Nemzeti Média- és Hírközlési Hatóság

5G biztonság –
a szabványosítás szemszögéből

Dr. Bartolits István
Technológiaelemző Főosztály

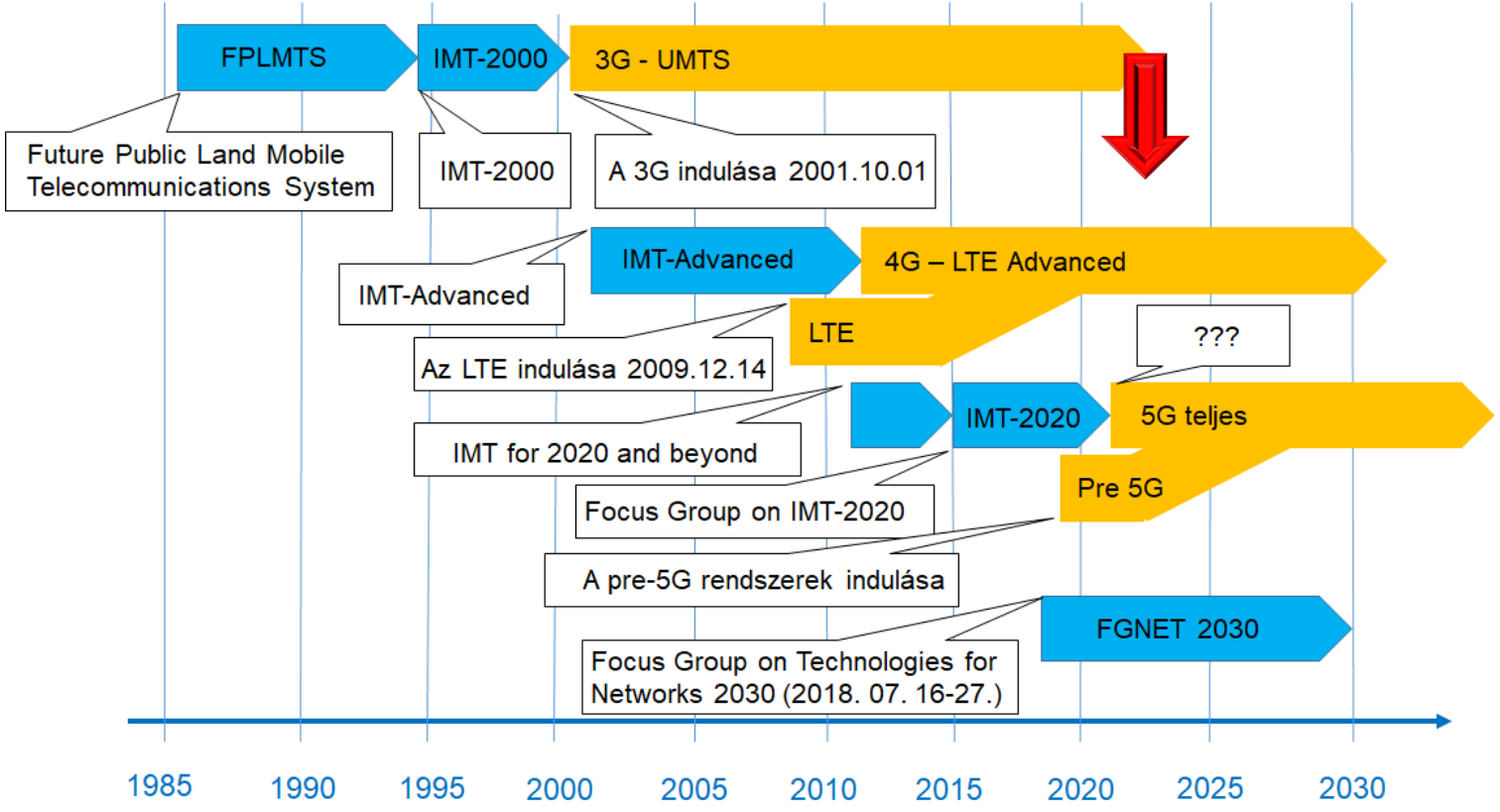
Hírközlés és kíberbiztonság
NMHH-HTE EIVOK tudományos konferencia 2022. május 26.

TARTALMI VÁZLAT

- Új biztonsági kihívások az 5G rendszerben
- Az 5G szabványosítás és következményei a biztonságra
- Az Open RAN kezdeményezés biztonsági kérdései
- A hálózatszeletelés és a biztonság
- Az 5G magánhálózatok és a biztonság

Új biztonsági kihívások az 5G rendszerben

A MOBIL HÁLÓZATOK BEVEZETÉSI LÉPCSŐI

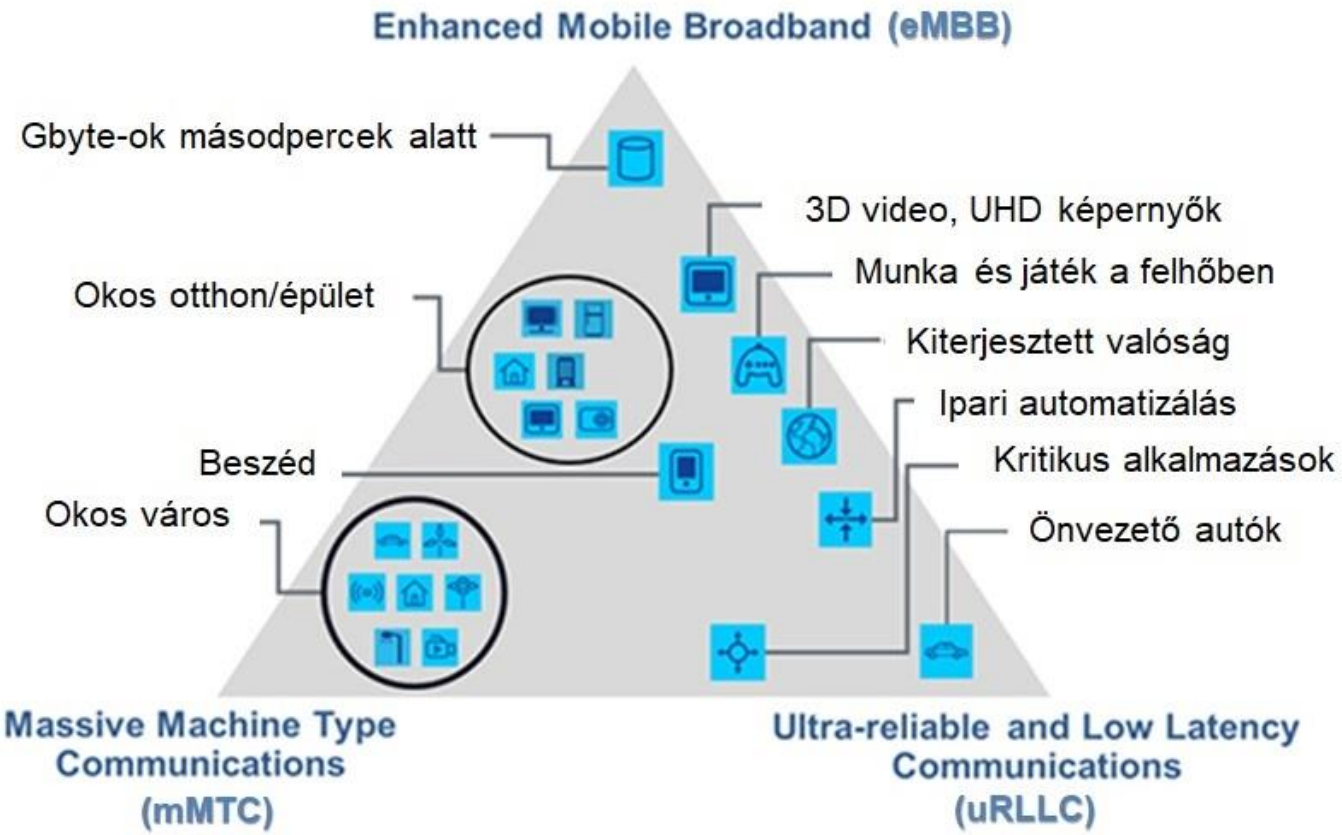


AZ 5G RENDSZERREL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

Az IMT-2020 legfontosabb célkitűzései (ITU-T Focus Group, 2015) :

- Magas felhasználói adatsebesség
- Igen nagy felhasználó-sűrűség kiszolgálása
- Igen kicsi késleltetés és magas megbízhatóság
- Tárgyak nagy tömegben történő hálózatra kapcsolása (IoT)
- Nagy sebességű mozgás (mobilitás) esetén is változatlan minőség
- Emelt szintű multimédia szolgáltatás
- Konvergens alkalmazások differenciált kezelése

AZ 5G RENDSZER KÖVETELMÉNYHÁROMSZÖGE



ÚJ ALAPELVEK, ÚJ BIZTONSÁGI KIHÍVÁSOK

- Az 5G rendszer sokkal összetettebb lesz, mint az előző generációk
- Az 5G rendszert sokkal szélesebb módon fogják használni, mint a korábbiakat
- Az 5G rendszerben sokkal több adat áramlik – és találkozhat egymással – mint az előző mobil rendszerekben

Következmény: Sokkal nagyobb szerepe van a biztonságnak, mint eddig

- ITU-T SG17: Security tanulmányi csoport
- Az IMT-2020 teljes specifikációs munkájában részt vett, hogy már a kezdetektől beépüljenek a biztonsági funkciók

AZ ITU-T 5G VÉGTŐL-VÉGIG BIZTONSÁGI VÁZA

Végberendezés biztonság	Hozzáférési hálózat biztonság	Maghálózat biztonság	Szolgáltatás és alkalmazás biztonság
Malwares Side channel attacks Zombies	Air interface security Fronthaul & backhaul security MEC security SDN/NFV security Cloud security	Network capability exposure security Inter network security SBA security Network slicing security SDN/NFV security Cloud security	Service security Big data security Web security Information security Cloud security

Általános biztonsági eszközök		
	Cryptography (including Quantum-safe Cryptogr.)	IDM PKI AI/ML (DLT)
	Security situation awareness	Authentication technologies (incl. Biometrics)
	Security emergency response	Threat intelligence handling
		Security testing and certification

AZ ITU-T 5G VÉGTŐL-VÉGIG BIZTONSÁGI VÁZA

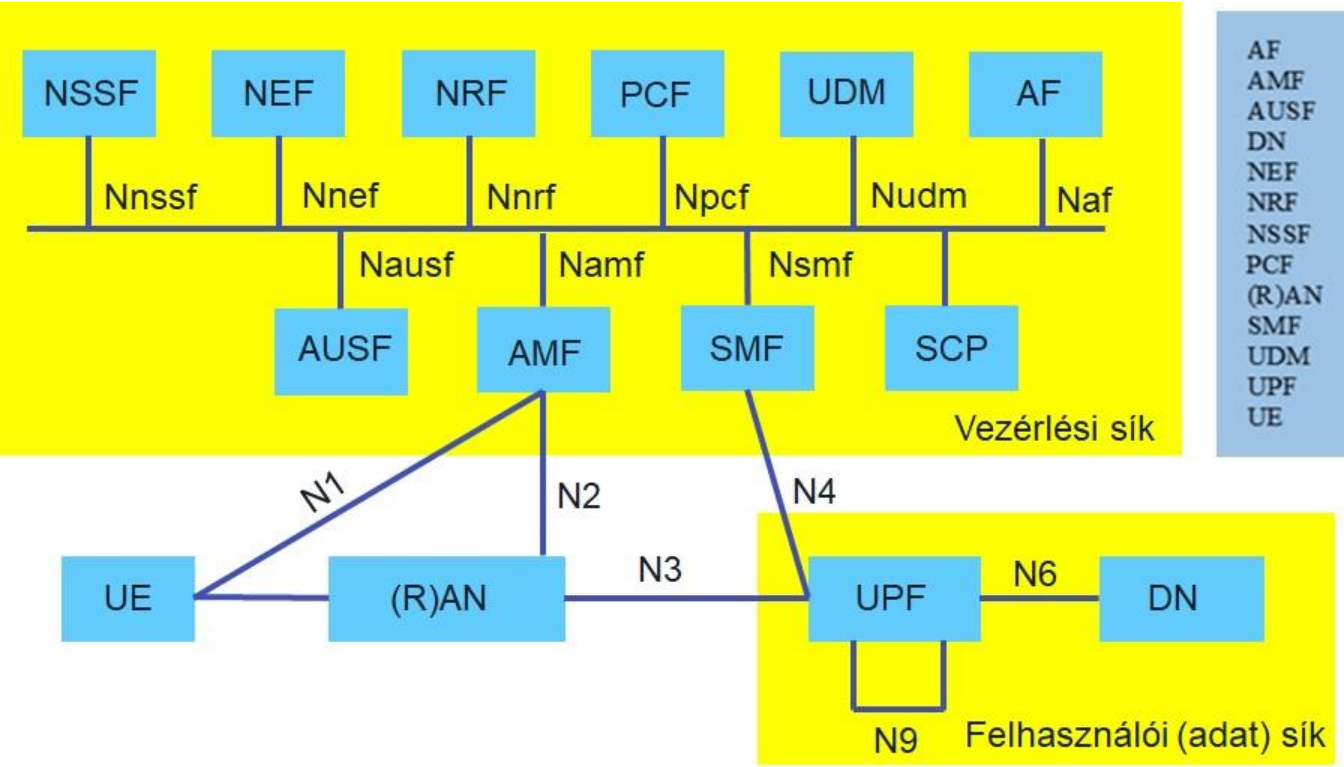
Végberendezés biztonság	Hozzáférési hálózat biztonság	Maghálózat biztonság	Szolgáltatás és alkalmazás biztonság
Malwares Side channel attacks Zombies	Air interface security Fronthaul & backhaul security MEC security SDN/NFV security Cloud security	Network capability exposure security Inter network security SBA security Network slicing security SDN/NFV security Cloud security	Service security Big data security Web security Information security Cloud security

Általános biztonsági eszközök		
	Cryptography (including Quantum-safe Cryptogr.)	IDM PKI AI/ML (DLT)
	Security situation awareness	Authentication technologies (incl. Biometrics)
	Security emergency response	Threat intelligence handling
		Security testing and certification

RENDSZERTECHNIKAI CÉLKITŰZÉSEK

- Az 5G rendszertechnika alapvető célkitűzései
  - Lapos hálózati architektúra
  - A vezérlési sík és az adatsík elválasztása
  - Minden funkció önálló egységbe – felhőnatív megoldások támogatása
  - Erőforrások optimális kihasználása – hálózatszeletelés
  - Magasszintű koordináció – orkesztráció a rendszer felett

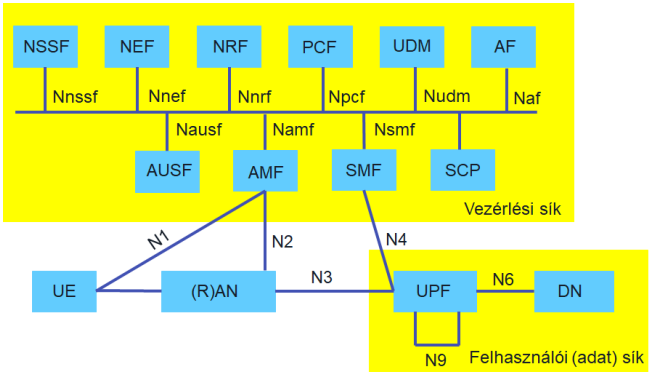
AZ 5G REFERENCIAMODELL ÉS A SERVICE-BASED ARCHITECTURE (SBA)



AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
DN	Data Network
NEF	Network Exposure Function
NRF	NF Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
(R)AN	(Radio) Access Network
SMF	Session Management Function
UDM	Unified Data Management
UPF	User Plane Function
UE	User Equipment

AZ 5G REFERENCIAMODELL - MAGYARUL
A funkciók elnevezése, értelmezése

- NSSF – Hálózati szeletválasztó funkció
- NEF - Hálózati funkciók közvetítése
- NRF – Hálózati adattárház funkció
- PCF – Irányelv szerinti vezérlés funkció
- UDM – Egységes Adatmenedzsment funkció
- AF – Alkalmazás funkció, alkalmazások megvalósítása
- AUSF – Hitelesítési szerver funkció
- AMF – Hozzáférés és mobilitás menedzsment funkció
- SMF – Viszony menedzsment funkció
- SCP – Szolgáltatás-kommunikációs proxy szerver

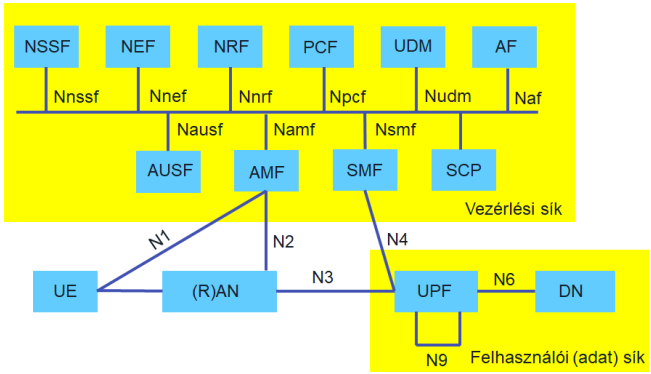


- UE – felhasználói készülék
- (R)AN – (rádiós) hozzáférési hálózat
- UPF – Felhasználói sík funkció
- DN - Adathálózat

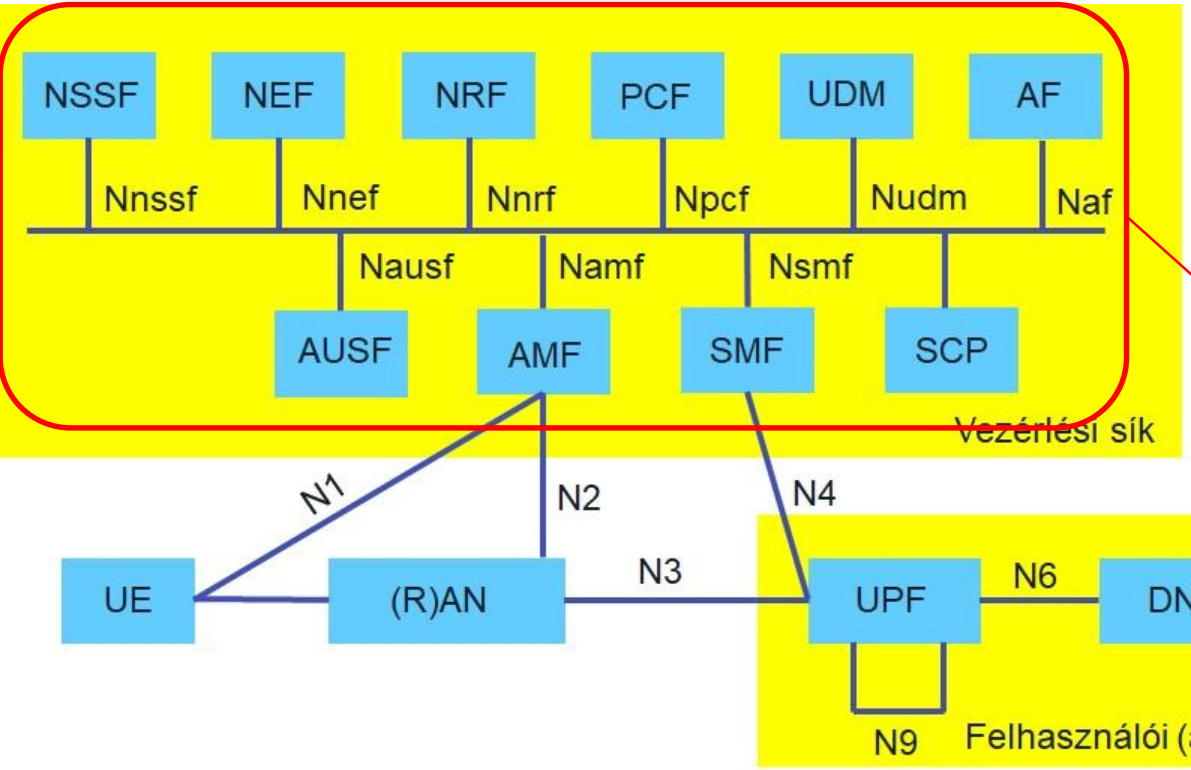
AZ 5G REFERENCIAMODELL - MAGYARUL
A referenciapontok értelmezése

Referenciapontok:

- N1 – a felhasználói készülék és a hozzáférés és mobilitásmenedzsment funkció között
- N2 – a rádiós hozzáférési hálózat és a hozzáférés és mobilitás menedzsment funkció között
- N3 – a felhasználói sík funkció és a rádiós hozzáférési hálózat között
- N4 – a viszony menedzsment funkció és a felhasználói sík funkció között
- N6 – a felhasználói sík funkció és az adathálózat között
- N9 – a felhasználói sík funkciók között



A SERVICE-BASED ARCHITECTURE (SBA) FOGALMA



AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
DN	Data Network
NEF	Network Exposure Function
NRF	NF Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
(R)AN	(Radio) Access Network
SMF	Session Management Function
UDM	Unified Data Management
UPF	User Plane Function
UE	User Equipment

SBA megoldás

A SERVICE-BASED ARCHITECTURE BIZTONSÁGI KÉRDÉSEI

- Az SBA esetében minden funkcionális egység egy buszra dolgozik, az SBI interfészen keresztül kommunikálnak
- Az egyes funkcionális modulok lehetnek felhőben is
- Az SBA megoldás eltér a korábbi maghálózati modellektől, ahol az egyes funkcionális modulok közvetlenül össze voltak kötve
- Ez új biztonsági problémákat vet fel
- A 3GPP és a GSMA ezen intenzíven dolgozik, vannak rá ajánlások, kérdés, hogy valóban implementálva lesznek-e
- Pl.: 3GPP TS 33 511, TS 33 512, TS 33 513, GSMA FS 21, GSMA FS 34, GSMA FS 36

A MULTI-ACCESS EDGE COMPUTING (MEC)

- A kis késleltetésű rendszerek kulcsa az információ közeli ponton történő feldolgozása.
- A lehetséges megoldás: Multi-access Edge Computing, korábban: Mobile Edge Computing (MEC)
- A hálózat peremén működő autonóm feldolgozó egység
- Szerepe lehet pl. a közlekedési infrastruktúrában (önvezető autók, váratlan közlekedési információk stb.)
- Közvetlenül a RAN hálózat adatainak a feldolgozása a központi rendszer beavatkozása nélkül Igen kis késleltetés (!)
- A teljes hálózat számára csak az aggregált adatok kerülnek megadásra – itt már a késleltetés nem lényeges
- Több helyen nevezik „fog computing”-nak is

A MEC ÉS AZ EDGE CLOUD BIZTONSÁGA

- A hálózaton akár több száz vagy több ezer MEC is működhet
- Lehetséges támadási pontok:
  - Nem biztonságos felhordóhálózat a MEC és a RAN hálózat elemei között
  - Amennyiben a MEC és a maghálózat nyilvános interneten van összekapcsolva, akkor támadás az internet felől
  - Megosztott infrastruktúra használata harmadik felek alkalmazásainál

A KVANTUMBIZTOS KRIPTOGRÁFIA BELÉPÉSE

Küszöbön áll a kvantumszámítógépek kereskedelmi megjelenése

- A jelenlegi rendszerekhez képest drasztikus kapacitás- és sebességnövekedés
- A nagy számítási igény által védett kriptográfiai megoldások ezzel pillanatok alatt feltörhetővé válnak
- Peter Shor (1994): az RSA, az ECDSA, az ECDH és a DSA törhetővé válik
- Helyettük poszt-kvantum titkosításra van szükség
- Erre tavaly év vége óta már van hazai jogszabály is (2013. évi L. tv.)
- A világ első poszt-kvantum 5G SIM kártyája: IDEMIA 2021. dec.

Az 5G szabványosítás és következményei a biztonságra

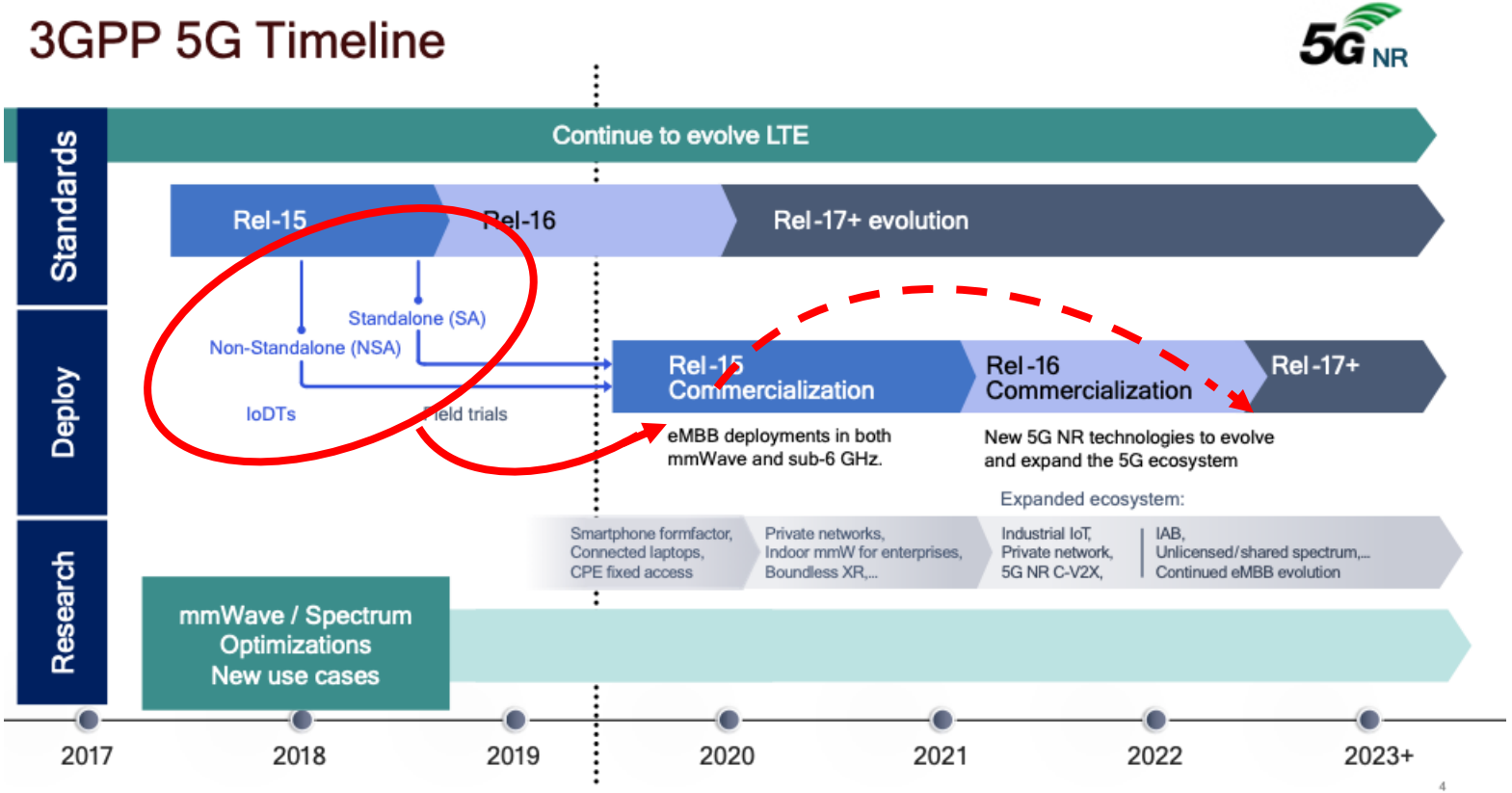
A 3GPP FELADATMEGOSZTÁSA ÉS MUNKACSOPORTJAI

Rádiós hozzáférési hálózat (RAN) TSG	Szolgáltatási/Rendszer Aspektusok (SA) TSG	Maghálózat & végberendezés (CT) TSG
RAN WG1 Layer 1 (Physical) space	SA WG1 Service requirements	CT WG1 Mobility management, Call control, Session management
RAN WG2 Layer 2 and 3 protocols	SA WG2 Architecture	CT WG2 Policy, QoS and interworking
RAN WG3 Access network interfaces +O&M	SA WG3 Security	CTWG3 Network protocol
RAN WG4 Performance requirements	SA WG4 Codecs, multimedia system	CT WG4 Smart card application
RAN WG5 UE conformance testing	SA WG5 Telecom management	
RAN WG6 Legacy RAN	SA WG6 Mission-critical services	

A 3GPP FELADATMEGOSZTÁSA ÉS MUNKACSOPORTJAI

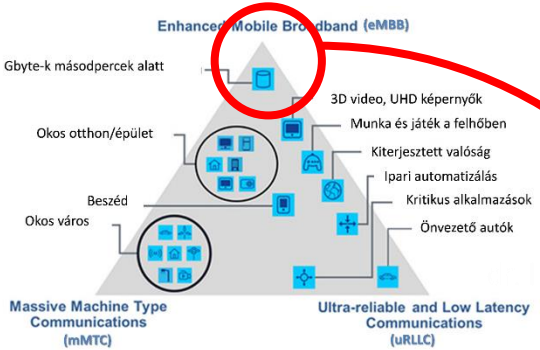
Rádiós hozzáférési hálózat (RAN) TSG	Szolgáltatási/Rendszer Aspektusok (SA) TSG	Maghálózat & vég-berendezés (CT) TSG
RAN WG1 Layer 1 (Physical) space	SA WG1 Service requirements	CT WG1 Mobility management, Call control, Session management
RAN WG2 Layer 2 and 3 protocols	SA WG2 Architecture	CT WG2 Policy, QoS and interworking
RAN WG3 Access network interfaces +O&M	SA WG3 Security	CTWG3 Network protocol
RAN WG4 Performance requirements	SA WG4 Codecs, multimedia system	CT WG4 Smart card application
RAN WG5 UE conformance testing	SA WG5 Telecom management	
RAN WG6 Legacy RAN	SA WG6 Mission-critical services	

A TYÚK VAGY A TOJÁS PROBLÉMA ÉS MEGOLDÁSA
5G Non Standalone és 5G Standalone New Radio



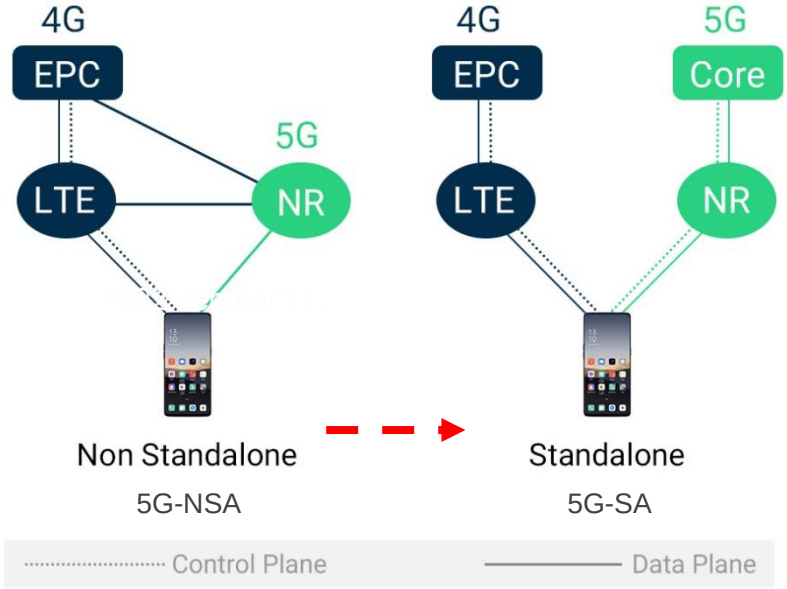
A TYÚK VAGY A TOJÁS PROBLÉMA ÉS MEGOLDÁSA

5G Non Standalone és 5G Standalone hálózat



ITU-T követelmények

4G hálózat + 5G NR (New Radio)
ez legyen a kezdeti megoldás



- A megoldás tökéletes az induláshoz, de megtartja a 4G hálózat korlátait.
- Amíg ezek a korlátok nem zavaróak, addig növelhető az eMBB, a mobil szélessáv élménye.
- Az 5G többi előnye viszont csak az 5G standalone hálózaton tud érvényesülni.

A SZABVÁNYOSÍTÁSI MENETREND KÉT FONTOS KÖVETKEZMÉNYE

Első következmény:

- A Non Standalone rendszerek még a 4G rendszer biztonsági szintjét képviselik, csak a rádiós hozzáférési hálózatban jelenik meg az 5G rendszer

Második következmény:

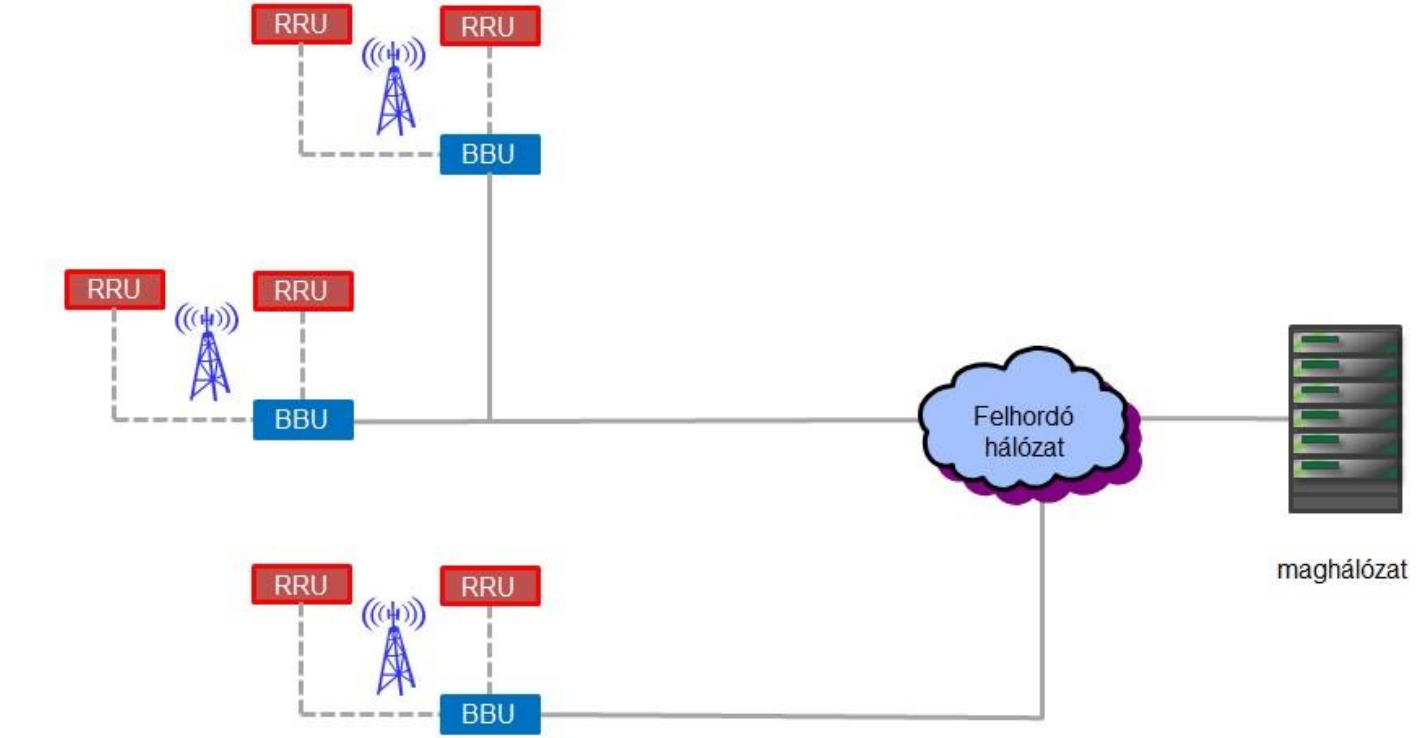
- A teljes – végtől végig terjedő – biztonsági megoldások csak a Release 17 bevezetésétől lesznek jelen a hálózatban
- A Release 17 befagyasztása 2022. március végén megtörtént, de még egy-másfél év, mire tömegesen is megjelenhet
- Jelenleg a világon döntő többségében NSA rendszerek üzemelnek a világban, így Magyarországon is

Az Open RAN kezdeményezés biztonsági kérdései

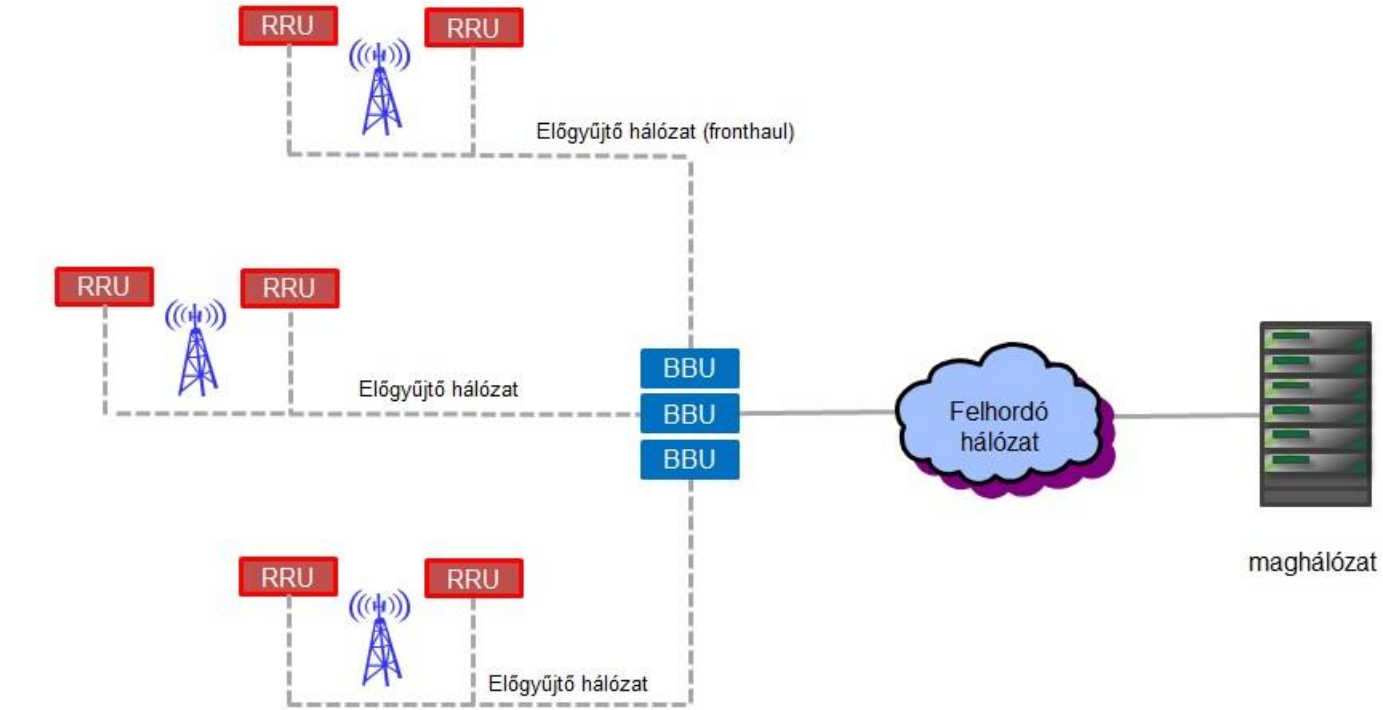
AZ OPEN RAN KEZDEMÉNYEZÉS HÁTTERE

- A beszállítók rendszerei olyan specifikus interfészeket használnak a megosztott RAN hálózatban, ahol a belső interfészek nem egységesek
  - Következmény: a kiválasztott beszállító kvázi monopolhelyzetbe kerül
  - Megoldására magalakult az O-RAN Alliance és olyan interfészt dolgoztak ki, ahol a RAN hálózat elemei beszállító-függetlenek
- Az EU Toolbox on 5G cybersecurity egyik kívánalma:
  - Biztosítják, hogy minden szolgáltató megfelelő, több értékesítőre kiterjedő stratégiával rendelkezzen **az egyetlen beszállítótól** (vagy több, hasonló kockázati profillal rendelkező beszállítótól) **való jelentős függés elkerülése vagy korlátozása érdekében**, így biztosítva nemzeti szinten a beszállítók közötti megfelelő egyensúlyt és **elkerülve a magas kockázatúnak tekintett beszállítóktól való függést**; ehhez el kell kerülni az egyetlen beszállítótól való függést, többek között a berendezések nagyobb interoperabilitásának előmozdítása révén;

A HAGYOMÁNYOS RAN HÁLÓZAT

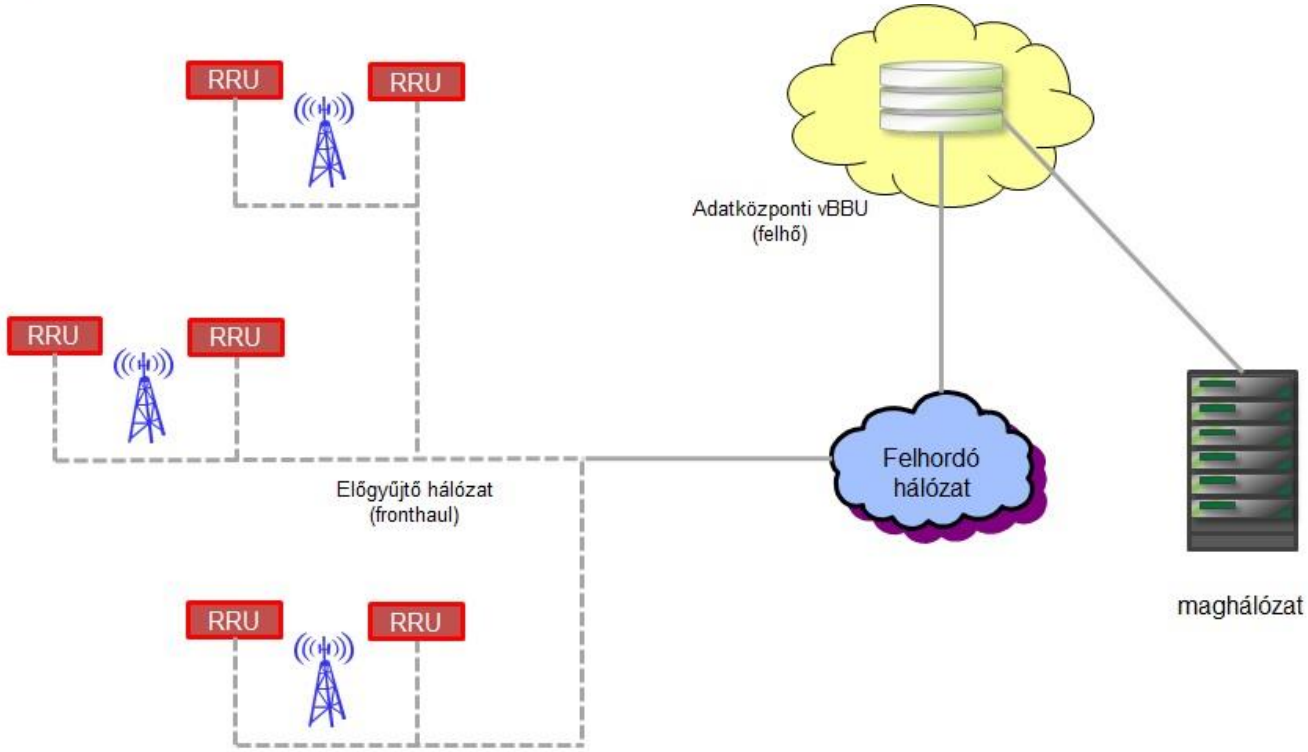


A KÖZPONTOSÍTOTT RAN HÁLÓZAT (BBU HOTELING)



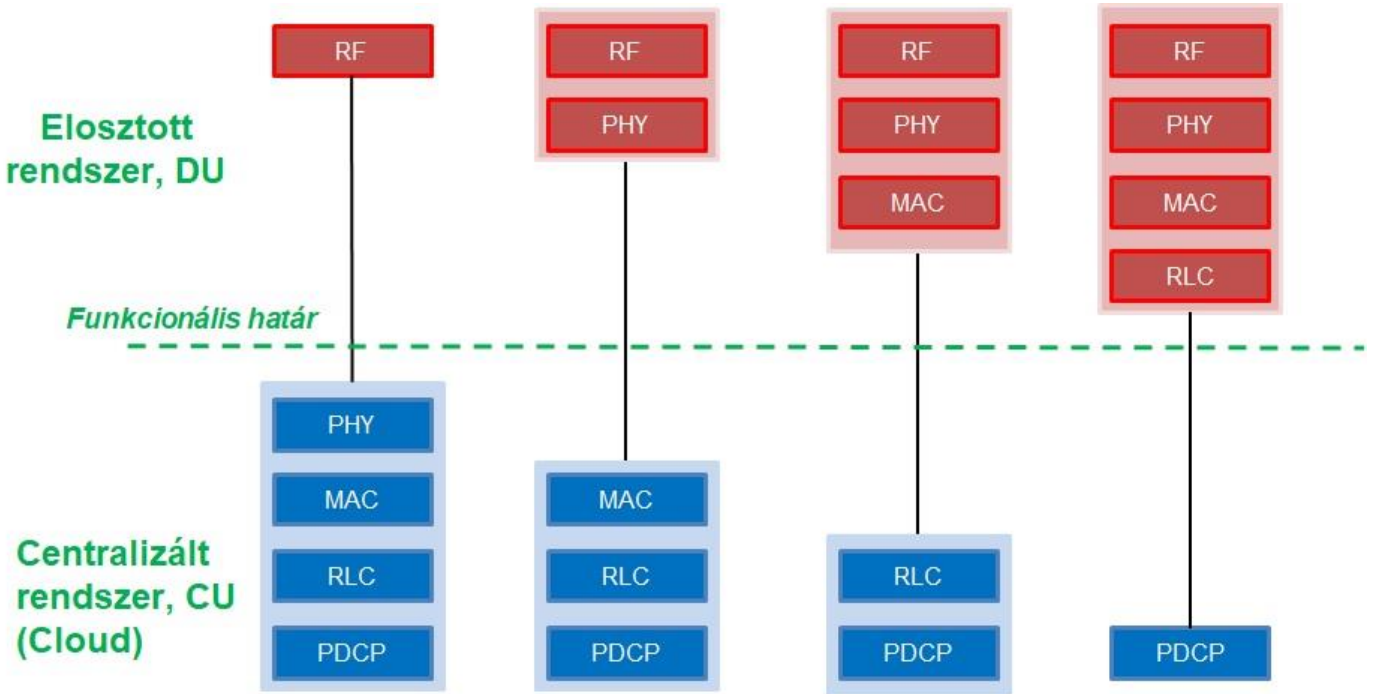
RRU – Radio Remote Unit BBU – Baseband Unit

A FELHŐALAPÚ C-RAN AZ 5G HÁLÓZATOKBAN

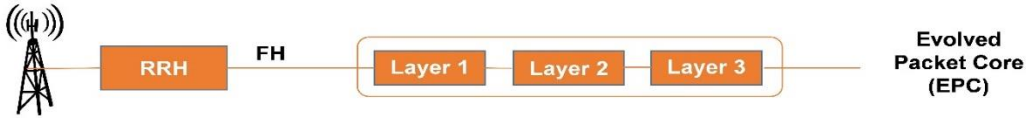


RRU – Radio Remote Unit BBU – Baseband Unit vBBU – virtual Baseband Unit

A RÁDIÓS EGYSÉG LEHETSÉGES MEGOSZTÁSI MÓDJAI



A GYÁRTÓFÜGGŐ MEGOLDÁSOKTÓL AZ O-RAN FELÉ



BBU

Gyártófüggő hardver és kialakítás
Nem támogatja több gyártó együttműködését

RRH – Radio Remote Head BBU – Baseband Unit FH - Fronthaul

DU

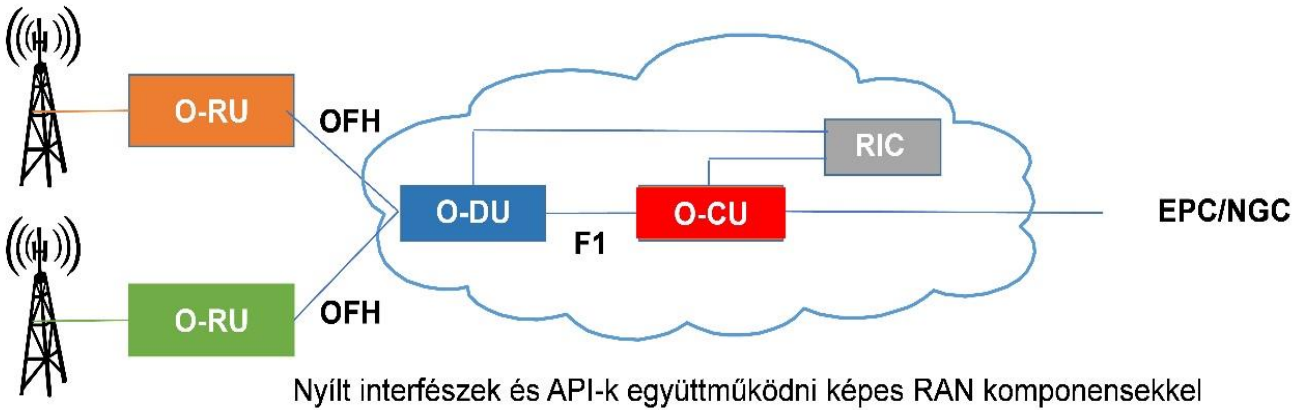
Gyártófüggő hardver
Nincs gyártói együttműködés

CU

Virtualizált gyártófüggő tervezés
Nincs gyártói együttműködés

RU – Remote Unit DU – Distributed Unit CU – Centralized Unit FH - Fronthaul

AZ O-RAN MEGOLDÁS ALAPGONDOLATA



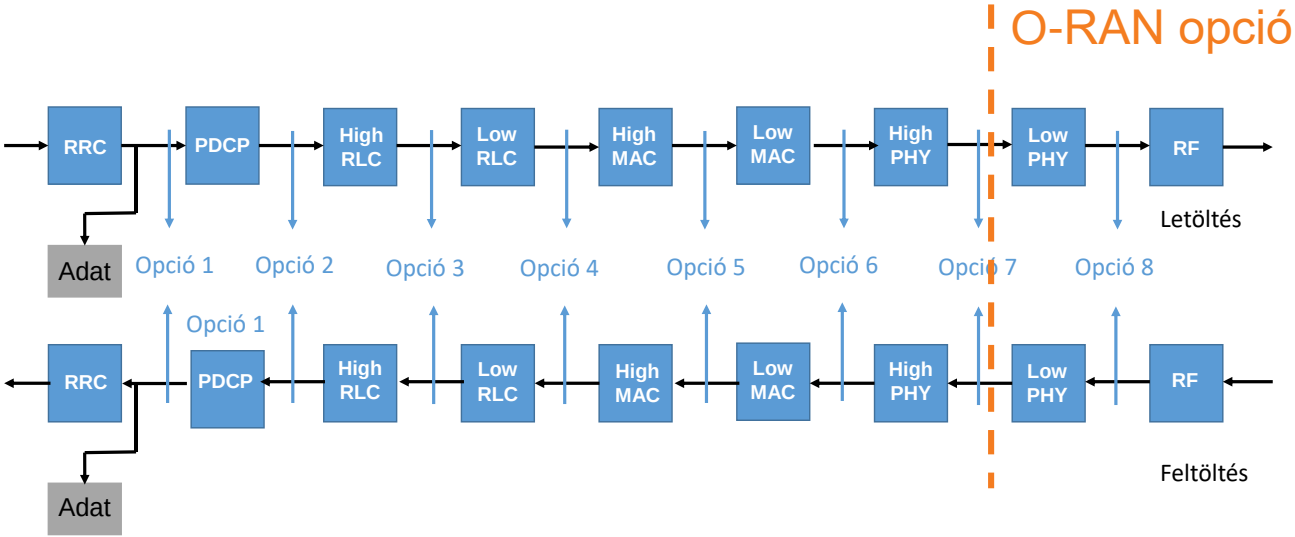
Nyílt interfészek és API-k együttműködni képes RAN komponensekkel
NFV modulok és referencia architektúra
Intelligencia és automatizmus a Plug and Play számára

O-RU – Open Remote Unit
OFH – Open Fronthaul

O-DU – Open Distributed Unit
RIC – RAN Intelligent Controller

O-CU – Open Centralized Unit

AZ O-RAN GYÁRTÓFÜGGETLEN MEGOSZTÁSI PONTJA



RRC – Radio Resource Control
PDCP – Packet Data Convergence Protocol
PHY – Physical

RLC – Radio Link Control
MAC – Medium Access Control
RF – Radio Frequency

AZ OPEN RAN BIZTONSÁGI KÉRDÉSEI

Az O-RAN Alliance intenzíven dolgozik a specifikáción
A felmerülő biztonsági kérdések:

- Az RU és a DU közötti integritás megteremtése biztonsági résektől mentesen, megfelelő titkosítási algoritmusok használata
- Egységes biztonsági rendszer kidolgozása a megosztott funkciókra
- Az egységes menedzsment rendszer biztonságos kialakítása TLS (Transport Layer Security) és digitális aláírás használatával
- Az O-RAN platformok, komponensek és alkalmazások teljes mértékű biztonsági rendszere

Ezeknek és más felmerülő biztonsági kérdéseknek a kezelésére az O-RAN Alliance külön biztonsági csoportot hozott létre.

A hálózatszeletelés és a biztonság

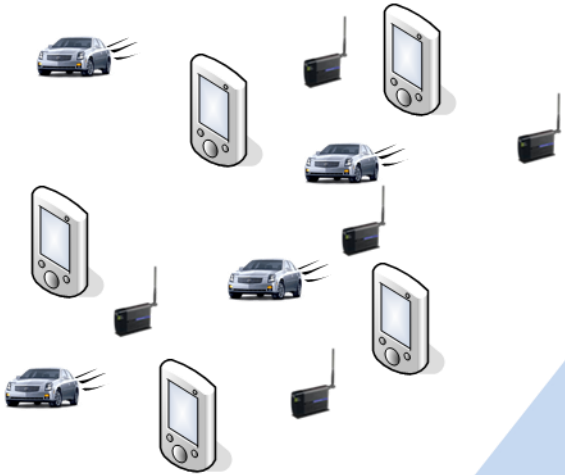
AZ ERŐFORRÁSOK OPTIMALIZÁLÁSA: A HÁLÓZATSZELETELÉS (NETWORK SLICING)

Az 5G hálózatoknak az egymással ellentétes követelményeket egyszerre kell kielégíteniük

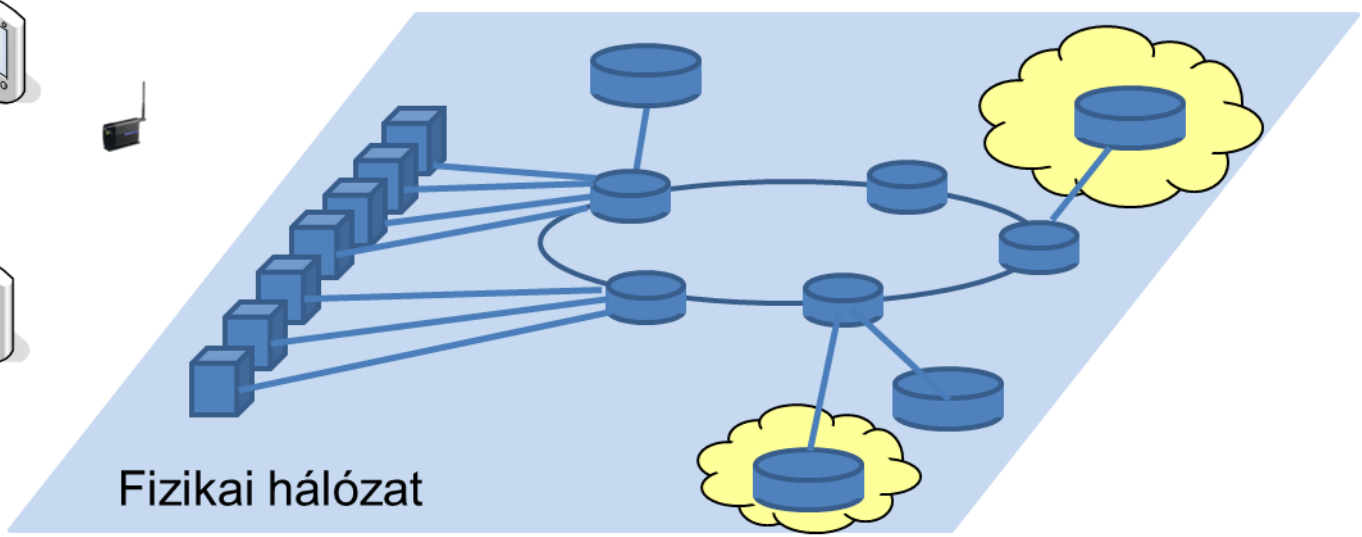
- Következmény: Olyan hálózat kell, melyben rugalmasan allokálhatók az erőforrások
- Az „ellentmondó” követelmények kezelésére az új elv a Network Slicing, a hálózatszeletelés elve
- A hálózatszeletelés elve lehetőséget ad a szolgáltatóknak arra, hogy az alkalmazási szükségletnek megfelelően optimalizált, végtől-végig terjedő virtuális hálózatot hozzon létre a szükséges mennyiségű erőforrással

Hogy néz ez ki a gyakorlatban?

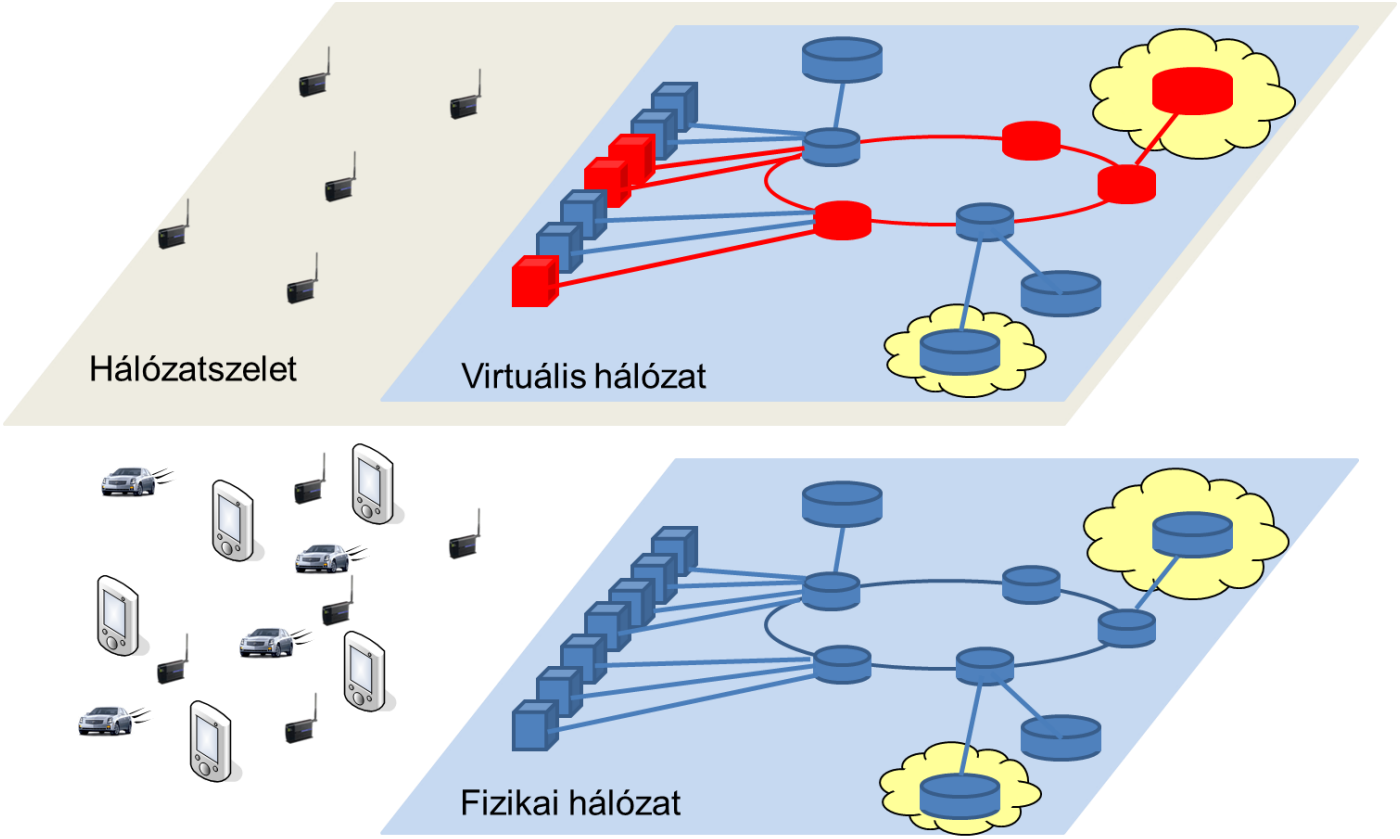
A HÁLÓZATSZELETELÉS ELVE
A fizikai hálózat és a különböző végberendezések



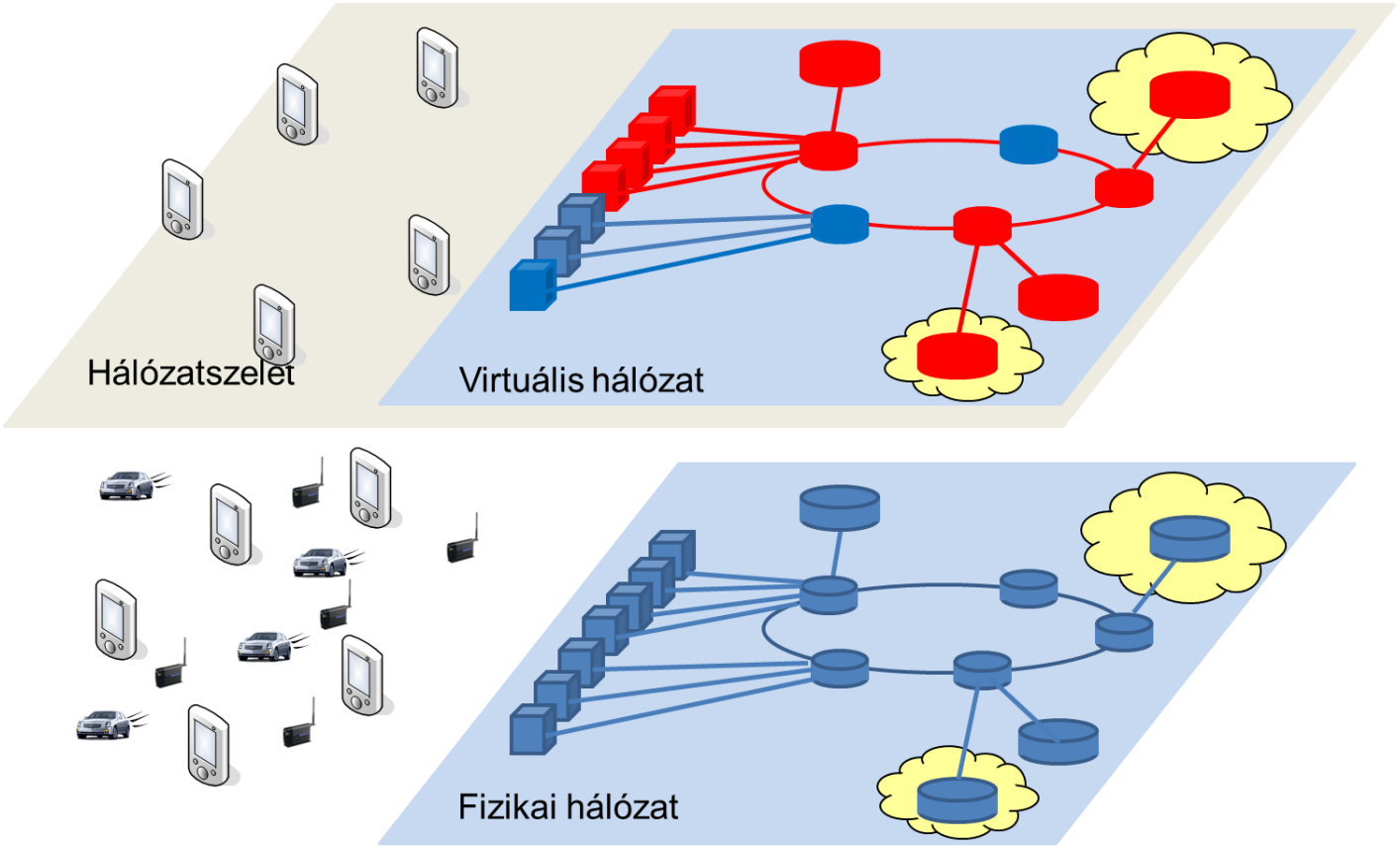
Végberendezések



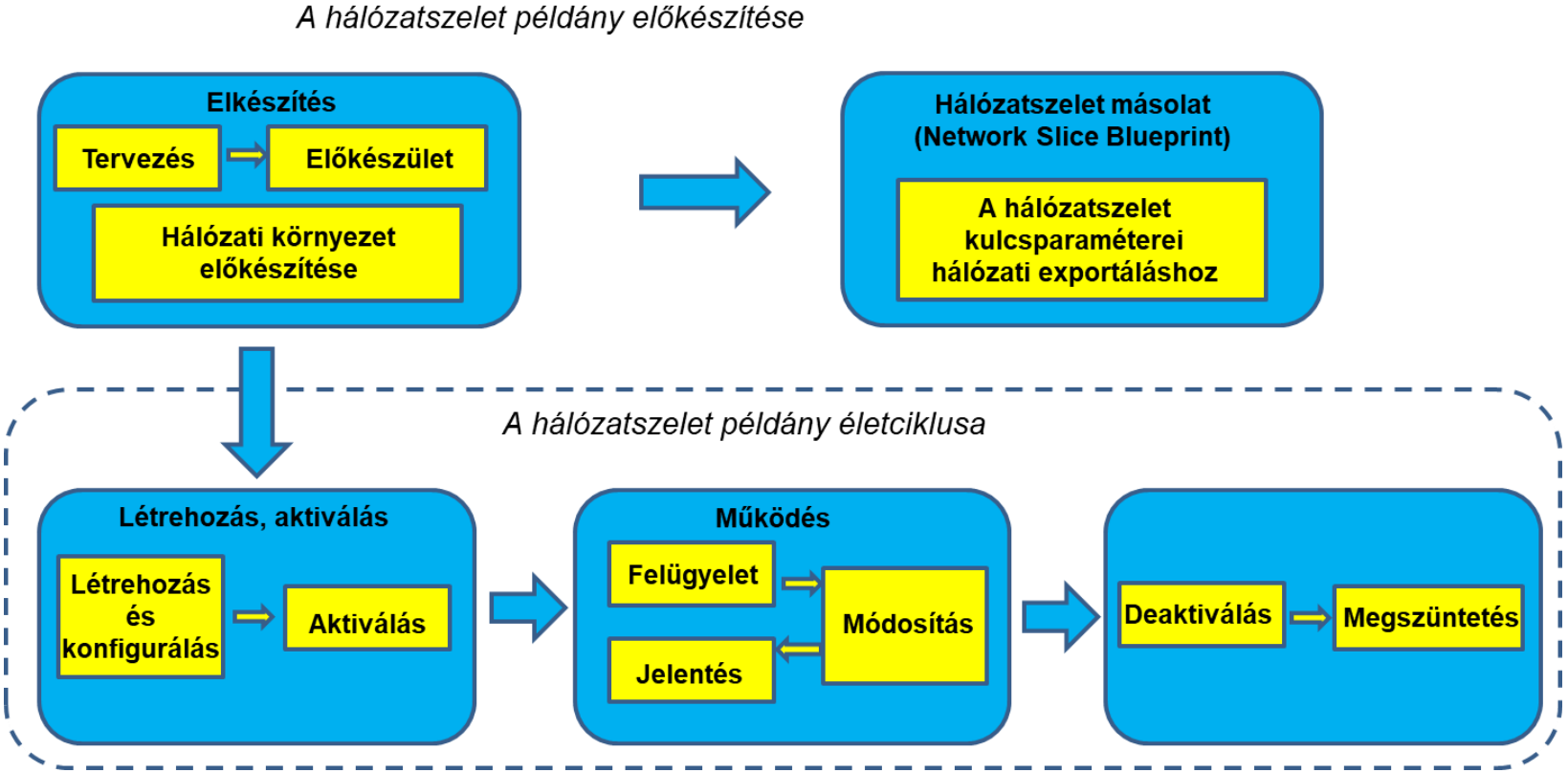
A HÁLÓZATSZELETELÉS ELVE
IoT szenzorok hálózatszelete (példa)



A HÁLÓZATSZELETELÉS ELVE
Mobil telefonok hálózatszelete (példa)



AZ 5G HÁLÓZATSZELET ÉLETCIKLUSA



A HÁLÓZATSZELETELÉS ÉS A BIZTONSÁG

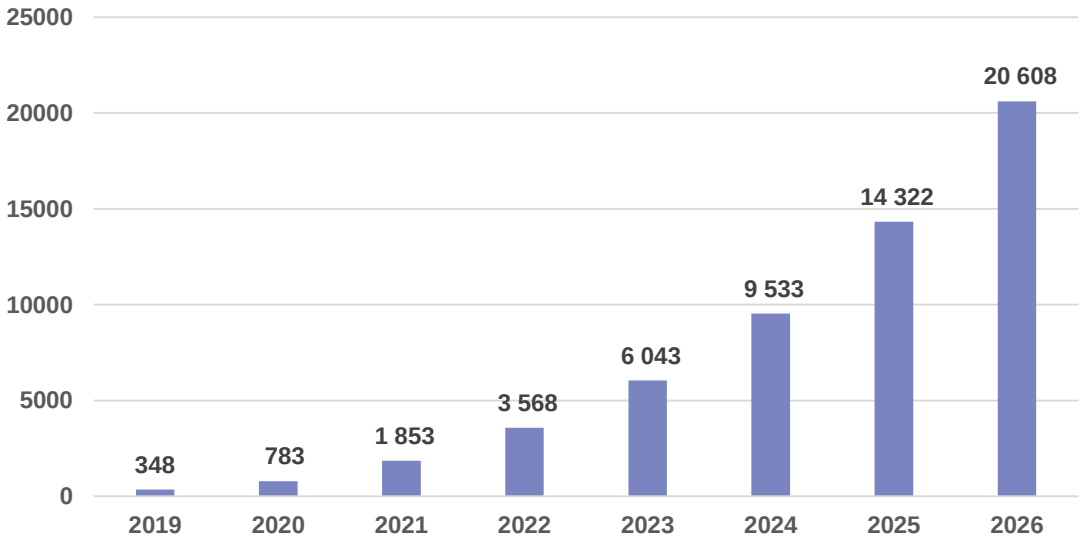
A hálózatszeletelés tehát az erőforrások optimális kiosztását hivatott megvalósítani

- Az erőforrások egy része a felhőnatív megoldásokban bővíthető
- Az erőforrások más része ugyanúgy korlátos, mint eddig (pl. átviteli kapacitások)
- Az ideális hálózatszeleteléshez célszerű a mesterséges intelligencia képességeit (is) használni
- Megakadályozandó viszont, hogy szélsőséges vagy hamis igényekkel egy hálózatszelethez indokolatlan mennyiségben rendeljen hozzá erőforrásokat – erre az orkesztrációs rendszernek is fel kell készülnie

Az 5G magánhálózatok és a biztonság

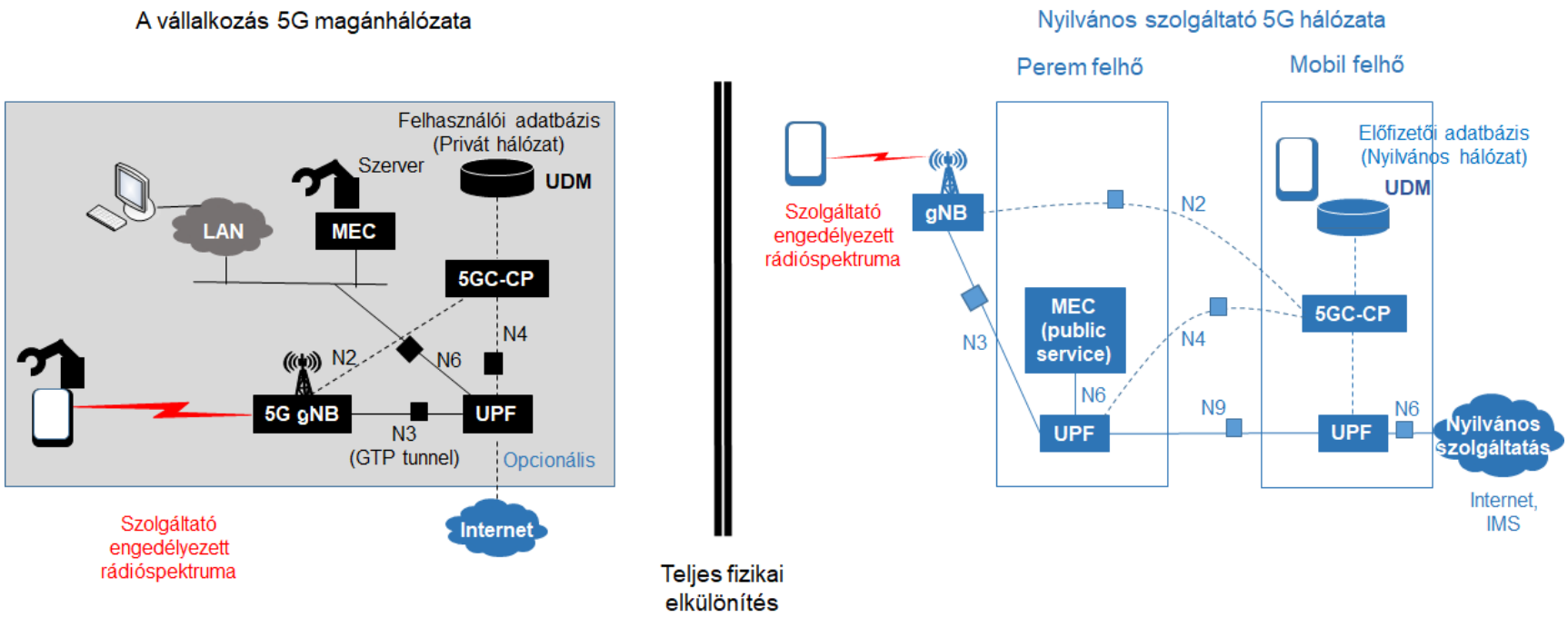
AZ 5G MAGÁNHÁLÓZATOK TERJEDÉSE

A magánhálózatok terjedése és az Ipar 4.0 kiszolgálása egy markáns trend, amit az 5G rendszerek fognak kiszolgálni



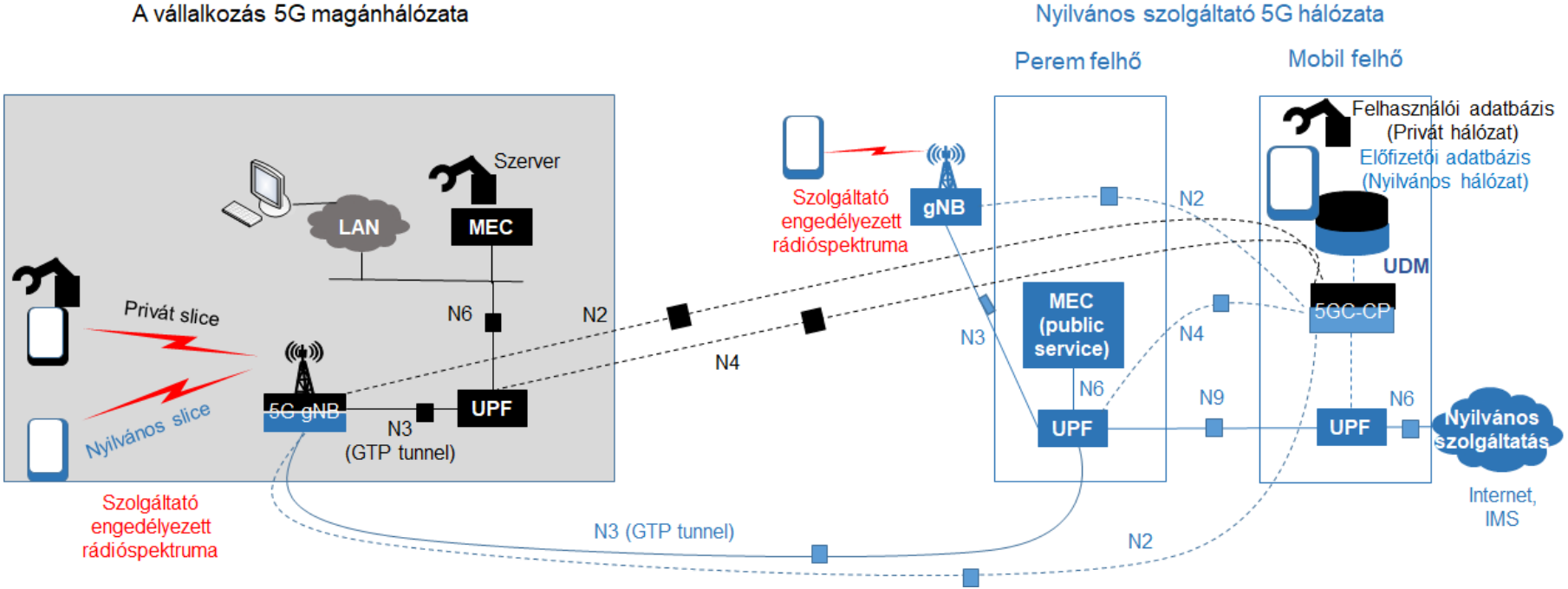
Forrás: Analysys Mason, 2021

A TELJES IPARI BIZTONSÁG…



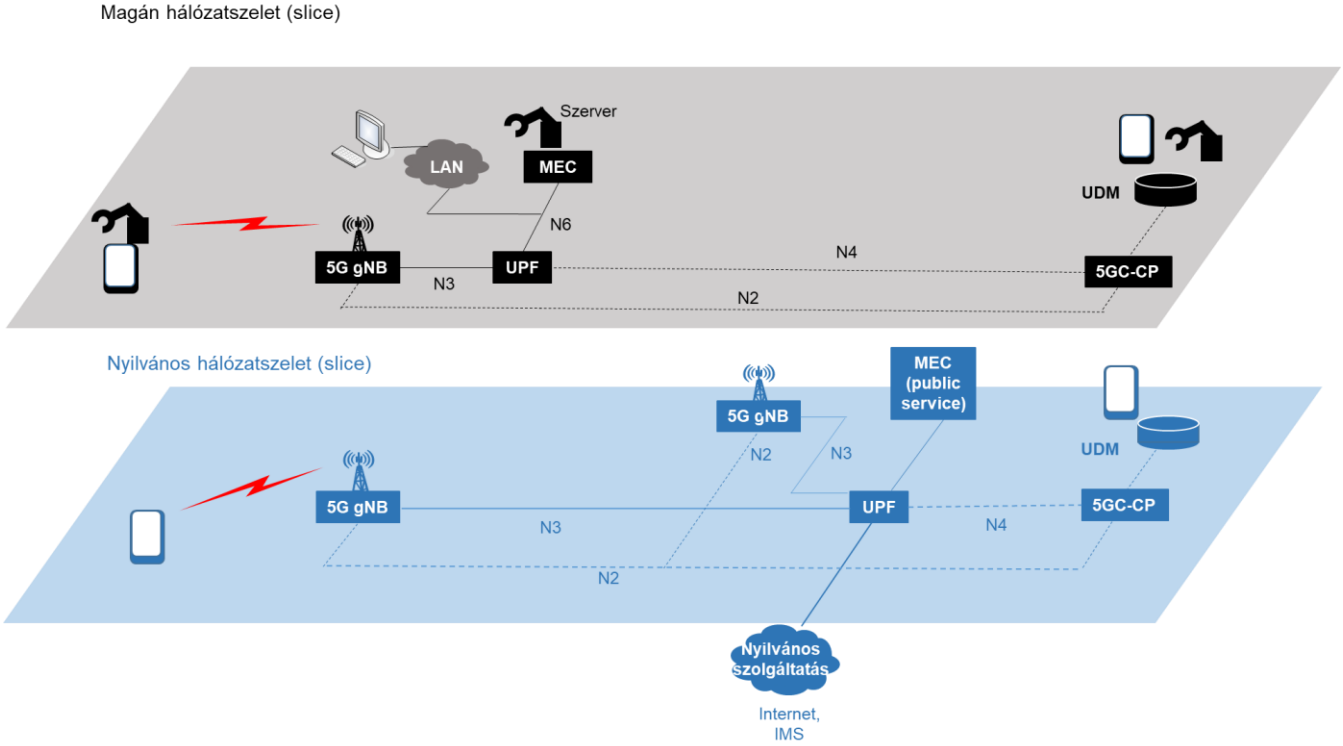
AZ IPARI ADATOK BIZTOSÁGA HÁLÓZATSZELETELÉSSEL

A RAN hálózat és a vezérlési sík megosztása egy üzem és a nyilvános hálózat között



AZ IPARI ADATOK BIZTONSÁGA HÁLÓZATSZELETELÉSSEL

A RAN hálózat és a vezérlési sík megosztása egy üzem és a nyilvános hálózat között



AZ IPARI ADATOK BIZTONSÁGA HÁLÓZATSZELETELÉSSEL

A megoldás lényege:

- A nyilvános szolgáltató nyújtja a vezérlési sík funkciókat, a nyilvános mobil hozzáférés RAN hálózatát és a szükséges frekvenciaspektrumot
- A magánhálózat kezeli az adatsíkot, az adatok így nem mennek ki a gyárkapun kívülre
- Az SLA-t helyben lehet biztosítani, bár a hálózat kezelését a nyilvános szolgáltató látja el

Köszönöm a figyelmet!