEGYZÉK

[1] G. Litjens et al., “A survey on deep learning in medical image analysis,” Medical Image Analysis, vol. 42, pp. 60–88, Dec. 2017.

[2] E. Alsentzer et al., “Publicly available clinical BERT embeddings,” in Proceedings of the Clinical NLP Workshop, 2019, pp. 72–78.

[3] A. E. W. Johnson et al., “MIMIC-III, a freely accessible critical care database,” Scientific Data, vol. 3, no. 1, pp. 1–9, 2016.

[4] T. Saito and M. Rehmsmeier, “The Precision-Recall Plot is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets,” PLOS ONE, vol. 10, no. 3, 2015.

[5] E. A. Lee, “Cyber Physical Systems: Design Challenges,” in 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing, 2008.

[6] M. Chan, D. Estève, C. Escriba, and E. Campo, “A review of smart homes—Present state and future challenges,” Computer Methods and Programs in Biomedicine, vol. 91, no. 1, pp. 55–81, 2008.

[7] M. Satyanarayanan, “The emergence of edge computing,” Computer, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[8] P. Rajpurkar et al., “CheXNet: Radiologist-Level Pneumonia Detection on Chest XRays with Deep Learning,” arXiv preprint, arXiv:1711.05225, 2017.

[9] E. J. Topol, “High-performance medicine: the convergence of human and artificial intelligence,” Nature Medicine, vol. 25, pp. 44–56, Jan. 2019.

[10] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. T. Dudley, “Deep learning for healthcare: review, opportunities and challenges,” Briefings in Bioinformatics, vol. 19, no. 6, pp. 1236–1246, 2018.

[11] A. L. Beam and I. S. Kohane, “Big data and machine learning in health care,” JAMA, vol. 319, no. 13, pp. 1317–1318, 2018.

[12] V. Gulshan et al., “Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs,” JAMA, vol. 316, no. 22, pp. 2402–2410, 2016.

[13] G. Litjens et al., “A survey on deep learning in medical image analysis,” Medical Image Analysis, vol. 42, pp. 60–88, 2017.

[14] M. Gymrek et al., “Identifying Personal Genomes by Surname Inference,” Science, vol. 339, no. 6117, pp. 321–324, 2013.

[15] K. El Emam et al., “A Systematic Review of Re-Identification Attacks on Health Data,” PLOS ONE, vol. 6, no. 12, 2011.

[16] L. Floridi et al., “AI4People—An ethical framework for a good AI society,” Minds and Machines, vol. 28, no. 4, pp. 689–707, 2018.

[17] Z. Obermeyer et al., “Dissecting racial bias in an algorithm used to manage the health of populations,” Science, vol. 366, no. 6464, pp. 447–453, 2019.

[18] A. A. Helwan, “Brain Tumor Detection Using Convolutional Neural Network,” Encyclopedia,

[19] EdrawMax, “NLP Templates,” EdrawMax

[20] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, “Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data,” Future Generation Computer Systems, vol. 43–44, pp. 305–314

[21] L. Zhang et al., “Digital twin-driven cybersecurity testbed for industrial control systems,” Journal of Information Security and Applications, vol. 78, p. 103803, Apr. 2024

[22] Yu–Ju Lin, Ci-Bin Lan, és Chin-Yin Huang, „A Realization of Cyber-Physical Manufacturing Control System Through Industrial Internet of Things”, International Journal of Advanced Manufacturing Technology, vol. 102, no. 1–4, pp. 1–14, Jan. 2019.

[23] Hospital Software Development Service, IndiaMART

[24] M. Fatima, “How far can machine learning go in healthcare?” LinkedIn

[25] Research – Bioinformatics Program, Brigham and Women's Hospital

[26] R. Sunilkumar, “Safeguarding your data: A guide to encrypting credentials,” Medium, Mar. 13, 2024.

2.55. Az Ipar 4.0 technológiák alkalmazása a Siemens Amberg okosgyárában Digitalizáció, automatizálás és fenntarthatóság az elektronikai gyártásban

Az Ipar 4.0 technológiák alkalmazása a Siemens Amberg okosgyárában

Digitalizáció, automatizálás és fenntarthatóság az elektronikai gyártásban

Lakatos Bálint

Mérnökinformatikus Bsc. lakatosbalint1029@gmail.com

Ez az dolgozat bemutatja a Siemens, illetve a Siemens Amberg-i okosgyár példáján keresztül az Ipar 4.0 technológiák alkalmazását. Elemzem a digitalizáció, automatizálás, mesterséges intelligencia, digitális ikrek és IoT integrációját a gyártási folyamatok optimalizálása és fenntarthatóbbá tétele érdekében. Bemutatásra kerülnek továbbá a Siemens Xcelerator platform előnyei,a DEGREE keretrendszer ,a kiberbiztonság jelentősége, valamint az ipari innovációk gazdasági és környezeti hatásai.

Kulcsszavak: Siemens Amberg, Ipar 4.0, digitalizáció, automatizálás, mesterséges intelligencia, digitális ikrek, Siemens Xcelerator, IoT, fenntarthatóság, kiberbiztonság

TARTALOM

Tartalom 1
1 Bevezetés 3
2 A Siemens történeti áttekintése 3
3 A Siemens Amberg általános jellemzése és kapcsolata az intellel 4
4 Automatizálási rendszerek és vezérlési architektúr 5
4.1 Ipari automatizálás szerepe az Ipar 4.0-ban 5
4.2 Programozható logikai vezérlők: SIMATIC S7-1500 6
4.3 Felhasználói felületek és interaktív vezérlés: HMI panelek 8
4.4 Az egységes fejlesztői környezet: TIA Portal 8
4.5 Virtuális beüzemelés és többfelhasználós mérnöki munka 9
5 Szenzorhálózatok és IoT eszközök integrációja 9
5.1 Az ipari IoT és szenzorhálózatok szerepe az Ipar 4.0-ban 9
5.2 Szenzorhálózatok gyakorlati alkalmazása a Siemens Amberg gyárában 9
5.3 1. Környezeti paraméterek valós idejű felügyelete 9
5.4 2. Gépállapot-felügyelet és prediktív karbantartás 10
5.5 3. Minőségellenőrzés intelligens szenzorokkal 10
6 Siemens Xcelerator 10
6.1 A Siemens Xcelerator bemutatása 10

6.2 Válogatott IoT-kompatibilis portfólió 11
6.3 Nyílt partnerökoszisztéma 11
6.4 Digitális piactér és együttműködés 11
6.5 Modularitás, API-k és szolgáltatásként kínált megoldások 11
7 Digitális ikrek 11
7.1 A digitális iker fogalma és működése az iparban 11
7.2 A Siemens ambergi gyártósor digitális ikerének megvalósítása 12
7.3 A virtuális beüzemelés folyamata 12
8 KIBERBIZTONSÁG 13
8.1 A kiberbiztonság jelentősége az Ipar 4.0-ban 13
8.2 A Siemens védekezési stratégiája: Defense-in-Depth modell 13
9 Mesterséges intelligencia és gépi tanulás 13
9.1 A mesterséges intelligencia szerepe az iparban 13
9.2 Az AI demokratizálása a Siemensnél 14
9.3 Az AI bevezetésének fejlődési szakaszai 14
9.4 AI alkalmazások a Siemens Amberg gyárában 15
9.5 Prediktív karbantartás mesterséges intelligenciával 15
9.6 Minőségellenőrzés mesterséges intelligenciával 16
10 Fenntarthatóság és energiahatékonyság 17
10.1 A DEGREE stratégia áttekintése 17
10.2 Decarbonization – Üvegházhatású gázok kibocsátásának csökkentése 18
10.3 Erőforrás-hatékonyság és körforgásos gazdaság 18
10.4 Fenntarthatósági kormányzás és etikai vállalások 18
10.5 A Siemens DEGREE stratégia teljesítménymutatói 18
11 Erőforrás-hatékony termékfejlesztés és körforgásos innovációk 20
11.1 Bioműanyagok alkalmazása az ipari termékekben 20
11.2 Az Eco Design és az EcoTech címke szerepe 21
12 Eredmények összegzése 21
13 KÖVETKEZTETÉS ÉS SZEMÉLYES REFLEXIÓ 22
14 Köszönetnyilvánítás 23
15 IRODALOMJEGYZÉK 23

1 BEVEZETÉS

Az Ipar 4.0 egyik alapvető jellemzője a gyártási és üzleti folyamatok teljes körű digitalizálása és hálózatba kötése. Ez lehetővé teszi a gépek és rendszerek közötti valós idejű kommunikációt és az automatizált döntéshozatalt. A technológia gerincét képező kiberfizikai rendszerek révén a fizikai és virtuális világ szoros integrációja valósul meg.[1]

Az elmúlt évtized ipari fejlődésének középpontjában az Ipar 4.0 koncepciója áll. Ennek motorja a digitalizáció, a mesterséges intelligencia és a valós idejű adatvezérelt döntéshozatal térnyerése. A Siemens ambergi elektronikai gyára az egyik legismertebb példa arra, hogyan válhat egy hagyományos ipari üzem a technológiai innováció, fenntarthatóság és hatékonyság globális mintájává, kihasználva az Ipar 4.0 által kínált lehetőségeket.

2 A SIEMENS TÖRTÉNETI ÁTTEKINTÉSE

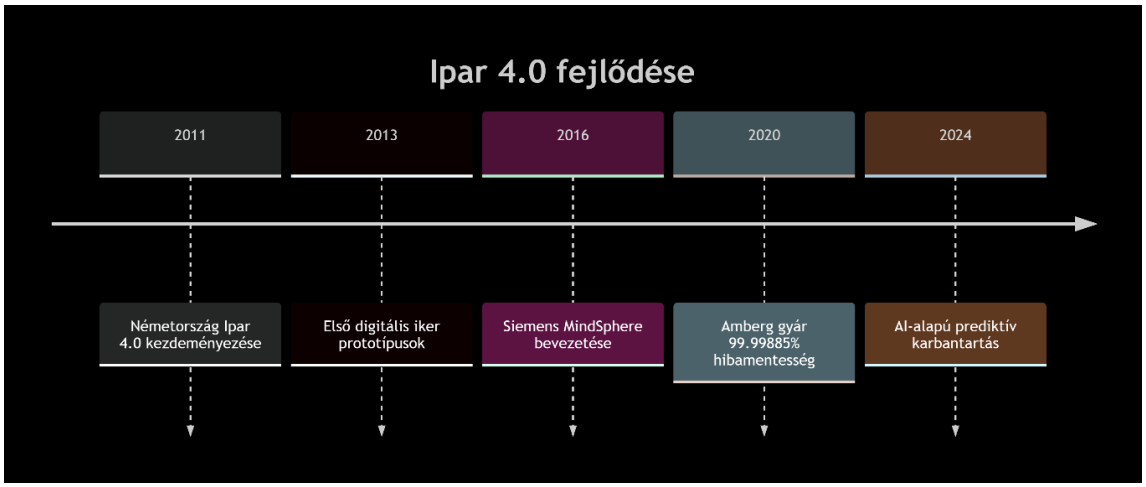
A A Siemens vállalat története egészen 1847-ig nyúlik vissza, amikor Werner von Siemens megalapította Berlinben a „Telegraphen-Bauanstalt von Siemens & Halske” nevű céget. A cég első áttörő innovációja egy mutatós távíró volt, amely a korábbi Morse-rendszernél megbízhatóbb kommunikációt tett lehetővé. A vállalat már a kezdetektől fogva aktívan exportált, többek között Oroszországba és az Egyesült Királyságba is.

Az 1866-ban bekövetkezett technológiai fordulat során Werner von Siemens felfedezte a dinamoelektromos elvet, amely forradalmasította az elektromos energia előállítását, és ezzel megalapozta a Siemens elektromosipari szerepét. A vállalat a következő évtizedekben aktívan részt vett vasúti villamosítási projektekben és városi világítási rendszerek kiépítésében is.

A 20. század elején a Siemens már nemzetközi nagyvállalatként működött: 1903-ban létrejött a Siemens-Schuckertwerke, majd a Siemens & Halske részvénytársasággá alakult, világszerte több mint 50 országban volt jelen. A két világháború azonban komoly kihívásokat jelentett: a hadiipari termelés miatt a második világháborút követően a cég több gyáregysége megsemmisült, és reputációja is súlyosan sérült. A háború után a Siemens újjáépítette tevékenységét Nyugat-Németországban, és új üzleti területeken is megjelent, mint például az orvostechnikai eszközök és félvezetők gyártása. 1966-ban a vállalat három korábbi szervezet összeolvadásával jött létre a mai Siemens AG. Az 1966 és 1988 közötti időszakban a vállalat intenzív kutatás-fejlesztésbe kezdett az automatizálás, a számítástechnika és a telekommunikáció területén, előkészítve az alapokat a későbbi ipari digitalizációhoz.

1989-ben nyitotta meg kapuit a Siemens Amberg-i Elektronikai Gyára (Electronic Works Amberg, EWA), amely már ekkor is az ipari automatizálás élvonalába tartozó rendszerek gyártására specializálódott. Ez az üzem vált később az Ipar 4.0 egyik mintagyárává, és a Siemens digitális stratégiájának központi elemévé.

A 2007 utáni időszakban a Siemens célul tűzte ki, hogy vezető szerepet töltsön be a digitalizáció terén, különösen az ipar világában. Ebben az időben indultak el olyan úttörő koncepciók, mint a „Digital Enterprise” és a digitális ikrek alkalmazása. Az Amberg gyár ennek jegyében teljesen digitalizált és hálózatba kapcsolt intelligens gyártási rendszerré fejlődött, amely tökéletes példáját adja annak, hogyan valósul meg az Ipar 4.0 víziója a gyakorlatban.



1. ábra Az Ipar 4.0 technológiai fejlődésének idővonala 2011 és 2024 között.

A Siemens Xcelerator platform bevezetése tovább erősítette ezt a folyamatot, amelynek révén az Amberg-i üzem a világ egyik legfejlettebb okosgyárává vált. [2]

3 A SIEMENS AMBERG ÁLTALÁNOS JELLEMZÉSE ÉS KAPCSOLATA AZ INTELLEL

A Siemens ambergi Elektronikai Gyára (Electronic Works Amberg – EWA) az ipari digitalizáció és automatizálás mintapéldája, ahol a gyártás 75%-át gépek és számítógépek végzik. A gyártási folyamat teljes digitalizálása során minden egyes termék egyedi vonalkóddal rendelkezik, így annak teljes gyártási útvonala nyomon követhető. Ez lehetővé teszi a gyártási hibák gyors visszakeresését, okainak feltárását, valamint a hibákból való tanulást és a folyamatok azonnali optimalizálását.

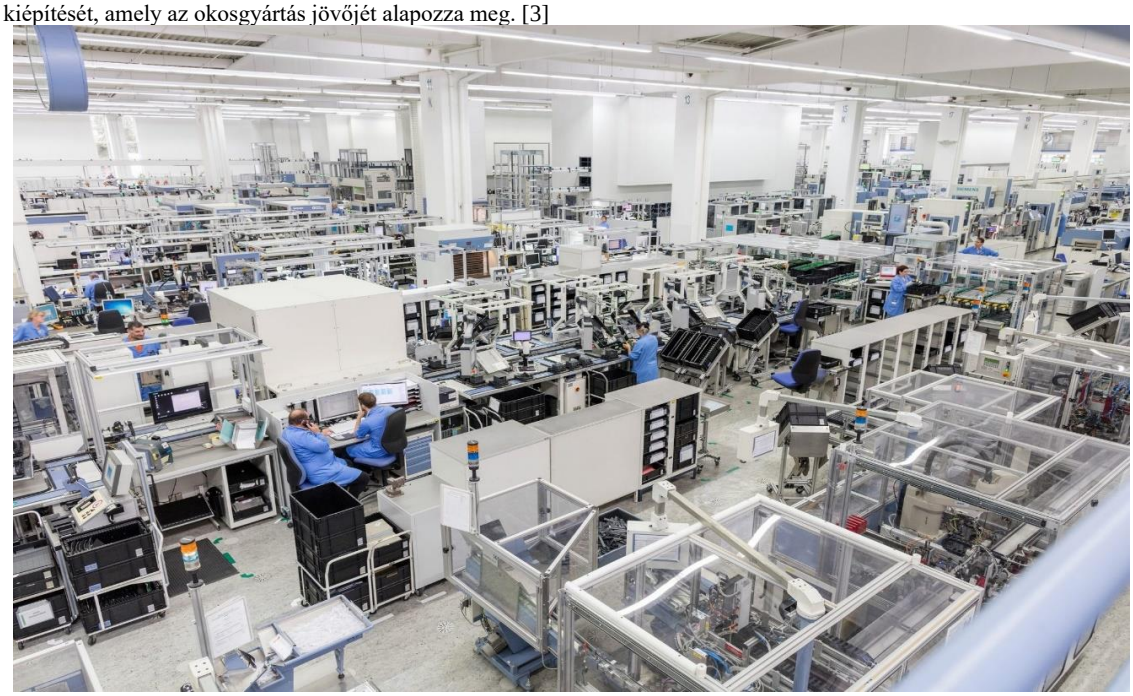
A termelési adatokat valós időben gyűjtik és a gyár irányítási rendszere (MES – Manufacturing Execution System) egy Intel Xeon alapú adatközpontban dolgozza fel. Napi szinten mintegy 50 millió gyártási adatpont kerül feldolgozásra. A rendszerek közötti kommunikáció az ipari Ethernet-alapú Profinet szabvánnyal történik, amely valós idejű adatcserét biztosít a gépek között, így a gyártósor különböző elemei (például robotkar és szállítószalag) precízen tudnak együttműködni.

Az EWA gyárban naponta 120 termékváltozatot állítanak elő, és a gyártósorok napi 350 átállást kezelnek. A termelés során alkalmazott digitális ikrek lehetővé teszik a gyártási folyamat szimulációját és tesztelését még azelőtt, hogy az fizikai valójában megvalósulna. Ezzel jelentősen csökkenthető az új termékek bevezetésének ideje és a hibalehetőség is.

A gyárban a hibamentességi arány elérte a 99.9991%-ot, amely a Six Sigma minőségi szintjéhez közeli érték. Ez a teljesítmény nem csupán technológiai eredmény, hanem a folyamatos fejlesztési ciklus szerves része, amelyben a gyártási visszacsatolások alapján módosulhat a termék- és folyamatdesign is.

A Siemens mindezt az Intel processzorokra és architektúrára épülő digitális infrastruktúrával érte el, amely a digitális gyártás sarokköveként szolgál. A Teamcenter szoftver biztosítja a digitális modell alapú vezérlést a teljes értékláncon keresztül. A szoftverek és a gépi vezérlés integrációjának köszönhetően a numerikus vezérlők programozási ideje 2 óráról 1 percre csökkent.

Az EWA nemcsak a Siemens zászlóshajó-gyárává vált, hanem modellként is szolgál más gyárak számára az Ipar 4.0 átállásban, mivel az itt szerzett tapasztalatokat és megoldásokat a Siemens szabványos termékeiben (pl. Digital Enterprise Suite, Simatic rendszerek) is alkalmazza. Az együttműködés az Intel-lel lehetővé tette egy olyan technológiai ökoszisztéma kiépítését, amely az okosgyártás jövőjét alapozza meg. [3]



2. ábra A Siemens Amberg-i gyár belső tere
(https://assets.new.siemens.com/siemens/assets/api/uuid:d4d65b0641bd9be3774669a3783aa422d08b2b0b/width:1125/quality:high/Fertigungs-und-Entwicklungsstandort-Amberg.webp)

Az EWA integrálja a mesterséges intelligenciát, peremhálózati számítástechnikát és prediktív analitikát a gyártási folyamatokba. Ezek a technológiák lehetővé teszik a gyártási hibák előrejelzését és a minőségellenőrzési folyamatok optimalizálását, például az X-sugaras végellenőrzések számának csökkentésével, ami hozzájárul a költségek és a gyártási idő csökkentéséhez.

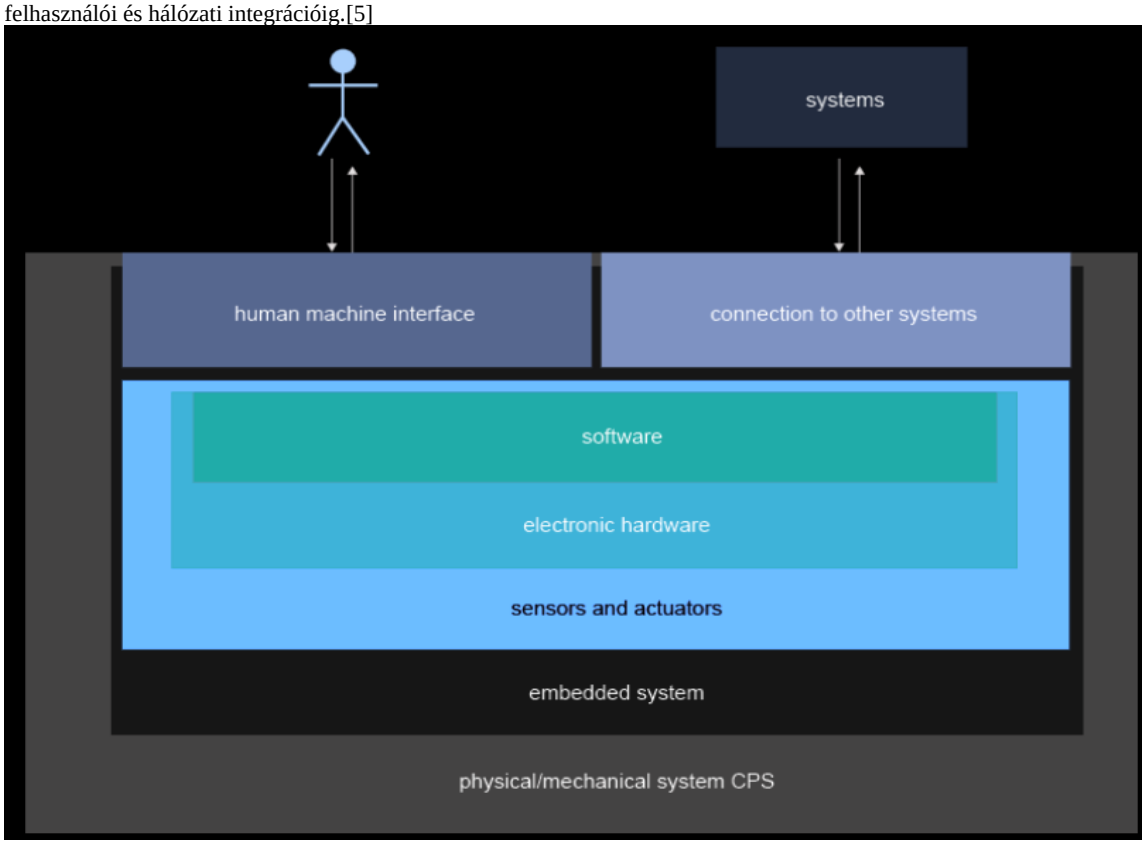
A Siemens Xcelerator ökoszisztéma részeként az EWA digitális ikreket, automatizációt és adatvezérelt működést integrál a teljes gyártási folyamatban. [4]

4 AUTOMATIZÁLÁSI RENDSZEREK ÉS VEZÉRLÉSI ARCHITEKTÚR

4.1 Ipari automatizálás szerepe az Ipar 4.0-ban

Az ipari automatizálás az Ipar 4.0 egyik kulcskomponense, amely lehetővé teszi az emberi beavatkozás minimalizálását, miközben növeli a gyártási folyamatok sebességét, pontosságát és megbízhatóságát. A programozható logikai vezérlők (PLC-k), szenzorhálózatok és decentralizált irányítási rendszerek összehangolt működése teszi lehetővé a valós idejű vezérlést és az intelligens gyártósorokat. A gyakorlatban ez olyan rendszerekhez vezet, ahol a gyártási ciklusok önoptimalizáló módon képesek alkalmazkodni a termelési igényekhez. Az alábbi ábra(lásd 3. ábra) jól szemlélteti, hogyan

épül fel egy modern, kiberfizikai alapú automatizálási rendszer a fizikai szinttől a digitális vezérlésen át egészen a felhasználói és hálózati integrációig.[5]



3.ábra A kiberfizikai rendszerek (CPS) rétegzett felépítése. (Forrás: [5])

4.2 Programozható logikai vezérlők: SIMATIC S7-1500

A Siemens Amberg-i gyára a gyártósorok körülbelül 75%-át teljesen autonóm módon üzemelteti, emberi beavatkozás nélkül, amely példátlan hatékonyságot és pontosságot biztosít az elektronikai termékek előállítása során. Az üzem központi elemei a SIMATIC S7-1500 sorozatú programozható logikai vezérlők (PLC-k), amelyek a Siemens automatizálási portfóliójának prémium kategóriás vezérlői közé tartoznak.[6]

4. ábra S7-1500 vezérlő(https://www.dailyautomation.sk/wp-content/uploads/2015/09/S7-1500-Inovat%C3%ADvny-diagnostick%C3%BD-syst%C3%A9m.jpg)

Ezek a PLC-k nanoszekundumos ciklusidővel működnek, így képesek a nagy sebességű és valós idejű vezérlésre, különösen az olyan érzékeny és precíziós folyamatok esetén, mint például az elektronikai gyártósorok forrasztási vagy anyagmozgatási műveletei. A moduláris és bővíthető architektúra lehetővé teszi a rendszer rugalmas adaptációját a gyártási igények változásához.

További előnyük, hogy a SIMATIC S7-1500 egységek integrált diagnosztikai és karbantartási funkciókkal is rendelkeznek, valamint opcionálisan biztonsági vezérlőmodulokkal (például S7-1500F fail-safe CPU-k), amelyek lehetővé teszik a működés fenntartását akár szenzorhibák vagy hardverproblémák esetén is.

A vezérlők a Totally Integrated Automation (TIA) Portal környezetben programozhatók, amely egységes fejlesztői felületet biztosít a PLC-ken kívül más rendszerelemek, mint például robotikai egységek, HMI panelek, ipari PC-k és különféle kommunikációs modulok konfigurálásához is. Ezek az eszközök egy IP-alapú hálózaton keresztül kommunikálnak, biztosítva a gyors és megbízható adatcserét .[7]

Egy gyakorlati példát említve: a nyomtatott áramkörök (PCB-k) gyártásakor a SIMATIC S7-1500 vezérlő szinkronizált módon irányítja a különböző gyártási alrendszereket, például a forrasztórobotokat, anyagmozgató rendszereket vagy az optikai minőségellenőrző egységeket.

4.3 Felhasználói felületek és interaktív vezérlés: HMI panelek

A gyárban a SIMATIC HMI Comfort panelek központi szerepet töltenek be a gyártási folyamatok felügyeletében és interaktív irányításában. Lehetővé teszik a folyamatok valós idejű vizualizálását, diagnosztikáját és beavatkozását a helyszínen, vagy akár távolról. A kezelőfelületek elérhetők webes böngészőn, illetve mobilalkalmazásokon keresztül is, így a gyártási folyamatok akár másik telephelyről is nyomon követhetők és befolyásolhatók.

5. ábra SCIMATIC HMI Comfort panel (https://assets.new.siemens.com/siemens/assets/api/uuid:b56d4bdc-6576-4f33-acdb-4813c4520f6d/width:1125/quality:high/tp900-comfort-inox-pct.png)

A panelek a WinCC vizualizációs szoftverrel együttműködve testreszabható grafikus képernyőket jelenítenek meg, melyeken keresztül az operátorok átláthatják a gyártósorok aktuális állapotát, hibajelzéseit, illetve a főbb teljesítménymutatókat (pl. ciklusidők, selejtarány, hőmérsékletértékek). Az intuitív érintőképernyős vezérlés lehetővé teszi a gyors beavatkozást: például gyártási paraméterek módosítása, berendezések manuális vezérlése vagy folyamatleállítás anélkül, hogy a PLC-programon változtatni kellene.[8]

Egy gyakorlati példával élve: ha a gyártósor egyik szakaszán túl magas hőmérsékletet észlel a rendszer, a HMI panel azonnali vizuális és hangjelzést küld, és lehetőséget nyújt az operátornak a hűtőrendszer azonnali manuális vagy automatikus aktiválására, megelőzve ezzel a termelés leállását vagy a selejttermékek keletkezését.

4.4 Az egységes fejlesztői környezet: TIA Portal

A Totally Integrated Automation Portal (TIA Portal) egy átfogó automatizálási szoftverplatform, amely lehetővé teszi a gyártórendszerek teljes életciklusának kezelését egyetlen, integrált környezetben. A platform központi eszközt kínál a PLC-k, HMI-k és hajtásrendszerek konfigurálására, ahol a különböző programozási nyelvek egységesen alkalmazhatók.

A TIA Portal lehetőséget biztosít a digitális tervezésre is: a gyártósorok virtuális prototípusai PLM-alapú (Product Lifecycle Management) modellezés révén tesztelhetők és optimalizálhatók még a fizikai telepítés előtt. A platform integrálható a Siemens Teamcenter rendszerével, amely lehetővé teszi a projektek és globális könyvtárak kezelését, valamint a tervezési, mérnöki és gyártási folyamatok összehangolását.

Az egyik legfontosabb előnye a teljes adatkonzisztencia: a rendszer automatikusan szinkronizálja a vezérlőprogramokban és a HMI felületeken végzett módosításokat, ezáltal jelentősen csökkenti a hibalehetőséget a rendszerintegráció során.

4.5 Virtuális beüzemelés és többfelhasználós mérnöki munka

A TIA Portal támogatja a többfelhasználós mérnöki munkát is, lehetővé téve, hogy több mérnök párhuzamosan dolgozzon ugyanazon a projekten, miközben a változások automatikusan szinkronizálódnak.

Egy gyakorlati példát említve: a gyártósorok virtuális beüzemelése a PLCSIM Advanced segítségével lehetővé teszi a vezérlőprogramok és a HMI felületek tesztelését még a fizikai telepítés előtt, ezáltal csökkentve a helyszíni beüzemelés idejét és költségeit. [9]

5 SZENZORHÁLÓZATOK ÉS IOT ESZKÖZÖK INTEGRÁCIÓJA

5.1 Az ipari IoT és szenzorhálózatok szerepe az Ipar 4.0-ban

Az ipari IoT-technológiák (IIoT) és a szenzorhálózatok kritikus szerepet töltenek be az Ipar 4.0 rendszerekben. Ezek az eszközök teszik lehetővé az adatok valós idejű gyűjtését, az állapotfigyelést, valamint a prediktív analitikát, amely csökkenti a karbantartási költségeket és növeli az üzemidőt . Az ipari környezetekben alkalmazott érzékelők és aktuátorok egyre fejlettebb kommunikációs protokollok (pl. OPC UA, PROFINET) segítségével kapcsolódnak az irányítási rendszerekhez. Az adatok aggregálása és elemzése közvetlenül hozzájárul az önoptimalizáló gyártási folyamatok megvalósításához, különösen az energiahatékonyság, minőségellenőrzés és gépdiagnosztika terén. Az IIoT rendszerek bevezetése egyre szorosabb kapcsolatot teremt a fizikai és digitális világ között. Ez a konvergencia új lehetőségeket nyit meg a gyártósorok adaptív vezérlése, a prediktív karbantartás és a termelési minőség folyamatos nyomon követése terén. Az IIoT rendszerek emellett elősegítik a horizontális és vertikális integrációt az ellátási lánc teljes hosszában, amely lehetővé teszi a valós idejű adatalapú döntéstámogatást és a termelés rugalmasságának növelését is.[10]

5.2 Szenzorhálózatok gyakorlati alkalmazása a Siemens Amberg gyárában

A Siemens Amberg gyárában a szenzorhálózatok és az ipari IoT (Industrial Internet of Things – IIoT) eszközök alkotják a gyártási folyamatok „idegrendszerét”. Ezek lehetővé teszik a valós idejű adatgyűjtést, elemzést és az automatizált döntéshozatalt.[11] A Siemens IIoT-megközelítésének lényege, hogy a gyártósoron elhelyezett érzékelők nem csupán adatokat gyűjtenek, hanem közvetlen kapcsolatban állnak a vezérlőrendszerekkel és a vállalati adatfeldolgozó rendszerekkel, például a TIA Portal, illetve OPC UA vagy PROFINET protokollok segítségével. Ez az összekapcsoltság biztosítja a folyamatos információáramlást az automatizálási szintek között.[12]

A gyárban az ipari IoT és szenzorhálózati megoldások gyakorlati alkalmazása három fő területen figyelhető meg:

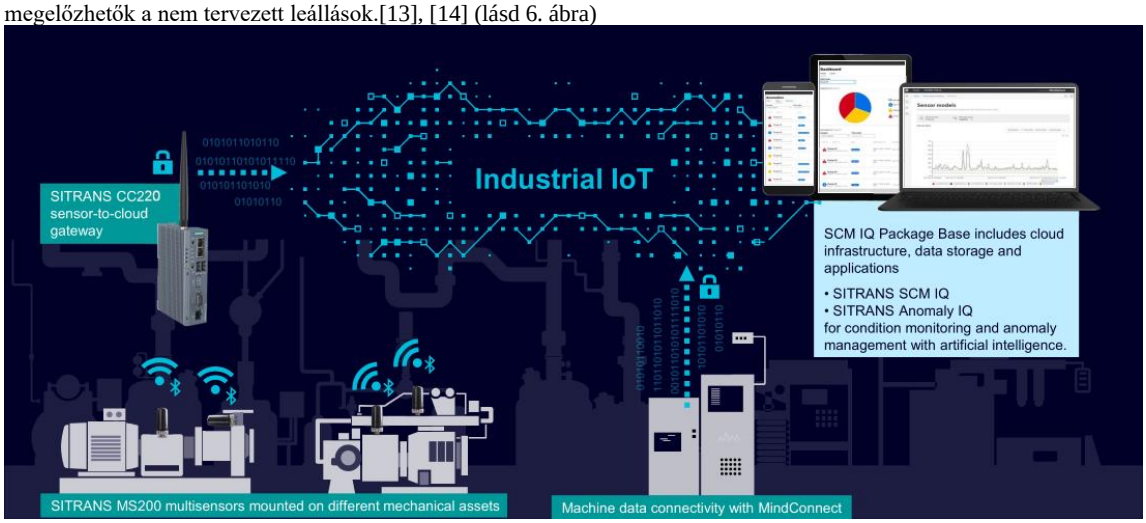
5.3 1. Környezeti paraméterek valós idejű felügyelete

A gyártási területeken elhelyezett szenzorok (pl. hőmérséklet, páratartalom és légminőség-érzékelők) folyamatosan figyelik a környezetet, biztosítva az optimális feltételeket a precíziós elektronikai gyártáshoz. Az érzékelők által

szolgáltatott adatok valós időben elemzésre kerülnek, így az eltérések azonnal detektálhatók, és szükség esetén automatikusan elindulhat a beavatkozás.[11]

5.4 2. Gépállapot-felügyelet és prediktív karbantartás

A gépek állapotának monitorozására a Siemens olyan intelligens IIoT-eszközöket alkalmaz, mint a SITRANS MS200 multiszenzor, amely rezgés- és hőmérsékletadatokat gyűjt. Ezeket az adatokat Bluetooth kapcsolaton keresztül a SITRANS CC220 ipari átjáró továbbítja, amely titkosítva juttatja el őket a SITRANS SCM IQ rendszerbe vagy a MindSphere platformra. A rendszer segítségével a gépek állapota valós időben nyomon követhető, és a prediktív karbantartás révén megelőzhetők a nem tervezett leállások.[13], [14] (lásd 6. ábra)



6.ábra A SITRANS MS200 multiszenzor és SITRANS CC220 átjáró működési elve az ipari IoT-rendszerben.(https://developer.siemens.com/sitrans-scm-iq/images/overview.png)

5.5 3. Minőségellenőrzés intelligens szenzorokkal

A gyár minőségbiztosítási folyamataihoz fejlett kamerarendszereket és lézeres szenzorokat használnak, amelyek nagyfelbontású képekkel és precíz mérésekkel azonosítják a gyártási hibákat. Ezek az eszközök valós időben végzik a termékek ellenőrzését, és szükség esetén azonnali korrekciót tesznek lehetővé, csökkentve ezzel a selejtarányt és biztosítva a magas minőségi sztenderdek betartását. [13]

6 SIEMENS XCELERATOR

6.1 A Siemens Xcelerator bemutatása

A Siemens Xcelerator egy nyílt, moduláris digitális üzleti platform, amelynek célja, hogy felgyorsítsa a vállalatok digitális transzformációját, különösen az ipari és infrastruktúra területeken. A Siemens 2022-ben indította el a platformot, és azóta egyre bővülő ökoszisztémát és szolgáltatásportfóliót kínál a világ számos iparága számára.[15]

A Siemens Xcelerator a következőkből épül fel:

6.2 Válogatott IoT-kompatibilis portfólió

Válogatott IoT-képes hardverek és szoftverek portfóliója: A Siemens Xcelerator egy gondosan összeállított portfóliót kínál, amely IoT-kompatibilis hardvereket, szoftvereket és digitális szolgáltatásokat tartalmaz. Ezeket a megoldásokat a nyitottság, interoperabilitás, modularitás és a "szolgáltatásként" való elérhetőség elvei szerint tervezték. A portfólió célja, hogy megkönnyítse a digitális átalakulást az ipar, az épületek, az energiahálózatok és a mobilitás területén.[15]

6.3 Nyílt partnerökoszisztéma

Partnerökoszisztéma: A platform nemcsak technológiát, hanem egy élő közösséget is kínál, amely fejlesztőkből, partnerekből és ügyfelekből áll. A Siemens célja, hogy egy nyílt, kooperatív ökoszisztémát hozzon létre, ahol a szereplők közösen fejleszthetnek és oszthatnak meg digitális megoldásokat.[15], [16]

6.4 Digitális piactér és együttműködés

Digitális piactér: A Siemens Xcelerator Marketplace egy interaktív online platform, amely megkönnyíti a partnerek közötti kapcsolattartást, a megoldások megosztását, integrálását és testreszabását. A piactér célja, hogy segítse az ügyfeleket az iparág-specifikus kihívások kezelésében, a teljes körű megoldások felfedezésében, valamint a partnerökoszisztémában elérhető szakértőkkel való kapcsolatfelvételben .[15]

6.5 Modularitás, API-k és szolgáltatásként kínált megoldások

A Siemens célja, hogy teljes termékportfólióját (hardver és szoftver) moduláris felépítésűvé, API-alapúvá és felhőkapcsolatra késszé tegye. Ezzel a megközelítéssel lehetővé válik, hogy a partnerek és ügyfelek gyorsan és rugalmasan fejlesszenek saját megoldásokat, a szoftveres fejlesztés sebességével. A hardverek is dinamikusan frissíthetővé válnak, sőt akár „as-a-service” modellben is elérhetők lesznek. [15], [16]

7 DIGITÁLIS IKREK

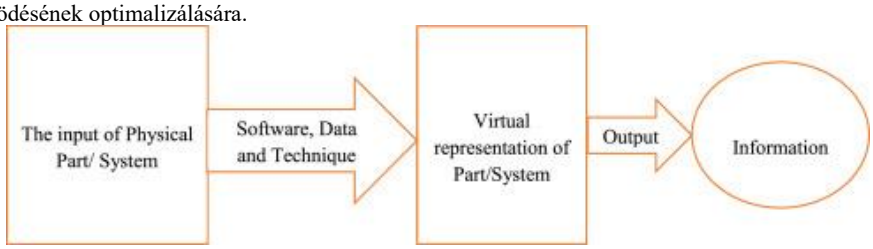
7.1 A digitális iker fogalma és működése az iparban

A digitális iker (digital twin) egy virtuális modell, amely az IoT eszközök fizikai alkatrészeit és viselkedését valós időben tükrözi, figyelembe véve az eszközök teljes életciklusát. A digitális iker létrehozásához érzékelőket használnak, amelyek valós idejű adatokat gyűjtenek a fizikai világból. Ezek az adatok folyamatosan frissítik a digitális modellt, amely lehetővé teszi a fizikai eszközök és rendszerek részletes, dinamikus elemzését. A digitális iker segítségével a valós idejű adatok azonnal elérhetővé válnak, lehetővé téve a valós világbeli eszközök és rendszerek működésének optimalizálását.

A digitális ikrek alkalmazása számos előnnyel jár: elősegíti a termelési folyamatok szimulációját, a gyártósorok hatékonyságának növelését, valamint lehetőséget ad a termelési hibák előrejelzésére és a karbantartási költségek csökkentésére. A digitális iker folyamatosan figyeli és elemzi a kulcsfontosságú mutatókat, mint például az energiafogyasztás, a gyártás minősége és a rendszer teljesítménye. Ezen adatok segítségével a vállalatok nemcsak a termelési folyamatokat optimalizálhatják, hanem fenntarthatósági céljaikat is elérhetik, mivel a digitális iker lehetővé teszi a termelési folyamatok energiahatékonyabbá tételét.

A digitális iker ezenkívül segít a nem tervezett leállások csökkentésében, mivel az IoT alapú rendszerek és a gépi tanulás révén képes előre jelezni a potenciális problémákat és javaslatokat tenni a karbantartás időzítésére. Az ipari rendszerek egyre inkább autonóm módon működnek, és a digitális ikrek elemzése alapján a rendszerek valós időben képesek alkalmazkodni a változó környezethez és követelményekhez.[17]

A digitális iker működésének alapelveit az alábbi ábra (lásd 7.ábra) szemlélteti, amely bemutatja, hogyan történik a fizikai rendszer adatinformációinak begyűjtése, virtuális reprezentációja és az ebből kinyert visszacsatolás alkalmazása a rendszer működésének optimalizálására.



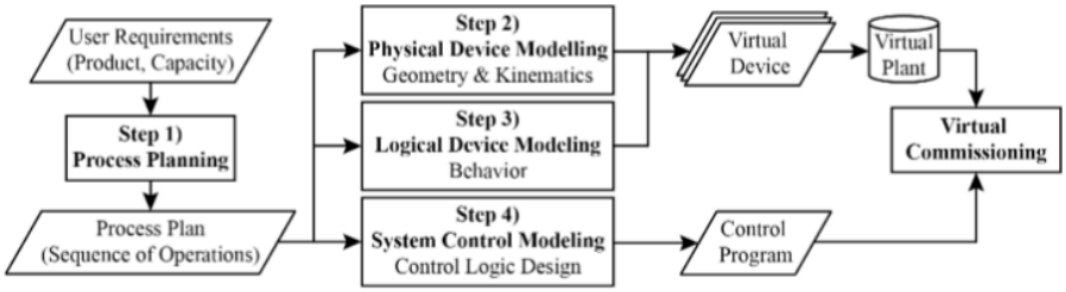
7. ábra A digitális iker rendszer működésének vázlata.(Forrás:[17])

7.2 A Siemens ambergi gyártósor digitális ikerének megvalósítása

Az ambergi gyártósor digitális ikre a Tecnomatix Process Simulate szoftverrel valósul meg mely lehetővé teszi a gyártóberendezések és robotcellák részletes 3D-s modellezését, beleértve azok kinematikai és logikai viselkedését is. A gyakorlatban a digitális iker létrehozása három fő komponensből áll: a geometriai és kinematikai modellből, a logikai viselkedési modellből, valamint a bemeneti és kimeneti jelek kezeléséből.

7.3 A virtuális beüzemelés folyamata

A Tecnomatix Process Simulate szoftver és a TIA Portal/PLC SIM Advanced integrációja lehetővé teszi az ipari gyártócellák teljes körű virtuális beüzemelését (virtual commissioning), amely során még a fizikai berendezések telepítése előtt validálható és optimalizálható a vezérlési logika. Az alábbi ábra(lásd 8. ábra) bemutatja a virtuális beüzemelés tervezési lépéseit, amelyek során a fizikai modell, a logikai működés és a vezérlőprogram szoros integrációban kerülnek kialakításra.



8. ábra A virtuális beüzemelés (Virtual Commissioning) tervezési folyamata lépésről lépésre(forrás:[18])

Ez a megközelítés nemcsak a fejlesztési idő és költségek csökkentésében jelent előnyt, hanem lehetővé teszi a gépelemek és vezérlők viselkedésének valós idejű szimulációját, tesztelését, valamint a szoftver-in-the-loop alapú hibakeresést is.[18]

8 KIBERBIZTONSÁG

8.1 A kiberbiztonság jelentősége az Ipar 4.0-ban

Az Ipar 4.0 kontextusában a kiberbiztonság kulcsfontosságú szerepet játszik a vállalatok versenyképességének megőrzésében és az ipari berendezések védelmében a kibertámadásokkal szemben, amelyek képesek az egész üzleti modellt megbénítani. A Cisco 2018-as éves kiberbiztonsági jelentései szerint a szervezetek 31%-a tapasztalt kibertámadást az operációs technológia (OT) területén, míg 38%-uk arra számít, hogy a támadások egyre inkább az informatikai rendszerekről (IT) az operációs technológiákra is kiterjednek. Bár a kiberbiztonságot 75%-ban prioritásnak tekintik a szakértők, csupán 16%-uk mondja azt, hogy a vállalatuk jól fel van készülve a kiberbiztonsági kihívások kezelésére. Ennek fő oka a pontos szabványok hiánya, amelyekhez a cégek viszonyíthatják magukat, valamint a szükséges vezetői és technikai készségek hiánya a megfelelő intézkedések végrehajtásához.[19]

8.2 A Siemens védekezési stratégiája: Defense-in-Depth modell

A Siemens ezen a területen is az úttörők közé sorolható, hiszen a kiberbiztonság nem kiegészítő, hanem integrált része a teljes gyártási ökoszisztémának. Egy többrétegű védekezési stratégiát (Defense-in-Depth) használnak, amely három fő pillérre épül:

1. Üzemszintű védelem

A fizikai infrastruktúra védelmét a Siemens saját üzemében RFID-alapú hozzáférés-ellenőrzéssel, beléptetőrendszerekkel és kameraalapú megfigyeléssel biztosítja. Emellett a munkavállalók rendszeres tudatosságnövelő képzésekben részesülnek, amelyek során az ipari kiberfenyegetések felismerésére és megelőzésére készítik fel őket.

2. Hálózati biztonság

A Siemens automatizálási hálózatait tűzfalakkal, behatolás-érzékelő rendszerekkel (IDS), valamint szegmentált hálózati architektúrával védi. A Zero Trust elv alkalmazása azt jelenti, hogy minden hálózati kapcsolat és hozzáférési kérelem hitelesítésre kerül még a belső rendszerek között is. Emellett VPN-alapú távoli hozzáférést használnak az IT és OT rendszerek közötti biztonságos kommunikációhoz.

3. Automatizálási rendszerek védelme

A Siemens, mint már említettem saját gyártóüzemeiben SIMATIC vezérlőegységeket használ, például az S7-1500 beépített biztonsági funkciókat tartalmaznak, így támogatják a jelszavas védelem, hozzáférés-korlátozás, titkosított kommunikáció (TLS) és programkód-védelem alkalmazását is. A vezérlőrendszerek és a HMI-k közötti kommunikáció titkosítva zajlik, csökkentve a lehallgatás vagy manipuláció esélyét.

4. Folyamatos kiberbiztonsági menedzsment

Rendszeres sebezhetőségi vizsgálatokat és folyamatos hálózati forgalomfigyelést végeznek. Emellett központi biztonsági frissítéskezelési rendszer gondoskodik arról, hogy a szoftverek és firmware-ek mindig naprakészek legyenek.[20]

9 MESTERSÉGES INTELLIGENCIA ÉS GÉPI TANULÁS

9.1 A mesterséges intelligencia szerepe az iparban

A mesterséges intelligencia (AI) fejlődése az iparban és a társadalomban új értékígéreteket hozott, amelyek jelentős gazdasági növekedést ígérnek. Becslések szerint 2030-ra az AI globális GDP-hez való hozzájárulása 13 és 15,7 billió dollár között mozoghat. Azonban a vállalatok számára nehézséget jelent az AI-technológiák, mint a gépi tanulás és a mélytanulás, széles körű alkalmazása, mivel az AI rendszerek hatékony bevezetése és méretezése a mai napig problémát jelent,

különösen a megfelelő AI készségekkel rendelkező szakemberek és az üzleti szakterületek közötti szoros együttműködés nélkül. Az egyik fő kihívás, hogy az AI alkalmazások nem szoftverfejlesztésre, hanem tanuló algoritmusok és hatalmas mennyiségű adatok feldolgozására építenek, ami új típusú kihívásokat támaszt a szervezetek számára.[21]

9.2 Az AI demokratizálása a Siemensnél

A Siemens az AI rendszerek bevezetését és méretezését szervezeti szinten valósítja meg. Ez a folyamat azt jelenti, hogy az AI alkalmazásokat a domain szakértők, adatkutatók és IT szakemberek közötti szoros együttműködéssel alakítják ki, lehetővé téve az AI potenciáljának gyors és hatékony kihasználását. Siemens AI demokratizálásának legfontosabb tanulsága, hogy az AI nem csupán a technológia kérdése, hanem a szervezeten belüli együttműködésről és a különböző szakmai területek integrálásáról is szól. Az AI alkalmazások sikeres bevezetéséhez kulcsfontosságú a domain szakértők, adatkutatók és IT szakemberek közötti szoros együttműködés, akik közösen azonosítják a megfelelő AI feladatokat és azokat integrálják az üzleti folyamatokba.[21]

9.3 Az AI bevezetésének fejlődési szakaszai

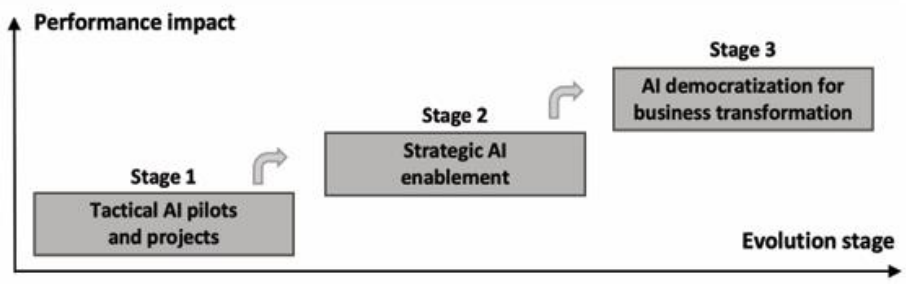
A Siemens három szakaszban valósította meg az AI demokratizálását:

1. Taktikai AI pilot projektek (2016 előtt): Az AI pilot projektek helyi fejlesztéseken alapultak, és kifejezetten egy-egy szűkebb területre koncentráltak, például a Siemens postaládarendszerében az irásfelismerésre. Ezek az AI megoldások nem voltak szoros kapcsolatban a vállalati IT rendszerekkel és nem hoztak létre széleskörű alkalmazásokat. Az AI alkalmazásokat ad hoc módon fejlesztették.

2. Stratégiai AI lehetőségek (2016-2018): 2016-ban Siemens vezetése már az AI fontosságát hangsúlyozta a vállalati stratégiában, és létrehozta a Next47 nevű innovációs egységet, amely az AI alkalmazások fejlesztését és startup cégektől való beszállítást támogatta. Az AI Lab megnyitása is ezen időszak alatt történt, amely lehetőséget adott domain szakértők és adatkutatók közötti együttműködésre, így gyorsan konkrét AI alkalmazásokat fejlesztettek ki.

3. AI demokratizálása és üzleti átalakítás (2019-től): A harmadik szakasz célja az AI alkalmazások széleskörű bevezetése volt, amelyek képesek átalakítani termékeket, szolgáltatásokat és folyamatokat. Ekkor már Siemens globális AI platformot hozott létre, amely lehetővé tette az adatgyűjtést és gépi tanulási folyamatokat. Az AI Akadémia létrehozása pedig segítette a munkavállalók AI ismereteinek bővítését, hogy az AI minden szinten hozzáférhetővé váljon a szervezetben.

Az alábbi ábra szemlélteti (lásd 9. ábra) az AI bevezetésének három fejlődési szakaszát – a kezdeti pilot projektektől egészen az üzleti folyamatok átalakításáig. Ez az evolúciós modell rávilágít arra, hogyan nő az AI teljesítményre gyakorolt hatása az alkalmazás szervezetbe való integrálódásával párhuzamosan. [21]



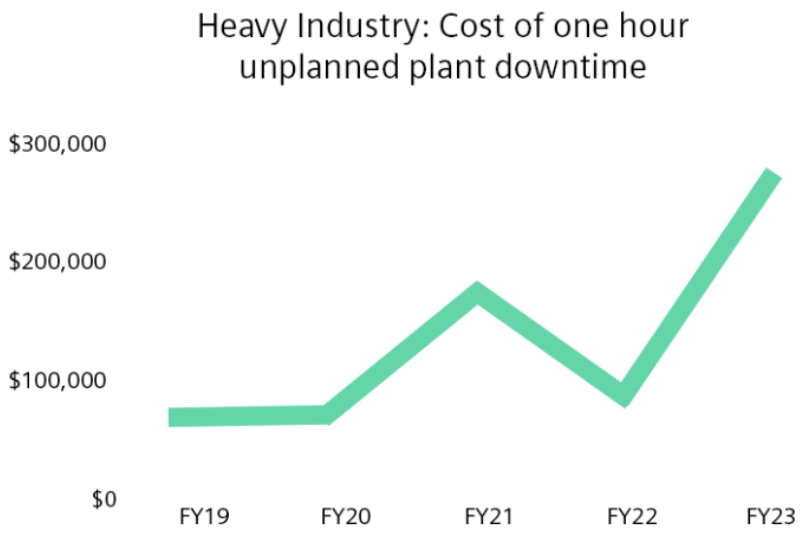
9. ábra A mesterséges intelligencia fejlődési szakaszai a Siemens gyakorlatában.(Forrás:[21])

9.4 AI alkalmazások a Siemens Amberg gyárában

Az ambergi gyár AI alkalmazásokkal forradalmasította a termelést. Ezek segítségével sikerült csökkenteni a minőségellenőrzési szűk keresztmetszeteket, valamint előre jelezni a karbantartási igényeket. Az AI alkalmazások, például az in-line minőségelőrejelzés és a prediktív karbantartás nemcsak a termelési folyamatokat optimalizálták, hanem lehetővé tették az AI megoldások skálázását más gyárakban is. [21]

9.5 Prediktív karbantartás mesterséges intelligenciával

A prediktív karbantartás alapját a valós idejű szenzoradatok, a gépek működésének naplózása, valamint a karbantartók viselkedésének elemzése képezi. A Siemens leányvállalata, a Senseye, olyan mesterséges intelligencián és gépi tanuláson alapuló prediktív karbantartási rendszert fejlesztett ki (Senseye PdM), amely képes előre jelezni a gépek és azok kritikus alkatrészeinek állapotromlását. A megoldás célja az állásidő csökkentése és a karbantartási folyamatok hatékonyabbá tétele. Ezt a célkitűzést támasztja alá a 2023-as ipari jelentés is(lásd 10. ábra), amely szerint a nem tervezett üzemleállások költsége az elmúlt öt évben drasztikusan megemelkedett. Különösen a nehéziparban figyelhető meg jelentős növekedés: az egyórás leállás költsége a 2019-es szinthez képest 319%-kal nőtt, meghaladva a 300 000 dollárt óránként. Ez az adat jól szemlélteti, miért vált a prediktív karbantartás stratégiai jelentőségűvé a modern ipari környezetben.[22], [23]

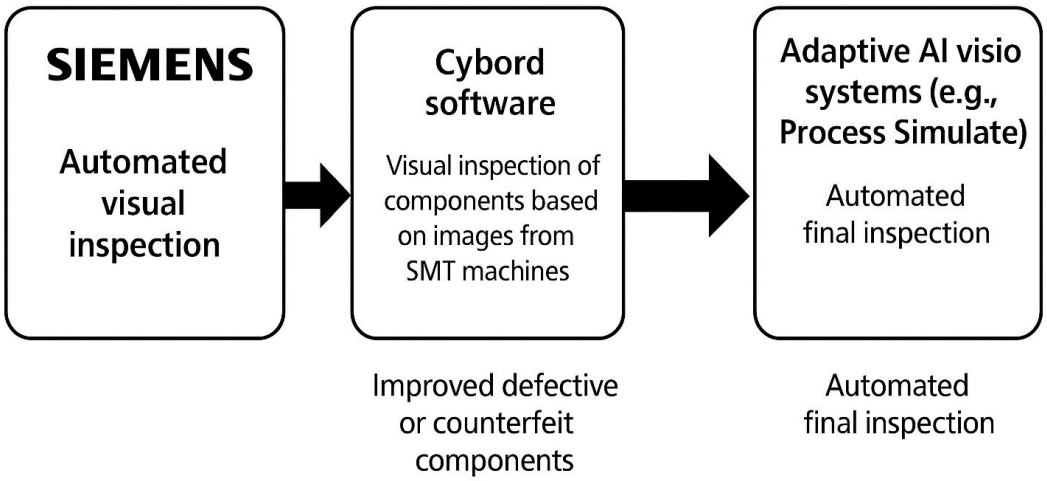


10. ábra A nem tervezett üzemleállás költségének alakulása a nehéziparban 2019 és 2023 között.(https://assets.new.siemens.com/siemens/assets/api/uuid:1b43afb5-2d07-47f7-9eb7-893fe7d0bc59/TCOD-2024_original.pdf)

9.6 Minőségellenőrzés mesterséges intelligenciával

A Siemens a minőségellenőrzés automatizálása terén is jelentős előrelépést tett mesterséges intelligencia alapú megoldásaival. Ennek egyik kulcseleme a Cybord szoftver, amelyet a Siemens Digital Industries Software OEM-partnerség keretében integrált saját gyártási analitikai portfóliójába.

A Cybord egy valós idejű vizuális ellenőrző rendszer, amely az SMT (felületszerelt technológiai) gépek által készített képek alapján 100%-os alkatrészellenőrzést tesz lehetővé még a nyomtatott áramkörökre történő elhelyezés előtt. A rendszer nem befolyásolja a gépek gyártási sebességét, ugyanakkor jelentősen javítja az alkatrészek hitelességének és minőségének ellenőrizhetőségét, csökkentve ezzel a hibás vagy hamisított alkatrészek előfordulását, valamint a visszahívások kockázatát. A megoldás önálló rendszerként vagy MES-rendszerbe integrálva is használható, így rugalmasan illeszthető a gyártók folyamataiba, különösen a beszállítói láncban tapasztalható bizonytalanságok idején. Az ellenőrzés folyamata a következő ábrán megtekinthető (lásd 11. ábra)



11. ábra Siemens és a Cybord közös mesterséges intelligencia alapú minőségellenőrzési rendszer működési folyamata

Emellett a Siemens adaptív AI-vízió rendszerei, mint például a Process Simulate, a végellenőrzési folyamatok automatizálását támogatják. Ezek a rendszerek akár 80%-kal csökkentik a manuális ellenőrzési igényt, miközben fokozzák a felületi hibák észlelésének pontosságát, ezzel új szintre emelve a minőségbiztosítást.[24], [25]

10 FENNTARTHATÓSÁG ÉS ENERGIAHATÉKONYSÁG

10.1 A DEGREE stratégia áttekintése

A Siemens vállalatcsoport az elmúlt évtizedben következetesen olyan integrált megközelítést alkalmazott, amely nemcsak a környezeti hatások csökkentését célozza, hanem üzleti előnyöket is biztosít a hosszú távú versenyképesség fenntartása érdekében. A Siemens 2001-ben elindított DEGREE fenntarthatósági stratégiája olyan átfogó keretrendszerként szolgál, amely a fenntartható fejlődés három alappillérét (gazdasági, társadalmi, környezeti) ötvözi a Stakeholder- és SDG- (ENSZ Fenntartható Fejlődési Célok) megközelítésekkel.

A DEGREE mozaikszó a Siemens fenntarthatósági stratégiájának hat fő fókuszterületét jelöli:

D – Decarbonization (Szén-dioxid-mentesítés)

E – Ethics (Etika)

G – Governance (Irányítás)

R – Resource Efficiency (Erőforrás-hatékonyság)

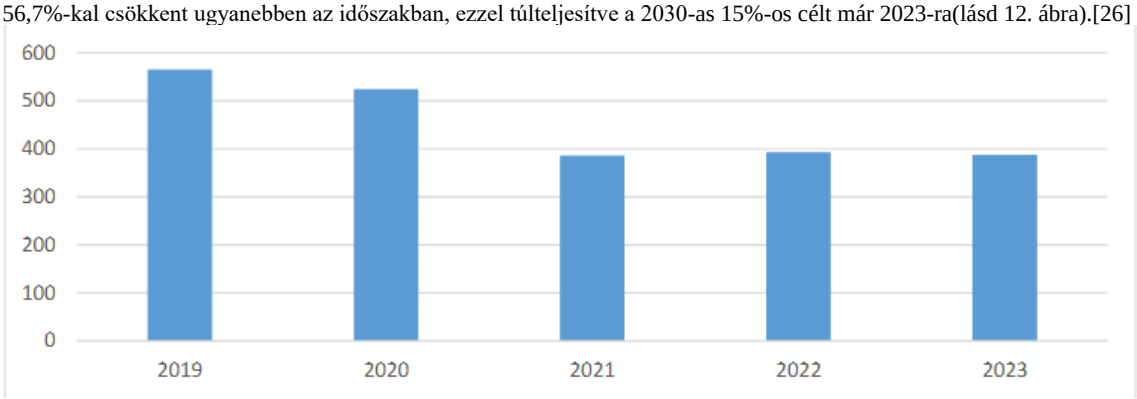
E – Equity (Méltányosság)

E – Employability (Foglalkoztathatóság)

Ez a stratégia 2030-ig és 2050-ig terjedő ambiciózus célokat határoz meg, beleértve a teljes karbonsemlegességet, az újrahasznosítási arányok növelését, valamint a társadalmi méltányosság és munkavállalói jólét előmozdítását.[26]

10.2 Decarbonization – Üvegházhatású gázok kibocsátásának csökkentése

A Siemens jelentős előrehaladást ért el a szén-dioxid-kibocsátás mérséklésében. A vállalat 2019 és 2023 között 31,5%-kal csökkentette működési tevékenységeiből származó üvegházhatású gázok kibocsátását, miközben célja 55%-os csökkentés elérése 2025-ig. Különösen kiemelkedő a villamosenergia-fogyasztásból származó kibocsátás esete, amely 56,7%-kal csökkent ugyanebben az időszakban, ezzel túlteljesítve a 2030-as 15%-os célt már 2023-ra(lásd 12. ábra).[26]



12. ábra A Siemens működési tevékenységeiből származó üvegházhatású gázkibocsátás alakulása 2019 és 2023 között (ezer tonnában).(Forrás:[26])

10.3 Erőforrás-hatékonyság és körforgásos gazdaság

Az erőforrás-hatékonyság javítása szintén a Siemens egyik fő célkitűzése. A vállalat célja, hogy 2030-ra 100%-ban robusztus öko-dizájnnal rendelkező termékeket állítson elő, valamint elérje a nulla hulladéklerakót. 2019 és 2023 között a nem veszélyes hulladék újrahasznosítási és visszanyerési aránya 265 ezer tonnáról 203 ezer tonnára csökkent (-23,1%), ami ugyan előrelépést mutat, de még nem éri el a kívánt 50%-os csökkentési célt. Ez arra utal, hogy további beruházásokra és környezettudatos innovációkra van szükség.[26]

10.4 Fenntarthatósági kormányzás és etikai vállalások

A vállalat etikai és kormányzási irányelvei szintén szerves részét képezik a fenntarthatósági törekvéseknek. A compliance-tréningek résztvevőinek aránya és az oktatási kiadások 2020 és 2023 között jelentős növekedést mutattak. A Siemens 2023-ban 416,3 millió eurót fordított munkavállalói képzésekre, amely jelentős előrelépést jelent a COVID-időszakhoz képest.[26]

10.5 A Siemens DEGREE stratégia teljesítménymutatói

Table 1 Siemens DEGREE fenntarthatósági stratégia teljesítménye (1999–2023)(Forrás:[26])

Sustainability	KPIs	KPI Targets	2023	2022	2021	2020	2019	2019-2023
Decarbonization	1. Greenhouse Gas Emission	55% Zero (0)	3%	2%	26%	-7%	565	-31.50%

Sustainability	KPIs	KPI Targets	2023	2022	2021	2020	2019	2019-2023
	from Siemens Operations							
	2. Greenhouse Gas Emission from Electricity consumption	15% Zero (0)	-13.80%	-9.10%	17.50%	-50.80%	360	-54.17%
	3. Greenhouse Gas Emission from Supply Chain in upstream ops	15% Zero (0)	-4.06%	14.10%	-1.09%	-11.30%	11,500	-3.98%
Ethics	1. Compliance Trainings	461000	472,140	446,090	374000			459,115
	2. Spending on employee education and training (In Million â,¬)	416.3	416.3	374.6	322.2	321	391	414.667
	3. Average training hours per employee	11.1%30	11.10%	16.30%	-0.57%	-17.90%	-17%	1.79%
Governance	1. Corporate responsibility self-assessments	5096	5096					
	2. Retiring expected within next 5 years	10.30%	10.30%	10.30%				
Resource efficiency	1. Quota of product with robust eco design	100%	50%	35%	26%			

Sustainability	KPIs	KPI Targets	2023	2022	2021	2020	2019	2019-2023
	2. Waste to landfill	50%	14%	18.00 %	15.00 %			
	3. No. of hazardous waste	14%	18.00 %	15.00 %	11.80 %			
	4. Recycling & Recovery (non-Hazardous waste)	12.7	15	11.8	22.3	257	265	
	5. Recycling & Recovery (Hazardous waste)	203.8	7.2	10	6.1	265		
Equity	1. Female share in top management	30%	30.80 %	27.70 %	27.50 %	18.40 %	18.50 %	12.30 %
	2. Employees' access to Siemens share plans	100%	43.50 %	44.50 %				-56.50%
Employability	1. Digital learning hours per employees	25	23	21	17	21	21	2
	2. Access to medical care	100%	99.60%	99%				-1%

11 ERŐFORRÁS-HATÉKONY TERMÉKFEJLESZTÉS ÉS KÖRFORGÁSOS INNOVÁCIÓK

11.1 Bioműanyagok alkalmazása az ipari termékekben

A Siemens elkötelezett a körforgásos gazdaság elvei mellett, amelyek célja az anyagok és termékek élettartamának meghosszabbítása, a hulladék minimalizálása, valamint az erőforrások felelősségteljesebb felhasználása. Az előző ponthoz kapcsolódóan a vállalat a DEGREE fenntarthatósági stratégiája keretében különös figyelmet fordít az anyaghatékonyság (Resource Efficiency) és dekarbonizáció területére, ennek érdekében újragondolja termékei tervezését, gyártását és anyaghasználatát.

Ezen törekvések egyik kiemelkedő példája a SIRIUS 3RV2 megszakító, amely az első elektromos biztonságtechnikai termék, amelyben biomassza-alapú műanyagokat alkalmaznak. A termék gyártása során a hagyományos fosszilis alapanyagokat megújuló forrásokból, például mezőgazdasági hulladékból származó biometánnal váltják ki. A használt

anyagok a BASF által kifejlesztett Ultramid BMBcertTM és Ultradur BMBcertTM azonos mechanikai és funkcionális tulajdonságokat kínálnak a hagyományos műanyagokkal, miközben évente mintegy 270 tonna CO_2-egyenérték kibocsátás csökkenést eredményeznek.

11.2 Az Eco Design és az EcoTech címke szerepe

A SIRIUS 3RV2 megszakító ezen túlmenően alacsonyabb teljes élettartam alatti energiafogyasztással is rendelkezik, mint elődei, ami tovább növeli környezeti előnyeit. A termék megfelel a Siemens EcoTech címkének is, amely átlátható információkat nyújt a termék környezeti teljesítményéről a vásárlók számára.[27]

13. ábra SIRIUS 3RV2 circuit breaker(https://assets.new.siemens.com/siemens/assets/api/uuid:a45d7bbc-efe9-47e5-bbbd-48914d2b5371/width:1920/quality:high/sirius-3rv2-motor-starter-protectors-circuit-breakers.webp)

Ez a fejlesztés nemcsak a Siemens belső célkitűzéseivel van összhangban, például a 90%-os Scope 1 és 2 kibocsátáscsökkentési cél 2030-ig, hanem elősegíti a vállalat Eco Design irányelveinek megvalósítását is, amely szerint 2030-ig a termékcsaládok 100%-a megfelel majd az erőforrás-hatékony tervezési követelményeknek.[27]

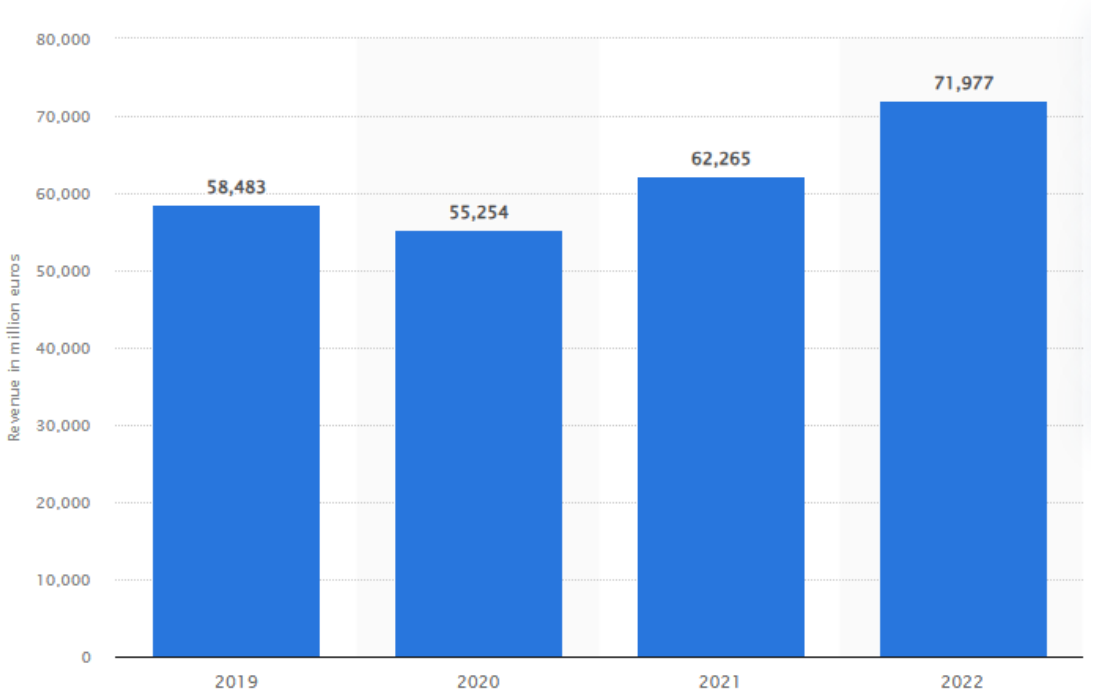
12 EREDMÉNYEK ÖSSZEGZÉSE

Az EWA évente több mint 17 millió SIMATIC terméket gyárt, ami körülbelül másodpercenként egy termék előállítását jelenti. A gyárban naponta 350 gyártási változtatást hajtanak végre, és körülbelül 50 millió folyamat- és termékadatot dolgoznak fel az optimalizálás érdekében. A digitalizáció és az automatizálás révén a gyár képes gyorsan alkalmazkodni az egyedi ügyféligényekhez, és a termékek gyártását akár 24 órán belül elindítani. Az új termékek bevezetésének ideje 50%-kal csökkent más Siemens gyárakhoz képest, a gyártósorok átállási ideje pedig szintén a felére csökkent.Az új

termékek bevezetésének ideje 50%-kal csökkent más Siemens gyárakhoz képest, a gyártósorok átállási ideje pedig szintén a felére csökkent[28]

Az EWA-ban a gyártási minőség eléri a 99,99885%-ot, ami kevesebb mint 12 hibát jelent egymillió termékre vetítve. Ez a kiváló minőség a digitális ikrek, a mesterséges intelligencia és az edge computing technológiák integrációjának köszönhető. A gyárban alkalmazott mesterséges intelligencia algoritmusok előrejelzik a gyártási hibák valószínűségét, így csökkentve a szükséges minőségellenőrzési tesztek számát, például az időigényes röntgenvizsgálatokat. Ez a megközelítés nemcsak a termelési kapacitást növelte, hanem 500 000 euró megtakarítást is eredményezett a beruházási költségekben. [28], [29]

A Siemens globális pénzügyi teljesítménye szintén tükrözi a digitalizáció és automatizálás beruházásainak pozitív hatását, amely nemcsak a gyártási eredményekre van jótékony hatással, hanem a vállalat hosszú távú pénzügyi stabilitására és növekedésére is(lásd 14. ábra).



14. ábra A Siemens éves bevételeinek alakulása 2019 és 2022 között (millió euróban).(Siemens AG - revenue 2022| Statista)

13 KÖVETKEZTETÉS ÉS SZEMÉLYES REFLEXIÓ

A Siemens Amberg-i okosgyára egyértelműen bizonyítja, hogy az Ipar 4.0 technológiák nem csupán jövőbeli lehetőségeket, hanem már jelenleg is működő, mérhető előnyöket kínálnak. A digitalizáció, az automatizálás, a mesterséges intelligencia, a digitális ikrek és az ipari IoT eszközök integrációja nemcsak a termelési hatékonyságot növeli, hanem

hozzájárul a fenntarthatósági célok eléréséhez is. Az olyan átfogó stratégiák, mint a Siemens DEGREE keretrendszere, bizonyítják, hogy a technológiai fejlődés kéz a kézben járhat a környezeti és társadalmi felelősségvállalással.

Személyes véleményem szerint a Siemens példája azt mutatja meg, hogyan valósulhat meg a digitális transzformáció a gyakorlatban, ha azt rendszerszintű gondolkodás, folyamatos innováció és fenntarthatósági elkötelezettség vezérli. Különösen inspirálónak tartom azt, ahogy a vállalat a mesterséges intelligencia és a digitális ikrek alkalmazásával képes proaktív módon reagálni az ipari kihívásokra, és olyan környezetet teremt, ahol az adatalapú döntéshozatal mindennapos gyakorlattá válik.

A dolgozat készítése során megerősödött bennem az a hit, hogy a jövő mérnökei,köztük én is kulcsszerepet játszanak majd abban, hogy az ipar technológiai újításaival összhangban egy fenntarthatóbb, hatékonyabb és emberközpontúbb világot hozzunk létre.

14 KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném kifejezni hálámat a Széchenyi István Egyetemnek, valamint különösen Hajdu Csaba Tanár Úrnak, hogy az Ipar 4.0 tantárgy keretein belül lehetőséget biztosított számomra az esszé elkészítésére.

15 IRODALOMJEGYZÉK

[1] M. Hermann, T. Pentek, and B. Otto, ‘Design Principles for Industrie 4.0 Scenarios’, in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Jan. 2016, pp. 3928–3937. doi: 10.1109/HICSS.2016.488.

[2] ‘Company development’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/company/about/history/company.html

[3] ‘siemens-enabling-continuous-improvement-solution-brief.pdf’. Accessed: Apr. 19, 2025. [Online]. Available: https://www.intel.de/content/dam/www/public/emea/de/de/images/photography/siemens-enabling-continuous-improvement-solution-brief.pdf

[4] ‘Siemens unveils breakthrough innovations in industrial AI and digi ...’ Accessed: Apr. 19, 2025. [Online]. Available: https://press.siemens.com/global/en/pressrelease/siemens-unveils-breakthrough-innovations-industrial-ai-and-digital-twin-technology-ces

[5] ‘How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective’, *World Acad. Sci. Eng. Technol. Int. J. Mech. Aerosp. Ind. Mechatron. Manuf. Eng.*, vol. 8, no. 1, pp. 37–44, Nov. 2014, doi: 10.5281/ZENODO.1336426.

[6] ‘SIMATIC S7-1500 - Take control of innovations’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500.html

[7] ‘simatic-st70-complete-english-2024.pdf’. Accessed: Apr. 19, 2025. [Online]. Available: https://cache.industry.siemens.com/dl/files/167/109744167/att_1289050/v1/simatic-st70-complete-english-2024.pdf

[8] ‘SIMATIC HMI operator control and monitoring systems’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/products/automation/simatic-hmi.html

[9] ‘Totally Integrated Automation Portal’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal-variant.html

[10] L. Yang, ‘Industry 4.0: A survey on technologies, applications and open research issues - PDF Free Download’, c.coek.info. Accessed: Apr. 19, 2025. [Online]. Available: https://c.coek.info/pdf-industry-40-a-survey-on-technologies-applications-and-open-research-issues-.html

[11] ‘Internet of Things | Starting the IoT Journey’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/products/financing/siemens-financial-insight-center/starting-the-iot-journey.html

[12] ‘PROFINET’, siemens.com Global Website. Accessed: Apr. 19, 2025. [Online]. Available: https://www.siemens.com/global/en/products/automation/industrial-communication/profinet.html

[13] ‘New Smart Condition Monitoring solution with IIoT sensors for indu ...’ Accessed: Apr. 19, 2025. [Online]. Available: https://press.siemens.com/global/en/pressrelease/new-smart-condition-monitoring-solution-iiot-sensors-industrial-plants

[14] ‘Insights Hub industrial IoT | Siemens Software’, Siemens Digital Industries Software. Accessed: Apr. 19, 2025. [Online]. Available: https://plm.sw.siemens.com/en-US/insights-hub/

[15] ‘Siemens launches Siemens Xcelerator – an open digital business p ...’ Accessed: Apr. 19, 2025. [Online]. Available: https://press.siemens.com/global/en/pressrelease/siemens-launches-siemens-xcelerator-open-digital-business-platform-accelerate-digital

[16] ‘Shaping digital transformation together’, Siemens Xcelerator. Accessed: Apr. 19, 2025. [Online]. Available: https://xcelerator.siemens.com/global/en/ecosystem.html

[17] M. Javaid, A. Haleem, and R. Suman, ‘Digital Twin applications toward Industry 4.0: A Review’, *Cogn. Robot.*, vol. 3, pp. 71–92, Jan. 2023, doi: 10.1016/j.cogr.2023.04.003.

[18] R. Ružarovský, ‘(PDF) A general take on a Tecnomatix Process Simulate´s Digital Twin creation and its exchange of information with the TIA Portal and PLC SIM Advanced’. Accessed: Apr. 19, 2025. [Online]. Available: https://www.researchgate.net/publication/359150067_A_general_take_on_a_Tecnomatix_Process_Simulates_Digital_Twin_creation_and_its_exchange_of_information_with_the_TIA_Portal_and_PLC_SIM_Advanced

[19] M. Lezzi, M. Lazoi, and A. Corallo, ‘Cybersecurity for Industry 4.0 in the current literature: A reference framework’, *Comput. Ind.*, vol. 103, pp. 97–110, Dec. 2018, doi: 10.1016/j.compind.2018.09.004.

[20] ‘Industrial cybersecurity for automotive manufacturing’, Automotive & Transportation. Accessed: Apr. 19, 2025. [Online]. Available: https://blogs.sw.siemens.com/automotive-transportation/2024/08/16/industrial-cybersecurity-for-automotive-manufacturing/

[21] B. van Giffen and H. Ludwig, ‘How Siemens Democratized Artificial Intelligence’, Mar. 01, 2023, *Social Science Research Network, Rochester, NY*: 4928166. doi: 10.2139/ssrn.4928166.
[22] L. Sunith Babu, J. Hemanth Kumar, B. Madhusudhan, V. Nitish Kumar, and R. Sujitha, ‘Application of Hyperautomation in Predictive Maintenance—A Technical Analysis’, in *Hyperautomation for Next-Generation Industries*, John Wiley & Sons, Ltd, 2024, pp. 299–323. doi: 10.1002/9781394186518.ch12.
[23] ‘TCOD-2024_original.pdf’. Accessed: Apr. 19, 2025. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:1b43afb5-2d07-47f7-9eb7-893fe7d0bc59/TCOD-2024_original.pdf
[24] ‘Using data visualization and AI quality control’, Siemens Digital Industries Software. Accessed: Apr. 19, 2025. [Online]. Available: https://webinars.sw.siemens.com/en-US/data-visualization-and-ai-quality-control-to-detect-defective-parts/
[25] P. R. Newswire, ‘Cybord Partners with Siemens Digital Industries Software - AI-Tech Park’. Accessed: Apr. 19, 2025. [Online]. Available: https://ai-techpark.com/cybord-partners-with-siemens-digital-industries-software/
[26] E. Zaye and O. Ogunyomi-Oluyomi, ‘Assessment of Supply Chain Sustainability Strategy on Sustainable Performance Indicators: Evidence from Siemens DEGREE Framework (2019-2023)’, *Int. J. Supply Chain Logist.*, vol. 9, no. 3, Art. no. 3, Feb. 2025, doi: 10.47941/ijscl.2553.
[27] ‘Siemens and BASF collaborate on driving circular economy’. Accessed: Apr. 19, 2025. [Online]. Available: https://www.basf.com/basf/www/global/en/media/news-releases/2024/06/p-24-215
[28] ‘Siemens-PLM-Smart-manufacturing-for-electronics-wp_tcm56-57766.pdf’. Accessed: Apr. 19, 2025. [Online]. Available: https://www.plm.automation.siemens.com/media/global/it/Siemens-PLM-Smart-manufacturing-for-electronics-wp_tcm56-57766.pdf?utm_source=chatgpt.com
[29] ‘Applying AI to industry part 2 - Thought Leadership’. Accessed: Apr. 19, 2025. [Online]. Available: https://blogs.sw.siemens.com/thought-leadership/2023/11/21/applying-ai-to-industry-part-2/

2.56. IOT ÉS OKOSGYÁRTÁS A GYÁRTÁSI FOLYAMATOKBAN

IPAR 4.0 TECHNOLÓGIÁK

IOT ÉS OKOSGYÁRTÁS A GYÁRTÁSI FOLYAMATOKBAN

HOGYAN FORMÁLJA ÁT AZ IOT A GYÁRTÁSI FOLYAMATOKAT?

KISS EDVÁRD

[redacted]

(GKNB_INTM087)
2024/2025/2

Tartalomjegyzék

1. Bevezetés *4*

2. Az IoT technológia alapjai *5*

2.1 Az IoT fogalma és felépítése 5

2.2 Tipikus ipari IoT-eszközök és szenzorok 6

2.3 Adatgyűjtés és -feldolgozás módszerei 7

3. Okosgyártás és az Ipar 4.0 ..... *8*

3.1 Az Ipar 4.0 fogalma és céljai 8

3.2 Az okosgyártás alapelvei 9

3.3 Az IoT szerepe az ipari digitalizációban 11

4. Az okosgyártás előnyei és alkalmazási területei *14*

4.1 Hatékonyságnövelés és átláthatóság 14

4.2 Prediktív karbantartás 15

4.3 Rugalmasság és gyors újraprogramozhatóság 15

4.4 Minőségellenőrzés és hibacsökkentés 15

4.5 Energiahatékonyság és fenntarthatóság 16

4.6 Alkalmazási területek különböző iparágakban 16

5. Az IoT és az okosgyártás kihívásai *16*

5.1 Magas kezdeti beruházási költségek 17

5.2 Adatbiztonsági és kiberfenyegetések 17

5.3 Szervezeti átalakulás és szakemberhiány 18

5.4 Adatmennyiség kezelése és rendszerek interoperabilitása 18

5.5 Folyamatos karbantartás és rendszerfrissítések 18

6. Esettanulmányok: iparági példák az IoT és az okosgyártás alkalmazására *19*

6.1 Autóipar: BMW – okosgyártási megoldások Regensburgban 19

6.2 Élelmiszeripar: Nestlé – gyártásmonitorozás és minőségbiztosítás 20

6.3 Logisztika és ellátásilánc-kezelés: Bosch – okos logisztikai központ 21

6.4 Kisvállalkozások: digitális átállás pilot programban – Arbot Mechatronikai Kft. 21

7. Az IoT és okosgyártás jövője és kihívásai *23*

7.1 Az IoT és okosgyártás jövője 23

7.2 Az IoT és okosgyártás kihívásai 23

8. Jövőbeli trendek és kilátások *23*
8.1 A digitalizáció fejlődési irányai a gyártásban.....24
8.2 IoT + mesterséges intelligencia = autonóm gyártás 24
8.3 A „lot size 1" koncepció – egyedi gyártás nagy tömegben.....25
8.4 A digitális ellátási lánc és a teljes gyár szintű szinkronizáció víziója 25
9. Összegzés és következtetések *25*
Felhasznált irodalom: *27*

1. Bevezetés

Ábra 1: Ipar 4.0 illusztráció

Az iparban zajló digitalizáció az elmúlt években jelentős átalakulást indított el, amelynek egyik legfontosabb iránya az úgynevezett ipar 4.0 koncepcióhoz kapcsolódik. Ennek keretében a hagyományos gyártási folyamatokat egyre inkább intelligens, hálózatba kötött rendszerek váltják fel, ahol a gépek, szenzorok és informatikai megoldások együttműködve segítik a termelés hatékonyabb és rugalmasabb lebonyolítását. Ennek az átalakulásnak az egyik kulcsfogalma az IoT, vagyis az Internet of Things (a dolgok internete), amely lehetővé teszi a fizikai eszközök és rendszerek folyamatos adatkommunikációját.

Az IoT és az okosgyártás (smart manufacturing) együtt egy új gyártási kultúrát képviselnek. Nem pusztán automatizálásról van szó, hanem olyan rendszerekről, amelyek képesek valós időben adatokat gyűjteni, értelmezni, majd ezek alapján döntéseket hozni vagy javaslatokat tenni a folyamatok optimalizálására. A cél nem csupán a gyorsabb termelés, hanem a minőség javítása, a hibák csökkentése, valamint a gyártás energia- és költséghatékonyságának növelése is.

A dolgozat célja az, hogy bemutassa, hogyan járul hozzá az IoT és az okosgyártás az ipari működés korszerűsítéséhez. Különösen fontos kérdés, hogy ezek a technológiák hogyan segítik elő a valós idejű döntéshozatalt, hogyan támogatják a prediktív karbantartást, és miként járulnak hozzá az erőforrások hatékonyabb felhasználásához. Bár a digitális átállás számos előnnyel jár, fontos beszélni a nehézségekről is: ilyen például a magas beruházási költség, az adatbiztonsági kihívások, vagy éppen az, hogy a munkavállalóknak újfajta kompetenciákat kell elsajátítaniuk.

A dolgozat során a technológiai alapfogalmak rövid ismertetése után konkrét iparági példákon keresztül kerül bemutatásra az IoT és az okosgyártás működése – ilyen például az autóipar vagy az elektronikai gyártás (pl. tévék gyártása). A cél nem elméleti túlmagyarázás, hanem annak megértése, hogyan néz ki ez a gyakorlatban, milyen eszközöket használnak, és mik az eredmények.

2. Az IoT technológia alapjai

2.1 Az IoT fogalma és felépítése

Az IoT (Internet of Things – a dolgok internete) egy olyan technológiai koncepció, amelynek lényege, hogy különféle fizikai eszközök – például szenzorok, gépek, járművek vagy akár teljes gyártósorok – hálózatba kapcsolva képesek egymással és központi rendszerekkel kommunikálni. Az eszközök adatokat gyűjtenek a környezetükről, majd ezeket az információkat továbbítják feldolgozásra, elemzésre, vagy akár automatikus beavatkozásra. Az így létrejövő rendszer alapja a folyamatos adatforgalom, ami lehetővé teszi a valós idejű visszacsatolást, optimalizálást és előrejelzést.

Egy ipari IoT-rendszer tipikusan három fő komponensből épül fel:

1. Érzékelők és beágyazott eszközök: ezek gyűjtik a fizikai világ adatait (pl. hőmérséklet, rezgés, nyomás, páratartalom stb.).
2. Adatkapcsolat: a mért adatok továbbításához szükség van valamilyen kommunikációs megoldásra – ilyen lehet például Wi-Fi, Bluetooth, mobilhálózat (4G/5G) vagy ipari szabványok (pl. OPC UA, MQTT).
3. Adatfeldolgozás és vezérlés: a beérkező adatokat központi szervereken vagy helyi eszközökön dolgozzák fel. Ebből lesznek információk, amelyeket döntéstámogatásra, automatikus szabályozásra vagy elemzésekre használnak.

Az ipari környezetben ez a hármas együttműködés alapozza meg a hatékony, digitálisan támogatott gyártási folyamatokat.

2.2 Tipikus ipari IoT-eszközök és szenzorok [1]

Az ipari IoT megoldásokban kulcsszerepet játszanak a különböző szenzorok és érzékelők, amelyek a fizikai világ változásait digitális jelekké alakítják. Ezek az adatok képezik az egész rendszer működésének alapját, hiszen ezekből „érti meg” a rendszer, hogy mi történik a gyártási környezetben.

Ábra 2: Szenzorok és alkalmazásuk a munkafolyamatokban

A leggyakrabban alkalmazott szenzortípusok közé tartoznak:

- Hőmérséklet-érzékelők: az optimális működési hőmérséklet biztosítása kulcsfontosságú például a gépek élettartamának meghosszabbításához vagy a termékminőség fenntartásához.
- Nyomásérzékelők: elsősorban folyadékokat vagy gázokat használó rendszerekben (pl. hidraulika, pneumatikus gépek) alkalmazzák.
- Rezgésérzékelők: a gépek állapotának figyelésére használják őket, például csapágyhibák vagy kiegyensúlyozatlanság előrejelzésére.
- Fény-, mozgás- és közelségérzékelők: ezek gyakran kapcsolódnak biztonsági vagy automatizálási rendszerekhez.
- Áramlásmérők, páratartalom-érzékelők, energiafogyasztás-mérők: specializáltabb alkalmazásokra szolgálnak, például környezeti feltételek ellenőrzésére vagy energiahatékonyság figyelésére.

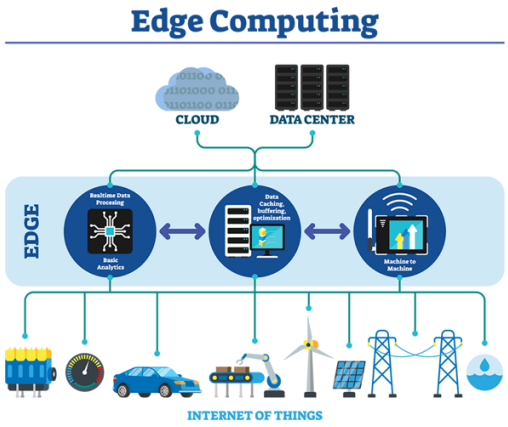
Ezeket az eszközöket sokszor edge-eszközökkel kombinálva alkalmazzák, amelyek a helyszínen képesek adatokat előfeldolgozni és csak a lényegi információkat továbbítani.

2.3 Adatgyűjtés és -feldolgozás módszerei

Az IoT-rendszerek egyik legnagyobb előnye, hogy az adatokat valós időben tudják begyűjteni, elemezni és felhasználni a működés javítására. Ehhez különböző adatfeldolgozási modellek használatosak, amelyek közül a két legfontosabb:

Edge computing [2]

Az edge computing lényege, hogy az adatfeldolgozás nem központilag, hanem helyben, közvetlenül az eszköz vagy a gyártósor közelében történik. Ez csökkenti az adatok továbbításához szükséges időt és sávszélességet, valamint csökkenti a késleltetést. Például, ha egy gép meghibásodás előtt túlzott rezgéseket mutat, az edge-eszköz ezt azonnal érzékeli, és akár automatikusan megállíthatja a gépet, még mielőtt komolyabb kár keletkezne.

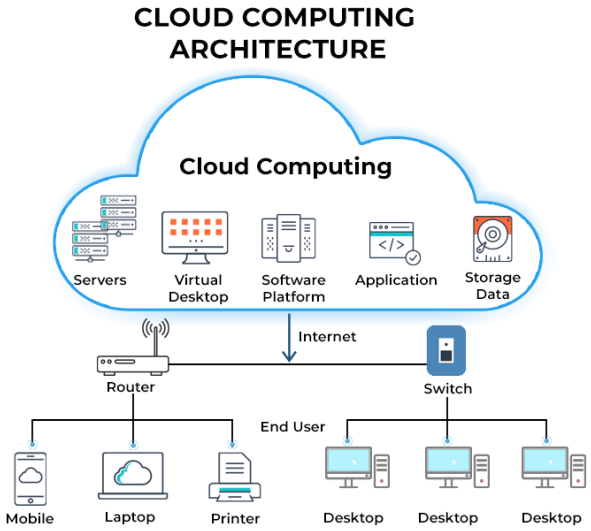


Ábra 3: Edge Computing működése

Cloud computing [3]

A felhőalapú megoldások lehetővé teszik, hogy a nagy mennyiségű adatot távoli szervereken tárolják és dolgozzák fel. Ez különösen akkor hasznos, ha hosszú távú elemzéseket, trendfigyelést vagy gépi tanuláson alapuló előrejelzést (pl. prediktív karbantartás) szeretnénk alkalmazni. A felhő előnye, hogy könnyen skálázható és hozzáférést biztosít a vállalat több részlege vagy telephelye számára.

A legtöbb ipari rendszer hibrid megoldást alkalmaz: az egyszerű, azonnali reakciókat edge-szinten kezelik, míg a hosszabb távú stratégiai döntésekhez szükséges elemzések a felhőben történnek.



Ábra 4: Cloud computing működési ábra

3. Okosgyártás és az Ipar 4.0 [6]

3.1 Az Ipar 4.0 fogalma és céljai

Az Ipar 4.0 (vagy negyedik ipari forradalom) az ipari termelés digitális átalakulását jelöli, amely az információs technológia, az automatizálás és az adatelemzés integrációján alapul. A cél nem pusztán az automatizálás, hanem a rendszerek intelligens összekapcsolása és önoptimalizálása.

A Fraunhofer Intézet meghatározása szerint az Ipar 4.0 a „kiber-fizikai rendszerek és az internet technológiáinak kombinációja az értékteremtési lánc minden pontján” (Kagermann et al., 2013).

3.2 Az okosgyártás alapelvei

Az okosgyártás – angolul *smart manufacturing* – lényege, hogy a gyártási folyamatokat adatvezérelt módon, valós időben megfigyelhetően és irányíthatóan működteti. Ez a szemlélet túlmutat a hagyományos automatizáláson: nemcsak arról szól, hogy gépek végeznek el bizonyos feladatokat ember helyett, hanem arról is, hogy a gyártórendszerek kommunikálnak egymással, adatokat osztanak meg, és ezek alapján képesek önálló döntéseket hozni vagy ajánlásokat tenni az operátoroknak.

Az okosgyártás működésének alapját az IoT-eszközökkel felszerelt gyártási infrastruktúra adja, ahol a különféle szenzorok, gépek, robotok, emberek és szoftverek mind hálózatba kapcsolva dolgoznak egy közös cél – az optimalizált termelés – érdekében.

Valós idejű adatelemzés és visszacsatolás

Az egyik legfontosabb jellemző, hogy a rendszer folyamatosan figyeli önmagát. A szenzorok valós idejű adatokat gyűjtenek (pl. hőmérséklet, nyomás, rezgés, energiafogyasztás), amelyeket elemző rendszerek dolgoznak fel – vagy helyben, ún. *edge computing* segítségével, vagy a felhőben. Ezek az adatok alapján a rendszer észlelhet például egy gép kopását vagy egy szokatlan működési mintát, és jelzést küldhet még azelőtt, hogy valódi meghibásodás történne.

Például egy gyártósoron működő CNC-gép rezgésmintázata eltér a megszokottól – az adatfeldolgozó algoritmus azonnal figyelmezteti a karbantartót, aki még időben be tud avatkozni. Ez az ún. prediktív karbantartás egyik tipikus esete.

Rugalmasság és skálázhatóság

Az okosgyártás másik fontos elve a rugalmasság: a rendszereknek gyorsan kell alkalmazkodniuk a termékváltoztatásokhoz, egyedi megrendelésekhez vagy piaci igényekhez. A gyártási paraméterek – például a soron következő termék mérete, színe, vagy akár az összeszerelési sorrend – digitálisan módosíthatók, sokszor emberi beavatkozás nélkül.

Ez különösen fontos a „mass customization” modellnél, ahol a tömegtermelés hatékonyságát egyesítik az egyedi termékek kínálatával. Például egy autógyártó ugyanazon gyártósoron állít elő többféle modellt vagy egyedi felszereltséggel ellátott járműveket – mindezt szoftveres vezérléssel, minimális gépátállási idővel.

Átláthatóság és integráció

Az okosgyártásban minden gép, rendszer és folyamat egy közös, integrált digitális platformon keresztül figyelhető és irányítható. Ennek az átláthatóságnak köszönhetően a vezetők és mérnökök pontos képet kapnak a termelés aktuális állapotáról: hány darab készült el, mennyi az állásidő, melyik szakaszon van torlódás, stb.

Ezt a célt szolgálják az ún. Manufacturing Execution System (MES) rendszerek, amelyek összekötik a fizikai gyártósort a vállalati szoftverekkel (pl. ERP – vállalatirányítási rendszer). Így az információ nem „szigetszerűen” tárolódik, hanem egységes adatáramlás valósul meg a gyár egészében.

Minőség és folyamatos fejlesztés

Az okosgyártás nemcsak a mennyiséget célozza, hanem a minőség biztosítását és javítását is. A digitális rendszerek képesek a gyártási folyamat közben – nem csak utólag – észlelni a hibákat. Egy AI-alapú kamerarendszer például felismeri, ha egy alkatrész hibásan lett összeszerelve vagy eltér a szabványos mérettől. A hiba azonnal kijelzésre kerül, így a selejt aránya csökken, a visszahívások valószínűsége pedig minimálisra mérsékelhető.

Emellett a folyamatosan gyűjtött adatok alapján a mérnökök és adatkutatók elemzéseket végezhetnek, és adatalapú döntéseket hozhatnak a gyártási folyamatok fejlesztésére – például a gépek optimális beállításáról, a nyersanyagok felhasználásának hatékonyságáról, vagy a logisztika újraszervezéséről.

Ábra 5: AI alapú kamerák

3.3 Az IoT szerepe az ipari digitalizációban

Az ipari digitalizáció egyik legfontosabb hajtóereje az Internet of Things (IoT), amely lehetővé teszi a fizikai gyártási eszközök, szenzorok, gépek és informatikai rendszerek közötti valós idejű, automatizált adatcserét. Az IoT segítségével az ipari környezet „láthatóvá" válik: minden eszköz és folyamat adatot termel, és ezek az adatok visszacsatolhatóak a döntéshozatalba – automatizált módon vagy emberi beavatkozással.

Miért kulcsfontosságú az IoT a gyártásban?

A hagyományos gyártási környezetekben az információk gyakran késve vagy hiányosan jutnak el az érintettekhez. Az IoT ezt a problémát oldja fel azáltal, hogy minden gyártási eseményt, gépállapotot vagy folyamatparamétert digitálisan nyomon követ, és az adatokat valós időben továbbítja a megfelelő helyekre – legyen az egy gyártósori kijelző, egy MES rendszer, vagy egy felhőalapú elemzőplatform.

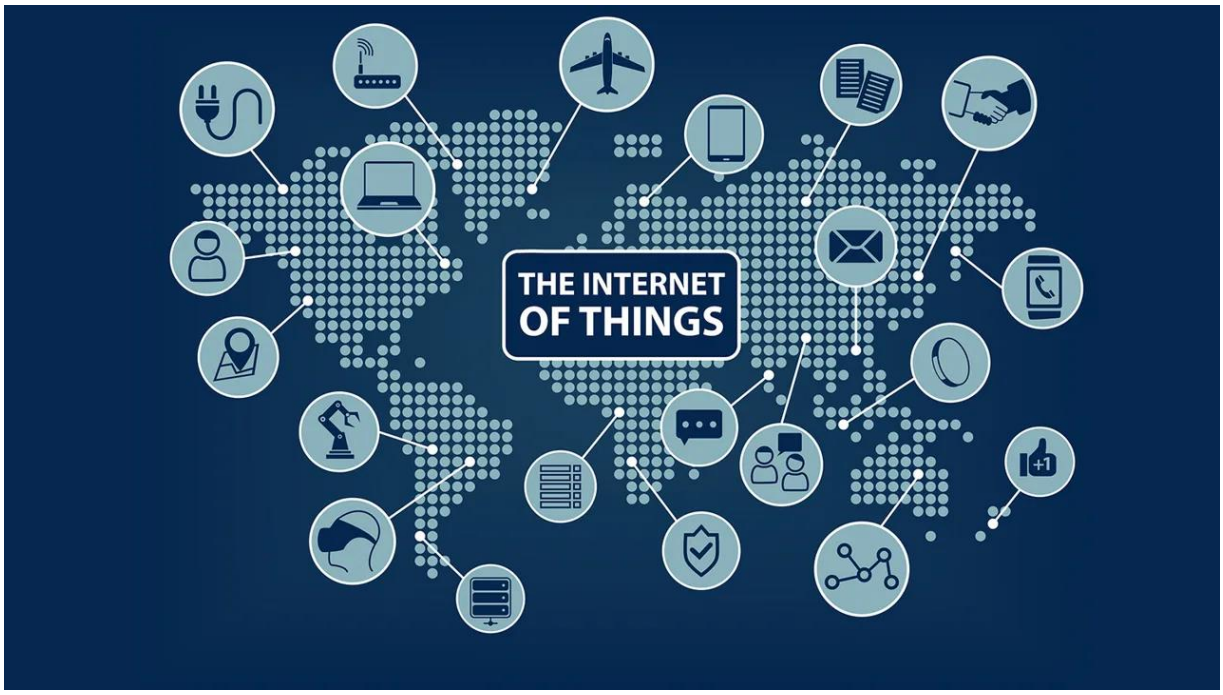
Ez a valós idejű kapcsolat lehetőséget ad:

- a gyártási folyamatok finomhangolására (pl. paraméterek automatikus módosítása szenzoradatok alapján),
- a karbantartási igények előrejelzésére,
- az energiafogyasztás optimalizálására,
- és a minőségellenőrzés automatizálására.

Az IoT és az adatáramlás [10]

Az IoT-eszközök által gyűjtött adatok útja a gyártási környezetben jellemzően több lépésen keresztül halad. Először a peremhálózaton (edge) történik előfeldolgozás, ahol például egy gépbe beépített érzékelő előre beprogramozott szabályok alapján értékeli az adatokat. Ha rendellenesség történik (pl. egy motor hőmérséklete átlépi a küszöbértéket), azonnali jelzést küld vagy leállítja a működést.

Ezek az adatok továbbhaladhatnak lokális szerverekre vagy felhőalapú rendszerekbe, ahol összetettebb elemzés történik – például trendfigyelés, gépi tanulás, vagy prediktív karbantartás előrejelzése. A rendszer ezután visszacsatolja az eredményeket a gyártási folyamatba: például egy gép automatikusan lassíthatja a működését, ha közeledik a túlterhelés határához.



Ábra 6: Internet of things illusztráció

IoT-integráció különböző rendszerekkel

Az IoT valódi ereje akkor mutatkozik meg, amikor integrált módon kapcsolódik más digitális rendszerekhez:

- MES rendszerekhez, amelyek irányítják és követik a gyártási folyamatokat;
- ERP rendszerekhez, amelyek a vállalati szintű erőforrás-tervezést és készletgazdálkodást végzik;
- digitális ikrekhez, amelyek modellezik a gyártási berendezéseket és szimulációkat futtatnak a működésről.

Ábra 7: ERP és MES vállalatirányítási rendszerek

Ez az integráció lehetővé teszi, hogy egy gép működési adatai azonnal befolyásolják a termelési tervet, az alapanyag-beszerzést vagy akár az ügyfél értesítését a szállítási idő változásáról. Az egész értéklánc agilisebbé és előreláthatóbbá válik.

Iparágak, ahol különösen erős az IoT jelenléte

Az IoT nem mindenhol ugyanolyan mértékben hasznosul, de vannak olyan iparágak, ahol a technológia kulcsszereplő:

- Autóipar – Az autógyárakban több ezer érzékelő működik egyszerre, valós időben monitorozva a gépek és szerelőrobotok működését. Emellett a beszállítói lánc is IoT-alapon optimalizálható.
- Élelmiszeripar – Itt a hőmérséklet- és páratartalom-érzékelők segítenek a szigorú előírások betartásában, és az egyes gyártási lépések pontos dokumentálásában.
- Elektronikai gyártás – Az alkatrészek pontos pozícionálása és a minőségellenőrzés is IoT-alapú képfeldolgozó rendszerekkel történik.

A digitalizáció előnyei számokban

- Egy 2023-as *McKinsey & Company* tanulmány szerint azok a gyártóvállalatok, amelyek teljes körű IoT-rendszereket vezettek be, átlagosan:
- 15–25%-kal növelték a termelékenységüket,
- 30%-kal csökkentették az állásidőket,
- és 20%-kal alacsonyabb energiaköltséget értek el a gyártás során.

4. Az okosgyártás előnyei és alkalmazási területei

4.1 Hatékonyságnövelés és átláthatóság

Az okosgyártás egyik legfontosabb előnye a gyártási folyamatok átláthatóságának javítása. Az IoT-eszközök és a digitális rendszerek lehetővé teszik, hogy a gyártási lépések valós időben nyomon követhetők legyenek. Az adatok folyamatos gyűjtése és megjelenítése révén gyorsabban észlelhetők az eltérések, hibák vagy gyenge pontok, így időben lehet beavatkozni.

A folyamatos adatáramlás segíti a vezetőket és mérnököket abban, hogy objektív adatok alapján hozzanak döntéseket, és ne utólag, hanem már a problémák kialakulásakor reagáljanak. Ez a működés nemcsak hatékonyabb, hanem biztonságosabb is, mivel kevesebb hibalehetőséget hordoz.

4.2 Prediktív karbantartás [4]

Az adatalapú karbantartás az egyik leggyakrabban emlegetett gyakorlati előnye az okosgyártásnak. Míg korábban a gépeket rendszeres időközönként ellenőrizték, az IoT-rendszerek képesek előre jelezni, ha egy berendezés hamarosan meghibásodhat. Ezt olyan szenzorok segítik, amelyek a rezgés, hőmérséklet vagy áramerősség alapján érzékelik az eltéréseket.

A prediktív karbantartás révén csökkenthető a nem tervezett leállások száma, és optimalizálható a karbantartási idő. Egyes tanulmányok szerint ezekkel a megoldásokkal akár 10–20 százalékkal is növelhető a gépek rendelkezésre állása. Ez nemcsak termelési szempontból jelent előnyt, hanem gazdaságilag is, hiszen kevesebb veszteséget jelent a leállás.

4.3 Rugalmasság és gyors újraprogramozhatóság

Az okosgyártási rendszerek jelentős rugalmasságot biztosítanak a termelés során. A digitális vezérlésű gépek és berendezések könnyen átállíthatók különféle termékek vagy gyártási mennyiségek előállítására. Ez a képesség különösen előnyös a piaci igényekhez való gyors alkalmazkodásban, például egyedi megrendelések esetén vagy szezonális termékek gyártásakor.

A hagyományos gyártósorokkal ellentétben az okosrendszerek újraprogramozása nem igényel hosszabb leállást vagy jelentős fizikai átalakítást. A digitális szoftveres környezetben a változások gyorsan végrehajthatók, így a vállalatok versenyelőnyhöz jutnak a gyors reakcióképesség révén.

4.4 Minőségellenőrzés és hibacsökkentés

Az automatizált minőségellenőrzés az egyik leggyakoribb alkalmazása az okosgyártásnak. Az érzékelők és a gépi látás rendszerek már a gyártás közben képesek felismerni a hibákat. A hibás darabokat így nemcsak utólag, hanem azonnal kiszűrik, ami jelentősen csökkenti a selejtarányt.

Ez a fajta ellenőrzés nemcsak hatékonyabb, hanem pontosabb is, mint az emberi vizsgálat. A hibacsökkentés eredményeként a gyártási folyamat megbízhatóbbá válik, ami különösen fontos az olyan iparágakban, mint az autóipar vagy a gyógyszergyártás, ahol a termékbiztonság alapkövetelmény.

4.5 Energiahatékonyság és fenntarthatóság

Az okosgyártás segítségével a vállalatok jobban átláthatják és optimalizálhatják az energiafelhasználásukat. Az IoT-eszközök részletes adatokat szolgáltatnak arról, hogy mikor, hol és mely gépek mennyi energiát fogyasztanak. Ezek alapján könnyen beazonosíthatók a pazarló működések, és célzott beavatkozásokkal csökkenthető az energiafelhasználás.

Ez nemcsak költségmegtakarítást jelent, hanem hozzájárul a fenntarthatóbb működéshez is. A környezeti szempontok ma már fontosak a vevők és a szabályozók számára is, így az energiahatékony gyártás reputációs előnyökkel is jár.

4.6 Alkalmazási területek különböző iparágakban

Az okosgyártás előnyei nem egyformán jelennek meg minden iparágban, de szinte mindenhol találhatók olyan folyamatok, amelyeken keresztül hasznot húznak a digitalizációból:

- Az autóiparban a logisztikai rendszerek és a beszállítói láncok szoros integrációja révén csökkenthető a raktárkészlet és pontosítható a gyártási időzítés.
- A gyógyszeriparban az érzékeny gyártási környezet folyamatos ellenőrzése biztosítja a minőséget és az előírásoknak való megfelelést.
- Az élelmiszeriparban a hőmérséklet és páratartalom szabályozása révén csökken a romlás kockázata és nő az élelmiszerbiztonság.
- A gépgyártás területén az egyedi termékek gyors átállásait és gyártását teszik lehetővé az újraprogramozható gyártósorok.

Ezek az alkalmazások jól mutatják, hogy az okosgyártás nemcsak a termelékenységet, hanem a minőséget, biztonságot és környezeti hatásokat is pozitívan befolyásolja.

5. Az IoT és az okosgyártás kihívásai

Bár az IoT-alapú rendszerek és az okosgyártás számos előnyt kínálnak a gyártás hatékonyságának, rugalmasságának és fenntarthatóságának növelése terén, a bevezetésük és működtetésük viszont nem zökkenőmentes. A technológiai, gazdasági és szervezeti szintű kihívások jelentős befolyással bírnak arra, hogy egy vállalat mennyire tudja sikeresen alkalmazni ezeket a megoldásokat.

5.1 Magas kezdeti beruházási költségek

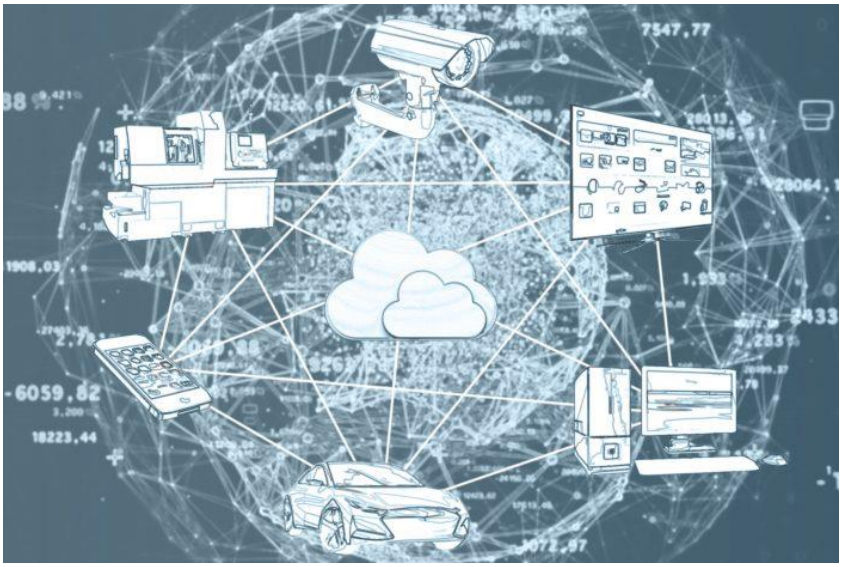
Az IoT-rendszerek bevezetése jelentős kezdeti beruházást igényel, különösen a hagyományos gyártási környezetek esetében. Az új érzékelők, adatgyűjtő rendszerek, hálózati infrastruktúra, felhőalapú megoldások és szoftveres vezérlőrendszerek kiépítése komoly anyagi ráfordítást követel.

Sok kis- és középvállalkozás számára ez az akadály önmagában elriasztó lehet, különösen akkor, ha a beruházás megtérülését (ROI) nem tudják rövid távon biztosítani. Emellett a meglévő gyártóberendezések digitalizálása is külön költségekkel jár, ha azok nem rendelkeznek integrálható vezérlőegységekkel.

5.2 Adatbiztonsági és kiberfenyegetések

Az IoT-rendszerek által generált és továbbított adatok érzékeny információkat tartalmazhatnak a gyártási folyamatokról, terméktervekről vagy ellátási láncokról. Ezen rendszerek internetre kapcsoltsága ugyan megkönnyíti az adatáramlást, de egyúttal új kockázatokat is létrehoz: a kibertámadások, adatszivárgások vagy rendszerszintű zsarolóprogramok jelentős veszélyt jelentenek.

A gyártócégeknek olyan védelmi megoldásokat kell alkalmazniuk, mint a tűzfalak, titkosított adatkapcsolatok, behatolásérzékelő rendszerek (IDS/IPS) vagy a



Ábra 8: Adatbiztonsági és kiberfenyegetések elleni védelem

végpontvédelmi eszközök. Ezen túlmenően a munkavállalók digitális tudatosságának növelése is alapvető, hiszen sok támadás emberi hibából ered.

5.3 Szervezeti átalakulás és szakemberhiány

Az IoT és az okosgyártás nemcsak technológiai, hanem kulturális és szervezeti változást is igényel. A gyártás hagyományosan hierarchikus és stabil rendszerekre épül, míg a digitalizált gyártás gyors alkalmazkodást és adatvezérelt döntéshozatalt követel. Ez sok esetben ellenállást vált ki a dolgozókból, különösen akkor, ha nem világos számukra a változás értelme vagy előnye.

További kihívást jelent a szakképzett munkaerő hiánya. A digitális rendszerek működtetéséhez és karbantartásához új kompetenciákra van szükség – például adatértékelés, szoftverhasználat, vagy hálózati ismeretek –, amelyekkel sok jelenlegi munkavállaló még nem rendelkezik. Az átképzés hosszú távon megoldást jelenthet, de rövid távon ez lassíthatja az átállást.

5.4 Adatmennyiség kezelése és rendszerek interoperabilitása

Az IoT-eszközök működésük során hatalmas mennyiségű adatot generálnak. Ezek strukturált és strukturálatlan formában is érkeznek, különféle formátumokban, gyakran valós időben. Ezt az adathalmazt nemcsak tárolni, hanem értelmezni és hasznosítani is kell.

Problémát okozhat továbbá, ha a gyártósorokon használt rendszerek nem kompatibilisek egymással. Különböző gyártók eszközei nem mindig képesek zökkenőmentesen együttműködni, és a szabványosítás hiánya miatt a rendszerintegráció bonyolulttá válhat. Az interoperabilitási problémák gátolhatják a zökkenőmentes adatáramlást és csökkenthetik a rendszer megbízhatóságát.

5.5 Folyamatos karbantartás és rendszerfrissítések

Bár az okosgyártás célja a gyártás optimalizálása, maga a rendszer is folyamatos figyelmet igényel. Az IoT-eszközök firmware-jeit, a szoftvereket, valamint a hálózati kapcsolatokat rendszeresen frissíteni kell, hogy megőrizzék a funkcionalitásukat és a biztonságukat.

A frissítések elmaradása nemcsak a teljesítmény csökkenéséhez, hanem biztonsági rések kialakulásához is vezethet. Az IT és az OT (Operational Technology) területek közötti együttműködés nélkülözhetetlen a rendszerek hosszú távú fenntarthatóságához.

6. Esettanulmányok: iparági példák az IoT és az okosgyártás alkalmazására

Az IoT-alapú rendszerek és az okosgyártás nem csupán elméleti lehetőségek, hanem számos iparágban már bevált gyakorlatként működnek. Az alábbi esettanulmányok arra szolgálnak, hogy konkrét példákon keresztül mutassák be, hogyan néz ki ezeknek a technológiáknak a valós alkalmazása különböző gyártási környezetekben.

6.1 Autóipar: BMW – okosgyártási megoldások Regensburgban

A BMW regensburgi gyára egyike azoknak az európai létesítményeknek, ahol az okosgyártás több szinten is működik. A gyárban több ezer érzékelő figyeli a gépek állapotát és a gyártási folyamat paramétereit. A rendszer valós időben figyeli a gyártósorokat, az adatok feldolgozása edge computing segítségével történik, így a hibákat azonnal ki lehet szűrni.

Ábra 9: Ipari szenzorok alkalmazás közben

Az egyik bevezetett megoldás a prediktív karbantartás, amely érzékelők segítségével előre jelzi, ha egy robotkar szervizelésre szorul. Ez csökkenti a nem tervezett leállások számát, és a termelés megbízhatóbban zajlik. A BMW ezen kívül digitális iker technológiát is használ: minden gyártott autó egy virtuális másolatot is kap, amely alapján visszakereshető minden folyamat, amelyen keresztülment.

6.2 Élelmiszeripar: Nestlé – gyártásmonitorozás és minőségbiztosítás

A Nestlé Svájcban és Franciaországban több gyáregységében is alkalmaz IoT-megoldásokat a minőségellenőrzés és az élelmiszer-biztonság növelése érdekében. A gyártósorokon szenzorok mérik a hőmérsékletet, páratartalmat, és más környezeti tényezőket, amelyek befolyásolják az élelmiszer minőségét.

Ábra 10: Mesterséges intelligencia alapú minőségellenőrzés

Ezeket az adatokat automatikusan továbbítják egy központi felügyeleti rendszerbe, amely képes időben riasztani, ha valamelyik paraméter eléri a határértéket. A gyártás során begyűjtött adatok hosszú távú tárolása lehetővé teszi a visszakereshetőséget és a szabályozási előírások betartását is. A Nestlé ezzel jelentősen csökkentette az emberi hibából eredő selejtarányt és javította az energiafelhasználás hatékonyságát is.

6.3 Logisztika és ellátásilánc-kezelés: Bosch – okos logisztikai központ

A Bosch németországi logisztikai központjában az IoT-eszközök nemcsak a gyártásban, hanem a raktározás és a szállítás területén is fontos szerepet játszanak. A cég RFID-alapú nyomon követési rendszert vezetett be, amely lehetővé teszi, hogy minden árucikk pontosan követhető legyen a teljes ellátási láncban. (lásd Ábra 3.)

Ábra 11: Bosch Rexroth RFID ID 15 rendszer a TS 2plus szállítópálya-rendszeren

Az automatizált rendszerek képesek előre jelezni, mikor melyik alkatrész érkezik meg, és melyik raktári polcon kell elhelyezni. Emellett mesterséges intelligenciával támogatott rendszerek segítenek a logisztikai folyamatok optimalizálásában: például az árumozgások előrejelzésében, útvonaltervezésben, vagy raktárkapacitás-elosztásban.

6.4 Kisvállalkozások: digitális átállás pilot programban – Arbot Mechatronikai Kft.

A nemesvámosi székhelyű Arbot Mechatronikai Kft**.** a hazai KKV-ipari digitalizációs mintaprogram keretében sikeresen valósított meg egy innovatív intralogisztikai fejlesztést. A projekt során egy 5G-kompatibilis, autonóm mobil robotplatformo**t** vezettek be, amely a gyártócsarnokon belüli belső anyagmozgatási feladatokat látja el.

A robot képes önállóan szállítani a félkész termékeket, göngyölegeket és egyéb anyagokat a különböző munkaállomások között, miközben valós időben kommunikál a gyártási

rendszerrel. A rendszer nem igényel előre telepített mágnescsíkokat vagy egyéb fizikai vezetősávokat, így rugalmasan alkalmazkodik a gyártási környezet változásaihoz.

Ábra 12: FANUC robotok

A megoldás bevezetésének eredményeként a vállalat jelentős mértékben csökkentette a manuális anyagmozgatásból adódó időveszteségeket és hibalehetőségeket. Emellett a robot működéséről származó adatok elemzése révén optimalizálták a belső logisztikai folyamatokat, növelve ezzel a termelékenységet és a munkavállalók hatékonyságát.

Ez az esettanulmány jól példázza, hogy a kis- és középvállalkozások számára is elérhetőek az ipar 4.0 megoldások, amelyek révén versenyképesebbé válhatnak a hazai és nemzetközi piacon.

7. Az IoT és okosgyártás jövője és kihívásai

7.1 Az IoT és okosgyártás jövője

- **Technológiai fejlődés és integráció:** Az IoT rendszerek és okosgyártási megoldások egyre fejlettebbé válnak, egyre szorosabb kapcsolat alakul ki a mesterséges intelligencia és a gépi tanulás között. Ez elősegíti a prediktív karbantartás és automatizált minőségellenőrzés továbbfejlesztését, valamint a termelés rugalmasságának növelését.
- **Valós idejű adatelemzés és döntéstámogatás:** A gyártási adatok valós idejű elemzése és feldolgozása lehetővé teszi a gyorsabb és pontosabb döntéshozatalt. Ez segíti a gyártókat abban, hogy gyorsan reagáljanak a piaci igényekre, és jobban alkalmazkodjanak a változó körülményekhez.
- **Szabványosítás és interoperabilitás fejlődése:** A globális ellátási láncok bővülése miatt egyre fontosabb lesz a különböző rendszerek közötti kompatibilitás és a szabványosítás, amely megkönnyíti az adatmegosztást és az együttműködést különböző gyártók között.

7.2 Az IoT és okosgyártás kihívásai [9]

- **Adatbiztonság és adatvédelem:** A digitalizációval együtt nő a kibertámadások veszélye, ezért kiemelt figyelmet kell fordítani a megfelelő biztonsági intézkedésekre, hogy megvédjék az érzékeny gyártási adatokat.
- **Munkaerő-átalakítás és képzés:** Az új technológiák alkalmazása új szakértelmeket követel, ezért elengedhetetlen a munkaerő folyamatos képzése és átképzése. Ez a vállalatok és oktatási intézmények közötti együttműködést is igényli, hogy a dolgozók alkalmazkodni tudjanak az új igényekhez.
- **Technológiai komplexitás és beruházási költségek:** Az okosgyártás rendszereinek bevezetése jelentős kezdeti beruházást és technológiai komplexitást jelenthet, ami kisebb vállalkozások számára nehézséget okozhat a rendszerbe állításban és fenntartásban.

8. Jövőbeli trendek és kilátások

A gyártás digitalizációja az elmúlt évtizedben olyan mélyreható változásokat indított el, amelyek az ipar jövőjét alapjaiban határozzák meg. Az IoT-technológia, a mesterséges intelligencia (MI), a gépi tanulás, a felhőalapú megoldások, valamint az adatelemzés együttesen olyan új trendeket eredményeznek, amelyek túlmutatnak a puszta automatizáláson. A cél immár nem csupán az, hogy a gépek hatékonyabban működjenek, hanem hogy az egész gyártási ökoszisztéma valós időben tanuljon, alkalmazkodjon és önálló döntéseket hozzon.

8.1 A digitalizáció fejlődési irányai a gyártásban

A gyártás digitalizációja ma már nem csupán szoftveres fejlesztéseket jelent, hanem egy komplex, hálózatba kapcsolt rendszer kiépítését, ahol minden fizikai eszköz (gépek, szenzorok, robotok) digitális jelekké alakítja a működését. Ezek az adatok valós időben kerülnek feldolgozásra, és visszacsatolással irányítják a termelést.

A jövő gyáraiban a gyártási folyamat minden lépése digitalizálva lesz, az anyagmozgatástól kezdve a minőségellenőrzésen át egészen a kiszállításig. Az olyan technológiák, mint az edge computing (helyi adatfeldolgozás), a felhőalapú platformok és az ipari 5G hálózatok még nagyobb adatátviteli sebességet és megbízható kapcsolatot biztosítanak.

Ezek a fejlesztések abba az irányba mutatnak, hogy a jövő gyártási rendszerei rugalmasabbak, adaptívabbak és energiatakarékosabbak lesznek. A fenntarthatóság és környezetterhelés csökkentése szintén kiemelt irány, amelyben az adatalapú optimalizálás (pl. energiafogyasztás csökkentése) kulcsszerepet kap.

8.2 IoT + mesterséges intelligencia = autonóm gyártás

Az ipari IoT-rendszerek egyik legnagyobb lehetősége, hogy a begyűjtött adatokból mesterséges intelligencia segítségével automatizált döntéshozatal valósulhat meg. A gépek nem csupán adatokat továbbítanak, hanem ezek alapján önálló működésre is képessé válnak. Ezt nevezzük autonóm gyártásnak.

A gépi látás, a hangalapú vezérlés, az MI-alapú hibafelismerés vagy az automatikus karbantartási értesítések mind ebbe az irányba mutatnak. Egy példa erre a Bosch által fejlesztett prediktív karbantartási rendszer, ahol a szenzoradatok alapján a gyártógépek előre "megérzik", ha karbantartásra van szükség, és emberi beavatkozás nélkül képesek jelezni ezt az üzemeltetésnek.

Az autonóm rendszerek lehetővé teszik, hogy a gyártási folyamatok még kisebb állásidővel, gyorsabb reakcióidővel és kevesebb hibával működjenek, miközben az emberi munkavállalók a felügyeleti, elemző és döntéshozói szerepkörökbe lépnek elő.

8.3 A „lot size 1” koncepció – egyedi gyártás nagy tömegben [7]

A tömegtermelés világában korábban elképzelhetetlen volt, hogy minden egyes termék személyre szabott legyen, és mégis költséghatékonyan készüljön. A „lot size 1” koncepció – vagyis az egyedi termékek tömegszerű gyártása – ezt a paradigmát írja felül.

Az okosgyártás lehetővé teszi, hogy ugyanaz a gyártósor akár minden ciklusban más terméket állítson elő, anélkül, hogy jelentős átszervezésre lenne szükség. A digitális ikerpárok, az adaptív gyártósorok, a robotkarok dinamikus programozhatósága és az MI által támogatott gyártástervezés mind hozzájárulnak a testreszabott termékek gyors előállításához.

Erre jó példa a Siemens ambergi gyára, ahol naponta több mint 1000 féle terméket állítanak elő ugyanazon a gyártósoron. Mindez automatizált logisztikával, intelligens raktárral és önvezető szállítóegységekkel történik, így a „lot size 1” modell már nem csak koncepció, hanem valóság.

8.4 A digitális ellátási lánc és a teljes gyár szintű szinkronizáció víziója [8]

A digitalizáció egyik hosszú távú célja, hogy ne csak az egyes gyárak váljanak okossá, hanem az egész ellátási lánc is. Ez azt jelenti, hogy a beszállítók, alvállalkozók, logisztikai partnerek és gyártók valós időben összehangoltan működnek.

A digitális ellátási lánc képes valós idejű adatok alapján reagálni a kereslet ingadozásaira, előrejelezni a nyersanyaghiányokat, vagy optimalizálni a készletezést és szállítást. Az MI-alapú ellátási láncok már képesek felismerni, ha egy szállítmány késik, és automatikusan módosítják a gyártási ütemtervet vagy új beszállítót javasolnak.

A végső cél a szinkronizált, önszerveződő gyártási ökoszisztéma, ahol minden szereplő – az alapanyaggyártótól a végső fogyasztóig – egyetlen digitális hálózat részeként működik. Ez nemcsak hatékonyságnövelést eredményez, hanem növeli az átláthatóságot, biztonságot és fenntarthatóságot is.

9. Összegzés és következtetések

A dolgozat célja az volt, hogy átfogó képet adjon arról, hogyan változtatja meg az IoT és az okosgyártás a gyártási folyamatokat. Az elméleti háttér és a gyakorlati példák segítségével jobban megérthetővé vált, hogy ezek a technológiák nemcsak kiegészítik a hagyományos ipari rendszereket, hanem alapvetően újragondolják azok működését. A

hangsúly egyre inkább a rugalmas, adatvezérelt, valós idejű döntéshozatalt lehetővé tévő rendszereken van.

Az IoT-eszközök, szenzorok és adatfeldolgozási módszerek beépítése a gyártásba jelentős előnyökkel jár. Lehetővé válik a prediktív karbantartás, a gyártás optimalizálása és az energiahatékonyság javítása. A konkrét példák – mint a Bosch RFID-alapú követőrendszere vagy a Fanuc prediktív karbantartási rendszere – jól mutatják, hogy ezek a technológiák már ma is kézzelfogható eredményeket hoznak.

A sikeres bevezetéshez viszont több feltétel is szükséges. Megfelelő infrastruktúrára van szükség, például gyors adatátviteli hálózatokra, megbízható szenzorokra és modern IT-rendszerekre. Fontos szempont az is, hogy a munkavállalók fel legyenek készítve a digitális átállásra – nemcsak technikai ismeretekre van szükség, hanem szemléletváltásra is. Emellett az adatbiztonság kérdését sem lehet figyelmen kívül hagyni, mivel a digitalizált rendszerek érzékenyebbé válnak a kiberfenyegetésekkel szemben.

Összességében az látszik, hogy az ipari digitalizáció nemcsak aktuális trend, hanem hosszú távon is meghatározó irány. Bár a kezdeti beruházási költségek és a szervezeti változások kihívást jelenthetnek, ezek idővel megtérülnek, főleg, ha figyelembe vesszük a növekvő hatékonyságot, a jobb termékminőséget és a gyorsabb reagálási képességet a piaci igényekre.

Személyes meglátásom szerint azok a vállalatok, amelyek most fektetnek be az okosgyártásba és az IoT-megoldásokba, hosszú távon versenyelőnyt szerezhetnek. Akik viszont halogatják a digitalizációt, könnyen lemaradhatnak, és nehezebben tudnak majd lépést tartani a technológiai fejlődéssel. Az ipar jövője egyértelműen az adatvezérelt, automatizált, fenntartható és rugalmas gyártási rendszerek irányába halad.

Az, hogy ez milyen gyorsan és milyen mértékben valósul meg, nagyban függ a vállalati döntéshozóktól, az állami és iparági stratégiáktól, valamint a megfelelő oktatási és képzési háttér biztosításától. A digitális átállás tehát nemcsak technológiai, hanem társadalmi és gazdasági kérdés is.

Felhasznált irodalom:

[1] *Hol járnak a vállalatok az ipari digitalizációban* - https://blog.eplm.hu/digitalizacios-terkep-vallalatok-az-ipari-digitalizacios-folyamatban-2/

[2] *Real-Life Use Cases for Edge Computing* - https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/

[3] *What is Cloud Computing? Definition, Benefits, Types and Trends* - https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/

[4] *McKinsey & Company (2021*). - *The Internet of Things: Catching up to an accelerating opportunity*. - https://www.mckinsey.com

[5] *Marketing Blog - ERP és MES vállalatirányítási rends*zerek - https://holon.hu/erp-es-mes-vallalatiranyitasi-rendszerek

[6] *Kagermann, H., Wahlster, W., & Helbig, J. (2013).* Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry. *Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering.* - https://www.acatech.de/wp-content/uploads/2018/03/Final_report__Industrie_4.0_accessible.pdf

[7] *Siemens Official Website* - https://new.siemens.com/global/en/company.html

[8] *Nemzeti Iparstratégia 4.*0 (Nagyvállalati Innovációs Programok) - https://www.ipar40.hu

[9] Az Internet of Things rendszerek biztonsági kihívásai - https://real.mtak.hu/175146/7/1155_Új%20típusú%20kihívások%20az%20infokommunikációba-100-136.pdf

[10] IGN Hungary - Mire jó az IoT, más néven Dolgok Internete? - https://hu.ign.com/iot/42660/feature/mire-jo-az-iot-mas-neven-dolgok-internete

2.57. MQTT protokoll alkalmazása okos éttermekben: Valós idejű szenzoradatok kezelése és integrációja egy IoTalapú vendéglátóipari rendszerben

MQTT protokoll alkalmazása okos éttermekben:

Valós idejű szenzoradatok kezelése és integrációja egy IoT-alapú vendéglátóipari rendszerben

Pálfi Dorián Mór [redacted]

gazdaságinformatikus, dorianpalfi@gmail.com

Kulcsszavak: MQTT, vendéglátás, szenzorhálózat, adatgyűjtés automatizálás

Témaválasztás indoklása

A témaválasztás kezdetben bizonytalanságot jelentett számomra, mivel nem volt egyértelmű, milyen irányba induljak el, illetve milyen gyakorlati igényre építhetném a dolgozatot. A félév elején egy családi beszélgetés során merült fel az ötlet: édesanyám munkájához olyan Excel-táblázatokat kellett készíteni, amelyek a hűtők, fagyasztók és más konyhai berendezések állapotát dokumentálják. Ekkor vetődött fel bennem a gondolat, hogy az ilyen jellegű papíralapú vagy manuális adatgyűjtést egy automatizált, digitális rendszer válthatná ki.

Datum	Temp-Kühlmöbel	Temp-Glacé -17	Flammi Ofen	Saladette	Kühlschubl	Pfannen-gestell	Rahm-maschine	Gestelle	Toaster	Gewürz-schrank	Eiskaffe-maschine	Unterschrift
01.03.25												
02.03.25												
03.03.25												
04.03.25												

1. ábra Excel táblázat egy éttermi berendezések állapotáról

Ez az elképzelés vezette a figyelmemet az MQTT protokoll felé, amelyet széles körben alkalmaznak IoT-rendszerekben valós idejű adatkommunikáció céljából. A témaválasztás végül ezen gyakorlati probléma elméleti megközelítésére épült.

Bevezetés

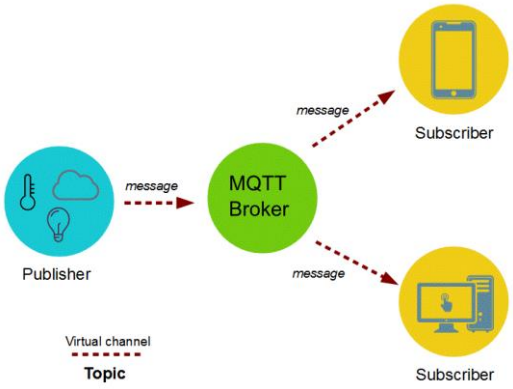
A dolgozat célja az MQTT (Message Queuing Telemetry Transport) protokoll elméleti vizsgálata egy éttermi környezetben, az IoT-technológiák alkalmazhatóságának szempontjából. A vizsgálat arra fókuszál, hogy a protokoll hogyan támogathatja az éttermet a működésében. A kiválasztás során fontos volt, hogy egy olyan technológiát válasszak ki, ami könnyen skálázható az éttermek dinamikus jellegéből kiindulva.

Az MQTT kis erőforrásigényű működésre optimalizált, ami alkalmassá teszi olyan alkalmazásokhoz, ahol korlátozott számítási vagy hálózati kapacitás áll rendelkezésre. A vendéglátóiparban ez lehetőséget ad például a hűtőegységek és más egyéb berendezések állapotfigyelésére vagy energiafelhasználási adatok gyűjtésére.

A dolgozat érinti az éttermi működéshez kapcsolódó műszaki elvárásokat, mint a különböző éttermekre vonatkozó szabályok és törvények fenntartása, illetve a folyamatok automatizálása. Emellett rövid összehasonlítást nyújt az MQTT és más IoT-kommunikációs protokollok között.

Az MQTT protokoll alapjai

Az MQTT egy könnyű, üzenetközvetítő protokoll, amelyet eredetileg alacsony sávszélességű, megbízhatatlan hálózati környezetekre terveztek. A protokoll fő jellemzője a publish-subscribe kommunikációs modell, amelyben a kliensek nem közvetlenül egymással kommunikálnak, hanem egy központi komponens, az úgynevezett „broker” segítségével cserélnek adatokat. A rendszerben a kliensek egy adott témára (topic) iratkozhatnak fel, és azok az üzenetek, amelyeket más kliensek ugyanarra a témára publikálnak, automatikusan továbbításra kerülnek hozzájuk.[1]



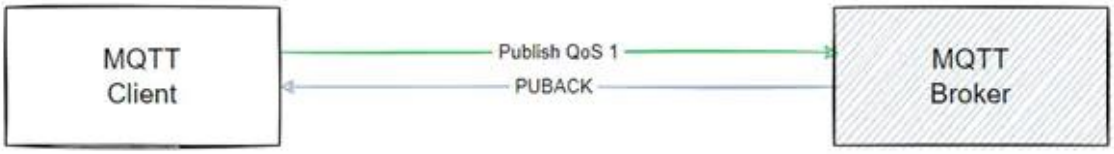
2. ábra MQTT protokoll működése

Az MQTT három minőségi szolgáltatási szintet (QoS -Quality of Service) támogat, amelyek azt határozzák meg, hogy az üzenetek továbbítása mennyire megbízható. Ezeket a szinteket azért vezették be, hogy a fejlesztők a saját rendszerük követelményei szerint választhassanak az egyszerűség és a biztonság között.[2]

- **QoS 0 :** Ebben az esetben az üzenetet a küldő elküldi, de nem vár visszajelzést arról, hogy a címzett megkapta-e. Ez olyan, mint amikor valaki bedob egy levelet a postaládába, de nem nézi meg, megérkezett-e a címzetthez. Ha az üzenet elveszik útközben, akkor nincs semmi utólagos ellenőrzés. Ezt a szintet akkor használják, ha nem gond, ha egy-egy üzenet elveszik, például ha egy szenzor másodpercenként küldi a hőmérsékletet, és néha kimarad egy-egy érték.

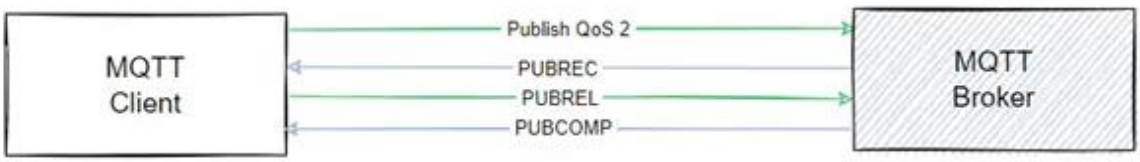
3. ábra MQTT QoS0

- **QoS 1 :** Itt a küldő addig próbálkozik az üzenet elküldésével, amíg visszajelzést nem kap arról, hogy a címzett megkapta azt. Ez olyan, mintha valaki telefonon keresztül próbál elérni, de nem veszed fel először ezért addig hív amíg nem veszed fel a telefont. Lehet, hogy az üzenetet többször is elküldi, ezért előfordulhat, hogy ugyanazt az adatot többször is megkapja a címzett. Ez a szint már megbízhatóbb, de kicsit nagyobb hálózati forgalmat eredménye.



4. ábra MQTT QoS1

- **QoS 2 :** Ez a legmegbízhatóbb, de egyben a legösszetettebb minőségi szint. A küldő és a fogadó között több lépéses visszaigazolási folyamat zajlik, amelynek célja annak garantálása, hogy az üzenet pontosan egyszer legyen továbbítva. Ez a megközelítés különösen akkor fontos, ha az információ duplikálása vagy elvesztése súlyos következményekkel járhat. Például egy asztalfoglalási rendszer, ahol egy foglalás megerősítését egyszer és csak egyszer kell feldolgozni, ha az üzenet elveszne, az ügyfél nem kapna visszajelzést, ha duplán érkezne be, feleslegesen foglalódna le két asztal.



5. ábra MQTT QoS2

A protokoll előnyei közé tartozik az alacsony sávszélesség-igény, az egyszerű implementáció, valamint a kis méretű vezérlőüzenetek. Ezek a jellemzők különösen alkalmassá teszik az MQTT-t olyan környezetekben való használatra, ahol erőforrás-korlátozott eszközök, mint például szenzorok, mikrokontrollerek működnek, és a hálózati kapcsolat minősége nem stabil.

A broker szerepe kulcsfontosságú az MQTT rendszer működésében, mivel ez a központi komponens felelős az összes üzenet elosztásáért a kliensek között. A publish-subscribe modell alapján a kliensek nem egymással kommunikálnak közvetlenül, hanem a brokerhez csatlakoznak. A broker fogadja a kliensek által küldött üzeneteket, és továbbítja azokat a megfelelő előfizetők felé a témáknak megfelelően.

A broker feladata nem merül ki az üzenettovábbításban. Képes kezelni a kliensek csatlakozását és lecsatlakozását, naplózni az eseményeket, valamint különböző biztonsági funkciókat is elláthat. Ilyen például a felhasználók hitelesítése, az üzenetküldési jogosultságok kezelése, valamint az adatforgalom titkosítása. Ezek különösen fontosak lehetnek olyan alkalmazásokban, ahol érzékeny adatok mozognak a hálózaton, például hűtőberendezések állapotjelentései egy éttermi rendszerben.

Az MQTT-hez többféle nyílt forráskódú broker érhető el, ezek közül a legismertebbek a Mosquitto és a HiveMQ. A Mosquitto egy könnyű, gyors és egyszerűen telepíthető megoldás, amely ideális kisebb rendszerekhez vagy oktatási célokra. A HiveMQ ezzel szemben fejlettebb funkciókkal rendelkezik, például webes kezelőfelülettel, integrált biztonsági beállításokkal és skálázhatósággal, ezért gyakrabban használják ipari környezetekben. A megfelelő broker kiválasztása tehát a rendszer méretétől, biztonsági követelményeitől, valamint az üzemeltetési környezettől függ.[3]

6. ábra Mosquitto logó

7. ábra HiveMQ logó

Az MQTT-hez hasonló kommunikációs protokollok és a választás indoklása

Az MQTT-n kívül még 3 kommunikációs protokoll merült fel, amiket gyakran használnak, ezeket az alábbiakban fogom felsorolni és ismertetni.[4], [5]

HTTP (Hypertext Transfer Protocol)

- **Kommunikációs modell**: kliens-szerver, kérés-válasz alapú. A kliens kérés küld a szervernek, amely válaszul adatot vagy visszaigazolást küld.
- **Kapcsolat**: minden kérés új TCP-kapcsolatot hoz létre, amely nem marad fenn.
- **Adatmennyiség**: a HTTP-keret viszonylag nagy méretű, sok fejléccel, ami túlzott erőforrás-felhasználást jelent kis IoT-eszközök számára.
- **Használhatóság IoT-ben**: jól dokumentált és széles körben támogatott, de nem ideális olyan rendszerekhez, ahol kis, gyakori adatokat kell valós időben továbbítani
- **Példa éttermi környezetben**: HTTP akkor lehet hasznos, ha ritkábban történik adatküldés, vagy ha emberi beavatkozás szükséges.

8. ábra HTTP logó

CoAP (Constrained Application Protocol)

- **Kommunikációs modell**: kliens-szerver, hasonló a HTTP-hez, de alapértelmezés szerint UDP protokollon működik, nem TCP-n. Kimondottan kis erőforrásigényű IoT-eszközökhöz készült, például szenzorhálózatokhoz, amelyek kis adatcsomagokat küldenek.
- **Valós idejűség**: gyors, de mivel UDP-re épül, nem garantált az adat kézbesítése. Lehetőség van ugyan visszaigazolásos üzemmódra, de az nem minden implementációban elérhető.
- **Üzenetirányítás**: nincs beépített broker vagy üzenetsor támogatás, mint az MQTT vagy AMQP esetén.
- **Példa éttermi környezetben**: CoAP akkor lehet hasznos, ha nagyon kis szenzorok vannak, amik csak alkalmanként adnak le mérést és nem kritikus a megbízható kézbesítés.

9. ábra CoAP logó

AMQP (Advanced Message Queuing Protocol)

- **Kommunikációs modell**: üzenetsor-alapú Publish-Subscribe modell. Támogatja az aszinkron kommunikációt, routingot, prioritásokat, visszaigazolásokat.
- **Megbízhatóság**: nagyon magas. Üzenetek garantáltan eljutnak a címzetthez, sőt támogatja az üzenetek tartós tárolását .
- **Erőforrásigény**: nagyobb számítási kapacitást igényel, mint MQTT vagy CoAP, ezért tipikusan nem mikrovezérlőkkel használják.
- **Biztonság és funkciók**: vállalati környezetekben ideális, összetett routing, access control, tranzakciók és audit funkciók érhetők el.
- **Implementáció**: összetettebb és nagyobb hardverigénye van.
- **Példa éttermi környezetben**: AMQP akkor lehet jó választás, ha az adatforgalmat egy központi rendszer felé kell irányítani megbízható módon, és nem gond a magasabb számítási igény.

10. ábra AMQP logó

MQTT (Message Queuing Telemetry Transport)

- **Kommunikációs modell**: Publish-Subscribe modell, amelyben a szenzorok üzenetet küldenek egy központi brokernek, a kliensek pedig a számukra releváns témákra iratkoznak fel. A közvetítést a broker végzi.
- **Protokoll jellemzői**:
  - TCP-alapú, így biztosított a kapcsolat megbízhatósága.
  - Háromféle QoS szintet kínál:
- **Erőforrás-igény**: Kifejezetten alacsony. Kevés adatot továbbít, kevés sávszélességet és processzort igényel. Ideális mikrokontrollerekhez.
- **Valós idejű képesség**: Képes azonnali mérésekre, például amikor egy hűtő eléri a kritikus hőmérsékletet, vagy egy fogyasztásmérő szokatlanul magas értéket mutat.

Protokoll	Kommunikációs modell	Üzenetméret	Kapcsolat típusa	Valós idejű támogatás	Implementációs összetettség
MQTT	Publish-Subscribe	Kis méretű	Állandó TCP	Igen (QoS szintekkel)	Egyszerű (könnyű broker és kliens)
HTTP	Kliens-Szerver	Nagyobb méretű	Kérés-válasz (TCP)	Nem	Egyszerű, de nem optimalizált IoT-re
CoAP	Kliens-Szerver	Kis méretű	Nem állandó (UDP)	Részben (nincs garantált kézbesítés)	Közepes (UDP alapú, de célzott IoT-re)
AMQP	Queue-based Publish-Subscribe	Nagyobb méretű	Állandó TCP	Igen (magas megbízhatóság)	Bonyolult (nagy rendszerigény)

11. ábra A protokollok összehasonlítás táblázatban

Az MQTT protokoll különösen jól alkalmazható éttermi környezetben működő szenzorhálózatokhoz, mivel egyszerre nyújt valós idejű adatkommunikációt, alacsony erőforrásigényt és könnyű implementálhatóságot. Míg más protokollok mint a HTTP, CoAP vagy AMQP bizonyos területeken jól teljesítenek, az MQTT a legtöbb szempontból optimális választás az IoT-alapú megfigyelési és automatizálási feladatokra.

A HTTP például elsősorban webes alkalmazásokhoz lett tervezve. Minden adatküldéshez új kapcsolatot kell létesíteni, ami feleslegesen terheli a hálózatot és az eszközöket, különösen akkor, ha kis mennyiségű szenzoradatokat küldünk gyakori időközönként. Ez nem hatékony, ha például hőmérsékletet vagy energiafogyasztást kell percenként jelenteni. A CoAP ugyan kisebb és gyorsabb protokoll, mint a HTTP, de mivel UDP-re épül, nem garantálja az üzenetek kézbesítését ez hűtők, fagyasztók megfigyelése esetén komoly kockázatot jelenthet. Az AMQP ezzel szemben üzleti szintű, komplex és megbízható protokoll, de a nagy rendszerigénye és összetett konfigurációja miatt kevésbé alkalmas egyszerű IoT-eszközök kiszolgálására, mint amilyeneket egy étterem használna.

Ezzel szemben az MQTT úgy lett megalkotva, hogy kis sávszélességen, alacsony teljesítményű, akkumulátoros eszközökön is stabilan működjön. A „publish-subscribe" modellje lehetővé teszi, hogy az eszközök ne közvetlenül kommunikáljanak egymással, hanem egy központi brokeren keresztül, ami egyszerűsíti a hálózat felépítését és bővítését.

Összességében az MQTT az ideális választás egy éttermi környezetben. Gyors, megbízható, energiahatékony és skálázható.

Éttermi környezet és az IoT alkalmazásának lehetőségei

Az éttermek működésében egyre nagyobb szerepet kapnak az automatizált rendszerek, amelyek célja a működési hatékonyság növelése, a hibalehetőségek csökkentése, valamint az erőforrások optimális kihasználása.

Az alábbiakban felsorolom azokat az ötleteket, amelyek felmerültek bennem a téma kiválasztása során, majd kifejtem, hogy melyik miért maradt, illetve melyik miért került elvetésre.

A hűtők hőmérsékletének mérése egy elég egy értelmű vonal volt, hiszen a kezdeti táblázatban már benne vannak a különböző hűtők, tehát erre valószínű lenne igény, hiszen ezt a folyamatot valakinek napi szinten el kell végeznie és ha ezt automatikusan elvégezné a rendszer az ember aki ezt a folyamatot végezte felszabadul és mással is tud foglalkozni. Illetve ha valami probléma lenne a hűtővel mondjuk, a hőmérséklete megemelkedik és leolvadás veszélye fenyeget, akkor azt a hőmérsékletmérővel előbb tudjuk meg, mint mikor azt a hűtőt legközelebb kinyitja valaki.[6]

A második ami maradt mint ötlet az a különböző berendezések áramfogyasztása. Egy étterem konyháján több áramkör van, adott esetben különböző funkciókat ellátó berendezések vannak egy áramkörre kapcsolva, ezért elegendő egy fogyasztásmérő áramkörönként. Ez azért lehet fontos információ egy étterem számára, mert így látja hogy az egyes áramkörök mennyit fogyasztanak, ha esetlegesen megugrik a villanyszámlája, visszatudja keresni hogy hol lehet a hiba, de eleve ha tönkre menne valami bármelyik áramkörön akkor egy pillantásra megtuja mondani melyik körön van probléma és már lehet hívni a szerelőket.

A utolsó ami bent maradt az egy páratartalom és hőmérséklet érzékelő, ami a konyhai és a vendégtérben történő szellőztetést. A jelenlegi tudásom szerint a konyhában a gépi szellőztetés kötelező eleme egy konyhának. Ezeknek a páraelszívóknak kötelező jelleggel folyamatosan mennie kell egy étterem konyhájában, de nem mindegy milyen teljesítménnyel, mennyi levegőt cserél. Fölöslegesen nem szeretne senki magasabb áramfogyasztást, így arra gondoltam hogy egy páratartalom mérővel lehetne ez szabályozni. Ugyanígy egy klíma berendezést lehetne vezérelni ugyanezzel az egy szenzor segítségével hiszen egyszere mér hőmérsékletet és páratartalmat. Ezzel a módszerrel a vendégtér szellőztetését is meg lehet oldani hiszen, manapság minden modern étterem vendégterébe van klíma.

Az egyik ötletem, ami végül nem kerül megvalósításra azaz RFID (Radio Frequency IDentification) technológiával való raktározás. Maga az terv az lett volna hogy minden hűtő, illetve fagyasztó ajtaján elhelyezünk egy RFID olvasót, a termékeken pedig egy RFID taget. A probléma akkor realizálódott bennem, mikor rájöttem hogy ez egy étteremben nem működne, hiszen egy babgulyáshoz nem egy kartondoboznyi bab kell, hanem mondjuk 2 konzerv. Ezért az ötlet elméleti szinten működött volna, de gyakorlatban több munka lett volna vele, mintha ez a rendszer elem nem valósul meg.

Ugyanilyen sorsra került a PIR (Passive Infrared), amivel a vendégtér lett volna monitorozva, míg rá nem világított egy étteremben dolgozó ismerősöm, hogy ez teljes mértékben felesleges, hiszen nem számít annyit hogy mennyi ember van vagy jön be az étterembe legalább egy pincér folyamatosan dolgozik így ezt a monitorozást a pincér elvégzi.

Utolsó nem megvalósítható ötletem az olajfáradság (TPM) mérő. Ez azért nem kerül be a dolgozatba, mert bár vannak olyan TPM mérők melyek képesek Bluetooth-al való kommunikációra a dolgozat témájába, mely a MQTT nem fér bele. A piacon jelenleg nem található MQTT-vel kompatibilis TPM mérő, így ez is kihagyásra kerül.

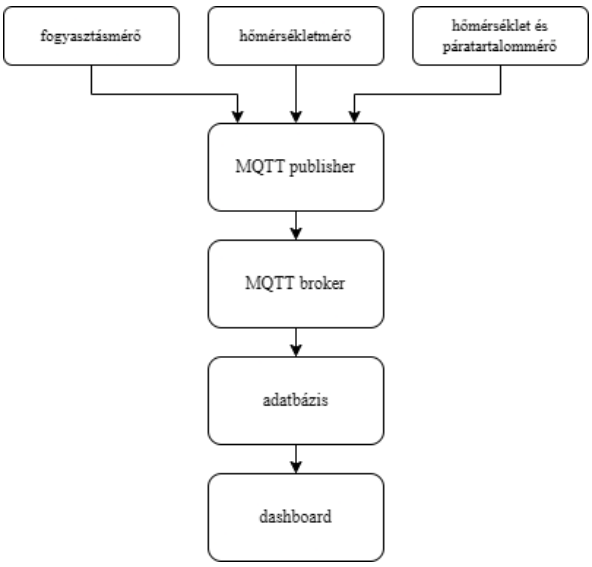
Elméleti rendszerterv és architektúra egy okos étteremre

Fontos kiemelni, hogy egy étterem működése dinamikus, ezért a használt technológiai megoldásoknak is rugalmasnak és jól skálázhatónak kell lenniük. Egy új szenzor vagy funkció bevezetése nem igényelheti az egész rendszer újratervezését, ezért előnyös, ha az architektúra moduláris és bővíthető. Az MQTT protokoll ebben is megfelelő választás, mivel támogatja az egyszerű integrációt új eszközök és szolgáltatások bevonásával.

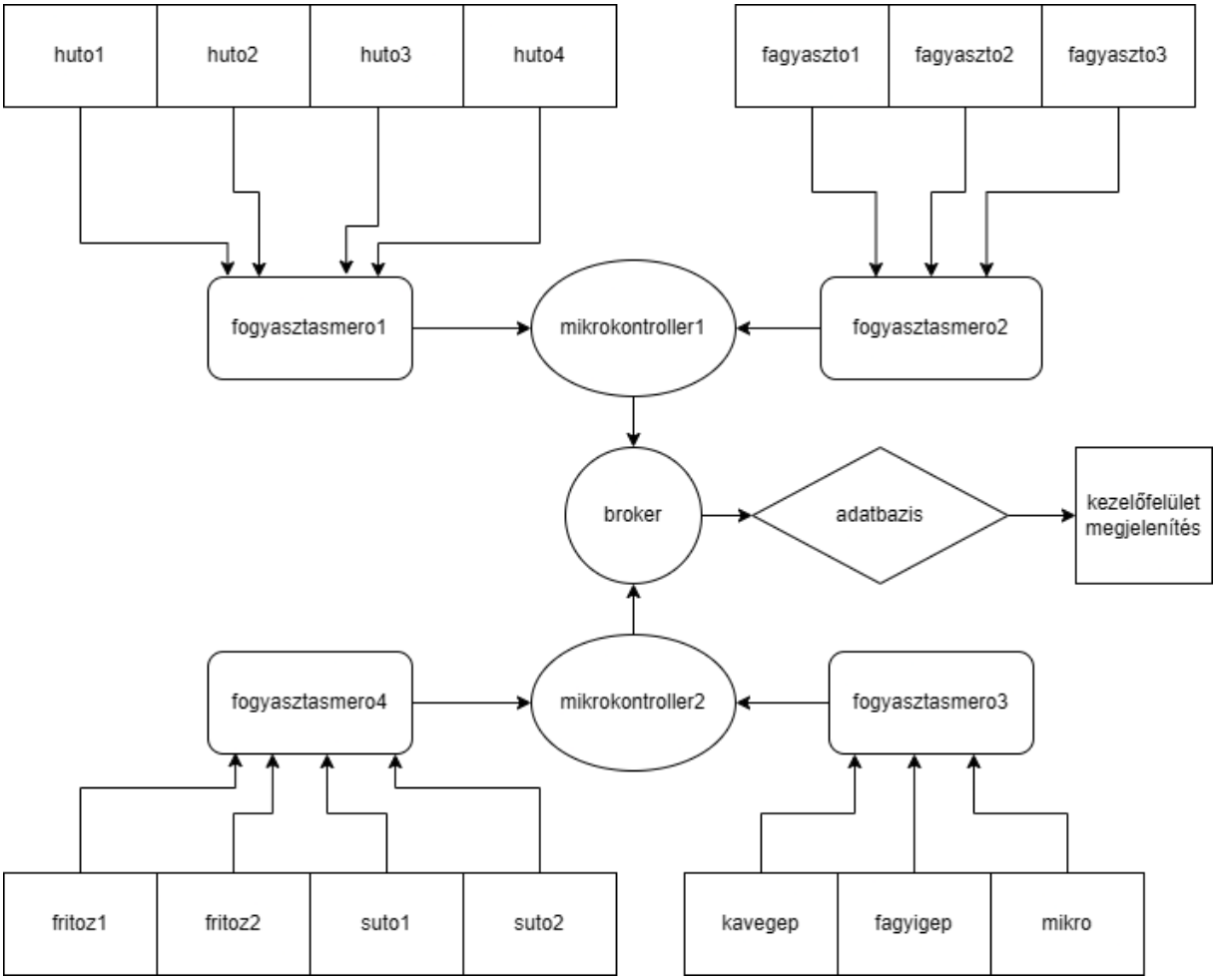
A rendszer négy fő komponensből áll:

- **Szenzorok**
- **MQTT publisherek**
- **MQTT broker**
- **Adatfeldolgozó és megjelenítő rendszer**

A rendszer működését az alábbi modellek szemléltetik:

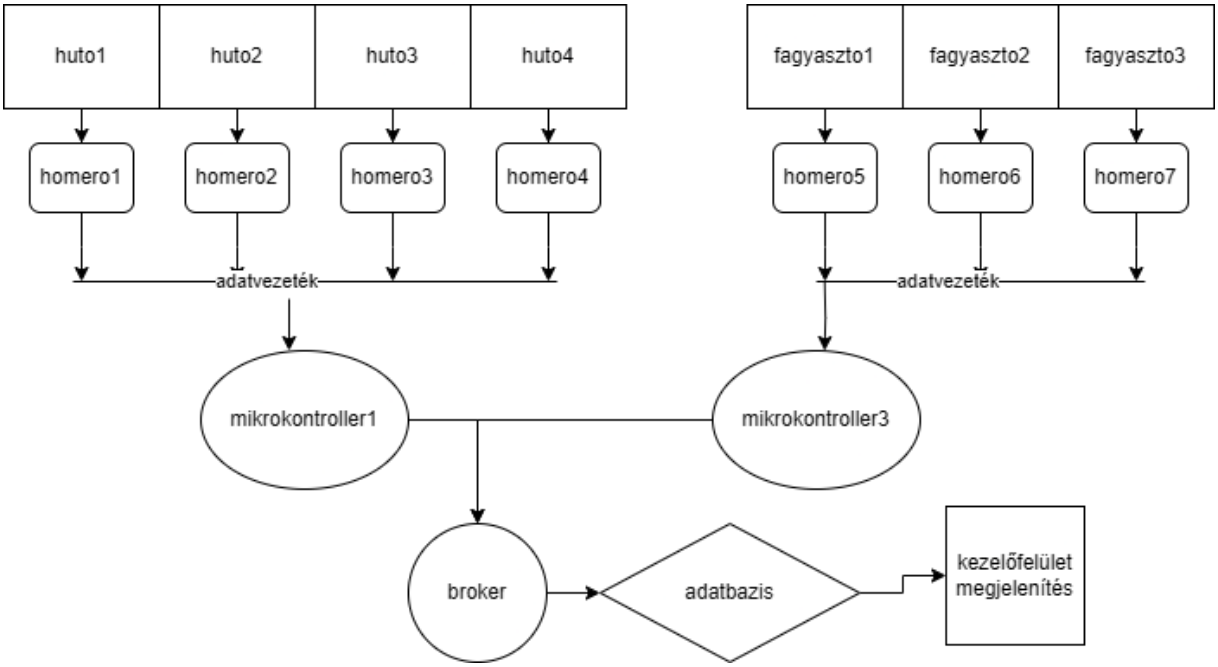


12. ábra Egyszerű architektúra modell



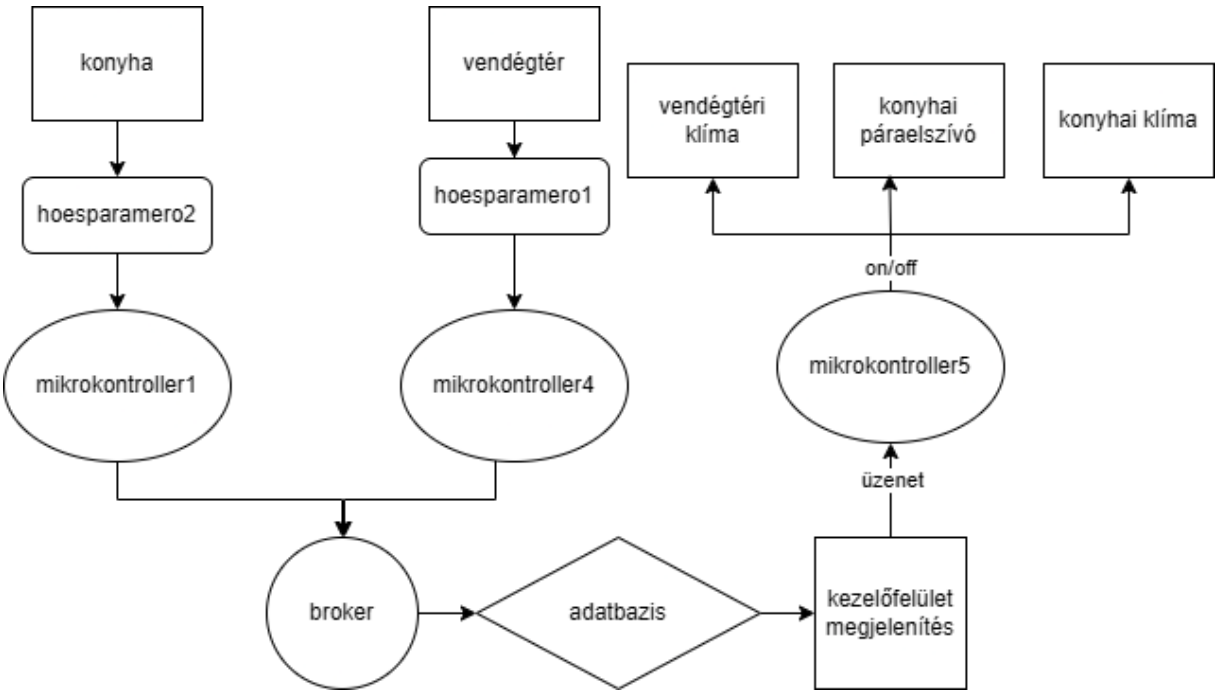
13. ábra Az áramfogyasztás architektúramodellje

Mivel az áramfogyasztásmérők egy adott áramkört mérnek ezért többet kell elhelyezni áramkörönként, így pontosabban tudjuk mérni az adott berendezések áramfogyasztását, amivel a hibákra is rálelhetünk ha az egyik áramkörön a fogyasztás hirtelen megugrik vagy leesik. A több mikrokontroller vagy MQTT publisher elhelyezése is indokolt hiszen a áramkörökre nem feltétlenül egy helyen tudjuk felhelyezni a mérőket, illetve ha másik helységben vannak a berendezések és fizikailag más helyen vannak akkor is indokolt a több mikrokontroller, mivel ezekre fizikailag kell rákapcsolni a szenzorokat.



14. ábra A hűtők és fagyasztók hőmérséklet mérőinek architektúra modellje

Itt a különböző hűtők különböző mérőit egy adatvezetékre lehet kötni, majd ezt egy publisherbe vezetni. Itt a kettő mikrokontrollert a hűtők és fagyasztók fizikai helyzete miatt egy követelmény. Jól látható hogy a hűtők hőmérő szenzorai ugyanarra a publisher-re vannak kötve mint a hűtők áramfogyasztásmérője. Ennek az az indoklása hogy technikailag ez megvalósítható és ezért beszerettem volna építeni a dolgozatba.



15. ábra A klímák és páraelszívó architektúrája

A helyiségekben elhelyezett hőmérséklet és páramérő szenzorok segítségével, a helyiségek automatikus szellőztetése és hő szabályozása látható az ábrán. A kezelőfelület egy másik publisher-nek üzenetet küld a szenzorok által mért adatok alapján, majd az üzenetet továbbítja a klíma berendezéseknek és a páraelszívónak. A jelenlegi elrendezésben különböző berendezések különböző üzeneteket is kaphatnak, így nem kell kompromisszumot kötni hogy a konyhában lenne nagyon meleg vagy a vendégtérben nagyon hideg.

A tervezett architektúra fő jellemzői:

- **Modularitás**: a rendszer új eszközökkel egyszerűen bővíthető.
- **Skálázhatóság**: több eszköz, étterem vagy funkció bevonása nem igényli a meglévő struktúra átalakítását.
- **Heterogén támogatás**: az MQTT architektúra lehetővé teszi, hogy különböző gyártók eszközei együttműködjenek egy egységes üzenetközvetítő rendszeren keresztül.

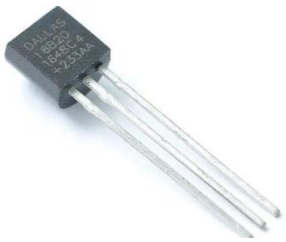
A rendszer megvalósításához szükséges főbb komponensek

A rendszer elméleti modelljének kialakításakor olyan hardver- és szoftverkomponenseket választottam, amelyek illeszkednek az MQTT-alapú adatkommunikációhoz, és megfelelnek az éttermi környezet technikai elvárásainak. A kiválasztás során elsődleges szempont volt, hogy az eszközök natívan támogassák az MQTT protokollt, mivel ez a rendszer alapját képezi. Emellett fontosnak tartottam, hogy a komponensek alacsony energiafogyasztásúak legyenek, mivel egyes részegységek folyamatos működésre vannak tervezve. A megbízhatóság is kiemelt szempont volt, különösen a szenzoradatok pontossága és az üzenetküldés stabilitása miatt. Végül olyan eszközöket részesítettem előnyben, amelyek viszonylag egyszerűen beüzemelhetők és programozhatók, így a rendszer megvalósítása nem igényel különösen bonyolult fejlesztői környezetet vagy ipari szintű szaktudást.

Szenzorok:

DS18B20 hőmérséklet szenzor

A DS18B20 egy digitális, 1-Wire protokollt használó hőmérséklet-érzékelő, amely kifejezetten jól használható ipari és félipari környezetekben, például hűtőegységek felügyeletére. Pontos (±0,5 °C), vízálló tokozással is elérhető, és egyetlen adatvezetéken több szenzor is láncba köthető, így különösen alkalmas több hűtőtér egyidejű megfigyelésére.[7]



16. ábra DS18B20 szenzor

DHT22 Hőmérséklet- és páratartalom szenzor

A DHT22 egy kombinált szenzor, amely képes egyszerre mérni a hőmérsékletet és a relatív páratartalmat. A szenzor digitális kimenetű, és ideális választás helyiségek figyelésére, ahol lehetőség van a klíma vagy páraelszívó automatikus vezérlésére.[8]

17. ábra DHT22 szenzor

PZEM-004T Energiafogyasztás-mérő modul

A PZEM-004T egy UART-kommunikációval működő fogyasztásmérő, amely képes valós időben mérni a feszültséget, áramerősséget, teljesítményt és energiafogyasztást. Kifejezetten hasznos nagy energiaigényű eszközök.[9]

18. ábra PZEM-004T fogyasztásmérő modull

Mikrokontroller

Az ESP32 egy alacsony fogyasztású, nagy teljesítményű mikrokontroller, amelyet az Espressif Systems fejlesztett ki. Beépített Wi-Fi és Bluetooth képességei miatt különösen népszerű az IoT-projektekben. Kétmagos processzorral, számos szenzorok kezelésére alkalmas interfésszel rendelkezik. Az ESP32 könnyen programozható, és natívan támogatja az MQTT protokollt.[10]

19. ábra ESP32 mikrokontroller

Központi egység

A rendszer központi egységeként egy Raspberry Pi 4-et választottam, ahol az összes fő komponens egyazon eszközön fut. A választásom azért esett erre az eszközre, mert a rendszer működtetéséhez nem volt szükség nagy teljesítményű hardverre, ugyanakkor fontos szempont volt, hogy minden szolgáltatás egy helyen, egyszerűen konfigurálható legyen.

A Raspberry Pi egy alacsony fogyasztású, ARM-alapú számítógép, amely képes Linux operációs rendszert futtatni. A rendszer szempontjából az volt a fő előnye, hogy elég erőforrással rendelkezik ahhoz, hogy a szükséges szoftverek párhuzamosan működjenek rajta, ugyanakkor kis helyigényű és viszonylag könnyen karbantartható.

Mivel a projektben nem cél egy elosztott vagy felhőalapú rendszer létrehozása, hanem sokkal inkább egy önálló, lokálisan működő egység bemutatása, a Raspberry Pi lehetővé teszi, hogy a különböző komponensek egymással gyorsan és hálózati késleltetés nélkül kommunikáljanak. Ezzel a megközelítéssel a rendszer egyszerű marad és a működése is jól nyomon követhető.

Összességében a Raspberry Pi szerepe ebben a rendszerben az, hogy a különálló technológiai elemeket egy működő egységbe integrálja. A használata nem csak technikailag volt indokolt, hanem gyakorlati szempontból is előnyös, mivel kevés beállítást igényel, és jól illeszkedik az egyszerű, mégis szemléletes rendszerarchitektúrához.[11]

20. ábra Raspberry Pi 4 modell B

Broker

MQTT broker-nek a nyílt forráskódú Mosquitto-t választottam. A rendszerben a Mosquitto közvetítőként működik az ESP32 mikrokontrollerek és a háttérrendszer között. Az ESP32-k által mért adatok MQTT-üzenetként érkeznek a brokerhez, amely ezeket az üzeneteket meghatározott topicok szerint továbbítja. A rendszer minden résztvevője csak azokhoz az adatokhoz fér hozzá, amelyekre fel van iratkozva, ezáltal biztosított a hatékony és szelektív kommunikáció.

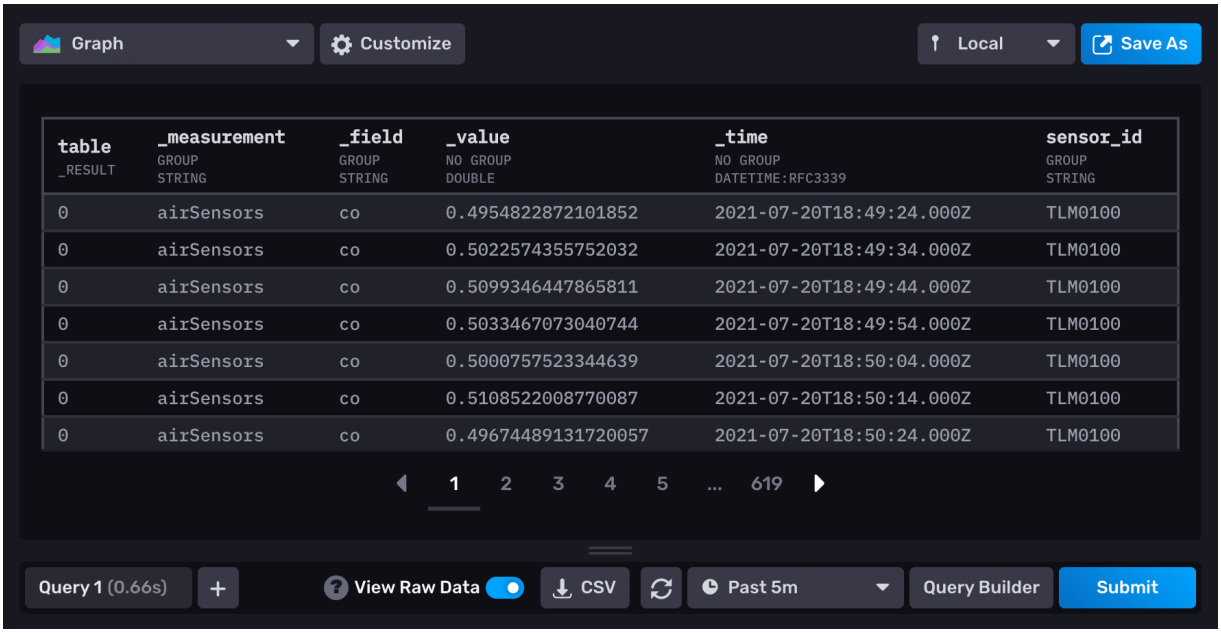
A Mosquitto egyik legfontosabb jellemzője, hogy egyszerűen konfigurálható és jól dokumentált, ami különösen hasznos olyan fejlesztési környezetekben, ahol nem cél túl bonyolult szoftverinfrastruktúra létrehozása. A Raspberry Pi-n történő futtatás során a Mosquitto kevés erőforrást igényel, így párhuzamosan több más szolgáltatás is működtethető mellette. A szoftver natív támogatást nyújt különböző hitelesítési és jogosultságkezelési megoldásokhoz, valamint lehetővé teszi TLS-titkosítás használatát is, ha a rendszer biztonsága indokolja.

Az MQTT broker jelenléte kulcsfontosságú a rendszer működése szempontjából, mivel nélküle a szenzorok nem tudnának kommunikálni sem az adatfeldolgozó egységgel, sem a felhasználói interfésszel. A Mosquitto ebben a szerepben egyszerre biztosítja a gyors, megbízható adatközvetítést, és egy olyan struktúrát, amely skálázható és bővíthető marad, ha a rendszer újabb szenzorokkal vagy funkciókkal egészül ki.[12]

Adatbázis

Az adatbázis választás során egy kifejezetten idősoros adatok tárolására tervezett adatbázis-kezelő rendszert választottam, amely jól illeszkedik olyan alkalmazásokhoz, ahol az adatok rendszeres időközönként érkeznek. A jelen projekt esetében, amelyben a rendszer által mért hőmérséklet, páratartalom és energiafogyasztási értékeket idősorosan kell naplózni és elemezni, az InfluxDB természetes választásnak számít, mivel pontosan ezekre az igényekre lett optimalizálva.

Az InfluxDB egyik legnagyobb előnye, hogy nem relációs adatmodellben gondolkodik, hanem időbélyeggel ellátott eseményekre épít, így az adatok nem táblákba, hanem úgynevezett *measurement*-ekbe kerülnek. Minden egyes bejegyzés tartalmaz egy időpontot, valamint opcionálisan címkéket, mint például a szenzorazonosítója vagy a helyszíne, ami lehetővé teszi az adatok gyors szűrését és lekérdezését időalapú feltételek szerint.



21. ábra InfluxDB adattábla

A rendszer szintű architektúrában az InfluxDB a Mosquitto brokert követi: miután az MQTT-n keresztül beérkezett az adat, az egy feldolgozó eszköz segítségével bekerül az InfluxDB-be. Innen már lehetőség van a Grafana vizualizációs eszközzel való integrációra, amely közvetlenül képes lekérni és megjeleníteni az InfluxDB-ben tárolt adatokat.

Az InfluxDB a könnyű telepíthetőség, a gyors lekérdezési képességek, valamint a kompakt adattárolás miatt is előnyös. Mivel a szenzoros adatok jellemzően sok, de kis méretű, gyakran érkező mérést jelentenek, fontos, hogy az adatbázis képes legyen ezt hatékonyan kezelni

anélkül, hogy jelentősen terhelné a rendszert. Ez különösen fontos olyan alacsony erőforrású környezetekben, mint például egy Raspberry Pi.

Összesítve az InfluxDB-ről:

- kifejezetten időalapú adatok kezelésére van optimalizálva,
- egyszerűen integrálható MQTT-alapú rendszerekbe,
- jól együttműködik a Grafana megjelenítővel,
- alacsony erőforrásigényű, így kis hardveren is jól működik,
- támogatja a pontos, időalapú lekérdezéseket, ami nélkülözhetetlen egy szenzorhálózattal működő rendszer esetében.

Adatfeldolgozó

A Telegraf egy nyílt forráskódú, plugin-alapú adatgyűjtő, amelyet az InfluxData fejlesztett ki, és kifejezetten időalapú adatgyűjtési feladatokra optimalizáltak. A szoftver célja, hogy a broker által továbbított adatokat strukturált formában közvetlenül az InfluxDB-be továbbítsa. Mivel a projekt során az MQTT protokollt alkalmazzuk a szenzoradatok továbbítására, a Telegraf használata logikusan illeszkedik az architektúrába.

A Telegraf működése plugin-alapú, ami azt jelenti, hogy külön modulok felelnek az adatok beolvasásáért, feldolgozásáért és továbbításáért. A Mosquitto brokerből érkező MQTT-üzenetekhez a beépített mqtt_consumer input plugint lehet használni, amely képes automatikusan feliratkozni egy vagy több topicra, majd a beérkező üzeneteket a megfelelő formátumban értelmezni és továbbítani.

A legnagyobb előnye, hogy használatához nincs szükség programozásra: a működés egyetlen konfigurációs fájlban definiálható, amelyben megadható például az MQTT broker címe, a topic neve, valamint az InfluxDB elérhetősége és adatbázisneve. Ezzel a megközelítéssel egyszerűen és gyorsan létrehozható egy adatgyűjtő lánc a szenzortól az adatbázisig.

A Telegraf használata különösen előnyös, mivel ugyanaz a fejlesztői csapat készíti, mint az InfluxDB-t, a két komponens jól együttműködik. Ez csökkenti az integrációs problémák esélyét, és leegyszerűsíti a fejlesztést. A rendszer így a szenzoros környezetből érkező adatokat gyorsan, megbízhatóan és strukturált módon tudja eljuttatni a feldolgozó és megjelenítő egységekhez.

```
[agent]
  interval = "10s"
  round_interval = true
  metric_batch_size = 1000
  metric_buffer_limit = 10000
  collection_jitter = "0s"
  flush_interval = "10s"
  flush_jitter = "0s"
  precision = ""
  hostname = ""
  omit_hostname = true

[[inputs.mqtt_consumer]]
  servers = ["tcp://localhost:1883"]
  topics = [
    "szenzorok/homerseklet",
    "szenzorok/paratartalom",
    "szenzorok/energiafogyasztas"
  ]
  qos = 0
  connection_timeout = "30s"
  client_id = "telegraf_mqtt"
  data_format = "json"
  json_time_key = "timestamp"
  json_time_format = "2006-01-02T15:04:05Z07:00"
  tag_keys = ["szenzor_id", "helyseg"]

[[outputs.influxdb_v2]]
  urls = ["http://localhost:8086"]
  token = "YOUR_INFLUXDB_TOKEN"
  organization = "YOUR_ORG_NAME"
  bucket = "YOUR_BUCKET_NAME"
```

22. ábra Telegraf config fájl példa

Magyarázat a config fájlhoz

[agent]: Meghatározza a Telegraf működésének alapbeállításait, például az adatgyűjtés és az adatok továbbításának időzítését.

[[inputs.mqtt_consumer]]: Ez a szakasz konfigurálja az MQTT brokerhez való csatlakozást. A ***servers*** mezőben adhatók meg a broker címei. A ***topics*** mezőben felsorolt témákra iratkozik fel a Telegraf. A ***data_format*** mező json értéke jelzi, hogy a bejövő üzenetek JSON formátumúak. A ***tag_keys*** mezőben megadott kulcsok értékei címkeként kerülnek mentésre az InfluxDB-ben.

[[outputs.influxdb_v2]]: Ez a szakasz határozza meg, hová küldje a Telegraf az összegyűjtött adatokat. A ***urls*** mezőben adható meg az InfluxDB címe. A ***token***, ***organization*** és ***bucket*** mezők az InfluxDB hitelesítéséhez és az adatok megfelelő helyre történő mentéséhez szükségesek.

Vizualizáció

Az adatvizualizációra egy korszerű, nyílt forráskódú adatvizualizációs platform lett kiválasztva, amelynek fő célja, hogy összetett, időalapú mérési adatokat könnyen értelmezhető, interaktív felületeken jelenítsen meg. A rendszer különböző szenzoroktól összegyűjtött adatai az InfluxDB időalapú adatbázisba kerülnek eltárolásra, a Grafana pedig ezeket használja fel grafikonok, mérők, táblázatok és más vizuális elemek létrehozásához.

A Grafana egyik legfontosabb tulajdonsága, hogy valós idejű megfigyelést tesz lehetővé. Ez különösen hasznos mivel a hűtőszekrények és fagyasztók állapotát folyamatosan figyelemmel kell kísérni. Illetve a helyiségek hőmérsékletéről és páratartalmáról is folyamatos méréseket kapunk. A rendszerben azonnal láthatja az aktuális értékeket a vezető vagy az adott kolléga, és így gyorsan reagálhat bármilyen rendellenességre.

23. ábra Grafana időjárás vizualizáció

A visszamenőleges adatelemzés is a Grafana egyik alaptulajdonsága. Mivel az InfluxDB időbélyeggel ellátva tárolja az összes mért adatot, lehetőség van napokra, hetekre vagy akár hónapokra visszamenőleg is grafikonokat készíteni. Ez hasznos például akkor, ha ellenőrizni kell, hogy egy adott hűtő hosszabb időn keresztül stabilan működött-e, vagy hogy mikor és milyen időtartamban lépte túl a megengedett hőmérsékletet.

A Grafana személyre szabható felhasználói felületeket kínál. Egy-egy dashboard több panelt is tartalmazhat, és minden panel külön konfigurálható: megadható, hogy mely szenzor mely mért adatai jelenjenek meg, milyen típusú grafikon ábrázolja azokat, és milyen időintervallumon belül. Ez lehetővé teszi, hogy a felhasználók az őket érdeklő adatokat saját igényeik szerint figyelhessék.

24. ábra Grafana időjárás vizualizáció 2

További hasznos funkció a riasztások beállítása. A rendszer képes automatikusan értesítést küldeni, ha egy mért érték túllép egy előre beállított határértéket. Például, ha egy hűtő hőmérséklete meghaladja a 10 °C-ot, a Grafana vizuálisan is figyelmeztetést jeleníthet meg, vagy akár e-mailt is küldhet az illetékes személynek. Ez a funkció különösen fontos az élelmiszerbiztonság szempontjából.

Végül érdemes megemlíteni, hogy a Grafana többféle adatforrást is támogat, nemcsak az InfluxDB-t. Amennyiben a rendszer bővülne, például új típusú szenzorokkal vagy külső adatszolgáltatókkal, ezek integrációja könnyen megoldható, ami hosszú távon is rugalmasságot biztosít a rendszer számára.

Összefoglalva, a Grafana ebben a rendszerben nem csupán egy grafikus felület, hanem a felhasználói szintű döntéstámogatás kulcseleme: lehetővé teszi az adatok valós idejű követését, hosszabb távú elemzését és az automatizált riasztásokat is. Mindez hozzájárul a rendszer megbízhatóságához, kezelhetőségéhez és átláthatóságához.[13]

A rendszer főbb funkciói

Funkcionalitás tekintetében a rendszer megvalósítja „Éttermi környezet és az IoT alkalmazásának lehetőségei” részben taglalt funkciókat. Ezeket kiegészítve a rendszernek van még pár funkciója.

Automatikus riasztás

A rendszer automatikus riasztási funkciója azt a célt szolgálja, hogy az éttermi szenzorhálózat által mért adatok alapján időben figyelmeztessen egy esetleges rendellenességre például, ha egy hűtőegység hőmérséklete meghalad egy előre meghatározott határértéket. A riasztás működése teljesen automatizált, és nem igényel emberi beavatkozást ahhoz, hogy a kritikus események felismerésre kerüljenek.

A működés logikája a következőképpen épül fel. A szenzorok által mért értékeket az ESP32 mikrokontrollerek MQTT-üzenetként továbbítják a Mosquitto brokerhez. Ezek az adatok egy. Telegraf-on keresztül bekerülnek az InfluxDB adatbázisba, ahol minden érték időbélyeggel rögzítésre kerül. A Grafana dashboard, amely az InfluxDB-t használja adatforrásként, képes nemcsak megjeleníteni ezeket az értékeket, hanem automatikusan monitorozni is azokat.

A riasztások beállítása a Grafana felületén történik, ahol az adott szenzorra vagy mért paraméterre rögzíthető egy vagy több feltétel. Például, ha egy hűtő hőmérséklete meghaladja a 10 °C-ot legalább 5 percen keresztül, a rendszer aktivál egy előre konfigurált riasztást. A Grafana különböző értesítési csatornákat támogat, például e-mail, Slack, Telegram vagy webhook, így a rendszer képes közvetlenül üzenetet küldeni az illetékes személyeknek vagy akár más rendszereket is aktiválni.

A riasztási logika így szervesen beépül az adatgyűjtő és feldolgozó architektúrába, és hozzájárul a rendszer megbízhatóságához, valamint az étterem működésének biztonságosabbá tételéhez.

Automatikus hőmérséklet- és páratartalom-szabályozás a helyiségekben

A szenzorok által mért adatok MQTT-n keresztül beérkeznek a rendszerbe, majd a Telegraf segítségével eljutnak az InfluxDB adatbázisba. Az itt tárolt értékeket folyamatosan figyeli egy külön funkciót ellátó ESP32 mikrokontroller, amely kizárólag a klímaberendezések és páraelszívók vezérléséért felel. Ez az ESP32 nem mér, nem továbbít adatokat, hanem az InfluxDB adatait lekérdezve dönt a beavatkozásról.

A vezérlési logika tehát nem szenzorszinten történik, hanem adatbázis-alapon, vagyis a döntés nem a mérés pillanatában születik, hanem egy háttérfolyamat alapján. Az ESP32 lekérdezi az InfluxDB-ből a legfrissebb hőmérséklet, majd ezeket összeveti előre definiált határértékekkel. Ha az értékek meghaladják a beállított küszöböket, az ESP32 egy digitális kimeneten keresztül vezérlőjelet ad, amely bekapcsolja a klímát.

Ez az architektúra azért különleges, mert a döntéshozatal nem az érzékelőnél vagy az MQTT-n keresztül történik, hanem a tárolt és aggregált adat alapján. Ez lehetővé teszi, hogy ne csak egyetlen pillanatnyi értékre reagáljon a rendszer, hanem akár átlagolt, szűrt vagy időbeli trendeket figyelembe vevő logikát is alkalmazzon. Ez csökkenti a téves riasztások és túlgyakori kapcsolgatás lehetőségét.

Ez a megközelítés tehát egy centrális, adatvezérelt automatizációs logikát valósít meg, ahol az ESP32 mikrokontroller már nem adatforrásként, hanem vezérlőegységként működik és közvetlen kapcsolatban áll a fizikai eszközökkel, amelyeket működtet. A döntés meghozatalát a mért adatokra épülő, központilag tárolt és elemezhető információk alapozzák meg, nem az egyes szenzorok aktuális állapota.

A páraelszívó automatikus vezérlése ebben az esetben nem ki- és bekapcsoláson alapul, hanem a készülék folyamatos működése mellett a teljesítmény dinamikus szabályozásán. Ez azt jelenti, hogy a rendszer az aktuálisan mért páratartalom értékek alapján határozza meg, milyen intenzitással dolgozzon a páraelszívó például alacsony, közepes vagy magas fokozaton.

A működés alapját továbbra is egy DHT22 szenzor adja, amely a konyhában folyamatosan méri a páratartalmat. Az adatokat az ESP32 mikrokontroller továbbítja MQTT-n keresztül a Mosquitto brokerhez, ahonnan azok a Telegraf segítségével bekerülnek az InfluxDB adatbázisba. Az adatbázisban rögzített értékek alapján egy külön, vezérlésre dedikált ESP32 rendszeresen lekérdezi a legfrissebb méréseket, és ezek alapján meghatározza a páraelszívó működési szintjét.

A szabályozási logika az alábbi módon épül fel:

- 85% felett: magas fokozat,
- 70–85% között: közepes fokozat,
- 55–70% között: alacsony fokozat,
- 40–55% között: minimum fokozat,
- 40% alatt: passzív fokozat.

A vezérlő ESP32 ezek alapján egy digitális kimenet segítségével változtatja a páraelszívó teljesítményszintjét.

Ez a fajta vezérlés nemcsak hatékonyabb páraszabályozást tesz lehetővé, hanem növeli a berendezés élettartamát is, mivel elkerülhetők a gyakori ki- és bekapcsolási ciklusok. A rendszer rugalmasságának köszönhetően a logika szükség esetén tovább bővíthető.

Használati esetek

Use Case 1: Szenzoradat küldése

- Szereplő: ESP32 mikrokontroller
- Cél: A mért értékek elküldése MQTT brokeren keresztül.
- Előfeltétel: A szenzor működőképes és csatlakoztatva van az ESP32-höz.
- Fő forgatókönyv:
    1. A szenzor adatot mér.
    2. Az ESP32 lekéri az adatot.
    3. Az ESP32 MQTT-n keresztül elküldi a mért adatot egy meghatározott topicra.
- Utófeltétel: Az üzenet sikeresen megjelenik a brokerben.

Use Case 2: Adatok mentése az InfluxDB-be

- Szereplő: Telegraf
- Cél: A brokerből érkező üzenetek átvezetése az InfluxDB adatbázisba.
- Előfeltétel: A Telegraf megfelelően konfigurált és fut.
- Fő forgatókönyv:
    1. A Telegraf feliratkozik az MQTT topicokra.
    2. Beolvassa a beérkező JSON-formátumú adatokat.
    3. Az adatokat feldolgozza és elmenti az InfluxDB-be.
- Utófeltétel: Az adatok időbélyeggel bekerülnek az adatbázisba.

Use Case 3: Adatok megtekintése a Grafana felületen

- Szereplő: Konyhai dolgozó / Rendszergazda
- Cél: Az InfluxDB-ben tárolt adatok grafikus megjelenítése.
- Előfeltétel: Grafana konfigurálva van és eléri az adatbázist.
- Fő forgatókönyv:
    1. A felhasználó belép a Grafana webes felületére.
    2. Megnyitja a megfelelő dashboardot.
    3. Megtekinti az értékek alakulását időben.
- Utófeltétel: Az adatok vizuálisan megjelennek a felületen.

Use Case 4: Automatikus riasztás küldése

- Szereplő: Grafana
- Cél: Kritikus értékek esetén értesítés küldése.
- Előfeltétel: Határértékek előre beállítva, értesítési csatorna konfigurálva.
- Fő forgatókönyv:
    1. A rendszer folyamatosan monitorozza az értékeket.
    2. Egy mért érték meghaladja a beállított határt.
    3. A rendszer automatikusan riasztást küld egy kör e-mailre.
- Utófeltétel: Az értesítés eljut a célszemélyhez.

Use Case 5: Rendszer konfigurálása

- Szereplő: Rendszergazda
- Cél: Az MQTT topicok, szenzornevek és vizualizációk beállítása.
- Előfeltétel: A rendszergazda rendelkezik a megfelelő jogosultságokkal.
- Fő forgatókönyv:
    1. A rendszergazda eléri a konfigurációs felületet vagy fájlt.
    2. Módosítja a beállításokat (pl. Telegraf config, Grafana dashboard).
    3. Elmenti a változtatásokat.
- Utófeltétel: A rendszer a friss konfigurációval működik tovább.

Összegzés és befejezés

Összeségében ez a feladat rámutatott, hogy mennyi feladat és munka van egy ilyen rendszer tervezés mögött. Ezzel az ötlettel is relatíve sok munka volt annak ellenére, hogy a rendszer egyáltalán nem bonyolult és próbáltam mindent kézzel foghatóan megfogalmazni és össze állítani. A közeljövőben elképzelhető hogy egy hasonló rendszert én is szeretnék megvalósítani, mivel szerintem ez ténylegesen hasznos és ezzel fejlődhetne a vendéglátóipar.

Irodalomjegyzék

[1] „MQTT Basics_ A Complete Guide on the Fundamentals of MQTT”.
[2] „MQTT QoS Levels Explained with Example | QoS 0 , 1, & 2”.
[3] J. Theocharis, „Comparing MQTT Brokers for the Industrial IoT”.
[4] „8 IoT Protocols and Standards Worth Exploring in 2024 | EMQ”, 2024.
[5] „MQTT vs HTTP: Ultimate IoT Protocol Comparison Guide | EMQ”.
[6] „How Can a Temperature Monitoring System Benefit a Restaurant? - Ruuvi”.
[7] „DS18B20 Datasheet(PDF) - Dallas Semiconductor”.
[8] T. Liu, „Digital-output relative humidity & temperature sensor/module DHT22 (DHT22 also named as AM2302)”.
[9] „PZEM-004T-V3.0”.
[10] „ESP32 Dual Core with Arduino IDE | Random Nerd Tutorials”.
[11] „raspberry-pi-4-product-brief”.
[12] „Eclipse Mosquitto”.
[13] „Get started with Grafana and InfluxDB _ Grafana documentation”.

2.58. Smart megoldások és technológiájuk okoslakás, okosotthon

Smart megoldások és technológiájuk okoslakás, okosotthon

Boksán Benedek

GIVK, benedekboksan@gmail.com

Tartalomjegyzék

1 Bevezetés 2
2 Az okosotthon fogalma és alapelvei 4
3 Alapelvek és célok 5
4 Alapvető és alkalmazott technológiák 6
5 Az IoT és kommunikációs protokollok 9
6 Mesterséges intelligencia és gépi tanulás 12
7 Gépi tanulás alkalmazásai 13
8 A Otthoni gépek tanulásának alapfolyamata 14
9 Funkciók és előnyök az okosotthonokban 16
10 Automatizált világítás, fűtés, árnyékolás 20
11 Biztonsági rendszerek 22
12 Energiagazdálkodás 22
13 A jövő trendjei 23
Irodalomjegyzék 24

1 BEVEZETÉS

Az okosotthonok (smart home) koncepciója az elmúlt évtized egyik legdinamikusabban fejlődő technológiai trendje, amely alapvetően átalakítja a hagyományos élőhelyeket, lakóövezeteket. Az intelligens otthonok mögött álló technológiai forradalom – köszönhetően az Internet of Things (IoT), a mesterséges intelligencia (AI), a felhőalapú rendszerek és a vezeték nélküli kommunikáció robbanásszerű fejlődésének – lehetővé teszi, hogy a lakóterek egyre inkább alkalmazkodjanak a felhasználók igényeihez, miközben kényelmet, biztonságot szolgáltatnak és energiahatékonyságot biztosítanak.

Az okosotthon lényege, hogy a háztartási eszközök, a világítás, a klímavezérlés, a biztonsági rendszerek és egyéb funkciók intelligens hálózaton keresztül kapcsolatban állnak, és a felhasználó számára testreszabható, automatizált folyamatokat hoznak létre. Ez a technológiai integráció nem csupán a mindennapi teendőket egyszerűsíti, hanem jelentős energia- és költségmegtakarítást is eredményez, miközben hozzájárul a fenntartható életmód kialakításához.

A digitális átalakulás gyors üteme lehetővé tette, hogy az okosotthon-megoldások már nem luxuscikkek, hanem egyre elérhetőbbek és megfizethetőbbek válnak a átlagos háztartások számára is. A piaci elemzések szerint az okosotthon-technológiák globális piaca 2023-ra elérte a 150 milliárd dollárt, és a következő években további exponenciális növekedésre számítanak. Ez a növekedés részben a fogyasztói igények változásának, részben pedig az innovatív technológiák, például a 5G hálózatok, a fejlett AI-algoritmusok és a hatékonyabb energiamenedzsment-rendszerek elterjedésének köszönhető.

Az okosotthonok fejlődésében kulcsszerepet játszanak a különböző kommunikációs protokollok, mint a Wi-Fi, a Zigbee, a Z-Wave és a Bluetooth Low Energy (BLE), amelyek lehetővé teszik az eszközök zökkenőmentes együttműködését és amelyekről később részletesen is lesz sor. Emellett a mesterséges intelligencia és a gépi tanulás alkalmazása révén ezek a rendszerek képesek tanulni a felhasználói szokásokból, és egyre pontosabban előrejelezni az igényeket. Például egy intelligens termosztát nemcsak beállítható távolról, hanem idővel megtanulja, hogy a család mikor érkezik haza, és ennek megfelelően előre felmelegíti a lakást.

Ezen esszé célja, hogy átfogó képet nyújtson az okosotthon-technológiák aktuális állásáról, bemutatva az alapvető működési elveket, a legfontosabb technológiai komponenseket és a jövőben várható fejlesztéseket. Különös hangsúlyt fektetünk a három legfontosabb területre: a kényelemre, a biztonságra és az energiahatékonyságra. Ezen túlmenően kitérünk a fenntarthatósági kérdésekre, valamint az okosotthonok társadalmi és gazdasági hatásaira.

Végül, de nem utolsósorban, a tanulmány áttekinti a jövő trendjeit, beleértve az 5G technológia integrációját, a házirobotok elterjedését és az okos városokkal való összehangolás lehetőségeit. Mindezek alapján megállapítható, hogy az okosotthonok nem csupán technológiai fejlemények, hanem egy olyan új életforma részei, amely egyre szorosabban összefonódik a modern társadalom igényeivel és a fenntartható jövő kihívásaival.

1. 1975-ben fejlesztették ki az első általános célú otthoni automatizálási hálózati technológiát, az X10-et. Ez egy kommunikációs protokoll elektronikus eszközök számára.

2 AZ OKOSOTTHON FOGALMA ÉS ALAPELVEI

Az „okosotthon” (angolul: smart home) kifejezés napjaink egyik legdinamikusabban fejlődő technológiai területére utal. Egy okosotthon nem csupán modern ház vagy lakás, hanem egy olyan komplex, integrált rendszer, amely lehetővé teszi a különféle háztartási eszközök, világítás, fűtési és hűtési rendszerek, szellőztető berendezések, biztonsági eszközök, szórakoztatóelektronikai rendszerek és egyéb háztartási funkciók intelligens hálózaton keresztül történő összekapcsolását és vezérlését. Ezek a rendszerek képesek egymással kommunikálni, adatokat megosztani, valamint központilag vagy decentralizált módon reagálni a felhasználó utasításaira és a környezetből érkező jelekre.

Az okosotthonok egyik legfontosabb jellemzője, hogy a vezérlésük háromféleképpen is történhet:

- **Manuális vezérlés:** Ebben az esetben a felhasználó közvetlenül irányítja az eszközöket, például okostelefon, tablet vagy számítógép segítségével. A felhasználó mobilalkalmazáson vagy webes felületen keresztül kapcsolhatja le a lámpákat, indíthatja el a mosógépet, vagy szabályozhatja a fűtést, akár otthon, akár távolról.

- **Automatizált vezérlés:** Az automatizálás lényege, hogy előre beállított időzítések vagy érzékelők alapján történik a működés. Például a mozgásérzékelő által észlelt jelenlét hatására felkapcsolódik a világítás, vagy a termosztát a külső hőmérséklethez igazodva szabályozza a fűtést.

- **Adaptív vezérlés:** A legfejlettebb szintet képviseli az adaptív vezérlés, amely mesterséges intelligencia (AI) segítségével tanulja meg a lakók szokásait és preferenciáit. Így például az otthon képes lehet felismerni, hogy a család minden hétköznap reggel 7:00-kor kel fel, és ehhez igazítva automatikusan beindítja a kávéfőzőt, felhúzza a redőnyöket és bekapcsolja a reggeli híreket a televízión.

Az okosotthon nem csupán a kényelmet szolgálja, hanem biztonsági, gazdaságossági és környezetvédelmi előnyöket is kínál. A technológiai fejlődés lehetővé teszi, hogy ezek a rendszerek egyre elérhetőbbé váljanak, így már nem csupán luxuskategóriának számítanak, hanem egyre több háztartásban jelennek meg.

3 ALAPELVEK ÉS CÉLOK

Az okosotthon-rendszerek tervezésekor és kivitelezésekor több kulcsfontosságú alapelvet és célt vesznek figyelembe, amelyek meghatározzák az ilyen rendszerek funkcióit és működését. Ezek közül a legfontosabbak:

- **Kényelem**
  Az egyik legfőbb cél a lakók életminőségének javítása a mindennapi rutinok automatizálása révén. Az okosotthon képes a különböző berendezések és szolgáltatások összehangolására, így a felhasználóknak kevesebb dolgot kell manuálisan elvégezniük. Például egy előre programozott „reggeli rutin" során a világítás fokozatosan felkapcsolódik, a fűtés vagy hűtés elindul, és a kávéfőző is automatikusan bekapcsol. Ezzel a technológia alkalmazkodik a felhasználók napi ritmusához és szokásaihoz.

- **Biztonság**
  Az okosotthonok másik kiemelt funkciója a biztonság növelése. A különböző érzékelők (mozgásérzékelők, nyitásérzékelők, kamerák, füst- és gázérzékelők) folyamatosan figyelik a környezetet, és veszély esetén azonnal riasztják a tulajdonost, sőt szükség esetén a hatóságokat is. Például ha a rendszer betörési kísérletet észlel, automatikusan értesítést küld a tulajdonos mobiltelefonjára, bekapcsolja a szirénát, és aktiválja a biztonsági kamerákat. Tűz vagy szivárgás esetén a rendszer azonnal lekapcsolhatja az elektromos áramot vagy a vízellátást, csökkentve a kár mértékét.

- **Energiatakarékosság**
  Az energiatudatos működés szintén alapvető cél. Az okos rendszerek képesek optimalizálni az energiafelhasználást azáltal, hogy csak akkor és ott kapcsolják be a világítást vagy a fűtést, ahol és amikor arra valóban szükség van. Egy intelligens termosztát figyelembe veszi a külső hőmérsékletet, a ház szigetelési adottságait és a bent tartózkodók napi programját, így hatékonyan szabályozza a fűtést, csökkentve a pazarlást. A világítás is automatikusan lekapcsolható, ha nincs mozgás az adott helyiségben, és a redőnyök automatikus vezérlésével a természetes fény optimális kihasználása is megvalósítható.

- **Távoli vezérlés**
  Az internetkapcsolattal ellátott rendszerek lehetővé teszik, hogy az otthon minden funkciója elérhető legyen akár a világ másik végéből is. Ez különösen hasznos lehet nyaralás vagy üzleti út alatt, hiszen a felhasználó ellenőrizheti, hogy bezárta-e az ajtót, lekapcsolta-e a világítást vagy beállította-e a riasztórendszert. Ezenkívül távolról is módosíthatók a beállítások, például ha egy hideg napon hazaindulás előtt szeretnénk felmelegíteni a lakást.

4 ALAPVETŐ ÉS ALKALMAZOTT TECHNOLÓGIÁK

Az okosotthonok működését és képességeit különféle technológiák együttműködése teszi lehetővé. Ezeket két fő kategóriába sorolhatjuk: hardveres komponensek és szoftveres platformok. A rendszer elemei közötti hatékony kommunikáció, az adatok feldolgozása és a vezérlés mind ezen technológiai alapokra épül. Az alábbiakban részletesen bemutatjuk, hogy milyen eszközök és rendszerek alkotják az okosotthon technológiai gerincét.

Főbb okosotthon komponensek:

Az okosotthon hardveres alapjai nélkülözhetetlenek a fizikai világ és a digitális vezérlés összekapcsolásához. Ezek az eszközök gyűjtik az adatokat, végrehajtják a parancsokat, és lehetővé teszik az automatizálást. A legfontosabb kategóriák közé a szenzorok, az aktuátorok és a központi egység tartoznak.

- Szenzorok
  A szenzorok (érzékelők) kulcsfontosságúak az okosotthonok működésében, hiszen ezek segítségével gyűjt adatokat a rendszer a környezetről. Ezek az adatok alapozzák meg az automatizált vagy adaptív döntéshozatalt.

- Mozgásérzékelők: Ezek az eszközök detektálják az emberi mozgást, és gyakran használják őket világításvezérlésre, riasztórendszerek részeként, vagy energiatakarékos megoldásokban. Például egy mozgásérzékelő automatikusan felkapcsolhatja a lámpát, ha belépünk egy szobába.

- Hőmérséklet-érzékelők: Szabályozzák a fűtési és hűtési rendszerek működését. Az intelligens termosztátok ezekre az érzékelőkre támaszkodva tartják fenn az ideális hőmérsékletet.

- Páratartalom-érzékelők: Ezek különösen hasznosak fürdőszobákban, konyhákban és pincehelyiségekben. Ha a páratartalom meghalad egy bizonyos szintet, a rendszer automatikusan bekapcsolhatja a szellőztetést vagy páramentesítőt.

- Fényérzékelők: Az érzékelt fényviszonyok alapján vezérelhető a világítás. Például este automatikusan felkapcsolódhatnak a lámpák, vagy sötétedéskor lehúzódnak a redőnyök.

- Aktuátorok
  Az aktuátorok azok az eszközök, amelyek a vezérlőegységek utasításait végrehajtják. Ők végzik el a „fizikai” munkát, vagyis kapcsolnak, mozgatnak, szabályoznak.

- Okos kapcsolók és aljzatok: Ezek lehetővé teszik a világítás, háztartási eszközök vagy akár a kávéfőző vezérlését is okoseszközökről vagy automatizált parancsok alapján.

- Motorizált redőnyök, árnyékolók: A fényérzékelők vagy időzítések alapján képesek automatikusan fel- vagy lehúzni a redőnyöket. Ez nemcsak kényelmi funkció, hanem az energiahatékonyságot is segíti – például meggátolja a nyári túlmelegedést vagy segíti a téli hőszigetelést.

- Intelligens termosztátok és radiátorszelepek: Ezek finoman szabályozzák az otthon hőmérsékletét, időzíthetők és távvezérelhetők. Tanulni is képesek, és alkalmazkodnak a lakók szokásaihoz.

- Központi egység (Smart Hub)
  Az okosotthon szíve a központi vezérlőegység, amely összeköti a különböző szenzorokat, aktuátorokat, valamint a felhasználói felületet.

- Smart Hub-ok: Ilyen például a Samsung SmartThings, a Google Nest Hub vagy az Amazon Echo. Ezek az eszközök összekötik a rendszer elemeit, koordinálják a működést, és lehetővé teszik a különböző gyártók eszközeinek együttes használatát. A Smart Hub gyakran tartalmaz hangvezérlési funkciót is, amely révén a felhasználók egyszerű hangparancsokkal irányíthatják otthonukat.

- Kommunikációs protokollok: A Smart Hub-ok különböző protokollokat használnak, mint például Wi-Fi, Zigbee, Z-Wave vagy Thread. Ezek biztosítják a stabil, gyors és biztonságos kommunikációt az eszközök között.

- 3.2 Szoftveres platformok
  A hardveres komponensek működését különféle szoftverek hangolják össze. Ezek kezelik a beállításokat, szabályozzák az automatizmusokat, és tárolják az adatokat. A szoftveres platformok lehetnek felhőalapúak vagy helyi vezérlésűek.

- Felhőalapú megoldások
  A felhőalapú rendszerek lényege, hogy az eszközök által gyűjtött adatokat interneten keresztül egy távoli szerveren (felhőben) tárolják, dolgozzák fel és elemzik. A felhasználó ezekhez egy applikáción vagy webes felületen keresztül fér hozzá, és a parancsokat az interneten keresztül küldi az otthoni eszközöknek.

- Google Home: A Google által fejlesztett platform, amely egyszerűen integrálható a Nest termosztátokkal, kamerákkal, okos lámpákkal és más eszközökkel. A Google Asszisztens segítségével hangvezérlés is megvalósítható.

- Apple HomeKit: Az Apple saját okosotthon-keretrendszere, amely a Home alkalmazáson keresztül kezelhető iOS eszközökről. A rendszer erősen fókuszál a biztonságra, és az Apple-ökoszisztémán belüli szoros integrációt kínál.

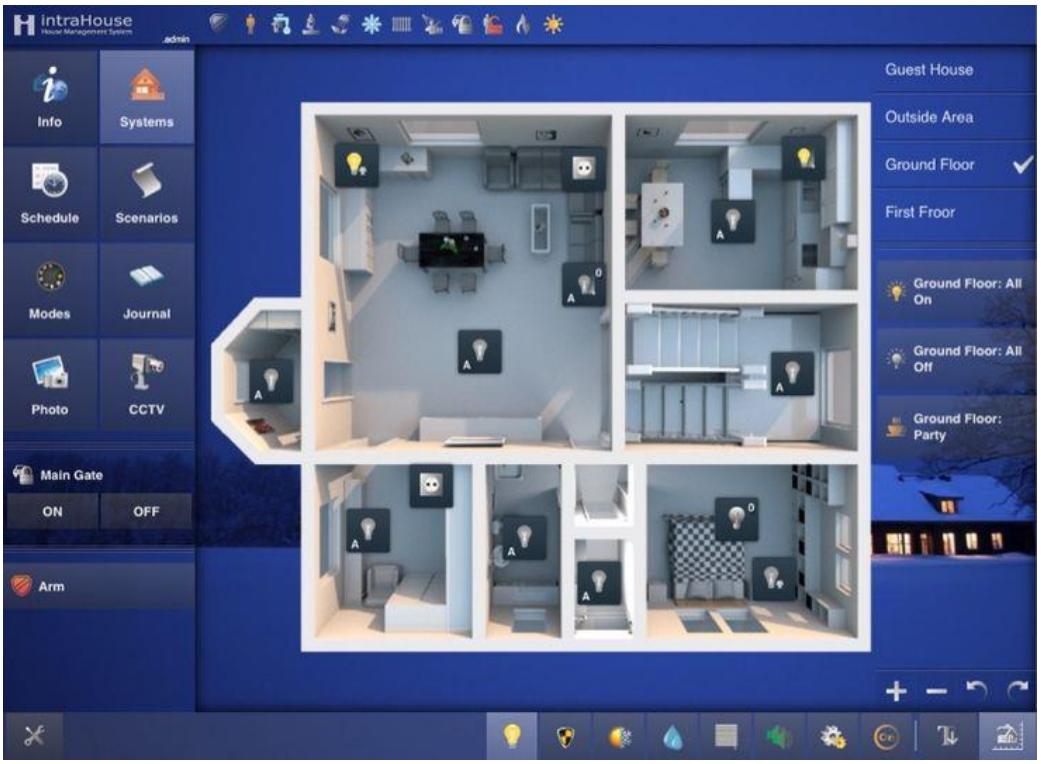
- A felhőalapú megoldások előnye, hogy rendkívül felhasználóbarátok, egyszerűen konfigurálhatók és a világ bármely pontjáról elérhetők. Hátrányuk viszont, hogy működésük az internetkapcsolattól függ, valamint az adatbiztonság kérdése sokak számára érzékeny téma lehet.

- Helyi vezérlés
  A helyi vezérlésre épülő rendszerek nem igényelnek állandó internetkapcsolatot, és a vezérlés az otthon belső hálózatán keresztül történik. Ez megnöveli az adatbiztonságot, valamint csökkenti az adatvédelmi kockázatokat.

- Home Assistant: Nyílt forráskódú szoftver, amely lehetővé teszi a felhasználó számára, hogy teljes mértékben személyre szabja az okosotthon működését. Támogatja a legtöbb ismert eszközt és protokollt. Fejlett felhasználóknak ajánlott, akik nagyobb szabadságot keresnek.

- OpenHAB: Szintén nyílt forráskódú megoldás, amely platformfüggetlen működést tesz lehetővé, és számos eszközt integrálhat. Különösen erős a szabályalapú automatizálás területén, és kifejezetten a helyi hálózati működésre lett optimalizálva.

- A helyi vezérlésű rendszerek előnye, hogy stabilabbak lehetnek az internetkimaradások idején is, emellett nem függnek külső szolgáltatóktól. Hátrányuk lehet a bonyolultabb konfigurálás és a technikai tudás szükségessége.



2. Az okosotthon általános komponenseinek vizuális megjelenítése

5 AZ IOT ÉS KOMMUNIKÁCIÓS PROTOKOLLOK

IoT (Internet of Things)

Az Internet of Things (IoT), magyarul „a dolgok internete”, egy olyan technológiai koncepció, amelynek lényege, hogy különféle fizikai eszközök – érzékelők, aktuátorok, háztartási gépek, ipari berendezések, járművek stb. – internetkapcsolaton keresztül képesek kommunikálni egymással és adatokat cserélni. Ezek az eszközök gyakran beágyazott rendszereket tartalmaznak, amelyek lehetővé teszik számukra, hogy környezeti adatokat gyűjtsenek, döntéseket hozzanak, vagy parancsokat hajtsanak végre – mindezt emberi beavatkozás nélkül vagy minimális felügyelet mellett.

Az IoT alapvető célja, hogy automatizálja a folyamatokat, optimalizálja az energiafelhasználást, növelje a hatékonyságot, valamint fokozza a kényelmet és a biztonságot. A rendszer kulcsfontosságú eleme a felhőalapú adatfeldolgozás, amely lehetővé teszi a begyűjtött adatok távoli elérését, tárolását és elemzését.

Az IoT egyik legfontosabb előnye, hogy a valós idejű adatok segítségével lehetőség nyílik gyors és pontos döntéshozatalra. Az ipari IoT (IIoT) például lehetővé teszi a gépek prediktív karbantartását, csökkentve ezzel a leállási időt és a költségeket. Az okosvárosok területén pedig olyan megoldások születnek, mint az intelligens közlekedési rendszerek vagy az automatizált közvilágítás.

Példák az IoT-eszközökre

Okos hőmérő (Nest Thermostat): Ez az eszköz képes tanulni a felhasználói szokásokat, és azok alapján automatikusan beállítani a fűtést vagy hűtést, ezáltal optimalizálva az energiafogyasztást. Távvezérléssel, mobiltelefonról is irányítható, és képes kommunikálni más okoseszközökkel.

Intelligens biztonsági kamera (Ring Doorbell): Ez a megoldás lehetővé teszi, hogy a felhasználó akár távolról is lássa és hallja, ki áll az ajtó előtt. A rendszer mozgásérzékelőt, mikrofont, kamerát és hangszórót használ, és valós idejű értesítéseket küld a felhasználó telefonjára. A rögzített videók felhőben tárolhatók, ami növeli a biztonságot.

Protokollok összehasonlítása

Az IoT rendszerek hatékony működéséhez elengedhetetlen a megfelelő kommunikációs protokoll kiválasztása. Ezek a protokollok határozzák meg, hogy az eszközök hogyan kommunikálnak egymással, milyen sebességgel, mekkora hatótávolságon, milyen energiafelhasználás mellett, és mennyire megbízhatóan. Az alábbiakban négy gyakran alkalmazott protokoll kerül összehasonlításra.

- **Wi-Fi**

A Wi-Fi az egyik legismertebb és legelterjedtebb protokoll, amelyet az IoT-eszközök kommunikációjára is használnak. Előnye a nagy adatátviteli sebesség, ami ideálissá teszi olyan alkalmazásokhoz, ahol videóátvitelre vagy nagy mennyiségű adat továbbítására van szükség (például biztonsági kamerák esetében). Ugyanakkor a magas energiafogyasztás miatt nem a legjobb választás akkumulátorral működő, kis teljesítményű eszközökhöz. Továbbá, a Wi-Fi-hálózat torlódása és a biztonsági kihívások is nehezítik az alkalmazását nagy léptékű IoT-rendszerekben.

- **Zigbee**

A Zigbee egy alacsony energiaigényű, alacsony adatátvitelű vezeték nélküli hálózati protokoll, amelyet kifejezetten az IoT igényeire fejlesztettek ki. A Zigbee mesh hálózatot használ, vagyis az eszközök egymás jeleit továbbítják, ezáltal megnövelhető a lefedettség. Hátránya, hogy hatótávolsága korlátozott, főként beltéri használatra alkalmas. Előnye viszont a kiváló energiahatékonyság, amely lehetővé teszi, hogy az eszközök akár éveken át is működjenek elemről.

- **Z-Wave**

A Z-Wave szintén alacsony energiaigényű protokoll, amely nagyon hasonlít a Zigbee-re, de más frekvenciasávban működik, így kevésbé érzékeny az interferenciára. Különösen népszerű az otthoni automatizálásban, mivel megbízható és stabil kommunikációt biztosít. Az egyik fő hátránya a magasabb költség, valamint az, hogy kevesebb gyártó kínál Z-Wave-kompatibilis eszközöket, mint Zigbee-alapúakat.

- **Bluetooth Low Energy (BLE)**

A BLE az okoseszközök (például fitneszkarkötők, okosórák) egyik leggyakrabban használt kommunikációs technológiája. Előnye az alacsony energiafogyasztás és az egyszerű párosítás, amely lehetővé teszi, hogy a felhasználók gyorsan csatlakoztassák eszközeiket okostelefonjukhoz. Ugyanakkor a rövid hatótávolság és a korlátozott sávszélesség miatt nem alkalmas nagyobb rendszerek kiépítésére vagy nagy adatmennyiség kezelésére.

A kommunikációs protokollok előnyei és hátrányai

Technológia	Előnyök	Hátrányok
Wi-Fi	Nagy adatátviteli sebesség; ideális videóátvitelhez és nagy adatmennyiséghez	Magas energiafogyasztás; hálózati torlódás; biztonsági kockázatok nagy rendszerekben
Zigbee	Alacsony energiafogyasztás; mesh hálózat; hosszú elemélettartam	Korlátozott hatótávolság; főként beltéri használatra
Z-Wave	Stabil, megbízható kommunikáció; alacsony interferencia; otthoni automatizálásra ideális	Magasabb költség; kevesebb kompatibilis eszköz érhető el
Bluetooth Low Energy (BLE)	Nagyon alacsony energiafogyasztás; gyors és egyszerű párosítás mobil eszközökkel	Rövid hatótávolság; korlátozott sávszélesség; nem ideális nagy rendszerekhez

6 MESTERSÉGES INTELLIGENCIA ÉS GÉPI TANULÁS

A digitális technológia rohamos fejlődésével párhuzamosan a mesterséges intelligencia (AI) és a gépi tanulás (machine learning – ML) egyre nagyobb szerepet kap a mindennapi életben. Míg korábban az automatizált rendszerek előre beprogramozott logika alapján működtek, addig a mai intelligens rendszerek már képesek tanulni, alkalmazkodni, és a felhasználó szokásai alapján döntéseket hozni. Ennek egyik legszemléletesebb és leggyorsabban fejlődő területe az okosotthon-technológia, ahol az AI és ML képessé teszi az eszközöket arra, hogy ne csak végrehajtsák a parancsokat, hanem valóban „értsék" is a környezetüket és a felhasználók igényeit.

AI az okosotthonban

Az okosotthonokban használt mesterséges intelligencia olyan rendszereket foglal magában, amelyek képesek kommunikálni a felhasználóval és más eszközökkel, valamint a kapott információk alapján döntéseket hozni. Ezek az AI-megoldások nemcsak a kényelmet szolgálják, hanem biztonságot, energiahatékonyságot és egyéni preferenciák szerinti működést is biztosítanak.

Az egyik legelterjedtebb formája az AI jelenlétének az otthonokban a hangvezérlés, amely lehetővé teszi, hogy a felhasználó szóban adjon utasításokat különféle eszközöknek. Ezek a rendszerek természetes nyelvfeldolgozást alkalmaznak, amelynek révén képesek értelmezni a hétköznapi beszédet. Egy ilyen rendszer nem csupán azt ismeri fel, hogy mit mondunk, hanem azt is képes megérteni, hogy mit akarunk vele elérni, és a háttéradatok – például a napszak, a korábbi használati minták, vagy az időjárás – alapján intelligens döntéseket hozhat.

A hangvezérlés azonban csak egyetlen példája annak, hogyan teszi az AI személyre szabottabbá az otthonokat. Egy másik fontos terület a prediktív szabályozás, amelynek során az intelligens rendszer képes a felhasználó napi rutinját megfigyelni és megtanulni. Így például a fűtés, a világítás, vagy a redőnyök működtetése idővel automatikussá válhat, anélkül, hogy azt manuálisan kellene beállítani. A rendszer előre tudja, mikor van szükség hőmérséklet-emelésre vagy világításra, és akkor aktiválja az adott funkciókat, amikor arra ténylegesen szükség van. Ez nemcsak kényelmet nyújt, hanem energia-megtakarítással is jár.

További jellemzője az AI-okosotthon rendszereknek, hogy képesek integráltan működni. Az egyes rendszerek – például biztonsági kamerák, zárak, termosztátok vagy világítás – közös platformon keresztül kommunikálnak, és az AI a különböző adatok összehangolása révén képes komplex döntésekre. Egy jól beállított rendszer például érzékelheti, hogy a felhasználó hazaérkezett, és ezzel egy időben felkapcsolhatja a kültéri fényt, kinyithatja az ajtót, bekapcsolhatja a fűtést, sőt, akár a kedvenc zene lejátszását is megkezdheti.

A prediktív szabályozás fejlettebb AI-megoldásai már nemcsak az eszközhasználat gyakoriságát, hanem a felhasználó viselkedésmintáit is képesek értelmezni. Egy adott rendszer például megfigyelheti, hogy a lakók melyik szobát használják leggyakrabban egy adott napszakban, és ehhez igazítja a világítási vagy hőmérsékleti beállításokat. Ezzel a rendszer nemcsak kényelmet biztosít, hanem csökkenti a felesleges energiafelhasználást is, amely hosszú távon anyagi megtakarításhoz vezet.

7 GÉPI TANULÁS ALKALMAZÁSAI

A mesterséges intelligencia (MI) és a gépi tanulás (ML) az okosotthonok technológiai hátterének két legmeghatározóbb pillére, de bár szorosan összekapcsolódnak, funkcióik és működésük eltérőek. Míg az MI az általános intelligens működést biztosítja – vagyis lehetővé teszi, hogy egy rendszer különböző forrásokból származó információk alapján „értelmesen" reagáljon –, addig a gépi tanulás az a terület, amely lehetővé teszi, hogy a rendszer a saját tapasztalataiból fejlődjön, önállóan tanuljon és alkalmazkodjon új helyzetekhez.

A gépi tanulás lényege, hogy az algoritmusok képesek nagymennyiségű adatot gyűjteni, azokat elemezni, és ezek alapján szabályokat, mintázatokat, összefüggéseket felismerni. Ez a folyamat teszi lehetővé, hogy a rendszer új szituációkra is releváns választ adjon anélkül, hogy külön be kellene programozni minden eshetőségre. Ahogy a Google mesterséges intelligenciáért felelős egyik vezetője fogalmazott: „Nem az a cél, hogy a gépet mindenre megtanítsuk, hanem hogy a gép maga tanulja meg, hogyan tanuljon." Ez a gondolat jól tükrözi a gépi tanulás lényegét és szerepét a modern technológiákban.

Az egyik legismertebb és legpraktikusabb alkalmazási terület az anomáliadetektálás. Az intelligens otthonokban ez azt jelenti, hogy a rendszer képes észlelni, ha valamely eszköz vagy viselkedés eltér a megszokottól. Például ha egy háztartási gép – mondjuk egy hűtőszekrény – hirtelen szokatlanul sok áramot kezd el fogyasztani, a rendszer ezt rögzíti, és figyelmeztetést küld a felhasználónak. Ez korai jelzés lehet egy műszaki meghibásodásról, vagy épp az energiapazarlás egyik forrására hívhatja fel a figyelmet. Ugyanez a logika alkalmazható a biztonsági rendszerekben is: ha például egy mozgásérzékelő éjjel aktivitást jelez, miközben a tulajdonos nyaralni van, a rendszer azonnal automatikusan riaszthat, bekapcsolhatja a világítást, kamerát, vagy aktiválhat egy előre beállított biztonsági protokollt. Ezek a funkciók egyre kifinomultabbak, és képesek különbséget tenni például egy kisállat mozgása és egy emberi jelenlét között.

A gépi tanulás másik figyelemre méltó területe a beszédfelismerés. Az okoseszközök – például Amazon Alexa, Google Assistant, Apple Siri – mind ilyen technológiára támaszkodnak, hogy értelmezzék a felhasználó verbális utasításait. Ami kezdetben sok esetben félreértésekkel járt, ma már egyre pontosabban működik, köszönhetően annak, hogy az algoritmusok folyamatosan „tanulnak". A rendszer idővel egyre jobban alkalmazkodik a felhasználó hangjához, beszédtempójához, kiejtéséhez, és nem csupán a szavakat érti meg, hanem a kontextust is felismeri. Egy felhasználó így ma már sokkal természetesebb módon kommunikálhat az eszközeivel. „A jó MI nemcsak érti, amit mondanak neki – hanem azt is, hogy mit akarnak vele közölni" – jegyezte meg egy természetes nyelvfeldolgozással foglalkozó kutató.

A fejlődő beszédfelismerési rendszereknek különösen nagy jelentősége van azok számára, akik valamilyen mozgáskorlátozással élnek. Számukra az, hogy hangutasításokkal irányíthatják otthonuk világítását, fűtését vagy akár zenelejátszóját, nemcsak kényelmi, hanem alapvető életminőségi előnyöket is jelent. Ráadásul a természetes nyelvi feldolgozásnak köszönhetően már nem csupán egyszerű parancsszavakat kell használni, hanem a rendszer képes értelmezni a bonyolultabb, hétköznapi nyelvezetet is. Így például egy olyan mondatra, hogy „Kapcsold le a villanyt, kérlek", a rendszer nemcsak azt tudja, hogy a világításról van szó, hanem azt is, hogy a felhasználó épp abban a helyiségben tartózkodik, ahol a világítást le kell kapcsolni – tehát helyileg is kontextusérzékenyen reagál.

Végső soron a gépi tanulás révén az okosotthon egyre intelligensebbé válik – nem csupán a szó technikai értelmében, hanem a felhasználó szempontjából is. Azáltal, hogy a rendszer adatokat gyűjt és elemez a mindennapi használat során, képes folyamatosan finomítani a működését. Ez vonatkozik a fűtés- és hűtésszabályozásra, a világítási szokásokra, az eszközhasználati preferenciákra, sőt akár az alvási vagy táplálkozási mintákra is. Az ilyen rendszerek hosszabb távon nemcsak kényelmesebbé, hanem takarékosabbá és biztonságosabbá is teszik az otthonokat.

8 A OTTHONI GÉPEK TANULÁSÁNAK ALAPFOLYAMATA

1. Adatgyűjtés (LOAD DATA)

- **Cél:** A modell tanulásához szükséges adatok összegyűjtése.

  Otthoni példa:

  - Okosotthon eszközök adatainak rögzítése (pl. hőmérséklet, páratartalom, energiafogyasztás).
  - Képek vagy hangfelvételek gyűjtése intelligens kamerákból/hangvezérlőkből.

2. Adatelőkészítés (LOTA - Load, Organize, Transform, Analyze)

- **Cél:** A nyers adatok tisztítása és strukturálása.

  Fontos lépések:

  - Hiányzó adatok kezelése.
  - Adatok normalizálása (pl. hőmérsékleti értékek skálázása).
  - Szükség esetén címkézés (felügyelt tanuláshoz).

3. Modell kiválasztása és tanítása (TRAIN MODEL)

- **Cél:** A gépi tanulási algoritmus "betanítása" az adatokra.

  Otthoni alkalmazások:

  - Besorolás (Classification): Pl. mozgásérzékelés alapján "családtag" vs. "idegen" felismerése.
  - Regresszió (Regression): Pl. energiafogyasztás előrejelzése a múltbeli adatok alapján.
  - Klaszterezés (Clustering): Pl. használati minták felismerése okos lámpák esetében.

4. Modell kiértékelése (EVALUATE MODEL)

- **Cél:** A modell pontosságának tesztelése új adatokon.

  Metrikák:

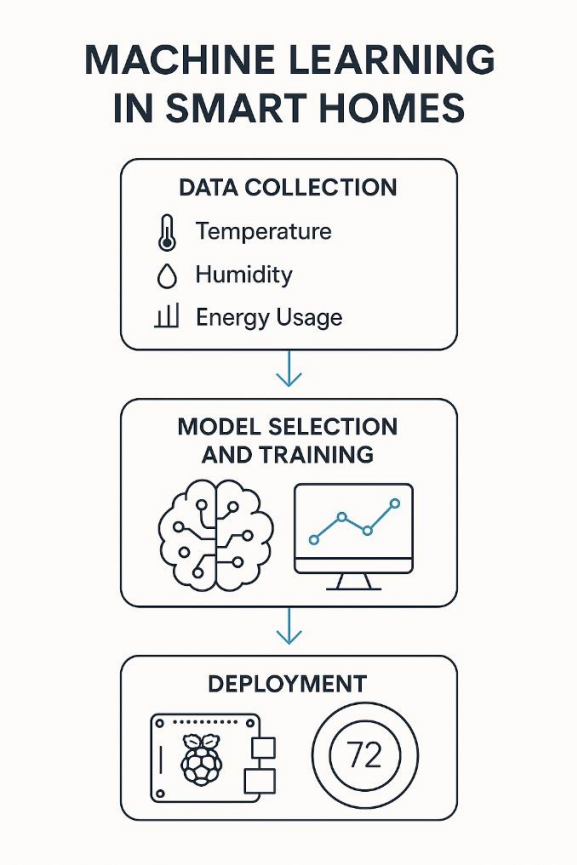
  - Pontosság (Accuracy).
  - Precizitás és visszahívás (Precision & Recall) biztonsági rendszereknél.
  - Hibaérték (MSE - Mean Squared Error) előrejelző modelleknél.

5. Hiperparaméter-hangolás (HYPERPARAMETER TUNING)

- **Cél:** A modell teljesítményének finomhangolása.
- Példák:
    - Tanulási ráta (Learning Rate) beállítása.
    - Neurális hálók rétegeinek optimalizálása.

6. Üzembe helyezés és folyamatos fejlesztés

- **Otthoni integráció:**
    - A modell beágyazása okoseszközökbe (pl. Raspberry Pi, okos termosztát).
    - Folyamatos adatgyűjtés és újratanítás (Online Learning).



3. Az okosgépek tanulásának alapfolyamata vizualizálva

9 FUNKCIÓK ÉS ELŐNYÖK AZ OKOSOTTHONOKBAN

Az okosotthonok technológiája nem pusztán a modern kor divatos vívmánya – ezek a rendszerek kézzelfogható előnyöket kínálnak a mindennapok során. A legfontosabb cél a felhasználók életminőségének javítása, a háztartási folyamatok kényelmesebbé, biztonságosabbá és energiahatékonyabbá tétele. Ebben a fejezetben három fő területet vizsgálunk meg részletesen: a kényelmet, a biztonságot és az energiahatékonyságot. Ezek az okosotthon leggyakrabban emlegetett és legfontosabb funkcionális előnyei.

Kényelem

Az okosotthon egyik legkézenfekvőbb előnye a megnövelt kényelem. A technológia lehetővé teszi, hogy az otthonunk alkalmazkodjon az életvitelünkhöz, ahelyett hogy nekünk kellene minden részletre odafigyelnünk. A felhasználók testre szabhatják a rendszert az igényeik szerint, és különféle automatizált forgatókönyveket hozhatnak létre.

Forgatókönyvek és jelenetek

A különböző eszközök integrációja lehetővé teszi, hogy egyetlen gombnyomással vagy parancsszóval több eszköz is egyszerre reagáljon. Az úgynevezett „jelenetek” vagy „forgatókönyvek” (angolul: scenes) például több eszköz egyidejű működtetését jelentik egy adott cél érdekében.

„Filmnézés mód”: Amikor a felhasználó elindítja ezt a jelenetet, a világítás automatikusan tompul vagy kikapcsol, a redőnyök leereszkednek, a hangrendszer és a televízió bekapcsol, így ideális környezet jön létre a mozizáshoz. Ez nemcsak kényelmes, de hangulati szempontból is jelentős élménynövekedést hoz.

„Reggeli rutin”: Az ébresztő megszólalásával együtt automatikusan felkapcsol a fürdőszobai világítás, bekapcsol a kávéfőző, elindul a reggeli hírek lejátszása, és a termosztát kényelmes hőmérsékletet biztosít az ébredéshez.

Távoli vezérlés

A másik fő kényelmi tényező a távoli elérés lehetősége. Az okosotthon rendszerek mobilalkalmazásokon vagy webes felületen keresztül bárhonnan vezérelhetők, amennyiben internetkapcsolat rendelkezésre áll.

Például egy utazás során a felhasználó ellenőrizheti, hogy lekapcsolta-e a világítást, bezárta-e az ajtókat, vagy éppen milyen hőmérséklet uralkodik otthon. Ha szükséges, módosíthatja a beállításokat, beengedhet egy vendéget az okoszár segítségével, vagy akár ellenőrizheti a kamerafelvételeket is.

Szülők gyakran használják ezt a lehetőséget arra, hogy megbizonyosodjanak arról: gyermekeik biztonságban hazaértek-e, vagy nem maradt-e bekapcsolva egy veszélyes eszköz, mint például a sütő.

A távoli vezérlés kiterjedhet hangalapú asszisztensekre is – például az Amazon Alexa vagy a Google Asszisztens –, amelyek lehetővé teszik, hogy szóban adjunk parancsokat akkor is, ha nem tartózkodunk közvetlenül a vezérelni kívánt eszköz közelében.

Okos zárak

Az okos zárak lehetővé teszik a kulcs nélküli hozzáférést. A hagyományos kulcs helyett digitális azonosítás történik, ami lehet:

- PIN-kód
- Mobiltelefonos alkalmazás
- Bluetooth/NFC kapcsolat
- Arcfelismerés vagy ujjlenyomat

Ez különösen előnyös lehet akkor, ha például vendégek vagy szolgáltatók (pl. takarítók, karbantartók) számára időszakos hozzáférést szeretnénk biztosítani anélkül, hogy fizikai kulcsot adnánk át. Továbbá bármikor visszavonható az adott kód vagy hozzáférés, így magas fokú kontrollt és rugalmasságot kapunk.

Riasztórendszerek

A modern okosriasztók többféle érzékelő segítségével képesek felismerni a gyanús aktivitásokat:

Mozgásérzékelők: Érzékelik, ha valaki áthalad egy adott területen. Beállíthatók úgy, hogy csak akkor jelezzenek, ha a házban senki nincs.

Nyitásérzékelők: Ajtókra és ablakokra szerelhetők. Ha egy nyílászárót jogosulatlanul kinyitnak, a rendszer automatikusan riasztást indít, vagy értesíti a tulajdonost.

Kamerarendszerek: A legtöbb modern biztonsági kamera mozgásérzékelővel van ellátva, sőt, néhány arcfelismerésre vagy rendszámfelismerésre is képes. A felhasználó valós időben betekinthet a felvételekbe, és értesítést kap, ha szokatlan mozgást észlel a rendszer.

Hangriasztók: Ha a rendszer betörést észlel, azonnal bekapcsolhat egy erős hangriasztót, amely nemcsak elriasztja a betörőt, hanem felhívja a környezet figyelmét is.

A biztonsági funkciók éjjel-nappal felügyeletet biztosíthatnak, és lehetőséget adnak a tulajdonosnak arra, hogy bármikor és bárhonnan reagáljon a fenyegetésekre.

Energiahatékonyság

Az energiatakarékosság nemcsak a környezetvédelem, hanem a háztartási költségek csökkentése szempontjából is rendkívül fontos. Az okosotthonok lehetőséget adnak arra, hogy optimalizáljuk az energiafelhasználást.

Okos hőmérséklet-szabályozás

A hagyományos termosztátokkal ellentétben az okos termosztátok „tanulni” is képesek. Megfigyelik a lakók jelenlétét, szokásait, és ezek alapján automatikusan szabályozzák a fűtést vagy hűtést.

Például ha a család minden nap reggel 8-kor elhagyja a lakást, a rendszer automatikusan lejjebb veszi a fűtést vagy klímát. Amikor délután 5 óra körül hazaérkeznek, a rendszer előre bekapcsolja a fűtést, hogy kellemes hőmérséklet várja őket.

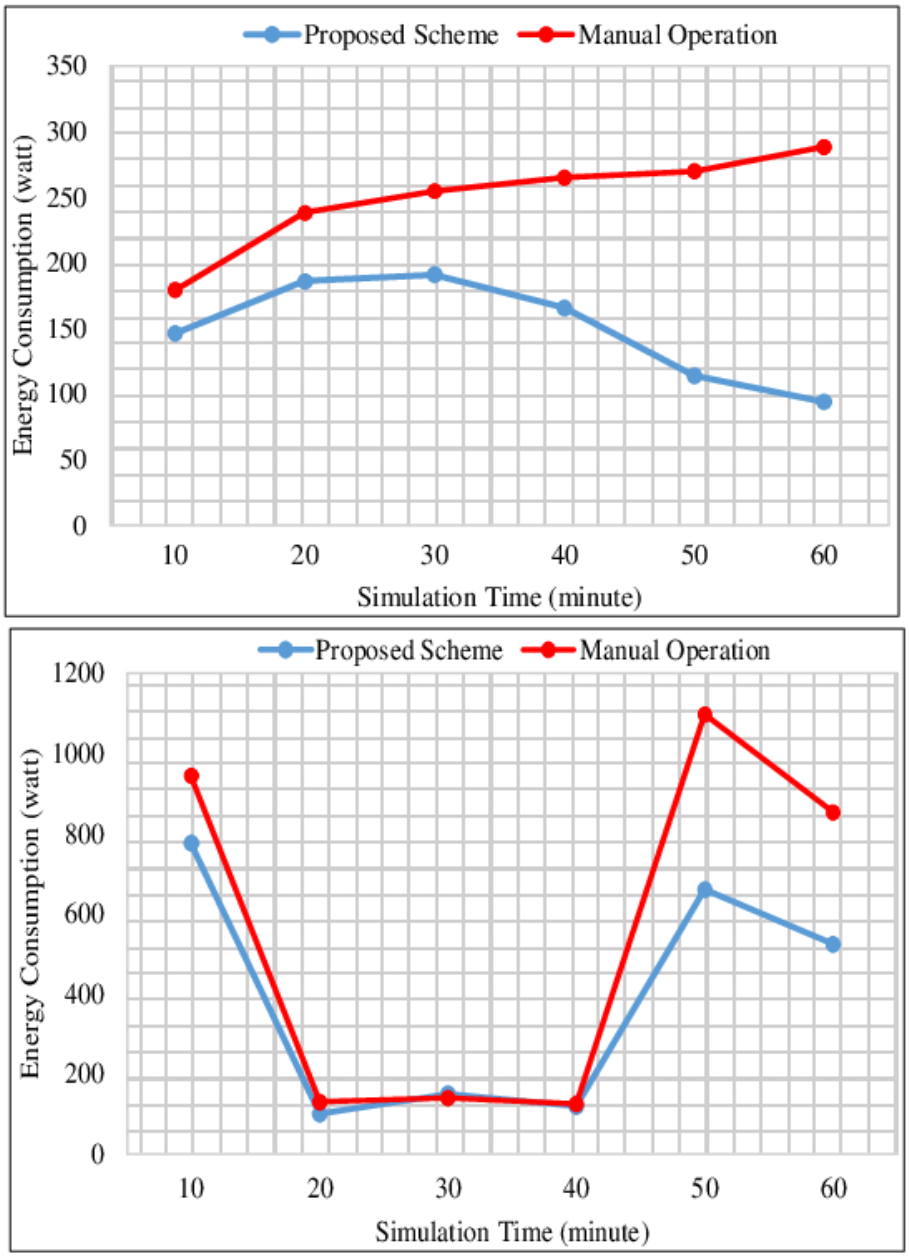
A geolokációs funkciók révén az is megoldható, hogy a rendszer akkor kezdje el felfűteni a lakást, amikor a család tagjai elindulnak hazafelé.Ez a fajta adaptív vezérlés jelentős energiamegtakarítást eredményezhet, anélkül, hogy a komfortérzet csorbulna.

Energiamonitorozás

Egy másik hasznos funkció az energiamonitorozás, amely valós időben követi nyomon az áram-, gáz- vagy vízfogyasztást. Az intelligens mérők és okos konnektorok révén pontosan láthatjuk, melyik eszköz mennyi energiát fogyaszt. A rendszer képes figyelmeztetni, ha valamelyik készülék túlzott fogyasztást produkál, vagy ha elfelejtettük kikapcsolni azt.

Néhány rendszer azt is lehetővé teszi, hogy időzítéseket állítsunk be a magasabb energiaáras időszakok elkerülésére, így pénzt takaríthatunk meg.

Az energiatudatos működés hosszú távon nemcsak a rezsit csökkenti, hanem hozzájárul a fenntartható jövőhöz is. Az okosotthonok által kínált részletes adatelemzés lehetővé teszi, hogy felismerjük a pazarló szokásokat, és hatékonyabban gazdálkodjunk az erőforrásainkkal.



4. Energia használat összehasonlitása egy okokotthon és egy normál otthon között

10 AUTOMATIZÁLT VILÁGÍTÁS, FŰTÉS, ÁRNYÉKOLÁS

Az otthonok automatizálása egyre szélesebb körben terjed el, és a legfontosabb területek közé tartozik a világítás, a hűtés-fűtés rendszerek és az árnyékolás vezérlése. Ezek a rendszerek nemcsak kényelmi funkciókat látnak el, hanem hatékonyan hozzájárulnak a biztonság, az energiahatékonyság és a jólét növeléséhez is. A korszerű okosmegoldások lehetővé teszik, hogy otthonaink környezeti viszonyait intelligensen, automatikusan vagy akár adaptívan is szabályozzuk. Az alábbiakban részletesen bemutatjuk az e három területhez tartozó technológiákat, működési elveiket, és azok előnyeit.

Intelligens világítás

Az intelligens világítás napjaink egyik legismertebb és legnépszerűbb okosotthon-funkciója. A világítás nemcsak a tájékozódást és látási viszonyokat szolgálja, hanem jelentős hatással van a hangulatunkra, produktivitásunkra, sőt az alvásminőségre is. A modern LED-technológia és az okosvezérlés kombinációja lehetővé teszi, hogy a világítást teljes mértékben a felhasználó igényeihez lehessen igazítani.

A legismertebb rendszerek – például a Philips Hue, LIFX, Yeelight vagy Nanoleaf – széles funkcionalitással rendelkeznek. A színváltás révén milliónyi árnyalat és fénytónus közül választhatunk. Reggeli ébredéshez vagy esti relaxációhoz meleg tónusú fényeket alkalmazhatunk, míg munka közben hidegebb, természetes fehér fényt, amely serkenti a koncentrációt.

A fényerő-szabályozás is az alapfunkciók közé tartozik, amely napszakhoz, természetes fényviszonyokhoz vagy épp mozgásérzékelőhöz igazítva automatikusan változhat. Ezt egészíti ki az időzítés lehetősége: például reggel a lámpa fokozatosan növeli a fényerőt, ezzel segítve a természetes ébredést, este pedig finoman halványul el, támogatva a pihentető elalvást. Mozgásérzékelés alapján a világítás automatikusan felkapcsolódik, például éjszaka a fürdőszobába menet, vagy ha valaki belép a garázsba.

A távoli vezérlés pedig azt jelenti, hogy akár egy másik országban tartózkodva is vezérelhetjük otthonunk világítását mobilalkalmazáson keresztül, így például ellenőrizhetjük, nem maradt-e égve egy lámpa, vagy szimulálhatjuk a jelenlétet.

Az egyik leginnovatívabb fejlesztés a circadian lighting, vagyis a cirkadián ritmushoz igazodó világítás. Ez a rendszer napközben hűvösebb, kékes fényeket biztosít, amelyek élénkítenek, míg este meleg fényekre vált, elősegítve a melatonin hormon termelését és a nyugodt alvást. Ilyen rendszer különösen hasznos lehet irodákban, kevés természetes fénnyel rendelkező otthonokban, vagy változó műszakban dolgozók számára, mivel segíti a biológiai óra alkalmazkodását.

Az intelligens világítás más rendszerekkel is könnyedén integrálható: egy „mozi mód” aktiválásakor például a lámpák elhalványulnak, a redőnyök leereszkednek és a multimédiás eszközök bekapcsolnak. Az időjárás-előrejelzés alapján automatikusan erősebb világítást kaphatunk borús napokon, ezzel javítva a komfortérzetet.

Intelligens klímavezérlés és fűtésszabályozás

A hőmérséklet-szabályozás az okosotthonok egyik legnagyobb energia-megtakarítási potenciállal rendelkező területe. A korszerű termosztátok, mint például a Nest Learning Thermostat, Ecobee, Tado vagy Honeywell Home, képesek önállóan alkalmazkodni a felhasználók rutinjához és preferenciáihoz.

Ezek az eszközök kezdetben kézi beállításokat igényelnek, de rövid idő elteltével algoritmusok segítségével megtanulják, mikor melyik helyiségben milyen hőmérséklet az ideális. A rendszer figyelembe veszi az otthon elhagyásának és visszatérésének idejét, a külső hőmérsékletet, a szigetelés hatékonyságát, sőt akár azt is, mennyi idő alatt fűthető fel egy-egy szoba.

A zónás fűtési rendszerek lehetővé teszik a helyiségenkénti hőmérsékletszabályozást. Egy nappaliban vagy fürdőszobában más lehet az ideális hőmérséklet, mint egy hálószobában. Az okos termoszelepek – például a Netatmo vagy Eve Thermo – révén ezeket külön-külön lehet szabályozni, ezzel is csökkentve a felesleges energiafelhasználást.

A termosztát működése nemcsak időzített, hanem geolokációs alapon is történhet. Amikor a család elhagyja az otthont, a rendszer automatikusan csökkenti a fűtési vagy hűtési teljesítményt. Ha a felhasználó hazaindul, a rendszer érzékeli ezt, és még megérkezés előtt beállítja a kívánt hőmérsékletet. Ez különösen praktikus, ha a lakás sokáig üresen áll, mivel optimalizálja a fogyasztást anélkül, hogy a kényelem csorbulna.

Az intelligens klímavezérlés nemcsak komfortosabb otthont eredményez, de jelentős megtakarítást is hozhat a fűtés- és hűtésköltségek terén, különösen hosszú távon.

Árnyékolás – Intelligens redőnyök és függönyök

Az árnyékolás automatizálása az egyik leglátványosabb és leghatékonyabb módja az energiafelhasználás optimalizálásának és a komfortérzet növelésének. Az intelligens árnyékolórendszerek – motorizált redőnyök, reluxák, sötétítők vagy függönyök – nemcsak a napfény bejutását szabályozzák, hanem hozzájárulnak az otthon hőmérsékleti stabilitásához is.

A legtöbb rendszer működtethető távirányítóval, mobilalkalmazással, de akár hangvezérléssel is (pl. Alexa vagy Google Assistant segítségével). A komplexebb megoldások automatizáltak: például reggel napfelkeltekor felhúzódnak a redőnyök, este pedig automatikusan leereszkednek. A beépített fény- vagy hőmérséklet-érzékelők lehetővé teszik, hogy a rendszer alkalmazkodjon a külső körülményekhez – például ha a nap túl erősen süt be, automatikusan lezár az árnyékolás, csökkentve ezzel a belső tér felmelegedését

Nyáron az automatizált árnyékolás csökkentheti a klímaberendezések szükségességét, télen pedig segíthet bent tartani a meleget. Ennek eredményeképpen egy jól hangolt rendszer akár 10–30%-kal is képes csökkenteni az energiafelhasználást.

A biztonsági funkciók közé tartozik a jelenlét-szimuláció: ha a ház üres, a rendszer véletlenszerű időpontokban húzza fel-le a redőnyöket, mintha a lakók otthon lennének. Ezt világításvezérléssel kombinálva még életszerűbb hatást lehet kelteni, ami jelentősen csökkenti a betörés kockázatát.

11 BIZTONSÁGI RENDSZEREK

Okos biztonsági megoldások

Az intelligens otthonok egyik legfontosabb és legkeresettebb funkciója a biztonság növelése. A hagyományos riasztórendszereket ma már egyre inkább felváltják a hálózatba kötött, felhasználóbarát, és távolról is vezérelhető okos biztonsági megoldások. Ezek célja nemcsak a betörések megelőzése, hanem a mindennapi biztonság növelése is – például tűz-, víz- vagy gázszivárgás észlelése, vagy akár az otthon tartózkodók védelme.

Az okos kamerarendszerek, mint például az Arlo vagy a Ring, felhőalapú tárhelyet használnak a felvételek tárolására, így az adatok nemcsak helyben, hanem online is biztonságban vannak. Ezek a kamerák képesek mozgásérzékelésre, éjjellátásra és kétirányú kommunikációra is. Ha a rendszer mozgást érzékel, automatikusan elindítja a rögzítést, és értesítést küld a tulajdonosnak, aki élőben betekinthet az eseményekbe. A videófelvételek később visszanézhetők, letölthetők, vagy akár meg is oszthatók hatóságokkal, ha erre szükség van. A felhőalapú megoldás egyik legnagyobb előnye, hogy a kamerák által rögzített adatok akkor is elérhetők, ha az otthonban magában történik károsodás vagy a kamera megsemmisül.

A biztonsági rendszerek másik fontos komponense az érzékelők alkalmazása. Az olyan eszközök, mint a Fibaro érzékelői, képesek figyelni az ajtók és ablakok nyitását, a vízszivárgás jelenlétét, vagy éppen a hőmérséklet és páratartalom változását. Egy nyitásérzékelő például azonnal jelzést küldhet, ha valaki megpróbál bejutni az otthonba – ez különösen hasznos lehet akkor, ha a lakók éppen nincsenek otthon. A vízérzékelők szintén nagy segítséget jelenthetnek: időben figyelmeztetnek egy szivárgásra, megelőzve ezzel a súlyosabb károkat. Ezek a szenzorok rendszerint más okoseszközökkel is összekapcsolhatók, például egy szivárgás észlelése után elzárhatják a főcsapot, így teljes automatizálással csökkentve a károk mértékét.

Az okos biztonsági rendszerek nemcsak a védelem szintjét emelik magasabb szintre, hanem nagyban növelik a kényelmet is. Egyetlen alkalmazásból figyelemmel kísérhetők a kameraképek, állíthatók a riasztási beállítások, és visszanézhetők a rendszer által rögzített események. A technológia fejlődése lehetővé teszi, hogy a biztonsági rendszer már ne csak rögzítse az eseményeket, hanem aktívan megelőzze vagy kezelje azokat.

12 ENERGIAGAZDÁLKODÁS

Megújuló energiaforrások és intelligens elosztás

Az intelligens otthonok másik kulcsterülete az energiatudatosság és a költséghatékony üzemeltetés. A megújuló energiaforrások, különösen a napelemes rendszerek egyre nagyobb szerepet kapnak az energiaellátásban, és ezek intelligens integrációja lehetőséget ad az önellátó otthonok megvalósítására. Az ilyen rendszerek nemcsak környezetkímélőek, de hosszú távon jelentős megtakarítást is eredményeznek.

A modern napelemes rendszerek már nem csupán áramot termelnek, hanem képesek azt okos módon elosztani és tárolni is. Egy intelligens inverter például felismeri, mikor van csúcstermelés – jellemzően napközben – és ilyenkor elindítja az energiaigényes eszközöket, mint például a mosógépet, a bojlert vagy az elektromos autó töltését. Ha a rendszer akkumulátoros energiatárolóval is ki van egészítve, akkor a nap közben megtermelt felesleges energiát eltárolhatja, és este vagy éjszaka használhatja fel azt. Ez a fajta optimalizáció csökkenti az elektromos hálózatra gyakorolt terhelést, és hatékonyabbá teszi a háztartások energiafelhasználását.

Az elektromos autók elterjedésével egyre fontosabbá válik az intelligens töltés is. Egy okos rendszer képes felismerni a hálózat terheltségét, és automatikusan olyan időpontban indítja el a töltést, amikor az áram olcsóbb és a hálózat kevésbé terhelt – például éjszaka. Ez nemcsak pénzt takarít meg, hanem hozzájárul az elektromos hálózat stabilitásához is. Az ilyen megoldásokkal az energiafogyasztás szinte észrevétlenül válik fenntarthatóbbá és hatékonyabbá.

A jövőben ezek a rendszerek egyre intelligensebbé válnak: a gépi tanulás segítségével képesek lesznek előrejelezni a háztartás energiaigényét az időjárás, a szokások és az eszközhasználat alapján, és automatikusan úgy optimalizálni a fogyasztást, hogy a lehető legkevesebb legyen az energiafelesleg vagy -hiány. A cél az, hogy az energia ne vesszen kárba, hanem ott és akkor legyen felhasználva, ahol és amikor valóban szükség van rá.

13 A JÖVŐ TRENDJEI

Új technológiák

Az intelligens otthonok fejlődése szorosan összefügg a távközlési és informatikai technológiák alakulásával. A közeljövő egyik legmeghatározóbb újítása az 5G hálózatok elterjedése, amely jelentősen meg fogja növelni az okoseszközök közötti adatátviteli sebességet és megbízhatóságot. Az 5G lehetővé teszi az eszközök szinte azonnali reagálását, így például a biztonsági rendszerek, egészségügyi szenzorok vagy akár a háztartási gépek még gyorsabban és pontosabban fognak reagálni a felhasználói utasításokra vagy a környezeti változásokra.

A háztartási robotok is egyre fontosabb szerepet kapnak a jövő otthonaiban. Az Amazon Astro például nemcsak takarításra használható, hanem otthoni megfigyelést is elláthat, vagy akár videóhívásokat is közvetíthet. Ezek a robotok képesek a lakáson belül mozogni, érzékelni az embereket és a környezetet, és szükség esetén kapcsolatba lépni más eszközökkel – például ha egy biztonsági kamera mozgást érzékel, a robot odagurul, és élő képet közvetít a tulajdonosnak. Ezek a rendszerek egyre inkább személyi asszisztens szerepet is betöltenek, hiszen képesek emlékeztetőket kezelni, zenét lejátszani vagy egyszerű beszélgetésekre válaszolni.

Okos városok integrációja

Az intelligens otthonok fejlődése nem áll meg a négy fal között – az okos városok koncepciója arra törekszik, hogy az egyéni otthonok is aktívan kapcsolódjanak a közösségi infrastruktúrához. Az intelligens közvilágítás például képes igazodni a gyalogosforgalomhoz vagy az időjárási viszonyokhoz. Ha egy utcában kevesen járnak éjjel, a világítás automatikusan halványabbra áll, csökkentve az energiafogyasztást. Ezzel szemben, ha mozgás érzékelhető, a fények felerősödnek, növelve a biztonságot.

A közműszolgáltatások is egyre intelligensebbé válnak. A víz-, gáz- és áramfogyasztást okosmérők monitorozzák, amelyek valós időben adatokat szolgáltatnak a szolgáltatóknak és a lakóknak egyaránt. Ezek az adatok alapján a rendszer automatikusan értesítést küldhet túlzott fogyasztás vagy rendellenes működés esetén. A jövőben az egyéni háztartások és

a városi rendszerek közötti adatcsere lehetővé teszi majd, hogy a város egyetlen, egységes, öntanuló és adaptív hálózatként működjön, ahol minden információ és energiaforrás optimálisan kerül elosztásra.

Irodalomjegyzék

Access, I. (2020). A Review of Smart Homes—Past, Present, and Future.

Computer Networks, E. (2021). Security and privacy in smart home environments: A systematic review.

O'Neil, M. M. (n.d.). *Smart Homes and Energy Efficiency*.

2.59. Humán-robot interakció szerepe és tervezési szempontjai a kiber-fizikai rendszerekben (CPS) Vizkeleti Gergő,

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

INFORMATIKA TANSZÉK
DEPARTMENT OF COMPUTER SCIENCE

Humán-robot interakció szerepe és tervezési szempontjai a kiber-fizikai rendszerekben (CPS)

Vizkeleti Gergő, [redacted]

Mérnökinformatikus, BSc, nappali

készítés dátuma: 2025.05.15

Tartalomjegyzék

1. Bevezetés 1

2. A CPS rendszerek áttekintése 1

3. A humán-robot interakció (HRI) alapjai 4

4. Emberi tényezők és felhasználói szempontok 5

5. Szenzoros és technikai háttér 7

6. Kommunikációs protokollok és interfészek 8

7. Gépi tanulás és adaptív interakciók 10

8. Ipari és gyakorlati példák 12

9. Társadalmi hatások és felhasználói elfogadás 14

10. Biztonsági és etikai kérdések 16

11. Jövőbeli kihívások és trendek 17

12. Összefoglalás, következtetések 19

Források 21

A tanulmány [14] – [22] források alapján,
azok tartalmának összevonásával és átdolgozásával készült.

1. Bevezetés

A kiber-fizikai rendszerek (Cyber-Physical Systems, CPS) az informatikai és fizikai világ mély integrációját jelentik, ahol beágyazott számítógépes rendszerek szenzorokon és aktuátorokon keresztül kapcsolatban állnak a valós környezettel. A CPS-ek jellemzően visszacsatolásos mechanizmusokat használnak: a fizikai folyamatokat beágyazott számítógépek figyelik és szabályozzák, miközben a fizikai folyamatok is hatással vannak a számítógépes vezérlésre.

A CPS alkalmazási területei igen szélesek, beleértve az egészségügyi eszközöket, intelligens közlekedési rendszereket, energiamenedzsmentet, környezetvédelmi szabályozást, aviatikát, megfigyelő robotikát, védelmi rendszereket, gyártást, okos épületeket és infrastrukturális hálózatokat. Ezekben a rendszerekben a fizikai komponensek nem csak egyszerű végrehajtók, hanem időben kritikus és biztonságfüggő szerepet töltenek be, amelyek különböznek a hagyományos informatikai komponensektől. A CPS-ek tervezési kihívásai között kiemelkedő az időzítés, a megbízhatóság és a biztonság kérdése.

Az IPAR 4.0 kezdeményezés keretében a kiber-fizikai rendszerek az ipari és termelési környezetekben is kulcsszerepet kapnak, lehetővé téve a valós idejű adatmegosztást, adaptív vezérlést és az autonóm döntéstámogatást. Az utóbbi években a humán-robot interakció (HRI) kutatása is előtérbe került, mivel a CPS-ekben egyre inkább szükség van az emberek és robotok közötti közvetlen együttműködésre. A HRI olyan interdiszciplináris kutatási terület, amely a robotok és emberek közötti hatékony, biztonságos és természetes kommunikáció megértésével, megtervezésével és értékelésével foglalkozik. Legyen szó ipari kollaborációról, egészségügyi asszisztenciáról vagy társadalmi robotokról, a humán tényezők figyelembevétele és a megfelelő tervezés kritikus a CPS rendszerek sikeréhez.

Az esszé célja, hogy részletes áttekintést adjon a humán-robot interakció szerepéről a kiber-fizikai rendszerekben, beleértve az emberi tényezőket, szenzorokat, kommunikációs protokollokat, adaptív algoritmusokat és a gyakorlatban alkalmazott példákat. A tanulmányban bemutatásra kerülnek a jelenlegi kutatási irányok és technológiai trendek, valamint kitérünk a közeljövő kihívásaira és etikai kérdéseire ebben a kontextusban.

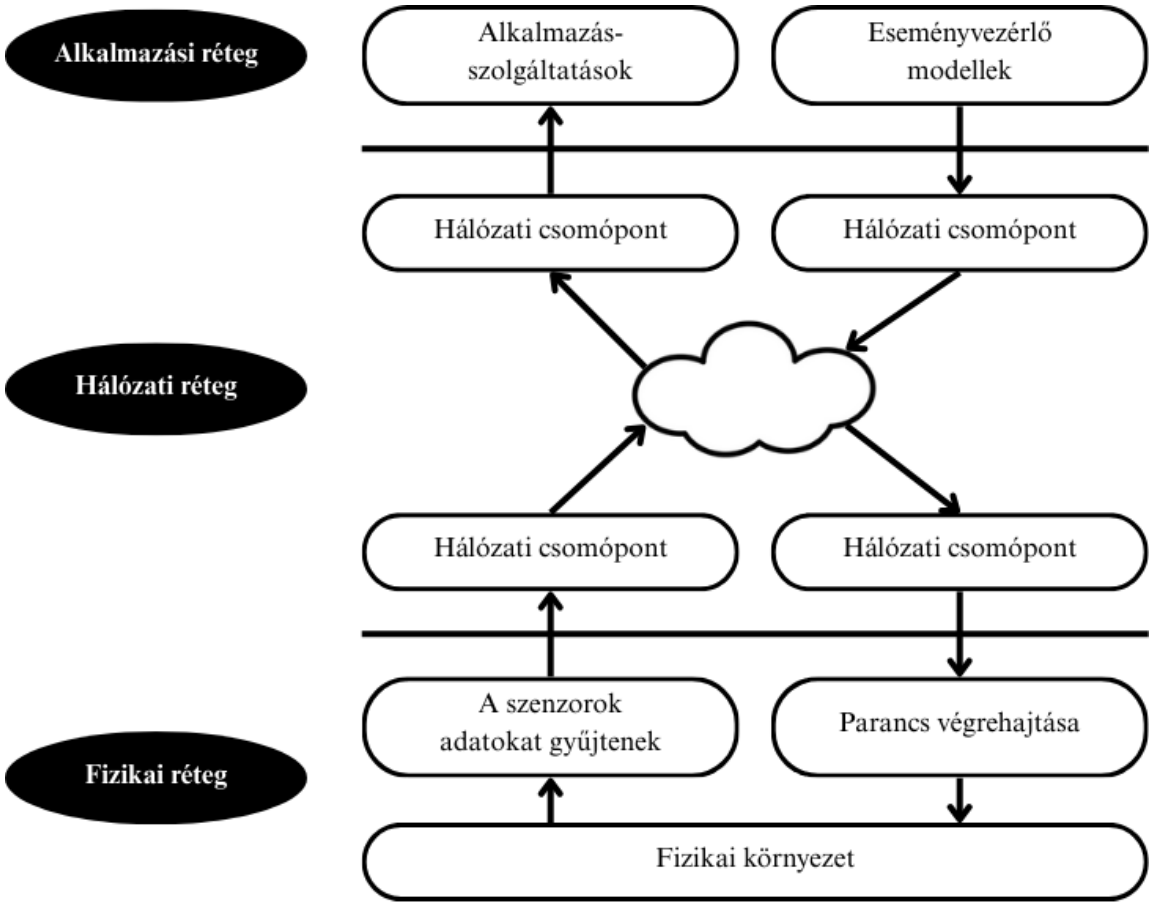
2. A CPS rendszerek áttekintése

A kiber-fizikai rendszerek (Cyber-Physical Systems, CPS) olyan komplex rendszerek, amelyekben a fizikai komponensek (pl. érzékelők, aktuátorok) és a számítási, kommunikációs komponensek (pl. algoritmusok, processzorok, hálózatok) szorosan integráltan működnek együtt. A céljuk, hogy intelligens, autonóm döntések révén képesek legyenek valós időben reagálni környezeti változásokra, és aktívan beavatkozni különböző folyamatokba. Ezek a

rendszerek képezik az alapját az ipar 4.0, okos városok, autonóm járművek és fejlett egészségügyi technológiák fejlődésének.

Egy CPS struktúrája tipikusan többrétegű [1. ábra]:

- Alkalmazási / Interfész réteg: biztosítja a fizikai és kiber réteg közötti valós idejű adatáramlást, szinkronizációt és visszacsatolást.
- Hálózati / Kiber réteg: számítási logikát biztosít – jellemzően valós idejű operációs rendszerek, vezérlő algoritmusok és kommunikációs protokollok segítségével.
- Fizikai réteg: érzékelők, aktuátorok, beágyazott rendszerek. Ez felelős a valós világ megfigyeléséért és befolyásolásáért.



1. ábra: A kiber-fizikai rendszerek (CPS) rétegzett architektúrája Forrás: saját szerkesztés [1] alapján

A folyamatos visszacsatoláson alapuló működés lehetővé teszi, hogy a rendszer adaptívan, a környezeti változásokra dinamikusan reagálva működjön. E tulajdonság különösen fontos olyan alkalmazásokban, ahol a pontosság, megbízhatóság és gyors reakcióidő kulcsfontosságú.

A kiber-fizikai rendszerek (CPS) számos területen alkalmazhatók, ahol a valós idejű adatfeldolgozás és a fizikai beavatkozás integrációja kulcsfontosságú. Az egészségügyben például megjelennek az intelligens protézisek, a távsebészet és a betegmonitorozó rendszerek,

amelyek révén a betegek állapota folyamatosan nyomon követhető, illetve akár távolról is végrehajthatók beavatkozások.

A közlekedésben az önvezető járművek és forgalomirányító rendszerek jelentik a legfőbb CPS-megoldásokat, lehetővé téve a közlekedés biztonságosabbá és hatékonyabbá tételét. Az ipari gyártásban az okos gyárak, az elosztott vezérlési rendszerek és a prediktív karbantartás alkalmazása révén nő a termelékenység és csökkennek az állásidők.

Az energiaágazatban a CPS-ek az intelligens hálózatok (smart grid) és a megújuló energiaforrások dinamikus kezelése révén biztosítják a hatékony és fenntartható energiaelosztást. A védelem és haditechnika terén a precíziós időzítésű kommunikációs rendszerek és az autonóm drónok alkalmazása kiemelt jelentőségű, különösen a gyors reagálást és nagy megbízhatóságot igénylő műveletek során.

Az infrastruktúra területén az intelligens épületek és a környezeti monitoring rendszerek révén a CPS-ek hozzájárulnak az energiahatékonysághoz, a biztonsághoz és a környezeti állapotok folyamatos ellenőrzéséhez.

Újabb kutatási irányok foglalkoznak a kognitív funkciókkal ellátott CPS-ekkel, ahol a rendszer nemcsak adaptálódik, hanem prediktív módon tervez és tanul a korábbi eseményekből. Ehhez gépi tanulási modelleket és nagy adathalmazokon végzett elemzéseket alkalmaznak.

A CPS tervezésének főbb kihívásai:

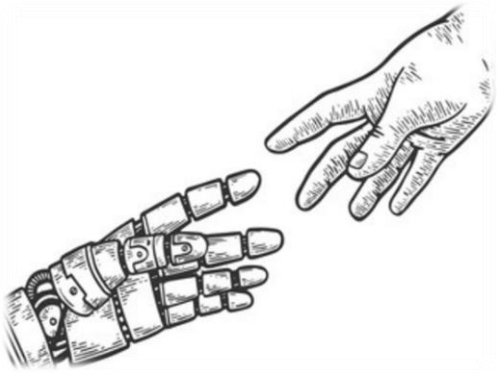
- Időzítés és párhuzamosság kezelése: a fizikai világ folyamatos időben működik, így az események időzítése létfontosságú (real-time rendszerek).
- Hibakezelés és megbízhatóság: a rendszernek robusztusnak kell lennie hardver- és szoftverhibákkal szemben.
- Biztonság és adatvédelem: mivel sok CPS kritikus infrastruktúrában működik, fontos a külső támadások elleni védelem.
- Skálázhatóság és interoperabilitás: több alrendszer integrálása során biztosítani kell az egységes kommunikációt és együttműködést.
- Felhasználó-központú működés: a rendszernek figyelembe kell vennie az emberi tényezőket (erről részletesen a 4. fejezet szól).

A CPS-ek tehát nem csupán technikai rendszerek, hanem komplex ökoszisztémák, ahol a valós és virtuális világ szoros együttműködésben, gyakran emberi közreműködéssel valósítja meg a célfeladatokat. Ez a komplexitás új tervezési, tesztelési és üzemeltetési módszertanokat igényel, amelyek biztosítják a megbízható és biztonságos működést különböző környezetekben.

3. A humán-robot interakció (HRI) alapjai

A humán-robot interakció (HRI) az a kutatási terület, amely a robotok és az emberek közötti kommunikáció, együttműködés és kölcsönhatás feltérképezésére és optimalizálására törekszik. A HRI célja olyan rendszerek tervezése, ahol a robotok hatékonyan, természetesen és biztonságosan működnek együtt az emberekkel, legyen szó ipari asszisztenciáról vagy társadalmi interakcióról.

Interakció szempontjából fontos megkülönböztetni két fő kategóriát: ha az ember és a robot térben vagy időben külön vannak (például Mars-rover távvezérlése), akkor távoli interakcióról beszélünk, ha pedig a közelben vannak (például egy szolgáltató robot a lakásunkban), akkor közeli interakció történik. Emellett az interakció során különböző feladatok adódhatnak: lehet mobil robotokról vagy manipulátorokról szó; a mobil robotoknál gyakori a távvezérlés (teleoperáció), míg a kéz-fizikai feladatnál a telemanipuláció is előfordul.



2. ábra: Az ember és a robot közötti kapcsolat szimbolikus ábrázolása. Forrás: [2]

A közeli interakcióban a robot segítő szerepet tölthet be, előfordulhat fizikai érintés, de ide tartozik a társadalmi jellegű interakció is, amikor a robot a társunkként viselkedik, például szociális robotok esetén [2. ábra]. A kommunikáció forrása lehet hang, gesztus, kijelző, testrészek mozgása, vagy akár szemkontaktus, mindez jelentősen befolyásolja az interakció természetességét és hatékonyságát.

Egy népszerű definíció szerint *„a HRI egy olyan tudományterület, amely a robotikai rendszerek megértésével, megtervezésével és értékelésével foglalkozik, amikor azokat emberek használják vagy emberekkel együttműködnek”*. Ez azt jelenti, hogy az interakció szempontjából nemcsak a technológiai problémák számítanak, hanem a tervezési folyamatban az ember által formálható tényezők is. Fontos hangsúlyozni, hogy a HRI nem egyszerűen a korábbi robotikai vagy mesterséges intelligencia kutatások újraértelmezése, hanem önálló tudományág, mely ötvözi az interdiszciplináris ismereteket (robotika, pszichológia, ergonómia, mesterséges intelligencia stb.).

A HRI alakulását jelző fontos mérföldkövek (például távsebészeti rendszerek, autóipari asszisztensek, humanoid robotok) mutatják a terület különlegességét és kihívásait. A modern HRI-ben különösen a tervezői szemlélet fontos: az interakció egyes formáit (és ezek hatékonyságát) a tervező tudja alakítani, miközben számos tudományág eredményei járulnak hozzá a rendszer működéséhez.

A következő részekben áttekintjük a HRI kulcstényezőit és az együttműködés fő típusait, hiszen a CPS rendszerekben a robotoknak gyakran emberekkel kell osztozniuk a munkaterületen, és „megérteni”, hogy mit várnak el tőlük az emberek. Az alábbi részekben

foglalkozunk az emberi tényezőkkel, a közös feladatokkal és a hatékony kommunikációval, amelyek mind elengedhetetlenek egy sikeres HRI megvalósításához.

4. Emberi tényezők és felhasználói szempontok

A HRI tervezésénél az egyik legfontosabb tényező az emberi felhasználók jellemzőinek és igényeinek figyelembevétele. Az emberi tényezők (human factors) körébe tartoznak az ember fizikai képességei és korlátai (ergonómia, antropometria), kognitív tulajdonságai (figyelem, terhelhetőség, szándékok és szándékfelismerés) és érzelmi reakciói (például bizalom vagy félelem).

Egy CPS-ben a robotoknak alkalmazkodniuk kell az emberi partnerük munkamódszeréhez és ritmusához is. Ha például egy robot erős ízületekkel rendelkezik, de nem igazodik hozzá, hogy a ember lassan, óvatosan mozog a környezetben, akkor az kényelmetlenséget vagy akár balesetet okozhat.

A felhasználói elfogadás szempontjából a bizalom és a biztonságérzet kulcsfontosságú. Közvélemény-kutatások és HRI vizsgálatok kimutatták, hogy a felhasználók számára a legnagyobb etikai aggályt a munkahelyek elvesztése (emberi munkaerő helyettesítése robotokkal) okozza. Ugyanakkor a HRI-hez kapcsolódó biztonsági kérdések (technológiai megbízhatóság, a robot mozgásainak előre jelezhetősége) és a robot szociális viselkedése (nonverbális jelzések, emberi arc és gesztusok megértése) is erősen befolyásolják, hogy a felhasználók mennyire szívesen használnak robotot a jövőben.

Az említett kutatás szerint a legfontosabb etikai tényezők a munkahely pótlása mellett a robot bizalmassága (trust) és a biztonság (safety), valamint az, hogy a robot milyen szociális jelzéseket ad. Ezek a tényezők hatással vannak a felhasználók jövőbeni szándékára is: azaz ha egy robot kezdetben magasra értékelt biztonsággal és meggyőző szociális képességekkel rendelkezik, akkor nőhet az emberek hajlandósága a robot használatára.

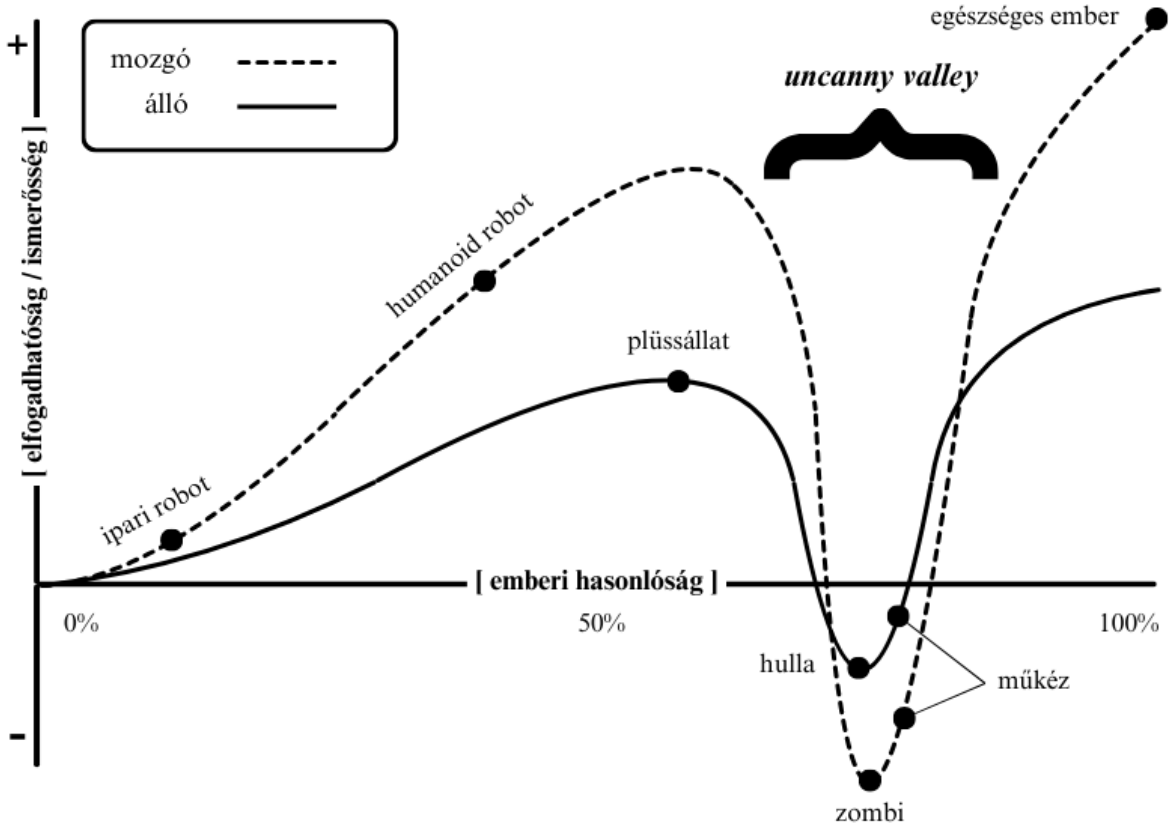
A tervezés során figyelni kell az ergonómiai szempontokra is: a robot által végzett feladatoknak illeszkedniük kell az ember testhelyzeteihez és mozgásaihoz. Például egy ipari robotos munka során a robot dönthet úgy, hogy a nehéz tárgyat felfelé emeli az ember számára, aki közben kényelmes testhelyzetben marad [3. ábra]; vagy a robot alkalmazkodik a személy látómezőjéhez, hogy ne akadályozza a látását munka közben.

3. ábra: Robot és ember közötti együttműködés gyári munkakörnyezetben – a fizikai és kognitív illeszkedés példája. Forrás: [3]

Kognitív szempontból pedig a robotnak törekednie kell arra, hogy interakciója áttekinthető és előrejelezhető legyen: a transzparencia (a robot belső állapotainak vagy döntéseinek megjelenítése) és az

egyértelmű kommunikáció segít abban, hogy az ember tudja, mit várhat a robottól. Ha a robot viselkedése kiszámítható (például kis feladatrészekre bontva jelzi a szándékait), az növeli a felhasználók bizalmát és csökkenti a kognitív terhelést.

Szintén fontos a társas jelenlét és az interakció személyessége: a túl sok vagy hiányzó emberi vonás ronthatja az elfogadottságot. Bár a kutatások szerint a robotok emberi archoz vagy hanghoz való hasonlítása (antropomorfizálás) elősegítheti a természetesebb együttműködést, túlzott emberi hasonlóság (uncanny valley jelensége [4. ábra]) taszító lehet. A tervezőknek tehát gondosan kell egyensúlyozni az interakció barátságossága és egyszerűsége között: el kell kerülnie a felhasználói stresszt (például bonyolult, nehezen tanulható kezelőfelületeket) és egyben támogatni kell a robothoz fűződő kedvező attitűd kialakulását (például megfelelő visszajelzéseken, hangjelzéseken keresztül).



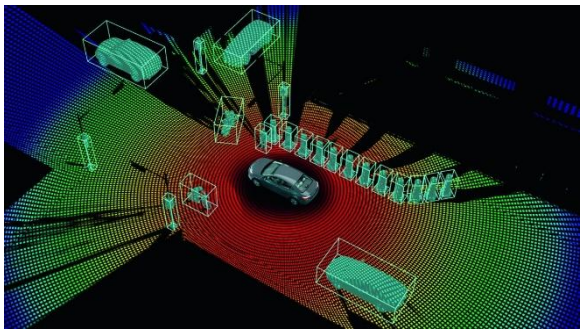
4. ábra: Az uncanny valley jelensége – az emberszerűség és az elfogadottság viszonya. Forrás: Saját szerkesztés [4] alapján

Összességében az emberi tényezők optimális kezelése nagyban növeli a rendszerek hatékonyságát és elfogadottságát, míg figyelmen kívül hagyásuk jelentős kockázatokat rejt, akár fizikai sérüléshez, akár a rendszer leállásához vezetve.

5. Szenzoros és technikai háttér

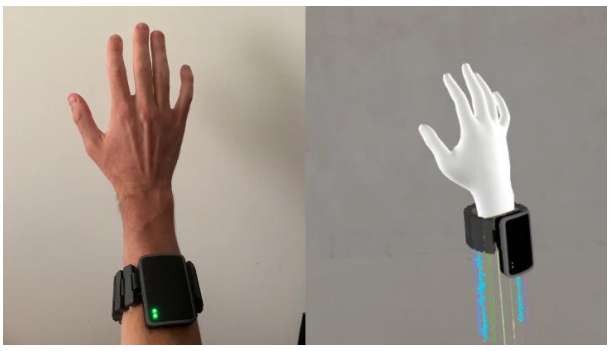
A CPS keretében a robotoknak és a velük együttműködő rendszereknek kiemelt mértékben kell építeniük különféle szenzorokra és műszaki megoldásokra. A szenzorok a HRI szempontjából kulcsfontosságúak, hiszen ezek segítségével érzékeljük a környezetet és a benne mozgó embereket. A modern kollaboratív robotok esetében egyaránt alkalmaznak belső szenzorokat (a robot saját állapotának figyelésére: pozíció, erő/nyomaték, motoráram, stb.) és külső szenzorokat (a környezet érzékelésére: kamerák, LIDAR, ultra- vagy infravörös szenzorok, mélységkamerák, vagy akár hang- és gázérzékelők).

A különböző érzékelők kombinálása (szenzorfúzió) révén a robotok pontosabban tudják érzékelni az ember jelenlétét és helyzetét. Például munkahelyi együttműködés során gyakori, hogy egy mélységérzékelő kamera és egy LiDAR [5. ábra] együtt monitorozza a környezeti mozgást, hogy detektálja a dolgozó mozgását és gyorsan reagáljon rá. Egy átfogó felülvizsgálat szerint a kollaboratív robotok mindenképp használnak többféle érzékelőt is, mert így válik lehetségessé a valós idejű ember-érzékelés és ütközés-elkerülés.



5. ábra: LIDAR szenzorral készített környezeti szkenneredmény: távolság-alapú objektumfelismerés és térbeli leképezés. Forrás: [5]

A leggyakrabban használt szenzorok közé tartoznak a különböző típusú kamerák (RGB, mélység/alapú, stereo), LIDAR és radar készülékek, ultrahangos távolságérzékelők, valamint a robotkarok és eszközök végén elhelyezett erőnyomaték-szenzorok. A kamerák segítségével a robot felismerheti a tárgyakat és embereket (például gépi látási algoritmusokkal), a LIDAR és ultrahangos érzékelők a távolságot mérik, a belső erőnyomaték-szenzorok pedig a fizikai érintkezések biztonságos kezeléséhez szükségesek.



6. ábra: EMG-alapú csuklópánt izomtevékenység érzékelésére, amely lehetővé teszi a robot számára az emberi szándék vagy fáradtság észlelését. Forrás: [6]

Az elektro- és neuromuszkuláris szenzorok (pl. EMG- és EEG-érzékelők [6. ábra]) mellett kifejlesztett viselhető eszközök (okosórák, kineziológiai érzékelők) lehetővé tehetik, hogy a robot az ember szándékait vagy fáradtsági szintjét is figyelembe vegye. Ezen kívül, a hangvezérléshez mikrofonok, a környezeti gázok, rezgések monitorozásához egyéb speciális szenzorok is integrálhatók a rendszerbe a kiterjedt CPS infrastruktúrában.

A szenzorok feldolgozásához szükséges a megfelelő hardver- és szoftveres háttér is. A beágyazott számítógépek általában valós idejű operációs rendszereket futtatnak, amelyek biztosítják, hogy az érzékelőkről érkező adatok feldolgozása meghatározott időkorlátokon belül megtörténjen.

A robotika területén elterjedtek például olyan middleware rétegek, mint a Robot Operating System (ROS), amely moduláris architektúrájával lehetővé teszi a szenzoradatok témákra (topics) való publikálását/előfizetését, és nagyszámú előre beépített algoritmust kínál a szenzorok kezelésére. A hardveroldalon fontosak a robot maniplátorok mozgásvezérlő egységei és motorvezérlői, melyek a szenzorokból érkező információkra reagálva tartják a stabil működést. A CPS-ben lévő robotrendszereknek emellett gyakran közvetlen kapcsolatban kell állniuk más hálózati eszközökkel és felhőszolgáltatásokkal, tehát a műszaki háttér része a hálózati interfészek (Ethernet, Wi-Fi, 5G modem) és a nagyobb rendszerekkel való protokollkompatibilitás is.

6. Kommunikációs protokollok és interfészek

Az ember-robot együttműködést támogató kiber-fizikai rendszerekben a kommunikációs protokollok és az interfészek létfontosságúak. A kommuniktációs protokollok biztosítják a robotok, szenzorok, vezérlők és ember-gép interfészek közötti adatcserét.

Ipari környezetben gyakoriak a valós idejű, determinisztikus protokollok [1. táblázat], például az EtherCAT, a PROFINET vagy az EtherNet/IP, amelyek alacsony késleltetésű adatátvitelt kínálnak és ipari Ethernet alapú gyártásirányító hálózatként szolgálnak. Ezeket gyakran kiegészítik hagyományosabb buszrendszerek (pl. CAN busz vagy PROFIBUS) kisebb autonóm egységek esetén. Az EtherCAT protokoll kiemelten alkalmazkodik a nagy sebességű és szinkronizált vezérléshez (például CNC gépekben és robotkarok vezérlésében), míg a PROFINET inkább integrált ipari automatizálási rendszerekben népszerű.

1. táblázat: Néhány fontos kommunikációs protokoll és technológia összehasonlítása a CPS/HRI környezetben.

Protokoll, technológia	Jellemzők és alkalmazási terület
EtherCAT	Real-time ipari Ethernet protokoll. Nagy sebességű, determinisztikus adatátvitel robotvezérléshez.
PROFINET	Ipari Ethernet protokoll, PLC-k és eszközök integrációja. Multi-vendor gyártóközi szabvány (pl. autóiparban elterjedt).
OPC UA	Platformfüggetlen ipari kommunikációs szabvány. Skálázható, Internet-előkészített, komplex adatmodellezés. Elterjedt ipar 4.0 rendszerekben.

MQTT	Könnyűsúlyú üzenetközvetítő (pub/sub) protokoll IoT-eszközök számára. Akár instabil hálózaton is működőképes, alacsony késleltetés.
DDS	Publish-Subscribe kommunikációs szabvány (több robotikai middleware, pl. ROS2 háttér). Skálázható, QoS beállításokkal (QoS: minőségbiztosítás).
CAN bus	Régebbi autóipari protokoll, egyszerű busz architektúra kis eszközök (pl. érzékelők/aktuátorok) számára.
Wi-Fi / 5G	Vezeték nélküli kapcsolódás. Wi-Fi ipari környezetben szabálytalan (ko), 5G (URLLC) csökkentett késleltetésű, ipari mobil robotokhoz.
Ethernet/IP, Modbus TCP	Ipari hálózati protokollok PLC és SCADA integrációhoz. Egyszerű szerver-kliens (Master-Slave) kommunikáció.

Magasabb szintű kommunikációhoz egyre elterjedtebb az OPC UA (Open Platform Communications Unified Architecture). Az OPC UA platformfüggetlen, skálázható szabvány, amely az ipari rendszerek hierarchiájának szinteit köti össze: az alsó vezérlőszinttől a menedzsment- és vállalati szintekig képes adatokat továbbítani. Az OPC UA-t éppen a heterogén eszközök összekapcsolására fejlesztették ki, és az internetre „felkészített” architektúrája, magas szintű biztonsági és adatmodellezési képességei miatt az ipar 4.0 sztenderdjének tekintik. Emellett feltörekvőben vannak könnyebb IoT-protokollok, például a MQTT és AMQP, melyek publikálás-előfizetés (pub/sub) modellben működnek, és kis adatcsomagok gyors továbbítására optimalizáltak. Ezek mobil vagy elosztott érzékelők számára hasznosak, de ipari alkalmazásban még kevéssé terjedtek el, részben a megbízhatósági igények miatt.

A robotikai kutatásban és fejlesztésben gyakori továbbá a ROS (Robot Operating System) használata, amely valójában nem protokoll, hanem szoftverkönyvtár és kommunikációs framework, amely beépített pub/sub mechanizmusokat kínál a szenzorok és algoritmusok közötti adatátvitelre (ROS 2-ben alapból a DDS protokollal). A ROS és a DDS kombináció lehetővé teszi, hogy a robot szenzorai és intelligens moduljai hatékonyan kommunikáljanak egymással moduláris felépítésben.

A kommunikációs interfészek részben a robot és az ember közötti felületet jelentik. Ezek lehetnek grafikus felhasználói felületek (képernyők, kijelzők), de ide tartoznak a természetes nyelvi, érintéses vagy gesztus alapú inputok is. Például egy CPS-ben elhelyezett érintőképernyő vagy VR (virtuális valóság) szemüveg lehetőséget ad a kezelőnek arra, hogy beavatkozzon vagy megváltoztassa a rendszer paramétereit. A hangvezérlés (mikrofon és

beszédfelismerés) és a gesztusérzékelés (pl. lézeres vagy kamera-alapú megoldások, mint a Kinect) lehetőséget ad a közvetlen, intuitív kommunikációra. Mivel az emberi interfészek általában nagyobb sebességet és részletességet igényelnek (például képernyőfrissítés vagy hangfeldolgozás), a hálózati protokollok közül gyakran IP-alapú megoldásokat (TCP/UDP alapúak) használnak, amelyeket szükség esetén valós idejű kiterjesztésekkel (pl. Time-Sensitive Networking, TSN) lehet kombinálni. Az interfészek biztonsági szempontból is kritikusak: a hálózati biztonság és titkosítás biztosítja, hogy a robot és az ember közötti adatcsere ne lehessen külső támadás célpontja.

Ezen protokollok és technológiák mellett a felhasználói interfészek (touchscreen, gombok, kijelzők, AR/VR headsetek, hangvezérlés) is nagymértékben meghatározzák az ember-robot párbeszéd minőségét. Az emberi kezelők és rendszergazdák olyan eszközöket igényelnek, amelyek lehetővé teszik számukra a rendszer állapotának monitorozását, gyors beavatkozást és hibajavítást – gyakran grafikus felületeken keresztül, valós idejű információ megjelenítéssel. Az interfészek és protokollok kombinációja határozza meg, hogy egy CPS milyen gyorsan és megbízhatóan reagál a külső ingerekre, és hogy a felhasználó mennyire érzékelheti azonnali visszajelzést a robot viselkedéséről.

7. Gépi tanulás és adaptív interakciók

A gépi tanulás (ML) és a mesterséges intelligencia (AI) technikák kulcsfontosságú szerepet játszanak a humán-robot interakció (HRI) fejlesztésében, mivel lehetővé teszik a robotok számára, hogy a dinamikus környezethez, illetve az egyéni emberi igényekhez és viselkedésmintákhoz alkalmazkodjanak. Az adaptív rendszerek célja, hogy a robot ne csak végrehajtó gép legyen, hanem aktív, tanulni képes társ a feladatmegoldásban.

- A felügyelt tanulás (supervised learning) segítségével a robot képes osztályozni vagy prediktív modelleket alkalmazni emberi viselkedésekre: például felismer arckifejezéseket, testtartásokat, érzelmi állapotokat vagy mozdulatokat. Ezzel elérhető, hogy a gép például azonosítsa a felhasználó zavarodottságát vagy figyelmét, és ehhez igazítsa válaszait.
- A mély tanulás (deep learning) még nagyobb rugalmasságot biztosít a vizuális és akusztikus ingerek feldolgozásában. Képfeldolgozó hálózatok révén a robot képes valós időben detektálni gesztusokat, arcfelismerést végezni, vagy a felhasználó tekintetirányát követni. A természetes nyelvi feldolgozás (NLP) alkalmazásával a robot értelmezheti a verbális utasításokat, és adott esetben kérdéseket is tehet fel a felhasználónak a pontosítás érdekében.
- A megerősítéses tanulás (reinforcement learning, RL) előnye, hogy nem igényel részletes előzetes címkézett adatokat. A robot saját tapasztalatai alapján tanulja meg, mely viselkedések vezetnek pozitív kimenethez – például milyen távolságot tartson a felhasználótól, vagy hogyan időzítse mozdulatait egy kooperatív feladat során. A

megerősítő tanulás különösen hatékony a szociális interakciók finomhangolásában és a természetes viselkedések kialakításában.

A robot adaptációja két szinten történhet:

- Viselkedésadaptáció: a robot külső működése, reakciói módosulnak. Például ha az ember fáradtabbnak tűnik vagy lassabb mozdulatokat végez, a robot csökkenti a mozgási sebességét, egyszerűsíti a gesztusait vagy változtat a válaszstílusán. Ez növeli a felhasználói komfortérzetet, különösen olyan területeken, mint a gondozás vagy az oktatás.
- Modelladaptáció: a robot belső reprezentációi (pl. feladatmodell, környezetmodell, társas viselkedési sablonok) változnak. Ennek során a robot új ismereteket integrál, például módosítja egy adott ember preferenciáiról alkotott elképzelését, vagy új működési stratégiát alakít ki. Az ARI robot esetében például a „komfortszint" dinamikus változtatása segített az emberi reakciókhoz való alkalmazkodásban.

A kognitív architektúrák és az ún. meta-tanulás is egyre fontosabbá válnak. Ezek révén a robot nemcsak egy adott viselkedésmintát tanul meg, hanem tanulási stratégiákat is képes kialakítani – például felismeri, mikor érdemes újratanulni valamit vagy módosítani a meglévő modellt.

A közelmúltban a nagy nyelvi modellek (LLM-ek) – mint a GPT vagy BERT – integrálása a robotikai rendszerekbe új szintre emelte a természetes nyelvi interakciókat. Ezek a modellek képesek kontextuális megértésre, érzelmekkel átszőtt válaszadásra, sőt, kreatív párbeszédre is. Egy robot, amely ilyen modellel van felszerelve, nem csupán utasításokat hajt végre, hanem dialóguspartnerként működik. Ez különösen fontos például szociális robotoknál, terápiás célú alkalmazásokban vagy oktatási kontextusban.

A szimulált tanulási környezetek (pl. virtuális világok, digitális ikrek) egyre gyakrabban szolgálnak a gépi tanulás előképzésére. Ezekben a robotok biztonságos, gyorsított környezetben szerezhetnek tapasztalatokat, mielőtt a való világban alkalmazásra kerülnek. A mély megerősítéses tanulás (deep RL) révén ezek a szimulációk valósághű viselkedést alakítanak ki, amely azonnal átültethető a fizikai rendszerre.

További fejlesztési irányok és trendek:

- Intenzívebb személyre szabás: a robotok egyre inkább képesek lesznek különböző emberekhez különböző viselkedési mintákat alkalmazni, akár identitásalapú profilozás alapján.
- Szándékdetekció és predikció: a robot előre érzékeli, mit szeretne az ember tenni vagy mondani, így proaktívan tud segíteni, csökkentve az interakció késleltetését.
- Kontinens tanulás (continual learning): a robot folyamatosan frissíti tudását, anélkül hogy elfelejtené a korábbiakat („katasztrofális felejtés" megelőzése).

A mesterséges intelligencia integrálása a HRI rendszerekbe tehát nemcsak technikai fejlődést jelent, hanem a felhasználói élmény és a robot elfogadottságának javulását is eredményezi. A jövő humán-robot rendszerei képesek lesznek komplex szociális helyzetek értelmezésére, valamint tanulni az egyedi emberi szokásokból, így valódi együttműködő partnerré válnak.

8. Ipari és gyakorlati példák

A humán-robot együttműködés gyakorlati alkalmazásai elsősorban az ipari gyártásban és a szolgáltató szektorban jöttek létre, de egyre több kreatív területen bukkannak fel [2. táblázat]. Az egyik legismertebb alkalmazás a kollaboratív robotok (cobotok) használata az összeszerelő és logisztikai feladatoknál. Ilyen például az autóiparban elterjedt KUKA LBR iiwa [7. ábra] vagy a Universal Robots sorozata, amelyek érintésérzékeny végekkel és beépített biztonsági funkciókkal vannak ellátva. Ezek a robotok közvetlenül dolgoznak együtt az emberekkel, például összeszerelési műveletekben (csavarozás, szerelés) vagy nehéz alkatrészek mozgatásában. Egy elemzés szerint a kollaboratív robotok fokozzák a termelés hatékonyságát és rugalmasságát azzal, hogy a kezelők döntéseit támogatják, és intuitív felületeikkel aktívan segítik a munkavégzést.

7. ábra: KUKA LBR iiwa kollaboratív robot emberrel közösen dolgozik az ipari összeszerelés során. Forrás: [7]

8. ábra: Pepper robot szociális támogatási célú humán-robot interakcióhoz. Forrás: [8]

Az ágazat gyakorlatában a folyamatok átszervezése is megfigyelhető: a robotok végzik a monoton vagy testreszabott munkarészleteket, míg az emberi operátorok a döntéshozó és minőség-ellenőrző szerepet töltik be. A CPS és HRI másik fontos területe az egészségügy és rehabilitáció. A műtéti robotok (pl. a da Vinci rendszer [9. ábra]) lehetővé teszik a távoli sebészeti beavatkozásokat, ahol az orvos virtuálisan irányítja a robotkarokat. A rehabilitációs robotok (pl. exoskeletonok [10. ábra]) együttműködnek a beteggel a mozgásterápia során, érzékelve a páciens erőnlétét és alkalmazkodva ahhoz. Az otthoni ápolásban is használnak humanoid vagy állatformájú segítő robotokat, amelyek a gyógyszeradagolástól kezdve a társas tevékenységekig széles körben alkalmazhatók. Például a Pepper [8. ábra] robotot is vizsgálták olyan iskolai környezetben, ahol autizmussal élő gyermekekkel dolgozott.

9. ábra: Műtéti robot (da Vinci) távolról irányított sebészeti beavatkozás közben. Forrás: [9]

10. ábra: Exoskeleton terápiás használatban, mozgássegítés céljából. Forrás: [10]

Ezeknél a alkalmazásoknál kiemelten fontosak az emberi tényezők – a robot empatizálása és a biztonságos interakció kritikus feltétel. A szolgáltatói szférában (vendéglátás, kereskedelem, közszolgáltatás) is egyre elterjedtebbek az interaktív robotok. A vendéglátóhelyeken robotpincérek vagy önkiszolgáló robotok (pl. italautomaták robotizált karral) jelennek meg, míg boltokban az ügyfélszolgálati robotok segítenek tájékozódni. Ipari példaként említhető továbbá az okos logisztika: önvezető targoncák és drónok együttműködnek az emberekkel a raktári rend és készletezés fenntartásában.

2. táblázat: Néhány gyakorlati HRI-alkalmazás az ipar és szolgáltatások területén.

Példa terület	Alkalmazás	Főbb jellemzők
Autóipari gyártás (összeszerelés)	cobot-ok (pl. KUKA LBR iiwa, UR sorozat)	Robotos karok csavarbehajtásra, alkatrészmozgatásra; érintésérzékelők, automatikus sebességkorlátozás.
Elektronikai és egyéb összeszerelés	Denoidus robotic assembly	Precíziós feladatok; ember gép együttműködés az apró alkatrészek szerelésénél.
Egészségügy (műtét, rehabilitáció)	Műtéti robotok (pl. da Vinci), Exoskeletonok	Távolműtétek robotkarokkal; testszegmentumok mozgatása terápiához; személyre szabott mozgástámogatás.
Okos logisztika és raktár	Önjáró targoncák, drónok, vizuális irányítás	Automatizált anyagmozgatás, ember-robot vegyes munkaterek, valós idejű pozíciókövetés.
Szolgáltatói robotika	Ügyfélszolgálati robotok (pl. Pepper), Hotelrobotok	Humán-szerű interakció, válaszkészség; humanoid megjelenés, arcfelismerés, többnyelvű kommunikáció.

A fenti példákból jól látszik, hogy a kollaboratív robotok és intelligens automatizálási megoldások terjedése erősíti a CPS és HRI kapcsolatát. A gyártási példákban a robotok már

nem egy elszigetelt cellában dolgoznak, hanem szoros kapcsolatban az emberi operátorral – ezt a rugalmasságot és integrációt nyújtja az ipar 4.0 paradigmája. Ugyanakkor más területeken, mint a szolgáltatóipar, egyre nagyobb szerepet kapnak a robotok szociális képességei és kényelme az ember számára: a cél az, hogy a robotok kiterjesszék a felhasználói élményt (például tanulás vagy idősgondozás esetén) és vegyék le a fizikai vagy rutinfeladatokat az ember válláról.

A gyakorlatban ezeknek az alkalmazásoknak a megvalósítása során számos technikai és tervezési szempont merül fel: például a robot fizikai kialakítása (zárt vagy nyitott végű kar, sebességstabilitás), a felhasználói interfész, és a környezet biztonsági feltételei mind nagyban befolyásolják az üzemeltethetőséget.

9. Társadalmi hatások és felhasználói elfogadás

A kiber-fizikai rendszerek (CPS) és a humán-robot interakció (HRI) terjedése nem csupán technológiai, hanem mélyen társadalmi jelentőséggel bíró változásokat is hoz magával. Az emberek és robotok közötti együttműködés elterjedése új viselkedési mintákat, attitűdöket és normarendszereket hív életre. A technológiai innováció sikere jelentős részben azon múlik, hogy a társadalom hogyan viszonyul a robotok jelenlétéhez, elfogadja-e azok működését, illetve milyen mértékű interakciót hajlandó kialakítani velük.

Közvélekedés és percepció a robotikáról:

A felhasználói elfogadás egyik legfontosabb befolyásoló tényezője az, ahogyan a robotokat a társadalom látja. A közvélemény gyakran két pólus között ingadozik: az optimista jövőkép szerint a robotok felszabadítanak bennünket az ismétlődő, nehéz vagy veszélyes munkák alól, míg a pesszimista megközelítés a munkahelyek elvesztését, a társas kapcsolatok gyengülését, sőt az emberi szerepek elidegenítését vizionálja.

Kutatások szerint a robotokkal kapcsolatos attitűdök országonként és kultúránként is jelentős eltérést mutatnak. Japánban például – ahol a robotokat gyakran pozitív, barátságos lényekként ábrázolják a populáris kultúrában – a társadalmi elfogadás sokkal magasabb, mint például Európa egyes részein, ahol a robotokat inkább veszélyforrásként érzékelik. Ez azt mutatja, hogy a kulturális előfeltevések és társadalmi narratívák jelentős szerepet játszanak abban, hogy az emberek hogyan értelmezik és fogadják el a HRI rendszereket.

A bizalom szerepe a technológiai elfogadásban:

A humán-robot interakció elfogadásának kulcstényezője a bizalom. A robotokat használó személyek számára fontos, hogy a gép viselkedése kiszámítható, megbízható és transzparens legyen. A bizalomépítés különösen kritikus azokban az alkalmazásokban, ahol a robot közvetlenül vagy közvetetten befolyásolhatja az ember biztonságát vagy jóllétét (például egészségügy, közlekedés, idősellátás).

A bizalom multidimenziós fogalom a HRI kontextusában: egyszerre vonatkozik a robot fizikai megbízhatóságára, a szoftveres döntések minőségére, valamint a szociális interakciók hitelességére. A vizsgálatok szerint a robot viselkedésének előrejelezhetősége, a visszajelzési mechanizmusok (pl. hangjelzés, vizuális kijelzés) és az emberi reakciókra adott válaszok mind hozzájárulnak a pozitív bizalmi megítéléshez.

Az antropomorfizálás hatásai:

A robotok emberhez hasonló megjelenése és viselkedése (antropomorfizálás) egyaránt lehet előnyös és problémás a felhasználói elfogadás szempontjából. Egyes vizsgálatok kimutatták, hogy az emberszerű tulajdonságokkal rendelkező robotokkal szemben empatikusabb, személyesebb viszony alakulhat ki, ami segíti az együttműködést, különösen társadalmi célú alkalmazásokban (pl. oktatás, szociális gondozás).

Ugyanakkor a korábban már említett „uncanny valley" jelenségre is figyelemmel kell lenni: ha egy robot túlzottan hasonlít az emberre, de mégis mesterséges hatást kelt, az kognitív disszonanciát és elutasítást válthat ki a felhasználóból. A sikeres tervezéshez tehát kulturálisan és funkcionálisan is illeszkedő mértékű antropomorfizációra van szükség, amely nem kelti a túlzott „emberi mímelés" érzetét, de mégis támogatja az intuitív interakciót.

Felhasználói edukáció és tanulási görbék:

A technológia elfogadása nem megy végbe automatikusan; gyakran oktatást, tréninget és ismeretterjesztést igényel. A CPS rendszerekben működő robotok kezeléséhez és használatához a felhasználóknak meg kell érteniük azok működési elveit, interakciós szabályait és határait.

A felhasználói edukáció egyik legfontosabb célja a robot működésével kapcsolatos bizonytalanságok csökkentése, ami közvetve a bizalom növekedéséhez is hozzájárul. Az intuitív kezelőfelületek, a multimodális visszajelzések (pl. hang+vizualitás) és a személyre szabható interakciós lehetőségek mind megkönnyítik a tanulást. Egyes kutatások szerint a gamifikált vagy VR-alapú oktatási modulok jelentősen gyorsítják a HRI rendszerek használatának elsajátítását, különösen idősebb vagy technikailag kevésbé jártas felhasználók esetén.

Társadalmi egyenlőtlenségek és inkluzív tervezés:

A robotika és CPS rendszerek fejlődése nem egyenletesen oszlik el a társadalom különböző rétegei között. A digitális írástudás, a hozzáférés technológiai eszközökhöz és az egyéni attitűdök mind befolyásolják, hogy ki és milyen mértékben részesül a technológia előnyeiből.

Fontos szempont tehát az inkluzív tervezés elveinek alkalmazása: a HRI rendszereket úgy kell kialakítani, hogy azok a lehető legszélesebb felhasználói kör számára hozzáférhetők, érthetők és használhatók legyenek. Ez különösen érvényes az idősek, fogyatékossággal élők vagy alacsonyabb technológiai háttérrel rendelkező felhasználók esetében. Az egyenlő hozzáférés biztosítása nem csupán morális, hanem gazdasági és társadalmi érdek is: a széles körű elfogadás elengedhetetlen a technológia hosszú távú fenntarthatóságához.

Sztereotípiák, média és robotkultúra:

A felhasználók robotokkal kapcsolatos attitűdjeit nagymértékben befolyásolja a médiában megjelenő robotábrázolás. A filmek, hírek, sci-fi történetek gyakran szélsőségesen idealizált vagy épp félelemkeltő képet festenek a mesterséges lényekről [11. ábra]. Ezek a narratívák – még ha tudományos-fantasztikus köntösben is jelennek meg – hatással vannak a közvélekedésre és így a tényleges technológiai elfogadásra.

11. ábra: Az „I, robot" c. filmben a robot mellkasán világító vörös fény azt jelzi, hogy a robotot viselkedését távolról felülírták, tehát eltér az alapvető programozásától, és veszélyt jelenthet az emberre, mivel nem követi a robotika Három Törvényét. Forrás: [11]

A robotika fejlesztőinek ezért érdemes figyelembe venni, hogyan kommunikálják termékeiket a társadalom felé. A pozitív példák, empatikus interakciók és valódi emberi értéket képviselő alkalmazások (pl. rehabilitációs robotok, oktatási partnerek, idősgondozó rendszerek) mind hozzájárulnak a negatív sztereotípiák lebontásához és a társadalmi elfogadás erősítéséhez.

10. Biztonsági és etikai kérdések

A CPS-ek (Cyber-Physical Systems) és a humán-robot interakciót (HRI) alkalmazó rendszerek esetében a biztonság és az etika kulcsfontosságú kérdéskörök. A fizikai és digitális világ közvetlen összekapcsolása új típusú veszélyforrásokat teremt, amelyek mind az emberi biztonságot, mind az adatvédelmet, illetve a társadalmi normákat érintik.

A biztonsági kockázatok nemcsak mechanikaiak, hanem informatikai és döntéshozatali jellegűek is. Az ipari robotok fejlődésével a korábban zárt, elkerített munkaterületeket felváltják a nyíltabb, emberrel közös terek, ahol a kollaboratív robotok (kobotok) működnek. Ez paradigmaváltást jelent: a robotnak folyamatosan érzékelnie és értelmeznie kell az ember jelenlétét, mozgását és szándékait. A Safety-by-Design elv alapján már a tervezés fázisában be kell építeni a megbízhatósági és védelmi mechanizmusokat, mint például redundáns szenzorrendszerek, prediktív ütközéselkerülő algoritmusok vagy dinamikusan szabályozható működési zónák.

Az ISO 10218 és a ISO/TS 15066 szabványok meghatározzák az együttműködő robotok biztonsági kritériumait, különös tekintettel a fizikai kontaktusokra. A „pain onset" küszöbök alapján végzett validációk lehetővé teszik az emberi szövetekre gyakorolt nyomás biztonságos szinten tartását. Ugyanakkor a szabványosítás csak minimális követelményeket fektet le — a technológiai fejlődés tempója gyakran megelőzi a szabályozást, így a gyártóknak önszabályozással kell előremutató megoldásokat alkalmazniuk.

A kiberbiztonság területén a támadási felületek száma jelentősen megnő egy CPS-ben. A robotok hálózati kapcsolatai (pl. távoli karbantartás, felhőalapú irányítás) lehetőséget teremtenek jogosulatlan hozzáférésre. A lehetséges fenyegetések közé tartozik az adathalászat, a szolgáltatásmegtagadásos (DoS) támadás, vagy a robot működésének manipulálása (pl. útvonalmódosítás, sebességváltoztatás). A zero trust elvű hálózatvédelem, behatolásérzékelő rendszerek (IDS), valamint a valós idejű titkosítás és hitelesítés kulcsfontosságúak a védelemben.

Az etikai kérdések túlnyúlnak a technikai kereteken. Az autonóm döntéshozatalt végző rendszerek esetén meg kell határozni, hogy milyen mértékű autonómiát adunk a robotnak, és hol húzódik a felelősség határa. Például egy orvosi segédrobot dönthet-e a beavatkozás elhalasztásáról, ha a szenzoradatok szerint az instabil? Vagy egy önvezető jármű választhat-e két lehetséges baleseti kimenet között?

A felelősségi lánc kérdése jogi szempontból is bonyolult: ki viseli a következményeket egy robot által okozott baleset után — a fejlesztő, a gyártó, a rendszerintegrátor, vagy a végfelhasználó? A jogi szabályozás gyakran nem tart lépést a technológia fejlődésével, így az átmeneti időszakban az etikai irányelvek (pl. IEEE Ethically Aligned Design) töltenek be irányadó szerepet.

Különös figyelmet igényel az adatvédelem. A HRI során a robotok jellemzően képet, hangot, mozgásmintát és más biometrikus adatokat rögzítenek. Az ilyen adatok érzékeny jellege miatt elengedhetetlen a GDPR-nak megfelelő adatkezelési gyakorlat. A robotoknak transzparens módon kell kezelniük az adatgyűjtést és -felhasználást, és lehetőséget kell biztosítani a felhasználónak az adatai törlésére vagy anonimizálására.

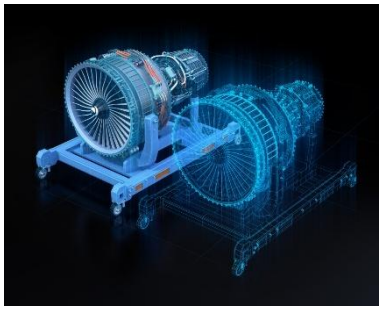
Végül a társadalmi hatásokat sem szabad figyelmen kívül hagyni. A robotizáció hosszú távon átalakítja a munkaerőpiacot. Miközben új, magasabb szintű munkahelyeket teremt, egyes alacsonyan képzett pozíciókat kiválthat, ami társadalmi egyenlőtlenségekhez vezethet. A technológiai fejlődés társadalmi elfogadottságát segítheti, ha a fejlesztés és bevezetés során figyelembe vesszük a közösségi részvételt, oktatást, és az inkluzív tervezési elveket.

A CPS-ekben zajló HRI csak akkor lehet hosszú távon sikeres és elfogadott, ha a biztonsági és etikai elvek szervesen beépülnek a fejlesztés, tervezés és üzemeltetés teljes ciklusába. A technológiai lehetőségek kiaknázása nem történhet a társadalmi, jogi és emberi értékek rovására.

11. Jövőbeli kihívások és trendek

A humán-robot interakció és a kiber-fizikai rendszerek jövője számos új technológiai és társadalmi kihívást vet fel. Egyrészt a technológiai trendek közé tartozik a számítási kapacitás növekedése, a szenzorok és mechatronikai eszközök miniatürizálása, valamint a felhő- és edge-computing fejlődése.

A digitális iker (digital twin [12. ábra]) koncepció például lehetővé teszi, hogy a valós robotok egy virtuális másolatát hozzuk létre, ahol szimulációk és előrejelzések alapján javítjuk a rendszer tervezését és karbantartását. A digitális iker lényege, hogy valós fizikai rendszerek adatai és egy párhuzamos virtuális modell között kölcsönhatás valósul meg, így valós időben tudjuk frissíteni a szimulációt. Ez különösen hasznos lehet olyan CPS-ekben, ahol sok ember és gép dolgozik együtt, hiszen a virtuális modell segítségével előre feltérképezhetők az együttműködés optimális stratégiái, új feladatok tervezhetők, és a váratlan események (pl. meghibásodás) modellezhetők anélkül, hogy a fizikai rendszert veszélyeztetnénk.



12. ábra: Digitális iker. Forrás: [12]

A felhasználói interfészekben (HRI szempontjából) a virtuális és kiterjesztett valóság [13. ábra] (VR/AR/MR) várható térnyerése hozhat áttörést. A kutatások szerint az AR technológiák képesek fokozni a felhasználó helyzetismeretét és biztonságát HRI során. Például egy gyártási feladathoz AR szemüveggel fedhetünk fel a valós környezetre illeszkedő utasításokat, vagy jelezhetjük a robot várható mozgását, így az ember mindig tisztában lehet azzal, mi fog történni. A kiterjesztett valóság emellett lehetőséget ad arra is, hogy a robot virtuális modelljét közvetlenül a fizikai téren belül lássuk, ezzel megerősítve az ember-robot szinkronizációját. A VR pedig tréning és szimuláció célra használható: a robot és az ember együtt gyakorolhatnak virtuális környezetben, mielőtt a valós térben együttműködnének.

13. ábra: A kép egy lehetséges AR-felhasználói felületet mutat, amely a valós környezetre vetíti az embert segítő információkat. Forrás: [13]

A mesterséges intelligencia területén a nagy nyelvi modellek (LLM-ek) és a kognitív robotok felé fordul a kutatás. Olyan rendszerek kidolgozása folyik, amelyek az emberi beszédet és viselkedést emberien értelmezik és válaszolják meg. A LLM-ek integrálása robotvezérlésbe lehetővé teszi, hogy a robotok egyszerű parancsok helyett összetettebb igényeket is megértsenek, kreatív módon oldjanak meg feladatokat, és adaptívabb párbeszédet folytassanak a felhasználóval. Emellett várható, hogy a gépi tanulás új területei (pl. öntanuló rendszerek,

federált tanulás) erősödnek meg, mert a több robot és CPS közötti adatszintű együttműködés lehetőséget ad arra, hogy egy robot tanuljon más robotok tapasztalataiból a felhasználóval való interakciókról.

További kihívást jelentenek a biztonság és normatív szabályozás jövőbeli kérdései: meg kell találni az egyensúlyt a innovációs potenciál és a biztonságos működés között. A társadalmi elfogadottság érdekében előírásokra és etikai irányelvekre lesz szükség (például adatvédelmi garanciák, felelősségi kérdések tisztázása).

A jövőbeli CPS-HRI rendszereknek szem előtt kell tartaniuk a több-ügynökös együttműködést is: a robotok közötti koordináció, a swarm-intelligencia (méhek módjára együtt dolgozó robotok) és a komplex mesterséges közösségek felépítése mind fontos trendek. Várható továbbá a működési környezetek heterogenitásának növekedése: a CPS-ek részeként emberek, robotok és IoT eszközök együttműködése egyre elterjedtebb lesz.

A közeljövő kulcstrendjei között szerepel a gazdagabb multimodális interakció (hang+gesztus+AR+VR), a mesterséges intelligencia mélyebb integrálása, illetve az ember-gép rendszerek teljes életciklusának digitális modellezése. Ezek az irányok új lehetőségeket nyitnak az HRI számára (például szemmozgás-vezérelt robotrendszerek vagy empatikus robotasszisztensek formájában), ugyanakkor kihívásokkal is járnak: nagyobb adatvédelmi és biztonsági kockázatokat, valamint etikai és jogi vitákat generálnak. A jövőben a HRI-kutatásnak nem csak technikai szempontból kell fejlődnie, hanem interdiszciplináris módon, hogy megfeleljen az emberközpontú rendszerek iránt támasztott növekvő követelményeknek.

12. Összefoglalás, következtetések

A tanulmány célkitűzése a kiber-fizikai rendszerek (Cyber-Physical Systems – CPS) és a humán-robot interakció (Human-Robot Interaction – HRI) közötti összefüggések elméleti és gyakorlati szempontú feltárása volt. A vizsgálat során részletes áttekintés készült arról, hogyan épülnek fel a CPS-ek, miként valósul meg bennük a fizikai és digitális rétegek integrációja, és milyen szerepet játszik ebben az ember-robot együttműködés.

A HRI kategóriáinak – kooperatív, kollaboratív és autonóm – bemutatásával kiemelésre került, hogy az interakció típusa meghatározza a rendszertervezés alapvető elveit. A közeli és távoli interakciók technológiai követelményei, valamint az emberi tényezők – úgymint bizalom, reakcióidő, biztonságérzet és ergonómia – jelentős hatással vannak a felhasználói élményre és a rendszer megbízhatóságára.

A CPS-ekben alkalmazott érzékelő- és szenzortechnológiák (pl. kamerák, LIDAR, haptikus visszacsatolás) lehetővé teszik a robotok számára a környezet és az emberi jelenlét pontos észlelését. E technológiák részletes ismertetésével alátámasztásra került, hogy a pontos érzékelés és a valós idejű visszacsatolás elengedhetetlen feltétele a biztonságos és hatékony HRI-nak.

A kommunikációs architektúrák vizsgálata során kiemelésre kerültek azok a protokollok (például ROS 2, MQTT, OPC-UA), amelyek biztosítják a különböző komponensek közötti valós idejű, szabványosított adatcserét. A főbb protokollok jellemzőit táblázatos formában is összegeztük, ezzel segítve az összehasonlíthatóságot és a gyakorlati alkalmazás szempontú értékelést.

A gépi tanulás alkalmazása révén lehetővé válik az interakciók adaptívvá és felhasználóközpontúvá tétele. A HRI ezen formáiban a rendszerek képesek a felhasználók viselkedési mintáinak felismerésére és ennek megfelelően a működésük finomhangolására, ami jelentős előrelépést jelent az interakció természetessége és hatékonysága terén.

Gyakorlati példák bemutatásán keresztül szemléltetésre került, hogyan alkalmazzák napjainkban a CPS és HRI megoldásokat különböző szektorokban. Az autóipari gyártósorokon megjelenő kollaboratív robotok, az egészségügyi ellátásban alkalmazott segítő robotok és a logisztikában működő autonóm rendszerek példája rávilágított a technológia sokoldalúságára és ipari jelentőségére.

A biztonsági és etikai kérdések tárgyalásakor a releváns szabványok (pl. ISO 10218, ISO/TS 15066) és a szabályozási környezet is bemutatásra került, hangsúlyozva azok szerepét a humán környezetben működő robotikai rendszerek tervezésében. Emellett reflektálás történt az olyan etikai dilemmákra is, mint a gépi döntéshozatal felelőssége, az adatok védelme és a munkahelyi szerepkörök átalakulása.

A jövőbeli fejlődési irányokat illetően megállapítható, hogy a digitalizált ikrek alkalmazása, a mesterséges intelligencia és nagy nyelvi modellek (LLM-ek) integrációja, valamint a kiterjesztett és virtuális valóságon alapuló interfészek elterjedése alapjaiban formálhatja át a HRI koncepcióját. Mindezen technológiai előrelépések ellenére továbbra is kiemelt jelentőségű az emberközpontú tervezés és az etikai szempontok érvényesítése.

Összegzésként megállapítható, hogy a CPS rendszerek működésének jövőbeli hatékonysága és elfogadottsága nagyban múlik azon, miként integrálják a humán-robot interakció elemeit. A robotoknak nem csupán a környezeti feladatok elvégzésére kell alkalmassá válniuk, hanem képesnek kell lenniük az emberi partnerekkel való kooperációra, az emberi viselkedés felismerésére és a kommunikációra. A jelenlegi kutatási és ipari trendek egyértelműen az ember és gép közötti természetesebb, intuitívabb együttműködés felé mutatnak, ahol a technológia nem csupán eszköz, hanem partnerként jelenik meg a felhasználó oldalán.

Források:

[1]: Pál Varga, CPS three-layers architecure [Kép], [Online]. Elérhető: https://www.researchgate.net/figure/CPS-three-layers-architecture_fig1_378576331
[Letöltés dátuma: 2025.05.15]

[2]: Shutterstock Image, Mechanical robot hand human reach each [Kép], [Online]. Elérhető: https://www.shutterstock.com/image-vector/mechanical-robot-hand-human-reach-each-1237265110
[Letöltés dátuma: 2025.05.10]

[3]: DeepAI által generált kép, [Kép], [Online]. Képet generálta: https://deepai.org/machine-learning-model/text2img
[Keletkezett: 2025.05.10]

[4]: Pernecker Dávid, Uncanny Valley 2015.07.16, [Kép], [Online]. Elérhető: https://filmtett.ro/uploads/Egyeb/uncanny-magyarazat(1).jpg
[Letöltés dátuma: 2025.05.11]

[5]: all-electronics.de, LIDAR sensor image [Kép], [Online]. Elérhető: https://www.all-electronics.de/assets/images/e/41224860-eb76596b.jpg
[Letöltés dátuma: 2025.05.11]

[6]: futureplc.com, EMG sensor [Kép], [Online]. Elérhető: https://cdn.mos.cms.futurecdn.net/4zkXvbAsncCfPd8HgHa2DX-1200-80.png
[Letöltés dátuma: 2025.05.11]

[7]: directindustry.com, KUKA LBR iiwa kollaboratív robot [Kép], [Online]. Elérhető: https://img.directindustry.com.ru/images_di/photo-g/17587-9726309.jpg
[Letöltés dátuma: 2025.05.11]

[8]: Wikipedia, Pepper robot [Kép], [Online]. Elérhető: https://upload.wikimedia.org/wikipedia/commons/e/ee/Pepper_the_Robot.jpg
[Letöltés dátuma: 2025.05.14]

[9]: Chinede General Hospital and Medical Center, da Vinci Műtéti robot [Kép], [Online]. Elérhető: https://cghmc.com.ph/wp-content/uploads/2022/09/cgh-davinci00-1024x609.jpeg
[Letöltés dátuma: 2025.05.14]

[10]: MDTAP Blog, Robotic Exoskeleton [Kép], [Online]. Elérhető: https://www.equipmentlink.org/blog/?p=4096, https://www.equipmentlink.org/blog/wp-content/uploads/2019/01/man-standing-300x246.png
[Letöltés dátuma: 2025.05.15]

[11]: „I, Robot” c. film részlet [Kép], [Online]. Elérhető: https://i.ytimg.com/vi/eI0uT7xqCwo/hq720.jpg?sqp=-oaymwEhCK4FEIIDSFryq4qpAxMIARUAAAAAGAElAADIQj0AgKJD&rs=AOn4CLCeinntRcpEklejs1VqZz4KoKP1WQ
[Letöltés dátuma: 2025.05.15]

[12]: blecan.com, Digital Twin [Kép], [Online]. Elérhető: https://www.belcan.com/wp-content/uploads/2023/01/Digital-Twin.jpg
[Letöltés dátuma: 2025.05.15]

[13]: metrology.news, lehetséges AR-felhasználói felület [Kép], [Online]. Elérhető: https://metrology.news/wp-content/uploads/2022/01/7-Ways-Augmented-Reality-Can-Upgrade-Manufacturing-Processes.jpg
[Letöltés dátuma: 2025.05.15]

[14]: OPSWAT, Kiber-fizikai rendszerek, 2025.04.24 [Online]. Elérhető: https://hungarian.opswat.com/blog/cyber-physical-systems-cps

[15]: webhosting.de, Kiber-fizikai rendszerek (CPS), [Online]. Elérhető: https://webhosting.de/hu/kiber-fizikai-rendszerek-cps-meghatarozas-alkalmazasok-joevo/

[16]: Fortinet, Cyber-Physical Systems, [Online]. Elérhető: https://www.fortinet.com/resources/cyberglossary/cyber-physical-systems

[17]: Wikipedia, Cyber-physical system, [Online]. Elérhető: https://en.wikipedia.org/wiki/Cyber%E2%80%93physical_system

[18]: Wikipedia, Human-robot interaction, [Online]. Elérhető: https://en.wikipedia.org/wiki/Human%E2%80%93robot_interaction#:~:text=Human%E2%80%93robot%20interaction%20(HRI),%2C%20design%2C%20psychology%20and%20philosophy.

[19]: ScienceDirect, Human-robot interaction, [Online]. Elérhető: https://www.sciencedirect.com/topics/computer-science/human-robot-interaction

[20]: Saleem, Z., Gustafsson, F., Furey, E. et al. A review of external sensors for human detection in a human robot collaborative environment. J Intell Manuf 36, 2255–2279 (2025). [Online]. Elérhető: https://doi.org/10.1007/s10845-024-02341-2

[21]: Dr. Kovácsházy Tamás, INFOTÉR 2015, Kiber-fizikai rendszerek jelentősége az Ipar 4.0 trendben, [Online]. Elérhető: https://konferencia2015.infoter.eu/_eloadasok/2/12-30-dr-kovacshazy-tamas.pdf#:~:text=%01%20Egy%20olyan%20elosztott%2C%20kiterjedt,3C%20angolul%3A%20Communicate%2C%20Compute%2C%20Control

[22]: Pernecker Dávid, Uncanny Valley, 2015.07.16, [Online]. Elérhető: https://filmtett.ro/cikk/az-uncanny-valley-jelensegrol

2.60. Szimulációs Gyártósor esszé

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

IPAR 4.0 TECHNOLÓGIÁK

Szimulációs Gyártósor esszé

Dala Márk

([redacted])

2024/25/2

Tartalom

Előszó 3
Kezdetek 4
Első nagy fejlesztés 10
Porondon 17
Fejlesztések 18
PLC program 21
Architektúra 22
Rövid utóélet 24
Személyes utóélet 25
Végszó 26
Műszaki forrás: 27

Videó jegyzék:

1. Video a hátlapok vágásának folyamatáról
2. Video az elbúcsúzó mozdulatsor tesztelése
3. Video az asztal vágási síkjának felvételéről
4. Video az asztal lábának elvágásának folyamata
5. Video az elkészült projectről

TIA Portal V19[1]. A Szimulációs gyártósor PLC programja itt.

Előszó

Ebben az esszében a Szombathelyi Puskás Tivadar középiskolában eltöltött elektronikai technikus képzésben való részvételem alatt készített Szimulációs gyártósort fogom bemutatni. Az építés helye a Szentgotthárdi Opel gyár Tudásközpontja, ahol a duális gyakorlat keretein belül képeztek minket és biztosítottak nekünk szakmai képzést, valamint az eszközpark is az ő tulajdonuk. Emiatt a szimulációs gyártósor azóta is a tudásközpontban tartózkodik. Az építés alatt, illetve a gyártósor utóéletét is az akkor készült képek és emlékek alapján kívánom bemutatni. A résztvevők hozzájárulásával.

1595

Kezdetek

Az Opel gyár területén zajló képzésünk során számos technológiai területtel ismerkedtünk meg Szabó László tanár úr vezetésével. A tananyag rendkívül széles spektrumot ölelt fel: mélyrehatóan foglalkoztunk a PLC-programozás [2] alapjaival és gyakorlati alkalmazásaival, megismertük a pneumatikai rendszerek [3] működését, valamint ezek elektropneumatikai [4] vezérlési lehetőségeit. Emellett betekintést nyertünk a mikrokontrollerek [5] világába, ahol a beágyazott rendszerek programozásával is foglalkoztunk. Nemcsak az elektronika, hanem a mechanikai tervezés is nagy hangsúlyt kapott: elsajátítottuk a 3D modellezés és nyomtatás [6] alapjait, valamint hálózatok létrehozását [7] és kezelését is gyakoroltuk.

Tizenegyedik osztályos korunkban kezdtük meg a képzést, és ahogy egyre mélyebben elmerültünk a különböző technológiákban, úgy nőtt bennem a vágy, hogy valami igazán maradandót alkossak. Egy olyan projektet szerettem volna megvalósítani, amely nemcsak kihívást jelent számomra, hanem amelynek eredménye valódi elégedettséggel töltene el. Kezdetben nem volt konkrét elképzelésem arról, hogy pontosan mit is szeretnék létrehozni, azonban hozzáférést kaptam néhány ritkán használt alkatrészhez, amelyek inspirációként szolgáltak a további tervezéshez.

Ezek az eszközök a következők voltak: kettő darab szállítószalag [8], egy korongok adagolására alkalmas adagoló [9], egy szelepsziget [10], valamint egy pneumatikusan működő átrakó [11]. A rendelkezésemre álló eszközök és az eddig megszerzett tudás alapján kezdett körvonalazódni a projekt iránya. Mivel leginkább a PLC-programozás állt közel hozzám, arra törekedtem, hogy a rendszer vezérlését teljes mértékben automatizáljam.

Szerencsére a tanár úr végig támogatott az egész projekt alatt, így hamar zöld utat kaptam arra, hogy azt csináljak az eszközökkel, amit szeretnék. A szerkezet összeállításának első lépéseként a terem végében elhelyezkedő satupadra [12] rögzítettünk kettő darab sávos alumínium lapot [13], amely megfelelően nagy felületet biztosított a munkánkhoz. (1. ábra) (2. ábra) A profilok felhelyezésében és az egész projekt során nagy segítséget nyújtott Laski Ákos, akkori osztálytársam.

1. ábra Felkerülő sávos alumínium

2. ábra Az iterációnak helyet adó satupad

Ezek után a fő irányvonal is kialakult. A rendelkezésre álló eszközök és a teremben található technológia lehetővé tették, hogy egy komplex, automatizált rendszert építsünk fel. A projekt alapját egy színfelismerésen alapuló szortírozó rendszer képezte, amelyben különböző eszközök összehangolt működésére volt szükség.

A teremben lévő 3D nyomtatóval, egy CraftBot Plus Pro [14] (4. ábra), különböző színű korongokat nyomtattunk, amelyek az adagolóból egy Arduino Braccio Robot [15] (3. ábra) segítségével az első szállítószalagra kerültek. Innen egy pneumatikus átrakó továbbította őket a második szalagra, ahol egy színérzékelő [16] beazonosította a korongokat. A rendszer utolsó lépéseként a robot az érzékelő által meghatározott szín alapján a megfelelő tárolóba helyezte a korongot.

Ehhez minden szükséges eszközünk rendelkezésre állt, kivéve az Arduino Braccio Robotot. Szerencsére Szabó László tanár úr támogatásának köszönhetően sikerült elérni, hogy a robotot megrendelhessük, így a tervünk megvalósítása hivatalosan is kezdetét vette.

3. ábra Arduino Braccio megérkezése

4. ábra CraftBot Plus Pro

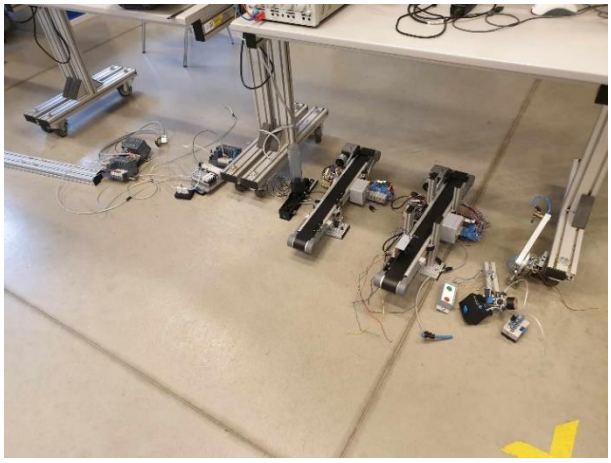
A kezdetek után viszont elérkezett a tanév vége, ami azt a helyzetet idézte elő, hogy további három héten keresztül dolgozhattunk az asztalon. Ez az időszak kulcsfontosságú volt, hiszen ekkor sikerült a projekt alapvető mechanikai és elektronikai elemeit a helyükre illeszteni. A harmadik hét végére a fő komponensek már működtek, és bár a robot még nem állt rendelkezésre, a rendszer alapvető folyamatai már tesztelhetők voltak.

A nyári szünet alatt nekem nem volt semmi dolgom, így a tanár úrral egyeztetve önszorgalomból tovább folytattam a munkát. Ez az időszak lehetőséget adott arra, hogy nyugodtan, megszakítások nélkül mélyedjek el a projektben. Ekkor készült el az első PLC-program, valamint a teljes vezetékezés. Kezdetben az S7 [17] fejlesztői környezetet használtam a programozáshoz, amely megfelelő alapot nyújtott a rendszer működésének kialakításához.

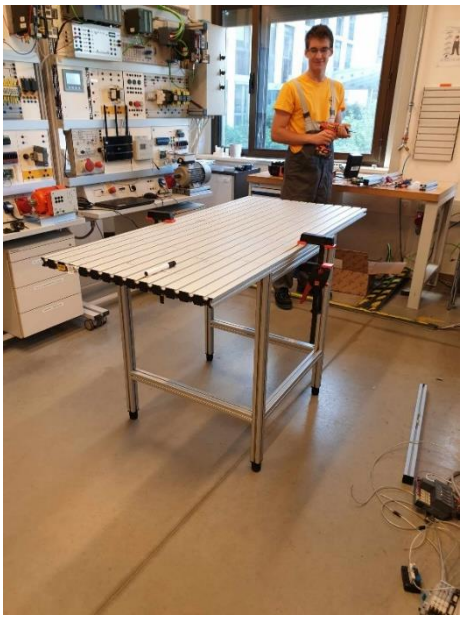
Ahogy haladtunk előre, úgy merültek fel újabb ötletek, amelyek tovább bővítették a projekt funkcionalitását. Az egyik legfontosabb fejlesztés a HMI [18] bevezetése volt, amely lehetőséget biztosított a programmódok közötti váltásra, hibajelzések megjelenítésére, valamint a rendszer egyéb paramétereinek vizuális kezelésére. A HMI integrálása során felmerült az igény egy korszerűbb fejlesztőkörnyezetre, így megfogalmazódott a gondolat, hogy áttérünk a TIA Portal V18-ra [19]. Ez a váltás technológiai szempontból is kihívást jelentett, ugyanakkor rengeteg új lehetőséget nyitott meg számunkra.

Ahogy szépen épült és fejlődött a projekt, a Tudásközpont vezetőjének is egyre jobban tetszett, és felvetette azt a lehetőséget, hogy ezt a rendszert bemutassuk a Szombathelyi Pályaorientációs Napon [20]. Ez az esemény kiváló alkalom volt arra, hogy a projektet szélesebb közönség elé tárjuk, és egyben promótáljuk az Opelt, valamint az iskolánkat is.

Innentől kezdve új szempontok kerültek a képbe, amelyek meghatározták a további fejlesztési irányokat. Az egyik legfontosabb kihívás a rendszer mobilitásának biztosítása volt, mivel a bemutatóra való szállítás megkövetelte, hogy az egész szerkezet könnyen mozgatható és stabil alapra épüljön. (4. ábra, 5. ábra) Ennek érdekében a tanár úrral kettesben egy megfelelő alapot készítettünk, amely biztosította az összes szükséges rendszer önálló működését. Ez a változtatás azonban azt is maga után vonta, hogy a teljes rendszert szétszereltük és újra össze kellett építeni, ami jelentős precizitást és türelmet igényelt.



5. ábra Eddig használt eszközök



6. ábra Elkészült asztallap

Első nagy fejlesztés

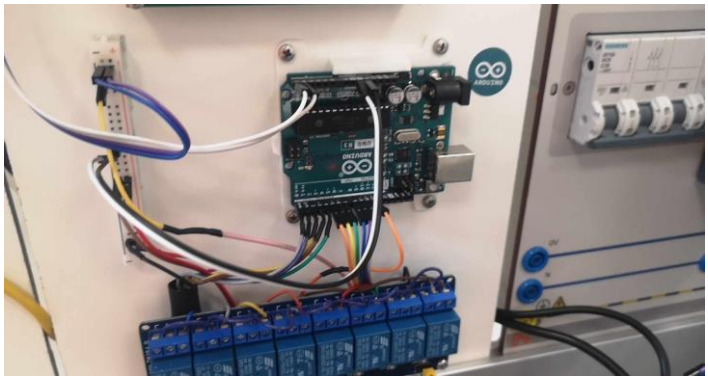
Az asztalra visszakerültek az elemek, és a rendszer tovább bővült, hogy megfeleljen az újabb kihívásoknak. A pneumatikai rendszer működtetéséhez szükség volt egy kompresszorra [21], amely az asztal alatt kapott helyet. A mikrokontrollerek és a PLC közötti kommunikáció megoldására a Node-RED [22] webszervert választottuk, amely lehetővé tette a hatékony adatcserét és vezérlést. Ennek következtében egy fedélzeti számítógépet [23] is el kellett helyeznünk az asztal alatt, amely biztosította a megfelelő számítási teljesítményt és a szükséges hálózati kapcsolódásokat.

A PLC két darab decentrális perifériával [24] volt összeköttetésben (8. ábra), és a rendszer működésének optimalizálása érdekében szinte minden bemenet és kimenet a decentrális perifériákba lett bekötve, kivéve néhány különleges esetet. Mivel a Node-RED webszerveren keresztüli kommunikáció WiFi [25] kapcsolatot igényelt, ezért egy Synology [26] router és egy switch [27] is bekerült a rendszerbe, biztosítva a stabil és gyors adatkapcsolatot.

A megnövekedett eszközök és kábelezés miatt több helyre volt szükségünk az asztalon, így egy hátlapot is felszereltünk. Ez nemcsak a kábelek rendezésében segített, hanem esztétikailag is egységesebbé tette a rendszert. A hátlap kivágásának és előkészítésének nagy részét én végeztem egy kis sarokcsiszolóval [28]. (7. ábra)

7. ábra Video a hátlapok vágásának folyamatáról

8. ábra Decentrális periféria hiba felfedezése



9. ábra Színérzékelési modul

Erre a pontra már megvoltak a konkrét terveink, hogy mit, hogyan és miképpen szeretnénk megvalósítani. A végső koncepciónk alapján a színérzékelést egy darab Arduino Uno [29] fogja végezni, (9. ábra) mellyel kezdetben csak egyszer vizsgáltuk meg a korong színét. Ekkor viszont azt tapasztaltuk, hogy a fényviszonyok folyamatos változásával a korongok folyamatosan más RGB [30] jeleket generáltak, emiatt különböző megoldásokkal rukkoltunk elő a fény hatásának minimalizálására. A végső megoldás egy zsiliprendszer [31] lett, amelyet egy másik Arduino Uno vezérelt, és ezzel elértük a célunkat. További megbízhatósági okokból a korongokat darabonként ötvenszer ellenőriztük, és ennyi méréssel állapítottuk meg a színt. Továbbá a PLC clock memory-ját [32] használva a szalagot is minimálisan mozgattuk, így megelőzve annak az esélyét, hogy egy esetleges szennyeződés hibás adatokkal szolgáljon.

10. ábra 3D nyomtatott magasítással ellátott robot

Ekkor már elkezdődött az utolsó tanítási évünk, melynek köszönhetően két hét alatt öt napunk volt az asztalon dolgozni. A robot megérkezésével főleg annak optimalizálásán törtük a fejünket. Első megoldásként a robotot az asztal síkjához rögzítettük, később pedig egy 3D nyomtatott emelvényre helyeztük, (10. ábra) amelyben szintén egy Arduino kapott helyet a Braccio gyári shieldjével, [33] ami lehetővé tette a robot vezérlését. A robotnak ekkor még bitek szerint adtuk a parancsokat. Ez azt jelentette, hogy a PLC bitjei egy szilárdtest-relén [34] keresztül jutottak el a robotot vezérlő Arduino-ba. Erre az Arduino bemeneti feszültség tűrése miatt volt szükség. Később ezt a módszert komplikáltsága és a megbízhatósági hibák miatt leváltottuk. A robotot Nagy Zétény osztálytársam programozta be első ízben, és neki köszönhetően lettünk kész a Szombathelyi Pályaorientációs Napra.

A promótáló jellege miatt több csalogató elemet is beépítettünk az asztalba. Ilyen volt az asztal beszélő képessége, amelyet szintén a Node-Red szólaltatott meg, valamint a robot minden mozzanatát és a színeket is narrálás kísérte. A korongok elfogyásakor zenei kísérettel a robot meghajolt, és tapsra sarkallta a közönséget, megköszönve a figyelmet. (11. ábra)

11. ábra Video az elbúcsúzó mozdulatsor tesztelése

Továbbá az M5 Stack [35] tanuló boardjának RFID-olvasóját [36] is felhasználtuk, (12. ábra) amelynek feladata az indítási jogosultságok kiadása volt. A folyamat úgy zajlott, hogy Ákos a bankkártyánk [37] kódját beleírta a boardba, és ha a jogosult személy kártyáját olvasta be, akkor lehetett elindítani az asztalt.

12. ábra M5 Stack tanuló board

Később kényelmi okok miatt ezt a lehetőséget felszámoltuk, és a LED-mátrixot, [38] valamint a kijelzőt használtuk, amely éppen olyan színben világított, amilyen korongot a robot a saját tárolójába helyezett.

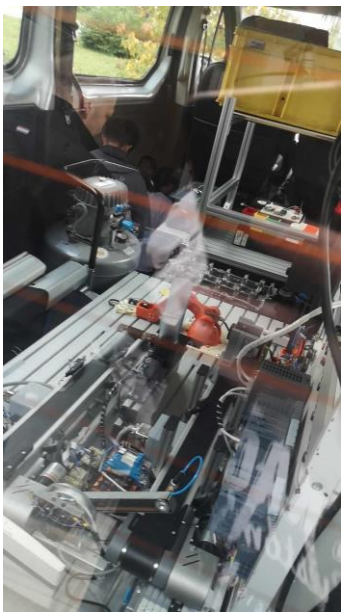
A szombathelyi jelenés előtt még volt egy fontos kérdés, amelyet meg kellett oldani: hogyan tudjuk az asztalt Szentgotthárdról Szombathelyre elszállítani? Az Opel biztosított nekünk egy mikrobuszt, [39] amely sajnos az asztal összeszerelt állapotában túl kicsinek bizonyult. Több lehetőséget mérlegelve végül amellett döntöttünk, hogy ebbe az autóba kell beférnünk. Ehhez a kábelezést [40] modulárissá [41] kellett tennünk, és minden lehetséges problémára fel kellett készülnünk. Az utolsó lépés az asztal kettéfűrészelése volt horizontálisan, [42] hogy magasságban az adott keretek közé kerüljünk. A műveletben Kolompár Erik vett részt. (13. ábra, 14. ábra)

13. ábra Video az asztal vágási síkjának

14. ábra Video az asztal lábának elvágásának folyamata

Ezen erőfeszítéseinknek hála a pályaorientációs nap előtti napon sikeresen bepakoltunk minden szükséges dolgot, és nagy reményekkel vártuk a holnapot. (15. ábra)

Másnap a Szombathelyi Haladás sportcsarnokban egy kis standot felállítva vártuk a látogatókat. (16. ábra)



15. ábra Az asztal szállításának módja

16. ábra Szombathelyen készült csoportkép

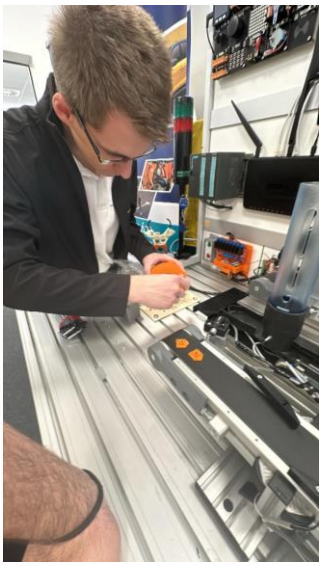
Porondon

A kétnapos esemény során több ízben is feszegettük a határainkat. (17. ábra) Soha nem volt az asztal napi 10 órában, szinte megállás nélkül járatva, ebből adódóan derült fény több ergonómiai és elgondolás béli problémára. Az egyik ilyen az előbb említett RFID-rendszer volt, ami az elhelyezése miatt alacsonyabb személyeknek problémát okozott (a hátfal bal felső sarkában). Ugyanilyen jellegű probléma volt a HMI elhelyezése is, és a PLC-robot kommunikáció megoldásával is adódtak problémák. Ezt később a rendszer komplikáltságára és a Wifi router nem optimális elhelyezésére vezettük vissza, miszerint egyesesetekben interferencia léphetett fel.

Maga az esemény jól sikerült. Sok érdeklődőt sikerült bevonzani. Legutolsó sorban pedig ez volt az első nagyobb léptékű esemény, így az Opelben is legkésőbb ekkor szereztek tudomást rólunk. A későbbiekben pedig a cég által egyre szélesebb kör ismerhette meg a projektünket.

A napos oldal pozitivitása mellett sajnos voltak nagyobb malőrök is. Az esemény során egy rossz programkód-módosítás következtében a robot nekiment az adagolónak, melynek következménye az volt, hogy a biztonsági törőelem a robot aljában eltört, és az 1. nap végén ezért nem tudtuk üzemeltetni az asztalt. (18. ábra)

A 2. nap reggelén Zétény sikeresen újra programozta, így nagyobb gond nélkül folytatni tudtuk az eseményt.



17. ábra Szerelés pillanatképe

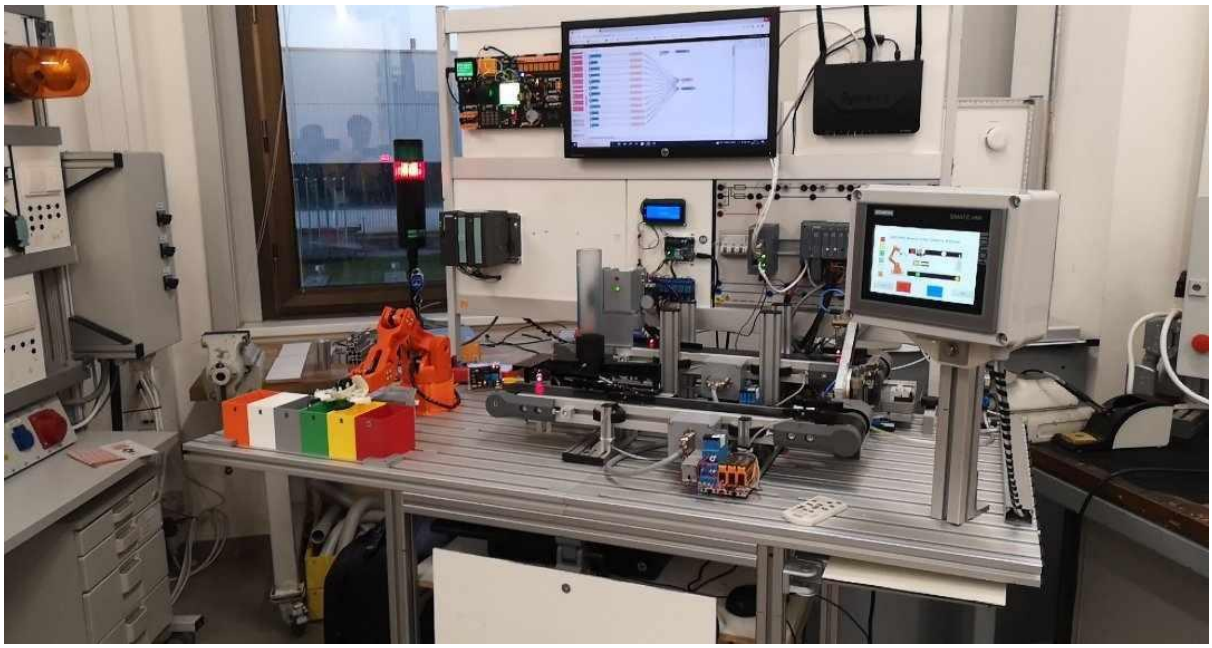
18. ábra Pillanatkép az eseményről

Fejlesztések

Miután visszaérkeztünk, az észrevételek alapján módosításokat hajtottunk végre. Ekkor tettük a robot alá a 3D nyomtatott magasítást, a vezérlő a Arduino integrálásával pedig sikerült kompaktabbá is tenni. Az új megoldás teljes mértékben Node-Red alapú volt. A PLC kimenetet felhasználva attól függően, hogy melyik bit [43] állt logikai egybe, [44] más-más decimális [45] számokká alakítottuk át Node-Red-ben. Ezekre a számértékekre kérdeztünk rá a robot vezérlő programjában. Így csak egy kábel kellett a kommunikációhoz, és ezzel a megoldással a beprogramozható mozdulatok száma végtelen lett.

Programszintű változások is ekkor következtek be. Teljes értékű hibakezelés ekkor valósult meg. A kiválasztott korongok HMI-n való megjelenítése. A felület átdolgozáson esett át, az ergonómiát előtérbe helyezve. A kézi irányítás bolond biztosabbá tétele, így már semmilyen körülmények között sem lehetett kárt tenni benne. Megjelent a többnyelvűség. Előre meghatározott elköszönések közül lehetett választani, ennek segítségével felhasználóbarát módon lehetett akár személy szerinti elköszönést is választani. Például a Vas Vármegyei Szakképzési Centrum Gépipari és Informatikai Szakgimnáziumának Igazgatójától és igazgató helyettesétől név szerint köszönt el az asztal. Volt lehetőség angol, francia és német elköszönésre is.

Az M5 Stack ekkor nyerte el végső formáját, így kikerült a bankkártyás kialakítása, amit leváltott a LED mátrix visszajelző rendszere. A HMI is optimálisabb helyre került, és a kibővült lehetőségeket sokkal többször és egyszerűbben használtuk. A wifi router is új helyet kapott, melynek köszönhetően az interferencia lehetőségét minimálisra csökkentettük. A képen az előbb lefestett változtatások után készült képet láthatunk. (19. ábra)



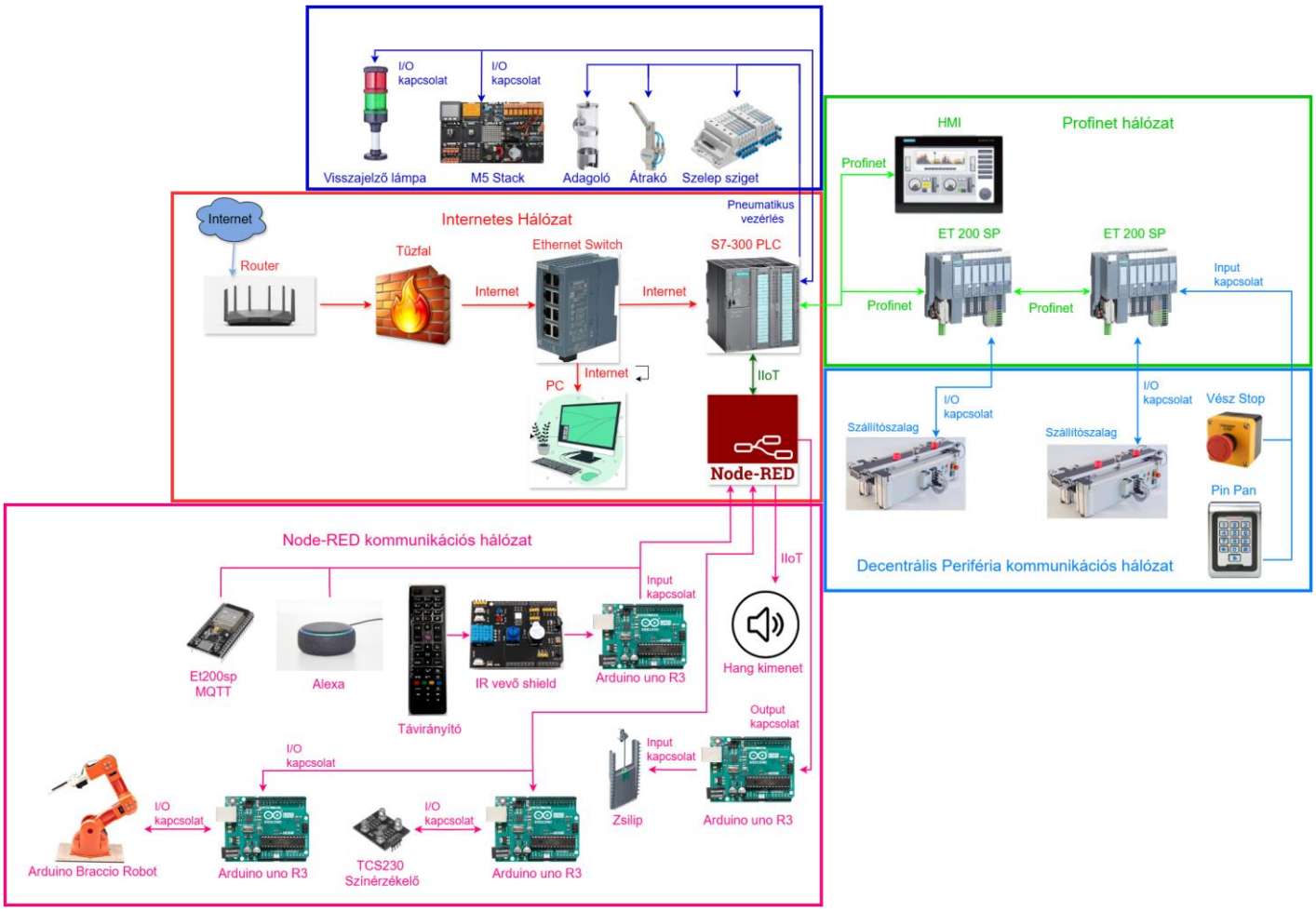
19. ábra Megújult kinézetű Szimulációs Gyártósor

Miután a projektet továbbfejlesztettük, újabb innovációk következtek. Mivel innentől a Tudásközpont vezetésének célja a képzés minél több részének bemutatása volt, ami számunkra is egy remek célnak bizonyult, mindig új kihívások elé állítva minket. Így olyan részletek is felkerültek, mint az Alexa. [46] Vele automatikusan lehetett ciklust indítani és leállítani, a robotot pedig különböző pozíciókba járatni. Ezen kívül volt egy általunk "demó módnak" nevezett programrész is, ami elindította az asztal összes mozgatható alkatrészét a Queen "We Will Rock You" [47] című zenéjére. A szállítószalagok szaggatottan jártak, a zsilip fel-le mozgott, az adagoló ki-be járt, a pneumatikus átrakó fel-le mozgott, és a robot egy táncot lejtett ebben a módban. A zene végeztével minden alapállásba került vissza. További részlet volt az MQTT [48] protokoll használata, amin minden indítás logját [49] tároltuk. A képen a HMI mellett látható projektor távirányítóval, [50] valamint egy Arduino-val, amivel sikeresen megoldottuk a kommunikációt, lehetővé téve, hogy az Alexához hasonlóan több funkció indítása távolról is lehetséges legyen. A biztonság növelése érdekében egy pinpad [51] is felkerült, mellyel az HMI-n történő indítási jogosultságot lehetett kiadni.

PLC program

A 7. Networkben [52] definiálva van a “Start öntartás”. [53] Ez egyfajta engedélyezés az automatikus [54] módra, mindennek, aminek jogosultsága van, illetve a hibajelek is ide futnak ki. Ez indítja el az adagolót, imenek a kimozgása az insert [55] parancsot indítja. Ez a 10. Network, ami a Node-reden keresztül viszi át a jelet. A robot az alsó szalagra helyezi a korongot és késleltetés után el is indul. A szalag végére érve leállítjuk és az ott elhelyezett érzékelő a pneumatikus átrakót indítja el. A szelepszigeten keresztül a kar lehajlik a 12-es network szerint. Vákummal felveszi a darabot és a levegő irányának módosítása után a korongot elhelyezi a felső szalagon. Az ottani érzékelő [56] pedig indítási parancsot ad ki a 15. network alapján. Amikor a korongot elsőre érzékeli a színszenzor akkor az késleltetés után a zsilip lemegy (18, 19). Minden érzékelés szaggatja a szalagot 2.5Hz-s frekvenciával. A zsilip lentlététől számítva 30 azonos színű érzékelésig vár a program (22…28). A kék szín itt egy céges esemény kapcsán került bele a programba. Kép, videó felvétel nem készült róla. Ezután a zsilip alappozícióba vált és a korong a szalag végén megáll ekkor a robotot a megfelelő programkóddal ellátjuk és a korongot a megfelelő helyre kerül. Amikor már nincs az adagolóba korong a Clap [57] aktiválódik (30) és a zene a 31. Clap triger network szerint változik. A 32. network az ütem végén állj-t [58] valósítja meg, míg a 33. a start gomb engedélyezésének a visszajelzésére szolgál. A további networkök a hibakezelést valósítják meg a 47. networkig. Ezután különböző robot pozíciók találhatóak meg, mint például Boot, amelyik pozícióban a robot program töltését lehet megcsinálni. Ezután van a demó mód, ami minden kezelő szervet mozgat és a robotot táncoltatja. Az utolsó network, pedig a összes szétválogatott korongok számszerű értékét számolja ki.

Architektúra



20. ábra A rendszerek kommunikációs hálózatai

A rendszernek két fő csomópontja van az egyik a Pc, amin a Node-Red minden PLC és mikrokontrollerekkel végbemenő kommunikációt lefolytat. A másik maga a PLC, ami fogadja az adatokat és minden utasítás onnan ered. Egy példa folyamat.: A gyártósort a távirányítón keresztül indítjuk el. Ekkor az Arduino-n lévő shield érzékeli és a board feldolgozza az így kapott hat jegyű kódot. Ezt a programmal összehasonlítva, soros Porton keresztül a Node-Redben a megfelelő bitet logikai egyre állítja. Ezt a PLC érzékeli az S7 modulnak köszönhetően még a Node-reden belül és ezt a jelet egy a PLC-s bitté

átkonvertálja. Innentől PLC belül már lehet dolgozni és elindul az automata üzemmód.

1615

Rövid utóélet

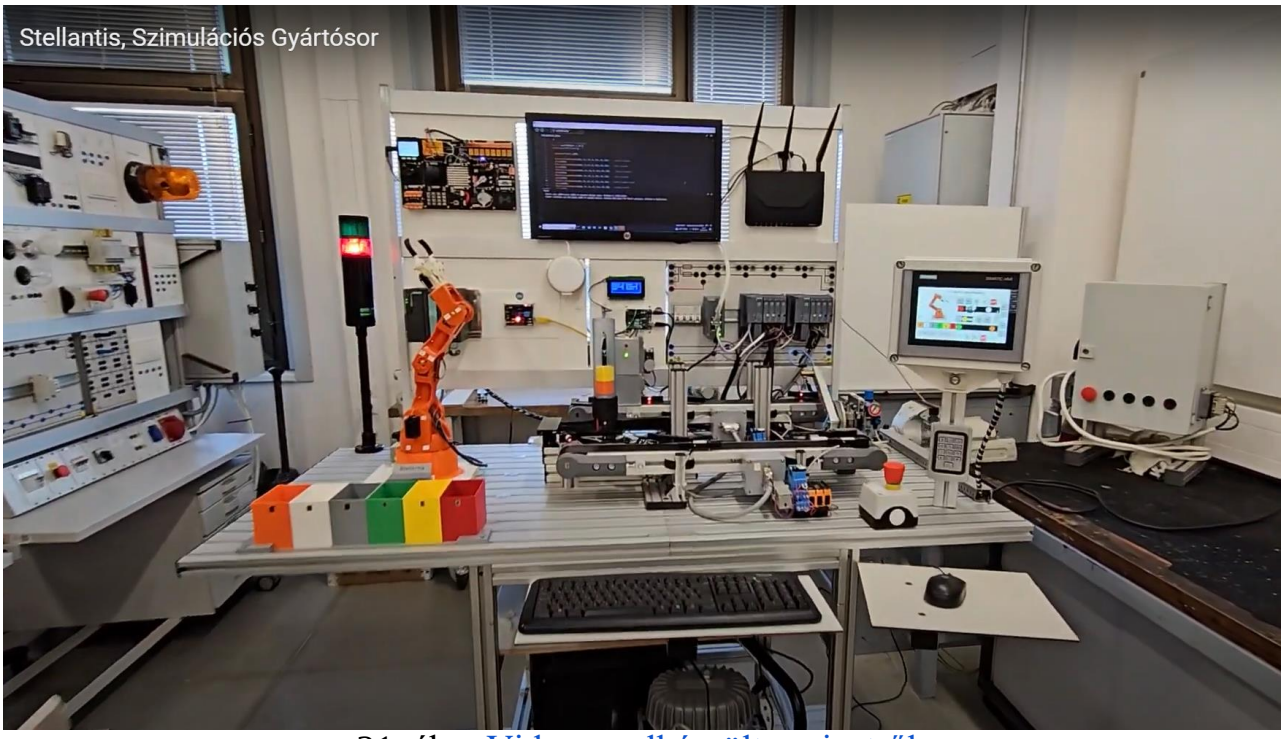
Mindezek után a projekt elérte a végső permutációját, melyen már nem történtek nagy változtatások. A 6 hónapig épített gyártósor mindent tudott, amit megálmodtunk. Minden információ az S7 300-as PLC-be [59] szolgáltatta az adatokat, amelyek mind Laski Ákos keze munkája volt, a robot programozásának kivételével. A PLC a Node-Red rendszeren keresztül kommunikált az eszközökkel, és LAN [60] hálózaton keresztül a decentrális perifériákkal. Az Opel számára ez kivételes lehetőség volt saját képzésének népszerűsítésére, amit készséggel ki is használt. Több tanulócsoport is tiszteletét tette nálunk, és főként az én előadásomban tudhattak meg többet a projektről, valamint arról, hogy milyen lehetőségeik vannak diákszemmel ennél a cégnél. Az Opel nem volt hálátlan, rengeteget köszönhetek nekik, a szakmai életemet hatalmas mértékben lendítették előre. Vendégek között ott volt a Széchenyi István Egyetem e-Mobilitás Központ tudományos vezetője, Dr. Fodor Dénes [61] is, akivel egy jóízű beszélgetés keretében prognosztizálta az egyetemi felvételemet. A legmeghatározóbb előadás pedig az Opel Szentgotthárd teljes igazgatósága előtt zajlott, ahol hatalmas megtiszteltetés keretében mindenki érdeklődve hallgatta az előadást, és talán egy kis újdonságot is tudtam nekik mondani, mutatni.

Személyes utóélet

Közeledett a technikusi évem vége, 2024-et írtunk. Februárban beadtam a jelentkezésemet a Széchenyi István Egyetemre, és májusban két állásinterjú után állásajánlatot kaptam, mint PLC-Specialista. Júniusban a sikeres technikusi vizsgát követően el is kezdtem dolgozni. Majd kaptam a levelet, miszerint az egyetemre csak nappali képzésben kaptam felvételt. Mint később kiderült, a középiskolám hivatalosan nem ad olyan képzést, melyet az egyetem elfogadott volna, és ezért csak gimnazistaként számolták a pontjaimat, ami csak a nappali képzésre biztosított elegendő pontszámot. Emiatt augusztus utolsó hetében felmondtam, és szeptemberben elkezdtem az egyetemi képzést.

Végszó

A bemutatott szimulációs gyártósor életem első, de remélhetőleg nem utolsó nagy volumenű projektje, amely nélkül szakmai felkészültségem és problémamegoldó képességem sem lenne ilyen szintű. A legtöbbet mégsem szakmai oldalon fejlődtem, sokkal inkább a szociális fejlődésem az, amit a legértékesebbnek érzek. Most már nem félek beszélni, előadni, sokkal inkább kiteljesedek mások előtt is. És nem utolsó sorban ennek a projektnek köszönhetően megannyi ajtó kinyílt, amelyek utat biztosítottak rövid, de annál tartalmasabb PLC Specialistaként eltöltött 3 hónapnak. (21. ábra)



21. ábra Video az elkészült projectről

Források:

[1] CNC.hu: TIA Portal V19, https://www.cnc.hu/2023/11/tia-portal-version-19-egyszeru-mozgasvezerles-minden-felhasznalo-szamara/, Elérés: 2025.02.20.

[2] Measure.hu: PLC-programozás módjai, https://www.measure.hu/megoldasaink/celgepgyartas?https://www.measure.hu/megoldasaink/celgepgyartas&gad_source=1&gclid=Cj0KCQiAwtu9BhC8ARIsAI9JHan3zkCopniScuX7bS_pJ8r4ARxQnJzouea9NwsmyoW56--sXMAKO3YaAiI9EALw_wcB, Elérés: 2025.02.20.

[3] Pneumatika Oktatás: Pneumatika, https://www.pneumatika-oktatas.hu/mi-a-pneumatika/, Elérés: 2025.02.20.

[4] Nemes Gáspár Szakközépiskola: Elektropneumatika, https://www.nemesgszi.hu/components/docs/MM-Elektropneumatika.pdf, Elérés: 2025.02.20.

[5] Mevo-Mix: Mikrokontroller, https://www.mevo-mix.hu/mikrovezerlok/mikrovez_okt_honlap.pdf, Elérés: 2025.02.20.

[6] Basiliskus3D: 3D Tervezés és Nyomtatás, https://basiliskus3d.hu/3d-technologiak/, Elérés: 2025.02.20.

[7] NIVE: Hálózatok Létrehozása, https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/6_0909_019_101115.pdf, Elérés: 2025.02.20.

[8] CHH Műszaki Kft.: Szállítószalag, chh.hu/uploads/download/szallitoszalagok_chh_muszaki_kft.pdf, Elérés: 2025.02.20.

[9] Neviatdi Blog: Pneumatikus adagoló, https://neviatdi.blog.hu/2014/01/05/mechanikus_adagolo_mukodese, Elérés: 2025.02.20.

[10] Bürkert: Szelepsziget, https://www.burkert.hu/hu/szerviz-es-tamogatas/tudastar/szoszedet/szelepsziget-1x1-meghatarozasa-kialakitasa-es-elonyei, Elérés: 2025.02.20.

[11] Széchenyi Egyetem: Pneumatikus átrakó, http://www.sze.hu/~jager/Erzekelok_beavatkozok/Tanuland%C3%B3_anyagok/pneumatikai_alapismeretek_festo_kiemelt_40_oldalig.pdf, Elérés: 2025.02.20.

[12] Babosi: Satupad, babosi.hu/femipar/munka.pdf, Elérés: 2025.02.20.

[13] Prefa: Alumínium lap sávos, prefa.hu/fileadmin/user_upload/_HU/EMI_Tuzterjedesi_hatarertek_vizsgalat_2015.pdf, Elérés: 2025.02.20.

[14] Craftbot: Craftbot Plus Pro, help.craftbot.com/craftbot-plus-pro-user-manuals/, Elérés: 2025.02.20.

[15] RS Online: Arduino Braccio, https://docs.rs-online.com/e477/0900766b814da22f.pdf, Elérés: 2025.02.20.

[16] Mérnökkapu: Színérzékelő, https://mernokkapu.hu/hogyan-mukodnek-a-fenyerzekelo-szenzorok/, Elérés: 2025.02.20.

[17] Southern PLCs: S7 programozói szoftver, https://www.southernplcs.com/pdfs/s7.pdf, Elérés: 2025.02.20.

[18] CorpWebStorage: HMI, https://corpwebstorage.blob.core.windows.net/media/28618/hmi.pdf, Elérés: 2025.02.20.

[19] Siemens: TIA Portal V18, assets.new.siemens.com/siemens/assets/api/uuid:618c7fec-fc25-4277-9b5b-393516b6cd77/TIA-V18-2023-web.pdf, Elérés: 2025.02.20.

[20] KK.gov.hu: Szombathelyi Pályaorientációs nap, https://kk.gov.hu/download/3/22/03000/Szerz%C5%91d%C3%A9s_T%C3%A1jol%C3%B3nap.pdf, Elérés: 2025.02.20.

[21] Műszeroldal: Kompresszor, muszeroldal.hu/measurenotes/kompresszor.pdf, Elérés: 2025.02.20.

[22] Unidel: Node-RED, unidel.edu.ng/focelibrary/books/Practical%20Node-RED%20Programming%20Learn%20powerful%20visual%20programming%20techniques%20and%20best%20practices%20for%20the%20web%20and%20IoT%20by%20Taiji%20Hagino%20(z-lib.org).pdf, Elérés: 2025.02.21.

[23] Széchenyi Egyetem: Számítógép architektúra, http://rs1.sze.hu/~horzsol/Architekt%FAra/Szamitogepek_architekturaja.pdf, Elérés: 2025.02.21.

[24] Siemens: Decentrális Periféria, support.industry.siemens.com/cs/document/109816723/simatic-decentrális-periféria-et200sp-ha-terméktájékoztató-az-et200sp-ha-f-io-moduljaihoz-(többnyelvű)?dti=0&dl=hu&lc=en-EE, Elérés: 2025.02.21.

[25] Széchenyi Egyetem: Wi-Fi, tilb.sze.hu/tilb/targyak/NGB_TA027_1/prot_wlan2.pdf, Elérés: 2025.02.21.

[26] Synology: DSM PDF Viewer, kb.synology.com/en-au/DSM/help/PDFViewer/PDFViewer?version=7, Elérés: 2025.02.21.

[27] Heath: Switch (Könyv), ia601501.us.archive.org/35/items/Heath2010SwitchHowToChangeThingsWhenChangeIsHard/%5BHeath%2C%202010%5D%20Switch%20-%20How%20to%20Change%20Things%20When%20Change%20is%20Hard.pdf, Elérés: 2025.02.21.

[28] Makita: Sarokcsiszoló, tomido.hu/kepek/sarokcsiszolo/makita_ga_9020//pdf/hasznalati_utasitas_ga9020.pdf, Elérés: 2025.02.21.

[29] Arduino: Arduino Uno, https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf, Elérés: 2025.02.21.

[30] PDF2Go: RGB, https://www.pdf2go.com/dictionary/rgb, Elérés: 2025.02.21.

[31] Interex-Waga: Zsiliprendszer, https://interex-waga.hu/storage/manuals/ajlnWMYpq8Wx/ERI%20zsilip.pdf, Elérés: 2025.02.21.

[32] Siemens: PLC Clock Memory, https://docs.tia.siemens.cloud/r/simatic_s7_1200_manual_collection_enus_20/plc-concepts/execution-of-the-user-program/cpu-memory/system-and-clock-memory, Elérés: 2025.02.21.

[33] DFRobot: Arduino Shield, https://image.dfrobot.com/image/data/Common/Arduino%20Shield%20Manual.pdf, Elérés: 2025.02.21.

[34] Phoenix Contact: Szilárdtest relé, https://www.phoenixcontact.com/hu-hu/termekek/egyedi-felvezetorelek-opt-24dc230ac-1-2967950?type=pdf, Elérés: 2025.02.21.

[35] M5Stack: M5 Stack tanuló board, https://docs.m5stack.com/en/app/demo-board, Elérés: 2025.02.21.

[36] Illumina: RFID olvasó, https://support.illumina.com/content/dam/illumina-support/documents/documentation/system_documentation/translations/rfid-reader-compliance-guide-1000000002699-hun.pdf, Elérés: 2025.02.21.

[37] MNB: Bankkártya használat, https://www.mnb.hu/letoltes/12-a-bankkartya-hasznalata.pdf, Elérés: 2025.02.21.

[38] Adafruit: LED mátrix, https://cdn-learn.adafruit.com/downloads/pdf/32x16-32x32-rgb-led-matrix.pdf, Elérés: 2025.02.21.

[39] Rendőrség: Mikrobusz műszaki leírás, https://www.police.hu/sites/default/files/dokumentacio_3._kotet_muszaki_leiras_1._resz_final.pdf, Elérés: 2025.02.21.

[40] Elektroprofi: Kábel, https://www.elektroprofi.hu/dynamic/Katalogusok/01__Kabel.pdf, Elérés: 2025.02.21.

[41] ELKO EP: Moduláris elektronikai eszközök, ELKO EP, 2018, https://www.mentavill.hu/files/AMPER/catalog/elko_modularis_elektronikai_eszkozok_2018.pdf, 2025.02.21.

[42] Lexiq: Horizontális, Lexiq, https://lexiq.hu/horizontalis#google_vignette, 2025.02.21.

[43] Gandon, F.: Bit/Byte, Carnegie Mellon University, 1999, https://www.cs.cmu.edu/~fgandon/documents/lecture/uk1999/binary/HandOut.pdf, 2025.02.21.

[44] Moodle: Logikai Egy, Moodle, https://moodle.jrobi.hu/Elmelet/Logikai_fuggvenyek_v2.pdf, 2025.02.21.

[45] Székely Gy.: Decimális számrendszerek, https://gy-szekely.cms.intezmeny.edir.hu/uploads/Szamrendszerek_7f7df759f9.pdf, 2025.02.21.

[46] Amazon Web Services: Alexa Privacy and Data Handling Overview, AWS, https://d1.awsstatic.com/product-marketing/A4B/White%20Paper%20-%20Alexa%20Privacy%20and%20Data%20Handling%20Overview.pdf, 2025.02.21.

[47] Tune Into English: Queen - We Will Rock You, Tune Into English, https://www.tuneintoenglish.com/wewillrockyou.pdf, 2025.02.21.

[48] CSJMU: MQTT, CSJMU, https://gyansanchay.csjmu.ac.in/wp-content/uploads/2022/08/MQTT.pdf, 2025.02.21.

[49] ICAP: Logaritmus táblázat, ICAP, https://icap.org.pk/files/per/students/exam/notices/log-table.pdf, 2025.02.21.

[50] BenQ: Projektor felhasználói kézikönyv, BenQ, https://esupportdownload.benq.com/esupport/Projector/UserManual/Projector_um_User%20Manual_20160726_195009BenQ%20MH750%20UM_HG.pdf, 2025.02.21.

[51] MagTek: Pin Pad dokumentáció, MagTek, https://www.magtek.com/content/documentationfiles/d99875462.pdf, 2025.02.21.

[52] Hybrid PLC: Network dokumentáció, Hybrid PLC, https://hybridplc.org/wp-content/uploads/chap16_S.pdf, 2025.02.21.

[53] Nemes Gábor: Öntartás, https://nemesgszi.hu/components/docs/iSmart_Konyv2.pdf, 2025.02.21.

[54] Colcombet, T., Daviaud, L., Zuleger, F.: Automata mód, IRIF, 2017, https://www.irif.fr/~colcombe/Publications/FCT17-colcombet-daviaud-zuleger.pdf, 2025.02.21.

[55] Angol-Magyar Szótár: Insert, https://angol-magyar-szotar.hu/insert.html#google_vignette, 2025.02.21.

[56] Szénásy G.: Érzékelők és aktuátorok, Széchenyi István Egyetem, https://www.sze.hu/~szenasy/Szenzorok%20%E9s%20aktu%E1torok/FESTO-Szenzorika.pdf, 2025.02.21.

[57] Angol-Magyar Szótár: Clap, https://angol-magyar-szotar.hu/clap.html, 2025.02.21.

[58] Siemens: Ütem végén állj, Siemens, https://cache.industry.siemens.com/dl/files/189/25034189/att_108735/v1/PGA_0310_hu_hu-HU.pdf, 2025.02.21.

[59] Siemens: S7-300 PLC dokumentáció, Siemens, https://cache.industry.siemens.com/dl/files/415/15390415/att_41918/v1/S7-300_IHB_e.pdf, 2025.02.21.

[60] AgendaAge: LAN hálózatok kialakítása, AgendaAge, https://www.agendaage.hu/tudasbazis/rezhalozat/helyi-lan-halozatok-kialakitasa, 2025.02.21.

[61] Széchenyi István Egyetem: Dr. Fodor Dénes - e-Mobilitás Központ tudományos vezetője, https://jkk-web.sze.hu/elerhetosegek/dr-fodor-denes/, 2025.02.21.

2.61. Az Okosotthonok jövője: automatizált intelligens rendszerek, felhőalapú támogatás és energiahatékonyság

Az Okosotthonok jövője: automatizált intelligens rendszerek, felhőalapú támogatás és energiahatékonyság

Féléves feladat Ipar 4.0 technológiák tantárgyból

Németh Gergő Barnabás, [redacted],
nemethgergobarnabas@gmail.com

Mérnökinformatikus Bsc.

Készítés dátuma: 2025.05.14.

Tartalom

Bevezetés 4

Vezető okosotthon-gyártók és megoldásaik: Google home, Amazon Alexa és Samsung SmartThings 6

Google home: 6

Amazon Alexa: 7

Samsung SmartThings: 7

Felhőalapú támogatással működő vezeték nélküli IoT-eszközök (okos termosztátok, okos világítás, okos konnektor, okos víz és gázérzékelők) 8

Távoli és Zónás vezérlés: 9

Nest Learning Thermostat: 10

Funkcionalitás és automatizálás 10

A Nest alkalmazás előnyei: 11

- Felhasználóbarát: 11
- Kiváló integrációs lehetőségek: 11
- Biztonságos adatkezelés: 11

Automatizált energiamenedzsment (IoT-alapú energiamenedzsment) 12

Mi az IoT- alapú energiamenedszment? 12

Edge-computing eszközök, okosmegoldások adatok helyben tárolásával 14

Gyorsabb reakcióidő 14

Megnövelt megbízhatóság: 14

Jobb adatvédelem: 14

Csökkentett sávszélesség-használat: 14

Adatvédelmi szabályozásoknak való megfelelés: 14

Skálázhatóság és rugalmasság: 14

Egy konkrét példa az edge-computingra: 15

Offline eseménytárolás (bizonyos ideig): 15

Trhead protokol(alkalmazása, integrációja) 16

Története: 16

Fogalma: 16

A Thread hálózatoknak négyféle eszköz létezik: 16

Hálózati vezérlő (Commissioner/Leader): 16

Router eszközök (Mesh Extender Device): 16

Átjáró eszközök (Borer Router): 16

Végponti eszközök (Battery Operated Device): 16
Zigbee: 17
A Zigbee hálózatok háromféle topológia alapján építhetők fel: 18
- Csillagtopológia (Star Topology): 18
- Fa topológia (Tree Topology): 18
- Mesh hálózat (Mesh Network): 18

Z-Wawe: 19
Home Assistant: 19
Loxone: 19
Loxone mini server: 20
A Loxone 3 különböző Miniserver modelleket kínál:[15] 20
- Miniserver (Standard): 20
- Miniserver Compact 20
- Miniserver Go: 20

Air Base Extension: 20
Tree Extension 21
Loxone biztonsági eszközei: 21
Touch Pure Tree 21
Weather Station: 21
Motion Sensor Tree: 22
Loxone Audioserver: 22
Smoke Detector: 23
Smart Ups bemutatása: 23
Sima Ups tipusok: 24
Standby UPS 24
Line-Interactive Ups: 24
Online/ Double-Conversion Ups 25
PIR (Passive Infrared Sensor – Passzív Infravörös Érzékelő) 25
Működési elv: 26
- Érzékelőelem: 26
- Optikai rendszer 26

Nyomásérzékelők okosotthonokban: 27
WPA3: 28
VPN: 29
Összegzés 31
Források: 33

Bevezetés

A mai világágban egyre jobban elterjednek azok a technológiák, elektronikai rendszerek, amelyek teljesen vagy nagy részben önállóan működnek. Ezek az élet bármelyik részén megfigyelhetőek. Ebben az esszében én az ilyen technológiákat fogom bemutatni az okosotthonok területén. Az okosotthonok olyan lakóterek, amik automatizáltak, intelligens rendszerekkel vannak felszerelve. Egy olyan átfogó kép alkotása a célom, amely bemutatja a jövő otthonait és az okosotthonokban elterjedt intelligens rendszereket. Ezek a technológiák először Amerikában és Kínában terjedtek el, már ott is jól látszott, hogy az ilyen elektronikai rendszerekkel olyan jövőt lehet létrehozni, amely egyszerre költséghatékony és az ökoszisztémát helyezi a középpontba. Az ilyen rendszereket gyakran felhőalapú szolgáltatások támogatják. Ezek a rendszerek nem csak adatokat gyűjtenek és tárolnak, hanem ezeket elemzik. Gyakran képesek előre jelezni az energiaigényt, felismerni a szokásokat és proaktívan reagálni a környezeti változásokra. Az energiahatékonyság nem csupán gazdasági, hanem környezeti szempontból is kiemelkedő fontosságú. Az okosotthonok képesek jelentős mértékben csökkenteni a felesleges energiahasználatot, elősegítve ezzel a fenntartható fejlődést.

Az okosotthonok lényege, hogy a különböző rendszerek és eszközök összekapcsolódnak, így egy központi vezérlőrendszeren keresztül irányíthatóak lesznek. Ez a központi rendszer lehet egy okostelefon, egy tablet, vagy egy dedikált érintőképernyős vezérlőpanel. A kommunikáció általában vezeték nélküli technológiákkal, például Wi-Fi-vel, Zigbee-vel vagy Z-Wave-vel történik. Például a világítás, termosztátok, légkondicionáló berendezések kezelése Az ilyen lakásokban egyre inkább elterjedt a mesterséges intelligencia is, ami az emberek szokásait figyeli meg, majd úgy állítja be az elektronikai eszközöket, hogy a leghatékonyabban működjenek a szokások szerint.

A mindennapokban egyre elterjedtebbé válnak az olyan intelligens eszközök, mint a hangvezérlésre alkalmas digitális asszisztensek (például a Google Nest vagy az Amazon Echo). Emellett gyakori az okostermosztátok, automatikusan szabályozható világítási rendszerek, valamint a programozható öntözőrendszerek és biztonságot növelő okoszárak használata is. Ezek a technológiák nemcsak kényelmesebbé teszik a lakók életét, hanem jelentős energiamegtakarítást is lehetővé tesznek.
Az okosotthonok egyik fő vonzerője, hogy képesek leegyszerűsíteni a mindennapi teendőket,

így több idő marad a pihenésre vagy más fontos tevékenységekre. A rendszeresen figyelt és optimalizált energiahasználat révén pedig jelentősen csökkenhetnek a havi kiadások. A korszerű biztonságtechnikai megoldások révén nő az otthon védelme, ráadásul egy modern, intelligens rendszerrel felszerelt ingatlan piaci értéke növelheti az ingatlannak az árát.

Az előnyök mellett nem szabad megfeletkezni a hátrányokról sem. Az okosotthonok egyik fő hátránya a magas kezdeti beruházási költség. Az eszközök és rendszerek gyakran nem kompatibilisek egymással, ami bonyolítja a telepítést és a működtetést, de ezt ki lehet küszöbölni egy jól megtervezett struktúra használatával. Problémát jelenthet, ha csak olyan eszközöket szerelnek fel egy ilyen okosotthonba, amelyek interneten keresztül működnek, ezért érdemes olyan eszközöket választani, amelyek offline módban is megfelelően működnek vagy akár Bluetooth/ Zigbee protokollon keresztül.

A jövőben az okosotthonok fejlődése tovább gyorsulhat a mesterséges intelligencia és az IoT (Internet of Things) technológiák fejlődésével. Várható, hogy egyre több eszköz lesz képes együttműködni, a rendszerek még inkább személyre szabottak és önállóbbak lesznek. Emellett olyan fejlesztések is megjelenhetnek, amelyek még jobban támogatják a fenntartható életmódot, például okos vízgazdálkodási megoldások.

Az okosotthonok tehát nem csupán egy kényelmi eszközökkel felszerelt lakóteret jelentenek, hanem egy olyan komplex rendszert, amely képes alkalmazkodni a lakók igényeihez, növelni az energiahatékonyságot, és hozzájárulni a fenntartható fejlődéshez. A technológia fejlődésével pedig egyre inkább az életünk szerves részévé válnak majd.

Vezető okosotthon-gyártók és megoldásaik: Google home, Amazon Alexa és Samsung SmartThings

Az okosotthon-technológia rohamos fejlődése révén egyre több gyártó kínál komplex és intelligens megoldásokat a lakások automatizálására. A piacot néhány meghatározó szereplő uralja, amelyek termékei és szolgáltatásai világszerte elterjedtek, és kulcsszerepet játszanak abban, hogyan formálódik a jövő otthona. A legismertebb és legmegbízhatóbb gyártók közé tartozik a Google Nest, az Amazon Alexa és a Samsung SmartThings, amelyek mind különféle területeken kínálnak fejlett, egymással is kompatibilis eszközöket.

Google home:

A Google Home egy intelligens okosotthon-vezérlő berendezés, amely az okosotthon központi vezérlőegységeként működik, és a Google Asszisztens segítségével hangutasításokra reagál, minél többet használjuk a virtuális asszisztenst, annál jobban alkalmazkodik a szokásainkhoz.[1] A beépített mesterséges intelligencia révén a felhasználók kérdéseket tehetnek fel, kereséseket fogalmazhatnak meg, zenét játszhatnak le. A rendszerhez kapcsolt kompatibilis okoseszközöket – például világítást, termosztátot, redőnyöket – szintén vezérelhetjük vele. Mindez történhet akár hangutasításokkal, akár okostelefonos alkalmazáson keresztül, távoli eléréssel is. Ennek a rendszernek a használata nagyon egyszerű mivel elég kimondani az „Ok Google” aktiválókifejezést, és a készülék azonnal készen áll a válaszadásra vagy a feladatok végrehajtására. A Google Home folyamatosan fejlődik, egyre pontosabban alkalmazkodik a felhasználó igényeihez. Az eszköz nemcsak kényelmet, hanem hatékonyabb otthoni működést is kínál, miközben modern és intelligens megoldást nyújt a mindennapi élethez. A Google home termékei könnyedén beilleszthetők bármely otthoni környezetbe, mivel letisztult, minimalista dizájnjuknak köszönhetően jól illeszkednek a modern lakberendezési stílusokhoz. Ez technológia nagy támogatással rendelkezik ezért, rendkívül sok eszközt tudunk összekapcsolni vele. Nagy előnyt jelent a Google home számára, hogy a Google integrálva van és ezáltal az összes szoftveres szolgáltatás elérhető rajta, mint például a Gmail, YouTube vagy akár a naptárfunkció is.

Amazon Alexa:

Az Amazon Alexa egy intelligens virtuális asszisztens, amely az Echo hangszórócsaládon keresztül nyújt hozzáférést az okosotthon-funkciókhoz. Az Alexa képes zenelejátszásra, információszolgáltatásra interneten való keresésre, valamint az eszköz irányítható hangvezérléssel is. Az Amazon egyik legnagyobb előnye a versenytársaival szemben, hogy rendkívül széles eszköztámogatással rendelkezik – szinte bármilyen okoseszköz-gyártó termékeit képes integrálni az Alexa rendszerébe. Ez azt jelenti, hogy a felhasználók sokkal nagyobb választékból válogathatnak eszközöket (világítás, biztonsági kamerák, termosztátok, konnektorok stb.), amelyeket könnyedén összekapcsolhatnak az Amazon Echo eszközeikkel. Ez a nyitottság és kompatibilitás különösen vonzóvá teszi az Amazon okosotthon-megoldásait. Az Amazon nemrégiben bemutatta az Alexa+ szolgáltatást, amely fejlett mesterséges intelligenciával bővíti az Alexa képességeit, lehetővé téve a természetesebb beszélgetéseket és a személyre szabottabb élményt.[2]

Samsung SmartThings:

A Samsung SmartThings egy okosotthon platform, amely lehetővé teszi a felhasználók számára, hogy intelligens eszközeiket egyetlen alkalmazáson keresztül vezéreljék és automatizálják.[3] A rendszer támogatja a Zigbee, Z-Wave és Wi-Fi protokollokat, így számos különböző gyártó termékével kompatibilis, a világítástól a zárakon át a termosztátokig. Fontos megjegyezni hogy a Zigbee és a Z-Wawe nem tud kommunikálni egymással ha csak Zigbbe chip van a termékben, de a Z-Wawe nincs akkor, ez fordítva is igaz. A SmartThings segítségével egyéni automatizációkat és rutinokat hozhatunk létre, amelyek a nap bizonyos szakaszaihoz, eseményekhez vagy akár a felhasználó tartózkodási helyéhez igazodnak.

A platform emellett hangvezérlést is kínál, mint például a Google Assistant és Amazon Alexánál is megfigyelhetjük. A SmartThings ökoszisztémája folyamatosan bővül, új eszközökkel és funkciókkal gazdagodva. A rendszer központi egysége a SmartThings Hub, amely összeköti az okoseszközöket és biztosítja a stabil kommunikációt. A felhasználók értesítéseket kaphatnak az otthonukban történő eseményekről, és távolról is ellenőrizhetik eszközeiket a mobilalkalmazás segítségével.

Felhőalapú támogatással működő vezeték nélküli IoT-eszközök (okos termosztátok, okos világítás, okos konnektor, okos víz és gázérzékelők)

A felhőalapú támogatással működő vezeték nélküli IoT-eszközök napjaink digitális környezetének meghatározó elemei, különösen az okos otthonok és az ipari automatizálási rendszerek területén. Az IoT (Internet of Things – dolgok internete) lehetővé teszi, hogy különféle eszközök – például okos termosztátok, világítótestek, konnektorok, valamint víz- és gázérzékelők – internetkapcsolat segítségével adatokat gyűjtsenek, továbbítsanak, és távolról vezérelhetők legyenek.

Ezen eszközök központi eleme a felhőszolgáltatás, amely biztosítja az adatkommunikációt, tárolást, feldolgozást és elemzést. A felhőalapú rendszer előnye, hogy a felhasználók bárhonnan, bármikor hozzáférhetnek eszközeikhez egy okostelefonos alkalmazáson vagy webes felületen keresztül. Ezáltal lehetőség nyílik az energiafogyasztás optimalizálására, biztonsági riasztások fogadására, vagy éppen a háztartási gépek működésének automatizálására.

Az egyik legfontosabb előnye az ilyen rendszereknek a valós idejű adatfeldolgozás, amely lehetővé teszi az azonnali reagálást különböző eseményekre – például szivárgás, túlmelegedés vagy távollét esetén.[4] Ez különösen fontos biztonságtechnikai szempontból, hiszen a rendszer akár automatikusan is beavatkozhat, például elzárhatja a vízvezetéket vagy kikapcsolhat egy veszélyesnek érzékelt eszközt. Még néhány példa: a termosztát alkalmazkodik az időjáráshoz, vagy a világítás automatikusan szabályozódik a napszak és mozgás alapján.

Az okos termosztátok nemcsak manuálisan szabályozhatók, hanem tanuló algoritmusok révén képesek alkalmazkodni a felhasználói szokásokhoz/igényekhez, ezzel energiát és költséget takarítva meg. Az okosvilágítás lehetővé teszi a fényerő és színhőmérséklet távoli szabályozását, vagy akár időzített be- és kikapcsolást, még azt is lehetővé teszik, ha valamikor elfelejtettük lekapcsolni a lámpát a lakásban, akkor azt távolról is le lehet kapcsolni. Az okos konnektorokkal nyomon követhető a csatlakoztatott eszközök energiafogyasztása, és automatikusan ki is kapcsolhatók, ha nincs rájuk szükség. A víz- és gázérzékelők pedig biztonsági szempontból létfontosságúak, mivel képesek azonnal riasztani szivárgás vagy túlfolyás esetén, sőt, automatikus elzáró rendszerekkel is összekapcsolhatók.

Az ilyen rendszerek nagy előnye, hogy könnyen bővíthetők és személyre szabhatók. A felhasználók új eszközöket adhatnak hozzá a rendszerhez anélkül, hogy komoly technikai ismeretekkel rendelkeznének. A modern IoT-eszközök sokszor plug-and-play módon működnek, vagyis a hálózatra csatlakoztatva automatikusan felismerhetők és konfigurálhatók.

Gazdasági szempontból is egyre vonzóbbak ezek a megoldások. A piacon elérhető eszközök ára folyamatosan csökken, miközben a funkcionalitásuk nő. A beruházás gyorsan megtérülhet, különösen olyan háztartásokban vagy vállalkozásokban, ahol magas az energiafogyasztás vagy fontos a távoli felügyelet.

A felhőalapú IoT-rendszerek biztonságát is folyamatosan fejlesztik. Az eszközök és platformok titkosított adatátvitel és kétfaktoros hitelesítés révén védik a felhasználói adatokat, minimalizálva a hackerek ártó hatásait. A helyi adatkezelési szabályozások, mint a GDPR, is egyre nagyobb figyelmet kapnak, így biztosítva a felhasználók adatainak védelmét.

A vezeték nélküli technológiák, mint például a *Wi-Fi, Zigbee vagy Z-Wave*, lehetővé teszik ezeknek az eszközöknek a gyors telepítését és könnyű integrálását a már meglévő rendszerekbe. Emellett a felhőalapú platformok gyakran biztosítanak integrációs lehetőséget különböző digitális asszisztensekkel (pl. Amazon Alexa, Google Assistant), amelyek segítségével a hangvezérlés is megvalósítható.

A felhőalapú rendszer további előnye az automatikus frissítés és karbantartás lehetősége. A gyártók távolról tudnak szoftverfrissítéseket küldeni az eszközökre, ezáltal javíthatóak a hibák, növelhető a biztonság és új funkciók is bevezethetők. Ez meghosszabbítja az eszközök élettartamát, és csökkenti a felhasználók karbantartási terheit.

Távoli és Zónás vezérlés:

A **távoli vezérlés** lehetőséget ad a felhasználóknak, hogy bárhonnan, bármikor irányítsák okosotthonuk rendszereit. Ez internetkapcsolat segítségével történik, és egy okostelefonos alkalmazás vagy webes felület segítségével érhető el. Ennek köszönhetően a felhasználóknak nem szükséges a házban tartózkodniuk ahhoz, hogy módosítsák az otthonuk működését. Például, ha egy felhasználó távol van otthonról, de szeretné, hogy a ház fűtése vagy hűtése elinduljon, mire hazaér, megfelelő hőmérséklet fogadja, akkor az okos termosztátot távolról is beállíthatja.[5]

A **zónás vezérlés** azt jelenti, hogy az okosotthon rendszerek képesek az egyes helyiségeket vagy zónákat külön-külön kezelni, függetlenül egymástól. Ez különösen hasznos, ha a ház különböző részei más-más módon igényelnek hőmérsékletet, világítást vagy egyéb beállításokat. A zónás vezérlés optimalizálja az energiafelhasználást és segít csökkenteni a felesleges költségeket.[6]

Nest Learning Thermostat:

A Nest Learning Thermostat az egyik legismertebb okos termosztát, amely az otthoni fűtés és hűtés rendszerek forradalmasítását célozza meg, és az egyik leginnovatívabb eszköz a piacon. A Google által kifejlesztett eszköz automatikusan tanulja meg a felhasználók napi rutinját, és képes alkalmazkodni az egyéni igényekhez, így optimalizálva az energiafelhasználást és maximalizálva a kényelmet.

Funkcionalitás és automatizálás

A Nest Learning Thermostat legnagyobb előnye az intelligens tanulás, valamint az energiatakarékosság. Nest rendszer képes akár 20-30%-os energia-megtakarítást is biztosítani a hagyományos termosztátokhoz képest. Az eszköz képes megfigyelni, hogy a felhasználó mikor tartózkodik otthon, mikor van távollétben, és ezen információk alapján automatikusan beállítja a megfelelő hőmérsékletet. Például, ha a felhasználó reggel rendszeresen felfűti a házat, a termosztát tanulni fog belőle, és a következő alkalommal már automatikusan elvégzi ezt anélkül, hogy manuálisan be kellene állítani.

A Nest termosztát a környezeti változásokra is reagál, és automatikusan módosítja a hőmérsékletet, figyelembe véve az időjárást vagy az otthoni környezet egyéb tényezőit. Ha például hidegebb napok jönnek, a termosztát előre beállíthatja a szükséges fűtést, míg melegebb időben csökkentheti a hőmérsékletet. Ezen kívül a **geofencing**[1] technológia segítségével a termosztát felismeri, ha a felhasználó elhagyja az otthont, és automatikusan csökkenti a fűtést, hogy energiát takarítson meg.

[1] A geofencing egy olyan technológia, amely lehetővé teszi, hogy egy eszközt vagy alkalmazást fizikai területhez (geográfiai zónához) kapcsoljunk.

Ez az eszköz is lehetővé teszi a zónás vezérlést is a felhasználók számára, valamint a távoli vezérlést egyaránt. A távoli vezérlés a Nest applikáción keresztül történik. Ez az alkalmazás a Google által lett kifejlesztve, amin keresztül elérhetjük a Nest eszközeit (Nest Thermostat,Nest Cam, Nest Hello). Az alkalmazás egy központi vezérlőfelületet biztosít, amely lehetővé teszi a felhasználók számára, hogy kezeljék és monitorozzák a különböző okos eszközöket, optimalizálják az energiafelhasználást, és biztosítsák otthonuk biztonságát.[7]

A Nest alkalmazás előnyei:

- ***Felhasználóbarát:*** Az alkalmazás könnyen kezelhető, intuitív és egyszerűen beállítható.
- ***Kiváló integrációs lehetőségek:*** A Nest alkalmazás jól integrálható más okos eszközökkel és digitális asszisztensekkel (pl. Google Assistant, Amazon Alexa).
- ***Biztonságos adatkezelés:*** A Google, mint nagy techvállalat, magas szintű adatvédelmet biztosít a GDPR[2] figyelemvételével, így a felhasználók biztonságban érzik adataikat.

[2] General Data Protection Regulation kezdőbetűiből képzett mozaikszó, magyarul általános adatvédelmi rendelet.

Automatizált energiamenedzsment (IoT-alapú energiamenedzsment)

Az automatizált energiamenedzsment (IoT-alapú energiamenedzsment) egy korszerű megközelítés az energiafogyasztás optimalizálására, amely az Internet of Things (IoT) technológiákra épül.

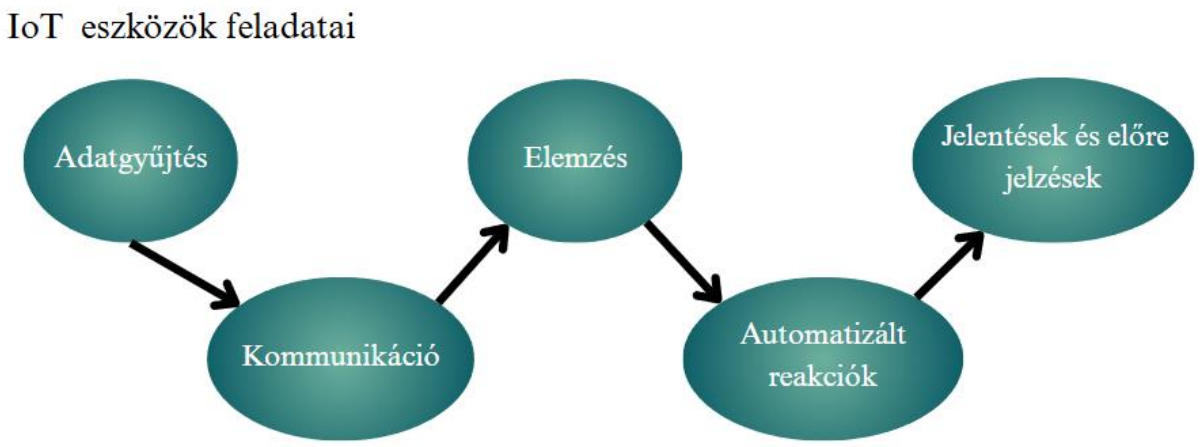
Mi az IoT- alapú energiamenedszment?

Az IoT-alapú energiamenedzsment rendszerek szenzorokat, okoseszközöket, adatgyűjtő modulokat és felhőalapú szoftvereket használnak annak érdekében, hogy valós időben monitorozzák, elemezzék és szabályozzák az energiafelhasználást.

Az „automatizált" kifejezés arra utal, hogy a rendszer képes emberi beavatkozás nélkül döntéseket hozni, például:

- lekapcsolja a feleslegesen működő berendezéseket,
- optimalizálja a fűtést, hűtést és világítást,
- előrejelzéseket készít az energiaigényekről.

Az IoT-alapú energiamenedzsment számos előnnyel jár mind háztartási, mind ipari környezetben. Lehetővé teszi az energiafogyasztás valós idejű nyomon követését és optimalizálását, így csökkenthető a pazarlás. Az automatizált rendszerek – például mozgásérzékelős világítás vagy intelligens termosztátok – képesek önállóan szabályozni a fogyasztást. Ez jelentős költségmegtakarítást eredményez, miközben növeli az energiahatékonyságot. Az IoT-eszközök által gyűjtött adatok részletes elemzést és átláthatóságot biztosítanak, így könnyen azonosíthatók a fejlesztendő területek. Emellett a rendszer segít a megújuló energiaforrások hatékonyabb integrálásában is. Az előrejelző algoritmusoknak köszönhetően a jövőbeni energiaigények is jobban tervezhetők. A karbantartás is proaktívvá válik, mivel a szenzorok időben jelezhetik a berendezések hibáit. Mindez nemcsak költséghatékonyabb működést eredményez, hanem hozzájárul a fenntarthatóbb és környezetbarát energiafelhasználáshoz is.[8]



1. (ábra) IoT eszközök feladatai, saját szerkesztésű ábra

Számos területen alkalmazzák az IoT-energiamenedszmentet, ilyen területek például: irodaházak, okosotthonok, mezőgazdaság, valamint az ipari létesítmények.

Edge-computing eszközök, okosmegoldások adatok helyben tárolásával

Az okosotthonok rohamos terjedésével egyre nagyobb hangsúly helyeződik az adatvédelemre és a megbízhatóságra. Az edge-computing eszközök és az adatok helyben tárolására épülő okosmegoldások kulcsszerepet játszanak ezeknek az igényeknek a kielégítésében.

Az edge-computing lényege, hogy az adatfeldolgozás és -tárolás a hálózat peremén, azaz az okoseszközök közelében történik, nem pedig egy távoli központi szerveren vagy a felhőben. Ez számos előnnyel járhat az okosotthonok szempontjából.[9]

***Gyorsabb reakcióidő*:** Mivel az adatok helyben kerülnek feldolgozásra, a rendszer sokkal gyorsabban reagál az eseményekre. Például, egy okos biztonsági kamera azonnal riasztást küldhet, ha mozgást érzékel anélkül, hogy az adatokat először egy távoli szerverre kellene továbbítania.

Megnövelt megbízhatóság: A helyi adattárolás csökkenti az internetkapcsolattól való függőséget. Ha az internetkapcsolat megszakad, az okosotthon alapvető funkciói, mint például a világítás vagy a fűtés vezérlése, különböző eszközök vezérlése továbbra is működhetnek.

Jobb adatvédelem: Az adatok helyben tárolása csökkenti a személyes adatok kiszolgáltatottságát a külső támadásokkal szemben. Mivel az adatok nem hagyják el a felhasználó otthonát, kisebb a kockázata annak, hogy illetéktelenek is hozzá tudjanak férni az adatokhoz.

Csökkentett sávszélesség-használat: Az edge-computing csökkenti a felhőbe irányuló adatforgalmat, ami különösen előnyös lehet korlátozott internetkapcsolat esetén.

Adatvédelmi szabályozásoknak való megfelelés: Bizonyos országokban szigorú adatvédelmi előírások vonatkoznak a személyes adatok tárolására és feldolgozására. A helyi adattárolás segíthet az okosotthon-felhasználóknak megfelelni ezeknek a szabályozásoknak.

Skálázhatóság és rugalmasság: Az edge-computing architektúra lehetővé teszi az okosotthon-rendszer könnyebb skálázását. Új eszközök hozzáadásakor a feldolgozási terhelés részben helyben marad, így kevésbé terheli a központi infrastruktúrát vagy az internetkapcsolatot. Ez különösen fontos lehet a jövőben, ahogy egyre több okoseszköz kerül egy háztartásba.

Az okosotthonokban az edge-computing eszközök lehetnek például okos hubok, amelyek képesek a hozzájuk csatlakoztatott szenzorok és eszközök adatainak helyi feldolgozására és tárolására. Emellett egyes okoseszközök, mint például a kamerák vagy a hangszórók, beépített edge-computing képességekkel is rendelkezhetnek.

Egy konkrét példa az edge-computingra:

A Google Nest Cam(akkumlátoros)[10], amely rendelkezik intelligens funkciókkal, helyben végzett elemzési képességekkel. Ez a kamera képes helyben, a kamerán lévő processzor segítségével megkülönböztetni az embereket, az állatokat és a járműveket. Ez azt jelenti, hogy a felhasználó pontosabb riasztásokat kaphat (pl. "embert látott a bejárati ajtónál" ahelyett, hogy "mozgást érzékelt"). Ez csökkenti a felesleges riasztások számát és a feltöltött adat mennyiségét. A kamerának további funkciója is elérhető, mint például:

Offline eseménytárolás (bizonyos ideig): Ha az internetkapcsolat megszakad, a Nest Cam (akkumulátoros) bizonyos ideig képes helyben tárolni az eseményeket. Amint a kapcsolat helyreáll, feltölti ezeket a felvételeket a felhőbe. Ez biztosítja, hogy ne maradjon le fontos eseményekről egy ideiglenes internetkimaradás miatt.

Összességében az ilyen edge-computing eszközökkel vagy hubokkal felszerelt otthonok sokkal megbízhatóbbak, és könnyebben megfelelnek a különböző adatvédelmi előírásoknak, mint a kizárólag felhőalapú tárolást alkalmazó rendszerek. Emellett csak a valóban létfontosságú adatokat továbbítják a felhőbe, amelyek más eszközöknek is létfontosságú lehet.

Trhead protokol(alkalmazása, integrációja)

Története: A Thread protokollt 2014-ben mutatta be a Thread Group, egy iparági konzorcium által, amelynek tagjai között olyan vállalatok szerepelnek, mint a Google Nest és a Samsung. A Thread célja, hogy egy egyszerűen telepíthető, skálázható és biztonságos hálózati protokollt biztosítson az okosotthon eszközeinek számára.

Fogalma: Thread egy IPv6-alapú kommunikációs protokoll, ami nyílt forrású, amelyet alacsony fogyasztású dolgok internetes eszközei számára terveztek. A Thread nagymértékben javítja a eszközök közötti kapcsolatok stabilitását az okosotthonokban, mivel ez a protokoll redundáns kapcsolatot tesz lehetővé az okos eszközök között. Egyetlen egy topológiát használ amit Mesh topológiának hívnak. Ez a topológia azt foglalja magába, hogy minden eszköz kommunikálhat a hálózat bármely más eszközével köztes csomópontokon keresztül. Ez biztosítja a hálózat rugalmasságát és megbízhatóságát, mivel több útvonal áll rendelkezésre az adatok továbbítására.[11]

A Thread hálózatoknak négyféle eszköz létezik:

Hálózati vezérlő (Commissioner/Leader): Feladata a hálózati eszközök csatlakozásának és eltávolításának menedzselése. Egy commissioner lehet a hálózaton, de kiesése esetén átveheti a szerepét egy másik eszköz (tipikusan valamelyik router eszköz).

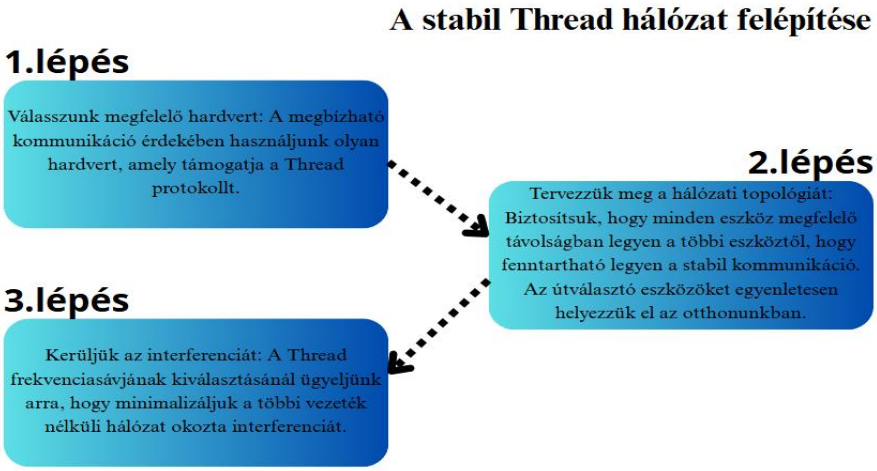
Router eszközök (Mesh Extender Device): Ezek az eszközök továbbítják az adatokat a hálózat különböző pontjai között és segítenek fenntartani a hálózat stabilitását.

Átjáró eszközök (Borer Router): Ezek az eszközök felelősek a thread hálózat egyéb hálózatokkal (pl.:WiFi, Ethernet, Zigbee, Z-Wave) való összekötéséért. Több border router lehet a hálózaton.

Végponti eszközök (Battery Operated Device): Alacsony fogyasztású, elemről vagy akkumulátorról működő eszközök, amelyek főként adatokat gyűjtenek és továbbítanak a routereken keresztül.

Nagy előnye a Threadnek hogy támogatja a vezeték nélküli kommunikációt is, amely elősegíti a könnyű telepítést vagy akar az üzemeltetést is. A nagy fejlesztők ezt a protokollt használják, mint például: a Google, Amazon, Samsung,

A Thread protokollon kívül a másik jelentős szabvány, a Matter szabvány. A Matter a **CSA** (Communication Standards Alliance) okosotthon kommunikációs szabványa, amely lehetővé teszi a különböző eszközök és rendszerek együttműködését és integrációját az otthoni intelligens rendszerekben.



2. ábra Stabil Thread hálozatok felépítése, saját ábra weboldal felhasználásával, https://okosotthonblog.hu/wiki/okosotthon/protokollok-es-standardok/thread/

Zigbee:

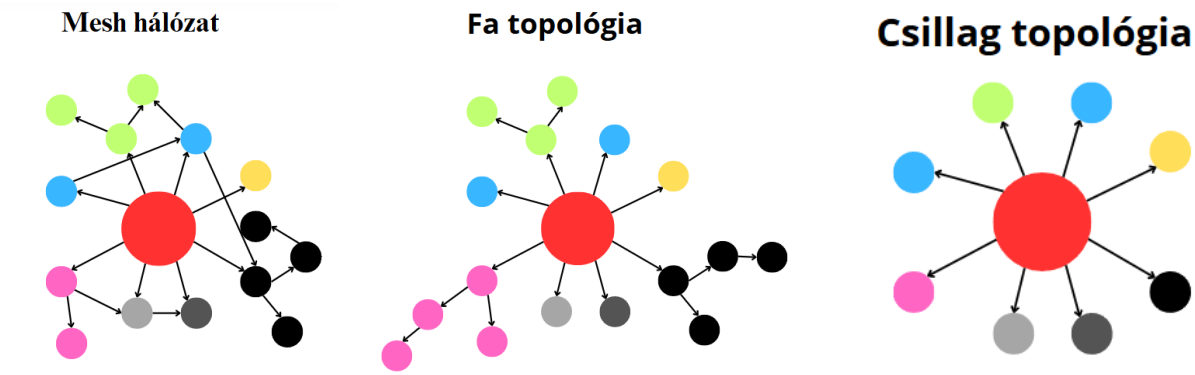
A Zigbee-t 2003-ban hozta létre a Zigbee Alliance, amely több mint 400 vállalat együttműködését tömöríti. Célja egy olyan vezeték nélküli hálózati protokoll kidolgozása volt, amely képes alacsony fogyasztás mellett nagy mennyiségű eszközt összekötni.

fogalma: A Zigbee egy alacsony energiafogyasztású, vezeték nélküli kommunikációs szabvány, amely kifejezetten a rövid hatótávolságú adatátvitelhez fejlesztettek ki. Elsősorban az IoT rendszerekben használják, ahol fontos a megbízhatóság és az alacsony energia fogyasztás.

A Zigbee is Mesh architektúrát használ ugyan úgy, mint a Thread protokoll. Zigbee választása ideális olyan rendszerekhez, mint a világítás, termosztátok, mozgásérzékelők és más okoseszközök, ahol az alacsony energiafogyasztás és az eszközök közötti gyors kommunikáció elsődleges szempont, viszont a adatátviteli sebessége alacsony, mivel jellemzően 20–250 kbps között mozog. Ezek az eszközök alacsony fogyasztásúak, és gyakran hosszú üzemidővel rendelkeznek, mivel ritkán továbbítanak adatokat, illetve készenléti üzemmódban tartózkodnak, amikor nincs kommunikáció.[12],[22]

A Zigbee hálózatok háromféle topológia alapján építhetők fel:

- ***Csillagtopológia (Star Topology):*** Itt minden végpont közvetlenül a koordinátorhoz csatlakozik. Ez egyszerűsített kommunikációt tesz lehetővé, de a hálózat megbízhatósága a koordinátor működésétől függ.
- ***Fa topológia (Tree Topology):*** A fa struktúrában a koordinátor egy hierarchikus rendszerben több routerhez kapcsolódik, és azok továbbítják az adatokat a végpontokhoz.
- ***Mesh hálózat (Mesh Network):*** Ebben a topológiában minden eszköz képes adatokat továbbítani, és több útvonalon is eljuthatnak az adatok a célállomásra. Ez a Zigbee legelterjedtebb hálózati felépítése, mivel növeli a hálózat megbízhatóságát és lefedettségét, valamint csökkenti az egyes eszközök kieséséből eredő problémákat.



3. ábra Topológiák (Zigbee), saját szerkesztésű ábra

Z-Wawe:

Z-Wave egy olyan típusú technológia protokoll, amely lehetővé teszi a vezeték nélküli eszközök közötti kommunikációt. 2003-ban kifejlesztették ki, de a Z-Wave igazi felívelése 2005-ben történt, a Z-Wawe Aliance megalakulásával. Jelenleg a Z-Wave-t több mint 40 millió termékben használják szerte a világon, beleértve a lakossági rendszereket, valamint a kereskedelmi környezetben is.
A Z-Wave hálózatot egy központi vezérlőegység (hub vagy gateway) irányítja. Ez a hub felelős az eszközök hozzáadásáért, konfigurálásáért és a közöttük lévő kommunikáció koordinálásáért. A felhasználók általában ezen a központi egységen keresztül, egy mobilalkalmazáson vagy webes felületen keresztül vezérelhetik az okosotthon rendszerüket. Ugyan úgy Mesh architektúrát használ, mint a Zigbee.

A Z-Wave egy biztonságra tervezett protokoll. A legújabb generáció, a Z-Wave Plus V2 (vagy Z-Wave Long Range), fejlett titkosítási eljárásokat alkalmaz, biztosítva a kommunikáció védelmét a külső behatolásokkal szemben.

A Z-Wawe előnye a Zigbee vel szemben, hogy ez kisebb frekvencia sávot használ ezért a zajos környezetben ez előnyösebb több eszközzel kompatibilis, valamint a hatótáv is nagyobb, igy ritkábban kellenek ismétlőpontok.[13],[22],[23]

Home Assistant:

A Home Assistant egy kiváló, nyílt forráskódú platform az otthoni automatizáláshoz. Az egyik fő erőssége, hogy a vezérlést helyben tartja, garantálva a gyors működést és az adatok biztonságát, applikáci. Támogatása rengetegféle okos eszközre is kiterjedhet. A felhasználók komplex, személyre szabott automatizmusokat hozhatnak létre eszközeik összekapcsolásával. Egyetlen, egységes felületet biztosít az egész okosotthon irányításához.[14]

Loxone:

A Loxone egy átfogó okosotthon-rendszer, amely intelligens vezérlést és menedzsmentet kínál az okosotthonok különböző elemeihez, mint például a világítás, fűtés, hangrendszer és árnyékolás. A Loxonenek a filozófiája egy egységes, saját fejlesztésű ökoszisztéma köré épül, amely optimalizált teljesítményt és zökkenőmentes kompatibilitást biztosít. A rendszer alapelvei közé tartozik a mindennapi feladatok automatizálása a kényelem növelése érdekében.

A Loxone célja, hogy olyan megoldást nyújtson, amely egyszerre kényelmes és energiatakarékos a házak felhasználói számára.

A rendszer központi eleme a Loxone Miniserver.A Miniserver intelligens érzékelőkkel érzékeli, mikor van szükség beavatkozásra, és parancsokat küld a megfelelő eszközöknek. A Loxone saját termékeinek előnyeit ötvözi a más gyártók eszközeivel való integráció lehetőségével, amelyek megfelelnek a bevált okosotthon iparági szabványoknak.

Loxone mini server:

A Loxone Miniserver a rendszer központi vezérlőegysége (rendszer magja), amely felelős a biztonságért, a kényelemért és az energiahatékonyságért. Számos beépített interfésszel rendelkezik, amelyek lehetővé teszik a különböző eszközök csatlakoztatását.

A Loxone 3 különböző Miniserver modelleket kínál:[15]

- ***Miniserver (Standard):*** Beépített LAN-nal, nagy teljesítményű relékkel, analóg és digitális bemenetekkel, valamint Loxone Tree és Link interfészekkel rendelkezik. Ez a modell a legátfogóbb vezetékes csatlakozási lehetőséget kínálja, ideális új építésekhez vagy nagyobb felújításokhoz, ahol kiterjedt vezetékes infrastruktúra kiépítése lehetséges.
- ***Miniserver Compact*****:** Egyesíti az Air Base Extension és Tree Extension funkcióit. Ez a modell integráltabb megoldást kínál, különösen hasznos olyan projektekhez, amelyek vezeték nélküli képességeket és hangfunkciókat igényelnek külön bővítmények nélkül, potenciálisan helyet és költséget takarítva meg.
- ***Miniserver Go:*** Vezeték nélküli verzió integrált Air interfésszel (akár 128 Air eszköz), Loxone Link akár 30 bővítményhez. Rugalmasan elhelyezhető . A Miniserver Go kifejezetten a meglévő otthonok okosítására lett tervezve, ahol az új vezetékek húzása nehézkes, a vezeték nélküli kommunikációt helyezve előtérbe. Rugalmas elhelyezése tovább egyszerűsíti a telepítést a meglévő otthonokban.

Air Base Extension: A Loxone vezeték nélküli mesh technológiája utólagos felszereléshez és olyan eszközök csatlakoztatásához, ahol a kábelezés nehézkes. A kommunikáció teljes mértékben titkosított IPSec használatával. Minden tápellátással rendelkező Air eszköz jelismétlőként működik, kiterjesztve a hatótávolságot és a stabilitást. Maximum 128 Air eszközt támogat az Air Base.[16]

***Tree Extension*:** A Loxone Tree technológia stabil és megbízható alapot nyújt az intelligens épületautomatizáláshoz. Egy saját fejlesztésű vezetékes busztechnológia, amelyet a perifériás eszközök, például érzékelők és aktorok kábelezési bonyolultságának (akár 80%-kal kevesebb kábelezés állítása szerint) és telepítési idejének csökkentésére terveztek. Rugalmas kábelezési topológiát kínál. Bővítményenként maximum 50 Tree eszközt támogat Tree áganként.[16]

Loxone biztonsági eszközei:

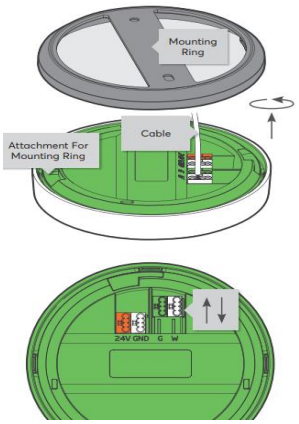
***Touch Pure Tree*:** A Loxone Touch Pure Tree egy elegáns és modern nyomógomb, amely a Loxone Tree technológiát használja a Miniserverrel való kommunikációhoz. Kialakításában a fejlesztők egy letisztult, üvegfelület hoztak létre és ez jellemzően öt érintési ponttal bír a különböző funkciók (pl. világítás, árnyékolás, zene) vezérlésére. Gyakran tartalmaz beépített érzékelőket is, mint például hőmérséklet- és páratartalom-érzékelő, így egyetlen eszköz több célra is használható a helyiségben. A Tree technológiának köszönhetően telepítése egyszerű, kevés kábelezést igényel, és közvetlenül a Tree Extensionre vagy a Miniserver Tree felületére csatlakoztatható.[17]

[17 kép link]

Weather Station: A Loxone Weather Station egy átfogó kültéri érzékelő, amely számos időjárási paraméter mérésére képes, biztosítva a szükséges információkat az épületautomatizálási feladatokhoz. Méri a külső hőmérsékletet, relatív páratartalmat, légnyomást, szélsebességet és szélirányt, valamint a csapadék mennyiségét és a fényerősséget (beleértve az alkonyat-érzékelést is). Az összegyűjtött adatok alapján a Loxone rendszer intelligensen tud reagálni a változó időjárási körülményekre, például automatikusan vezérelve az árnyékolókat erős napsütés vagy szél esetén, vagy optimalizálva a fűtési rendszert a külső hőmérséklet alapján. [18]

[18 kép link]

Motion Sensor Tree: A Loxone Motion Sensor Tree egy mozgásérzékelő, amely a Loxone Tree buszrendszeren keresztül kommunikál. Elsődleges feladata a mozgás érzékelése egy adott területen, ami alapvető információ a jelenlét-alapú automatizálási funkciókhoz, mint például a világítás vagy a fűtés automatikus kapcsolása, amikor valaki belép egy helyiségbe. A mozgásérzékelés mellett gyakran tartalmaz beépített fényérzékelőt is, így a rendszer csak akkor kapcsolja fel a világítást, ha mozgást érzékel és a környezeti fényerő egy meghatározott szint alatt van. Segít az energiamegtakarításban, hogy a funkciók automatikusan aktiválódnak, amikor szükség van rájuk. [19]



[19 kép link]

Loxone Audioserver:

A Loxone Audioserver egy olyan eszköz, amely lehetővé teszi a multiroom audió lejátszást a Loxone okosotthon rendszerében. Több zónát támogat, így a különböző helyiségekben eltérő zene is szólhat. Az Audioserver bővíthető további Stereo Extension modulokkal a zónák számának növeléséhez. A vezérlés a Loxone App-on keresztül történik.[20]

[20 kép link]

Smoke Detector:

A Loxone füstérzékelő egy vezeték nélküli, Air technológiás eszköz, amely elengedhetetlen eleme lehet az okosotthonok biztonsági rendszerének. Képes a füstképződést már a korai szakaszban, optikai érzékeléssel felismerni. Beépített akkumulátorral rendelkezik, így áramszünet esetén is működőképes. Veszély észlelésekor azonnal hangos riasztást és jól látható fényjelzést ad. Mivel integrálható a Loxone rendszerbe, a riasztás további automatizmusokat válthat ki, mint például a vészvilágítás bekapcsolása. Az eszköz figyelemmel kíséri saját energiaellátását, és időben jelzi az elem cseréjének szükségességét.[21]

[21 kép link]

Smart Ups bemutatása:

A smart UPS (intelligens szünetmentes tápegység) egy olyan fejlett eszköz, amely alapvető funkcióján az áramkimaradás. Átmeneti energiaellátás biztosításon túlmutatva intelligens képességekkel is rendelkezik. Míg a hagyományos UPS csupán egy akkumulátor, amely rövid ideig képes fenntartani a csatlakoztatott eszközök működését, addig a smart UPS aktívan kommunikál a környezetével és a felhasználóval, így sokkal kifinomultabb védelmet és vezérlést tesz lehetővé, különösen az egyre komplexebb okosotthonokban.

A "smart" jelző elsősorban a kommunikációs képességekre és az ebből fakadó hozzáadott funkciókra utal. Ezek az eszközök jellemzően hálózati csatlakozással (Ethernet vagy Wi-Fi) rendelkeznek, lehetővé téve a távoli felügyeletet és menedzsmentet. A felhasználók egy mobilalkalmazáson vagy webes felületen keresztül bárhonnan ellenőrizhetik a UPS állapotát, például az akkumulátor töltöttségi szintjét, a becsült hátralévő üzemidőt, vagy a pillanatnyi terhelést. Áramszünet esetén vagy egyéb rendellenességnél (pl. túlfeszültség) azonnali értesítéseket küldhetnek, így a felhasználó még távollétében is tudomást szerezhet a problémáról.

Az okosotthonok kontextusában a smart UPS kulcsfontosságú szerepet tölt be. Képes kommunikálni a központi vezérlőegységgel vagy közvetlenül a csatlakoztatott okoseszközökkel. Ez lehetővé teszi például a csatlakoztatott érzékeny berendezések – mint a szerverek, NAS-ok (hálózati adattárolók), vagy akár az okosotthon-központ – automatizált és

biztonságos leállítását, mielőtt az akkumulátor teljesen lemerülne. Ezzel megelőzhető az adatvesztés és a hardverkárosodás.

További intelligens funkciók közé tartozik a prioritizált áramellátás, ahol a felhasználó beállíthatja, hogy mely kritikus eszközök (pl. biztonsági kamerák, internet router) kapjanak energiát a lehető leghosszabb ideig.

A smart UPS-ek gyakran részletes naplót vezetnek az energiafogyasztásról és az áramellátási eseményekről, ami segíthet az energiamenedzsment optimalizálásában és a hálózati problémák felderítésében. Az ilyen típusú szünetmentes tápegységek tehát nem csupán passzív védelmi eszközök, hanem az okosotthon aktív, menedzselhető komponensei is. Példa egy ilyen Smart Upsre:APC Smart-UPS szünetmentes Tápegység(SMT2200IC)[24]

Sima Ups tipusok:

Standby UPS

Müködési elv: A Standby Ups normál működés közben a csatlakoztatott eszközök közvetlenül a hálózati áramtól kapják az energiát, miközben a UPS akkumulátora töltődik. A UPS figyeli a bejövő hálózati feszültséget. Áramkimaradás vagy jelentős feszültségingadozás esetén a UPS egy átkapcsoló segítségével nagyon gyorsan (kb2-4ms) átvált akkumulátoros üzemmódra, és az inverteren keresztül biztosítja a tápellátást a csatlakoztatott eszközöknek. Az inverter csak ilyenkor lép működésbe addig készenléti állapotba van.[25],[26]
Előnyök:

- Kisebb méret és súly.
- Költséghatékony

Hátrány:

- Rövid átváltási idő néhány érzékeny eszközt megzavarhat.

Line-Interactive Ups:

Működési elv: Hasonló a készenléti UPS-hez, de egy fontos kiegészítéssel: rendelkezik egy többágú autotranszformátorral (AVR - Automatic Voltage Regulation). Az inverter mindig az UPS kimenetére kapcsolódik. Az akkumulátor töltődik az inverteren keresztül, ha a bemenet normális. Amikor a bemeneten hiba van, a kapcsoló nyit és az áram az akkumulátorból folyik az UPS kimenetére. A Standby UPS-hoz képest az állandóan kimenetre kapcsolódó inverter

szűri és csökkenti az átmenő kapcsolási tranzienseket és ellát két független energia útvonalat. Az inverter szabályozta UPS működéséhez nagyon kis energia elegendő [25],[26]

Előnyök:

- Hatékony feszültség-stabilizálás (AVR).
- Általában jó ár-értéket képvisel.
- Jobb feszültségszabályozást biztosít, mint a standby UPS.

Hátrány:

- Nem nyújt tökéletes védelmet a hálózati zajok és torzítások ellen, mivel az inverter nem működik folyamatosan.

Online/ Double-Conversion Ups

működési elv: Ez a legmagasabb szintű védelmet nyújtó UPS típus. A bejövő váltakozó áramot (AC) először átváltja egyenárammá (DC), amely tölti az akkumulátort és táplálja az invertert. Az inverter ezt az egyenáramot visszaalakítja stabil, tiszta szinuszos váltakozó árammá (AC), amely folyamatosan táplálja a csatlakoztatott eszközöket. Ez azt jelenti, hogy az eszközök mindig az inverter által generált áramot kapják, függetlenül a bejövő hálózati áram minőségétől. Áramkimaradás esetén nincs átkapcsolási idő, mivel az akkumulátor és az inverter már eleve az áramútban van.[26]

Előnyök:

- Nincs átkapcsolási idő (nulla milliszekundum) áramkimaradáskor.
- Teljes körű védelem a feszültségingadozások, hálózati zajok, frekvenciaeltérések és egyéb áramellátási problémák ellen.

Hátrányok:

- Drága a beszerzése
- Sokkal nehezebb a többi Upsnél
- Több hőt termel a kettős konverzió miatt

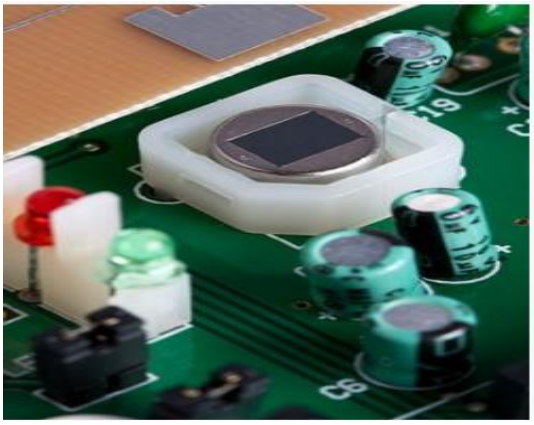
PIR (Passive Infrared Sensor – Passzív Infravörös Érzékelő)

A passzív infravörös (PIR) érzékelő egy elektronikus eszköz, amelyet széles körben alkalmaznak mozgás érzékelésére, leggyakrabban biztonsági riasztórendszerekben, automatikus világításkapcsolókban és okosotthon rendszerekben. Nevében a "passzív" szó arra utal, hogy maga az érzékelő nem bocsát ki semmilyen energiát, hanem a környezetéből érkező infravörös sugárzást detektálja.

Működési elv: Az élőlények, mint az emberek és állatok, testhőmérsékletük miatt jelentős mennyiségű infravörös energiát sugároznak. A PIR érzékelő ezt a hősugárzást használja fel a mozgás észlelésére. Az infravörös sugárzás (Infrared, IR) az elektromágneses sugárzás egy fajtája. Hullámhossza a látható fénynél nagyobb, de a mikrohullámnál és a rádióhullámnál kisebb. Az infravörös sugárzás elsősorban hősugárzást jelent. Minden anyag, aminek a hőmérséklete az abszolút nulla fok felett van, infravörös sugárzást bocsát ki magából.[27]

A PIR érzékelők az alábbi elemekből épülnek fel:

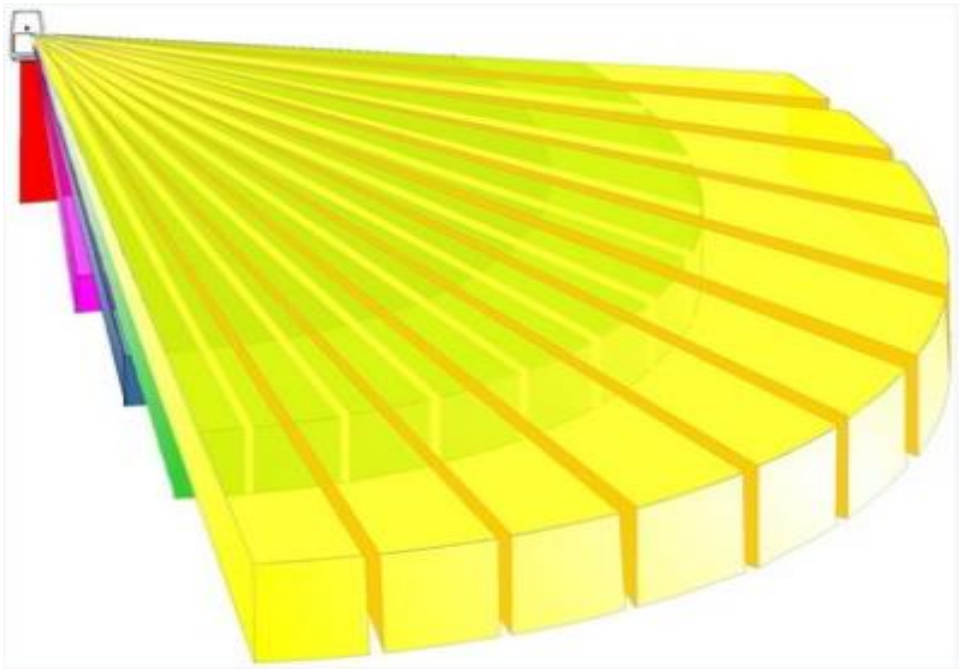
- ***Érzékelőelem:*** Az érzékelőelem a környezet hősugárzását, pontosabban annak változását érzékeli és az infravörös sugárzást villamos jelekké alakítja át. Az érzékelő fémtokban helyezkedik el, amelynek a tetején egy infraszűrővel ellátott kis ablak van. A gyártók arra törekszenek, hogy a PIR elsősorban a gyors hőmérsékletváltozásokra reagáljon.



Piroszenzor védőtokkal

https://www.oktel.hu/szolgaltatas/riasztoberendezesek/mozgaserzekelok/a-passziv-infra-es-felepitese/

- ***Optikai rendszer***: Az optikai rendszer feladata, hogy a környezet által kibocsátott és visszavert infravörös energiát az érzékelő elemre fókuszálja. A passzív infrák optikai rendszere lehet tükrös vagy Fresnel-lencsés.



Az infraérzékelő látótere felülnézetből

https://www.oktel.hu/szolgaltatas/riasztoberendezesek/mozgaserzekelok/a-passziv-infra-es-felepitese/

jelfeldolgozó áramkör: A passzív infra harmadik lényeges alkotóeleme a jelfeldolgozó áramkör. Folyamatosan figyeli a változásokat, felerősíti és kiértékeli azokat a jeleket, amelyeket a szenzorok összegyűjtöttek. Amennyiben ezek a jelek egy meghatározott megszólalási szintet meghaladnak, akkor egy relé működtetésével riaszt. [27]

Nyomásérzékelők okosotthonokban:

Az okosotthonokban a nyomásérzékelők fizikai erőhatás vagy súly jelenlétét detektálják egy adott felületen, így hozzájárulva az otthon automatizálásához és biztonságához. Gyakran használják őket rejtett biztonsági megoldásként, Ezek az érzékelők az okosotthon rendszerébe integrálva automatikus értesítéseket küldhetnek, vagy más eszközökkel összehangolt műveleteket indíthatnak el. Így a nyomásérzékelők diszkrét módon képesek növelni az otthoni környezet intelligenciáját és biztonságát.

WPA3:

A WPA3 (Wi-Fi Protected Access 3) egy fejlett Wi-Fi biztonsági protokoll, amelyet a Wi-Fi Alliance 2018-ban vezetett be a vezeték nélküli hálózatok védelmének javítása érdekében. Ennek a célja, hogy növelje a Wi-Fi hálózatok biztonságát.[28]

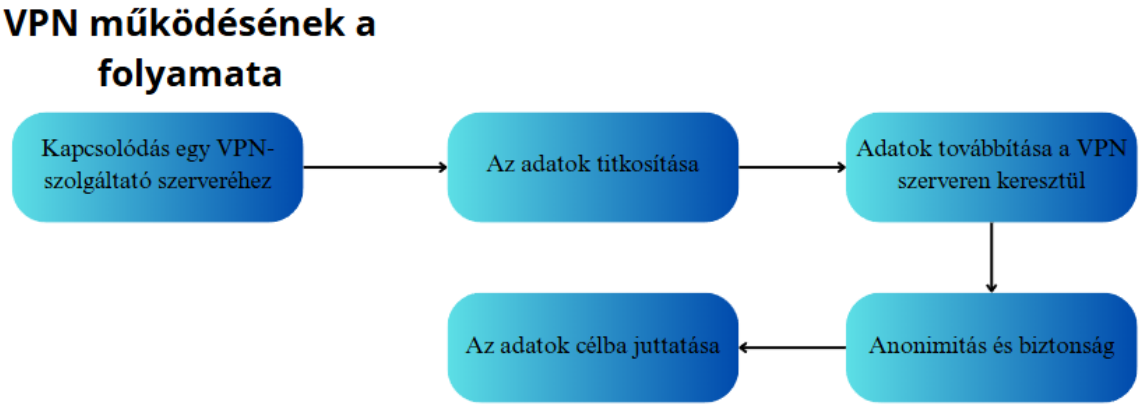
Számos fejlesztést tartalmaz, amelyek növelik a biztonságot és javítják a felhasználói élményt, többek között jobb védelmet kínálva a brute-force (nyers erő) támadások ellen. A WPA3 erősebb titkosítást alkalmaz az egyedi adatfolyamokhoz és egyszerűbb, mégis biztonságosabb jelszókezelést tesz lehetővé.

A protokollnak két fő változata létezik: a WPA3-Personal és a WPA3-Enterprise. A WPA3-Personal az SAE (Simultaneous Authentication of Equals) protokollt használja, amely a WPA2-ben használt PSK (Pre-Shared Key) módszert váltja fel, így még gyenge jelszavak esetén is hatékonyabb védelmet nyújt, és megakadályozza a hitelesítési adatok kiszivárgását a forgalom lehallgatása esetén is. Ezzel szemben a WPA3-Enterprise egy új, 192-bites titkosítás mellett egy speciális biztonsági csomagot is alkalmaz, amely szabványosított és megbízható titkosítási protokollokat használ, beleértve a 256-bites elliptikus görbéket (elliptic curve cryptography) és a HMAC-SHA384 hash eljárásokat.[28]

VPN:

A VPN, vagyis Virtual Private Network (virtuális magánhálózat), egy olyan technológia, amely lehetővé teszi, hogy biztonságos és titkosított kapcsolatot tudjunk létrehozni az eszközök és az internet között. Ezzel összekapcsolja az eszközöket egy távoli szerverrel, amely lehetővé teszi, hogy az internetet egy másik helyszínről is használni tudjuk, mintha fizikailag is ott lennénk.

A VPN segítségével el lehet rejteni az IP-címet. Emellett a VPN lehetővé teszi, hogy megkerüljük a földrajzi korlátozásokat is. Például, ha egy streaming szolgáltatás vagy weboldal egy bizonyos országban nem elérhető, a VPN segítségével úgy tehetünk, mintha egy másik országban lennénk, ahol az adott tartalom hozzáférhető.[29]



4. (ábra) VPN működése, saját szerkesztésű ábra, https://bytech.hu/VPN/

A hosszú távú megtakarításról: energiahatékonyság és fenntarthatóság

Az okosotthonok kulcsfontosságú szerepet játszanak a hosszú távú megtakarítások elérésében az energiahatékonyság és a fenntarthatóság révén. Mint ahogy a fentiekben is említettem, az intelligens termosztátok optimalizálják a fűtési és hűtési rendszerek működését, csökkentve ezzel a felesleges energiafogyasztást. Az automatizált világításvezérlés biztosítja, hogy a lámpák csak akkor égjenek, amikor valóban szükség van rájuk, így jelentős energiamegtakarítást eredményezve. Az okoseszközök képesek figyelemmel kísérni az energiafogyasztási szokásokat, és javaslatokat tenni a további optimalizálásra. A megújuló energiaforrások, mint például a napelemek, integrálása az okosotthon rendszerekben tovább növeli az energiafüggetlenséget és csökkenti a rezsiköltségeket. Az intelligens öntözőrendszerek a kert vízigényét a valós szükségletekhez igazítják, elkerülve ezzel a pazarlást. Az ilyen eszközök által biztosított adatok és elemzések segítségével a lakók tudatosabb döntéseket hozhatnak energiafelhasználásukkal kapcsolatban. Hosszú távon ezek a megoldások nemcsak a pénztárcát kímélik, hanem hozzájárulnak a környezeti terhelés csökkentéséhez is. Az energiahatékony működés és a fenntartható erőforrás-gazdálkodás révén az okosingatlanok piaci értéke is növekszik. Így az ilyen lakásokba történő befektetés egyben befektetés a jövőbe és a fenntarthatóbb életmódba.

Összegzés

Az okosotthonok világa rohamosan fejlődik, lehetővé téve otthonaink kényelmesebbé, biztonságosabbá és energiahatékonyabbá tételét. Számos gyártó és technológia verseng a felhasználók bizalmáért, különösen az egymással versenyképes megoldásokat kínálva az intelligens otthoni élmény megteremtésére. A piacot jelenleg néhány meghatározó szereplő uralja, amelyek átfogó, integrált ökoszisztémákat biztosítanak. A Google Home a hangvezérelt asszisztensére épít, míg az Amazon Alexa az Echo eszközökkel és a „Skills" alkalmazásréteggel bővíthető. A Samsung SmartThings a Zigbee és Z-Wave protokollok támogatásával nyújt nagyfokú rugalmasságot az eszközintegrációban.

Ezek a platformok jellemzően felhőalapú működésre épülő, vezeték nélküli IoT-eszközöket használnak, mint például okos termosztátok, világítási rendszerek, intelligens konnektorok, valamint víz- és gázérzékelők. Az alapfunkciók közé tartozik a távoli és zónás vezérlés, amely lehetővé teszi, hogy a felhasználók bárhonnan, valós időben monitorozhassák és módosíthassák otthonuk beállításait.

A Nest Learning Thermostat kiváló példája a fejlett funkcionalitásnak és a tanuló algoritmusokra épülő automatizálásnak. Ez az intelligens termosztát képes felismerni a felhasználói szokásokat, és automatikusan optimalizálja a fűtési-hűtési ciklusokat. A Nest alkalmazás intuitív, felhasználóbarát kezelőfelületet, széleskörű integrációs lehetőségeket és megbízható adatvédelmi megoldásokat kínál.

Az IoT-alapú energiamenedzsment lényege, hogy az internetre csatlakoztatott szenzorok és eszközök segítségével adatokat gyűjtünk az energiafogyasztásról, majd ezek elemzésével lehetőség nyílik az energiafelhasználás optimalizálására, költségcsökkentésre és a fenntartható működés elősegítésére.

A pereminformatikai (edge-computing) megoldások lényege, hogy az adatok feldolgozása nem a felhőben, hanem az eszközök közvetlen közelében, helyben történik. Ez számos előnnyel jár az okosotthonok számára: gyorsabb válaszidő, megnövelt rendszermegbízhatóság, fejlettebb adatvédelem, csökkentett hálózati terhelés, jobb megfelelés az adatvédelmi szabályozásoknak, valamint skálázhatóság és rugalmasság a hálózatok tervezése során. Jó példa erre az offline eseménytárolás, amikor az eszközök internetkapcsolat hiányában is képesek adatokat rögzíteni, amelyeket később szinkronizálnak.

Az okosotthoni eszközök közötti megbízható kommunikáció alapfeltétele a szabványosított protokollok alkalmazása. A Thread egy viszonylag új, alacsony energiafogyasztású, IPv6-alapú mesh hálózati protokoll, amely hatékony eszközkapcsolatot tesz lehetővé. A Zigbee szintén

elterjedt, kis energiaigényű vezeték nélküli megoldás, míg a Z-Wave egy másik népszerű, hasonló elven működő protokoll, amely ugyancsak mesh hálózatokat használ az eszközök összekapcsolására. A nagy technológiai platformok mellett egyre nagyobb szerepet kapnak az alternatív megoldások is: a Home Assistant egy nyílt forráskódú otthonautomatizálási rendszer, míg a Loxone egy professzionális, moduláris megközelítésű megoldás, amely a Miniserver architektúrájára épül.

Az intelligens otthonok működésének biztonságát és megbízhatóságát különféle kiegészítő eszközök támogatják. A Smart UPS (szünetmentes tápegység) biztosítja a zavartalan működést áramkimaradás esetén, míg a PIR (passzív infravörös érzékelő) hatékonyan alkalmazható mozgásérzékelésre. Az okosotthon-rendszerek védelme kiemelt fontosságú: a WPA3 a legkorszerűbb Wi-Fi biztonsági protokoll, míg a VPN (virtuális magánhálózat) titkosított kapcsolatot biztosít a távoli hozzáférés során.

Források:

[1] Chameleon Smart Home, "A Google Home okosotthonos rendszer," Chameleon Smarthome Blog,[Online]. Elérhető: https://chameleon-smarthome.com/blog/cikk/a-google-home-okosotthonos-rendszer

[2] SmartBuild, "Az Amazon Alexa okosotthon és az Echo működése," SmartBuild, [Online]. Elérhető:: https://smartbuild.hu/amazon-alexa-okosotthon/

[3] Samsung Electronics, "Smart home with Samsung SmartThings," Samsung US, [Online]. Elérhető: https://smartbuild.hu/amazon-alexa-okosotthon/

[4] Enerit, „Energia menedzsment rendszer”, *Enerit.hu*, [Online]. Elérhető: https://www.enerit.hu/energiamenedzsment-rendszer/

[5] Bosch Smart Home, „Twist - Control element and accessories”, *Bosch Smart Home UK*, [Online]. Elérhető: https://www.bosch-smarthome.com/uk/en/products/control-elements-and-accessories/twist/

[6] COMPUTHERM, „Zóna vezérlők és kiegészítők”, *Computherm.hu*, [Online]. Elérhető: https://www.computherm.hu/termekek/computherm-zona-vezerlok-kiegeszitok.html

[7] Google, „How to control your Nest thermostat with the Google Home app”, *Google Nest Help*, [Online]. Elérhető: https://support.google.com/googlenest/answer/9247510?hl=en

[8] Phoenix Contact, „IoT-alapú energiagazdálkodás”, *Phoenix Contact*, [Online]. Elérhető::https://www.phoenixcontact.com/hu-hu/technologiak/energiamenedzsment/iot-basiertes-energiemanagement

[9] IBM, „What is Edge Computing?”, *IBM Think*, [Online]. Elérhető: https://www.ibm.com/think/topics/edge-computing

[10] T. White, „Nest Cam Outdoor Review”, Terry White Blog, [Online]. Available: https://terrywhite.com/nest-cam-outdoor-review/

[11] Okosotthon Blog, „Thread protokoll”, *Wiki – Okosotthon Blog*, [Online]. Elérhető: https://okosotthonblog.hu/wiki/okosotthon/protokollok-es-standardok/thread/

[12] Bytech, „Zigbee ismertető”, *Bytech.hu*, [Online]. Elérhető::https://bytech.hu/zigbee/

[13] SmartBuild, „Z-Wave technológia”, *SmartBuild.hu*, [Online]. Elérhető: https://smartbuild.hu/z-wave/

[14] Home Assistant, „Home Assistant Project”, *Home-assistant.io*, [Online]. Elérhető: https://www.home-assistant.io/

[15] Loxone, „Miniserver”, *Loxone International*, [Online]. Elérhető: https://www.loxone.com/int/products/miniserver/

[16] Loxone, „Loxone Technology Overview”, *Loxone International*, [Online]. Elérhető: https://www.loxone.com/int/products/technology/

[17] Loxone, „Touch Pure Tree”, *Loxone Knowledge Base*, [Online]. Elérhető: https://www.loxone.com/enen/kb/touch-pure-tree-2/

kép: https://store.verdom.hu/touch-pure-flex-tree-antracit.html

[18] Loxone, „Weather Station Tree”, *Loxone Knowledge Base*, [Online]. Elérhető: https://www.loxone.com/enen/kb/weather-station-tree/

kép: https://shop.loxone.com/enen/product/100246-weather-station-tree

[19] Loxone, „Motion Sensor Tree”, *Loxone Knowledge Base*, [Online]. Elérhető:: https://www.loxone.com/enen/kb/motion-sensor-tree/

kép: https://www.loxone.com/enen/kb/motion-sensor-tree/

[20] Loxone, „Audioserver Technical Information”, *Loxone Products*, [Online]. Elérhető: https://www.loxone.com/enen/products/audioserver/technical/

kép: https://www.loxone.com/enus/products/audioserver/technical/

[21] Loxone, „Smoke Detector Air”, *Loxone Knowledge Base*, [Online]. Elérhető: https://www.loxone.com/enen/kb/smoke-detector-air/

kép: https://www.loxone.com/enen/kb/smoke-detector-air/

[22] Samsung, „Z-Wave vs. Zigbee”, *Samsung NZ Support*, [Online]. Elérhető: https://www.samsung.com/nz/support/mobile-devices/z-wave-vs-zigbee/

[23] Intelligens Világ, „Mi a Z-Wave?”, *Intelligensvilag.com*, [Online]. Elérhető: https://intelligensvilag.com/hirek/mi-a-z-wave-miert-eppen-o-miert-eppen-mi

[24] "APC Smart-UPS szünetmentes tápegység SmartConnect funkcióval SMT2200IC," Aqua.hu. [Online]. Elérhető: https://aqua.hu/szunetmentes-tapegysegek/apc-smart-ups-szunetmentes-tapegyseg-smartconnect-funkcioval-smt2200ic-t693286

[25] "UPS változatok," Muszeroldal.hu. [Online]. Elérhető: https://www.muszeroldal.hu/assistance/upsvaltozatok.pdf

[26] "Szünetmentes tápegységek (UPS): hogy működnek és miért fontosak," Villámgyorsvillanyszerelő.hu.. [Online]. Elérhető: https://villamgyorsvillanyszerelo.hu/szunetmentes-tapegysegek-ups-hogy-mukodnek-es-miert-fontosak/

[27] "A passzív infra és felépítése," Oktel.hu.. [Online]. Elérhető: https://www.oktel.hu/szolgaltatas/riasztoberendezesek/mozgaserzekelok/a-passziv-infra-es-felepitese/

[28] "WPA3 – a legújabb Wi-Fi biztonsági szabvány," Bytech.hu. [Online]. Elérhető: https://bytech.hu/wpa3/

[29] "VPN – Mi az a VPN és hogyan működik?" [Online]. Elérhető: https://bytech.hu/VPN/