ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD)
ÉRTEKEZÉSTERVEZET

KÚN GERGELY OTTÓ

Magas megbízhatóság kialakítása a korszerű vasúti kommunikációban

Témavezető: Dr. Wührl Tibor PhD

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025. március 31.

TARTALOMJEGYZÉK

BEVEZETÉS

Szakmai munkám során több éve foglalkozom infokommunikációs hálózatokkal, azok protokoll elemeivel. Az információ átvitelt biztosító hálózatok napjainkra már szinte teljesen digitalizáltak, vagyis az információk bitek segítségével kerülnek átvitelre. ’1’ és ’0’ értékekre alakítunk át bármilyen adatot felhasználástól függetlenül, legyen az beszédjel, video-jelfolyam, vagy gépek, berendezések közötti kommunikáció.

A korszerű vasúti rendszerek biztosító berendezései, valamint a vonatbefolyásoló rendszerek komponensei is digitális infokommunikációs infrastruktúrát használnak a kommunikációra. Ezen és hasonló ipari rendszerek működésbiztonságának megvalósítása korunk jelentős kihívásai közé tartozik.

A vasúti közlekedés hatékonyságának és biztonságának növelésére irányuló globális igény eredményeképp újabb és újabb innovációk kerültek alkalmazásba. A kezdeti időkben a jelző- és biztosítóberendezések mechanikus rendszerek voltak, amelyek kézi vezérléssel működtek. Az első ilyen rendszerek közé tartoztak a forgalmisták által manuálisan állítható váltók és jelzők, amelyek mechanikai összeköttetéseken alapultak.

Az elektromosság megjelenésével a mechanikus rendszereket elektromos jelző- és biztosítóberendezések váltották fel, amelyek nagyobb távolságokban is hatékonyan működtek. Az 1930-as években kezdtek elterjedni a (jelfogós) relés rendszerek, amelyek összetett logikai kapcsolások (alapáramkörök) révén biztosították a vonatok útvonalának vezérlését és a térközök biztosítását – a vágányfoglaltság felügyeletét és ezzel az ütközések elkerülését.

A relés rendszereket követően a számítógépes technológia megjelenése újabb mérföldkövet jelentett. Az 1970-es évektől kezdődően a számítógép alapú biztosítóberendezések (Computer-Based Interlocking, CBI) fokozatosan felváltották a relés technológiát. Ezek a rendszerek digitális jelfeldolgozást alkalmaznak, így megbízhatóbban, gyorsabban és hatékonyabban kezelik a vonatok mozgásának vezérlését és felügyeletét. A számítógép alapú megoldások lehetővé teszik a komplexebb és rugalmasabb vezérlést, a központosított távoli felügyeletet, az automatikus diagnosztikát. Legfontosabb jellemzőként pedig jelentősen csökkentik az emberi hiba előfordulásának lehetőségét. [35]

Napjainkban a modern számítógép alapú biztosítóberendezések integrált rendszereket alkotnak, amelyek nemcsak a vasúti pályaelemek, hanem a járművek és a forgalom teljes körű felügyeletét is lehetővé teszik. A vasúti közlekedés teljes automatizálását és biztonságának növelését az Automatic Train Control (ATC) fejlesztések célozzák meg. Az

ATC rendszerek világszerte számos országban működnek, különböző változataik és szintjeik léteznek, különböző vasúti és metróhálózatokon találhatók meg. [20]

Európában az European Train Control System (ETCS) kiépítése zajlik, mellyel – a megvalósított szinttől függően – valós időben nyomon követhetők a vonatok pozíciói, állapot adataik, továbbá a közlekedésükre vonatkozó utasítások és parancsok továbbíthatók, ezzel biztosítva a vasúti közlekedés akár teljes körűen automatizált, biztonságos és hatékony működését. A GSM-R (Global System for Mobile Communications – Railway) biztosítja az ETCS által igényelt vezeték nélküli kommunikációs infrastruktúrát, amely a modern vasúti forgalomirányítás egyik kulcseleme. A GSM technológia egyfelől kiforrottnak, robosztusnak mondható, másfelől viszont elavultnak mondható. Az 5G részben már a jelen és a közeli jövő technológiája, amely a vasúti kommunikáció következő generációját képviseli, és FRMCS (Future Railway Mobile Communication System) néven a GSM-R utódja lesz. [9,21]

A vasúti szektorban az automatizált, hatékony működést jelenleg számos infokommunikációs hálózat biztosítja, köztük számos hálózat továbbít olyan fontos információkat, amelyeken közvetlenül, vagy közvetetten emberéletek is múlhatnak. Emiatt nagyon fontos, hogy a továbbítandó információkat a kritikusságuk szerint osztályozzuk és megfelelő hálózatok kialakításával biztosítsuk a célba érésüket. [1,2]

Jelen értekezéstervezet arra keresi a választ, hogy a folyamatosan változó technikai és technológiai háttér, a szabványosítási törekvések, valamint a szakma által kialakított bevált gyakorlatok elvárásai hol és milyen módon találkoztathatók annak érdekében, hogy mindezek vegyítése a korábbinál korszerűbb, megbízhatóbb és a jövőbeni kihívásoknak is megfelelő rendszert eredményezzen. [6,47,48,49]

Az értekezéstervezet szerkezetének áttekintése

Munkám első fejezete a vasúti infokommunikációs rendszerekre vonatkozó szabványok, szabályozások és szakmai előírások áttekintésével alapozza meg a kutatásom tárgyát képező technológiai környezet bemutatását. Részletesen bemutatom az ETCS rendszert és kiszolgáló elemeiket, azok működését, mert jelenleg ennek alkalmazása határozza meg a vasúti hálózatok kritikus kommunikációs hálózatának működését.

A második fejezet a megbízható hálózati működés megvalósításához szükséges jelenlegi és néhány jövőbeli technikai megoldásokat mutat be. Foglalkozik a redundáns adatátvitel kialakításának lehetőségeivel, a késleltetés és szinkronizáció problémáival, valamint az időkritikus kommunikációs, azaz a determinisztikus hálózatok, követelményeinek kielégítésére szolgáló modern technológiákkal, mint például az MPLS, TSN és az IEEE 1588-alapú szinkronizációs megközelítések.

A harmadik fejezet a vasútbiztonságot megvalósító pályamenti építőelemeket és azok infokommunikációs kapcsolatait tárgyalja. Elemzi a kritikus és nem kritikus hálózati interfészeket, azok fizikai megvalósítását (optika, réz, vezeték nélküli átviteli közegek), valamint ezek megfeleltetését az egyes alkalmazott és alkalmazható technológiákkal. Ez a fejezet képezi az első tudományos tézisem alapját.

A negyedik fejezet a vasúti infokommunikációs hálózatokat veszélyeztető technikai tényezőket vizsgálja. Kitér a késleltetés, a csomagvesztés, a hibás konfiguráció és monitoring hiányosságainak hatásaira, valamint azokra a veszélyforrásokra, amelyek a hálózat megbízhatóságát és biztonságát csökkenthetik. A feltárt problémakörök a második tudományos tézis hátterét adják.

Az ötödik fejezet a korábbi elemzésekre építve információbiztonsági irányelveket fogalmaz meg a vasúti kommunikációs rendszerek számára. Ezen irányelvek célja a hibatűrés és megbízhatóság növelése és a kapcsolatos időtényezők csökkentése. Ez a fejezet szolgál a harmadik tudományos tézis alapjául.

Következő részekben az összegzett következtetések, az új tudományos eredmények, valamint az ajánlások és javaslatok találhatók. Az értekezéstervezet végén az irodalomjegyzék, kiegészítve tudományos közleményeimmel, foglalnak helyet, majd a táblázatok, ábrák és rövidítések jegyzéke és a köszönetnyilvánítás következnek.

A tudományos probléma megfogalmazása

A közelmúltban és napjainkban történt infokommunikációs fejlődés felgyorsította, felgyorsítja életünket. A modern digitális eszközök, vezetékes – elsősorban optikai – és rádiós átviteli módszerek fejlődése egyre nagyobb információtömeg szállítását teszi lehetővé minden másodpercben. Néhány évtizede elképzelhetetlen volt, hogy ilyen nagy adatmennyiség egyáltalán keletkezhet-e, de jelenleg a technológiák képességeinek, kapacitásának fejlődése és az adatmennyiség növekedése egy öngerjesztő folyamattá vált.

A vasúti közlekedés biztonságát biztosító rendszerek digitalizációja is megtörtént. A kezdetekben alkalmazott mechanikus biztosítási megoldásokat követték az elektromos, majd elektronikus áramkörökön alapuló megoldások. Napjainkra a digitális kommunikációs megoldások is egyre nagyobb teret nyernek a vasúti eszközök és rendszerek kommunikációjában. A digitális átállás nem csupán új technológiák bevezetését jelenti, hanem alapvető szemléletváltást is igényel a biztonságkritikus rendszerek tervezésében, kiépítésében és üzemeltetésében. A vasúti közlekedést kiszolgáló hálózatokban az új szemlélethez való helyes alkalmazkodás különösen fontos, mivel a hagyományosan hosszú életciklusú, magas megbízhatóságra optimalizált rendszerek helyett új, gyorsan fejlődő, sok esetben eredetileg kereskedelmi célra fejlesztett digitális technológiák kerülnek beépítésre. Ez számos technikai és rendszerszintű kihívást is felvet a megfelelő megbízhatóság és rendelkezésre állás tekintetében.

A kritikus infrastruktúrák hatékony működése és biztonsága kiemelt nemzetstratégiai jelentőséggel bír, hiszen ezek meghibásodása vagy kiesése súlyos következményekkel járhat a társadalom, a gazdaság és az állami működés szempontjából. Ezen belül a közlekedési és a vasúti közlekedés egyre nagyobb figyelmet kap, mivel mind személy-, mind áruszállítási szempontból alapvető szerepet játszik és egyre nagyobb súlyozást kap. A vasúti infrastruktúrák – ideértve a pályahálózatokat, a közlekedésirányító rendszereket és a kapcsolódó kommunikációs elemeket is – kritikusnak tekinthetők. A pályamenti elektronikus biztosító berendezések, valamint a vonatbefolyásoló rendszerek digitális kommunikációs hálózattal kapcsolódnak egymáshoz. Ezen hálózatokon közvetített információk hibátlan és megfelelő időben történő megérkezése elengedhetetlen a zökkenőmentes működéshez. Az információ „hatalom”, az információ hiány pedig sebezhetőséget, vagy akár teljes rendszer leállást is eredményezhet. [1,2]

Az információhiány több okból is felléphet: műszaki-technikai problémák (például interfészhiba, szoftveres meghibásodás, helytelen konfiguráció stb.) vagy emberi tevékenység következtében (mulasztás, szándékos károkozás, hálózati támadás). Kutatásomban elsősorban a műszaki eredetű problémákra fókuszálok: ezek elemzését, kategorizálását végzem el, és olyan módszereket, megoldásokat javaslok, amelyekkel csökkenthető az ebből eredő hibák előfordulásának valószínűsége és időbeli lefutása. A vizsgálatok középpontjában a vasúti kommunikációs rendszerek megbízhatósága áll, különös tekintettel az IP-alapú hálózatok működésére, ahol a késleltetés, a szinkronizáció és az adatforgalom menedzsmentjének technikai kérdései kulcsszerepet játszanak a rendszerbiztonság és megbízhatóság szempontjából. Maga az információ hiány fellépése komplex probléma csoport, mely sok és sokszor összetett problémaforrásra vezethető vissza, ezért nem kerülhető el, hogy az emberi tényezőkkel is foglalkozzak érintőlegesen.

Kutatásom célja nem csupán a problémák azonosítása és kategorizálása, hanem olyan konkrét irányelvek és javaslatok megfogalmazása is, amelyek segítségével optimalizálhatók az új technológiai kihívások alkalmazási problémái és mérsékelhetők a vasúti kommunikációs rendszereket érintő technikai és potenciális veszélyforrások hatásai. Ezek az irányelvek támogatást nyújthatnak a rendszertervezők, üzemeltetők és döntéshozók számára egy megbízhatóbb, rugalmasabb és ellenállóbb kommunikációs infrastruktúra kialakításában.

Célkitűzések

A vasúti pályamenti rendszerek kommunikációs interfészeinek átfogó feltérképezése és rendszerezése annak érdekében, hogy képet adjak az egyes alrendszerek közötti kapcsolatok sajátosságairól és az ezeket megfelelő szinten kiszolgáló interfésztechnológiákról.

A rendszerezett kommunikációs interfészek potenciális veszélyforrásainak beazonosítása és vizsgálata elsősorban olyan kockázatok terén, amelyek a hálózati kommunikációs kapcsolatok, vagy az adatcserén alapulnak.

A beazonosított kommunikációs rendszerekre vonatkozó veszélyforrásokkal szemben megelőző védelmi intézkedések meghatározása, amelyek hozzájárulnak a vasúti infokommunikációs rendszerek működésbiztonságának és megbízhatóságának növeléséhez.

A téma kutatásának hipotézisei

Az alábbi hipotéziseket fogalmaztam meg:

I. Hipotézis

Feltételeztem, hogy vasútbiztonsági megfontolások alapján a pályamenti rendszerek releváns kommunikációs interfészei rendszerezhetők és ez a rendszerezés útmutatást ad az egyes komponensek összekapcsolásánál célszerűen alkalmazandó interfésztechnológiák vonatkozásában.

II. Hipotézis

Feltételezem, hogy a rendszerbe sorolt vasútbiztonsági szempontból releváns interfészek potenciális veszélyforrásai beazonosíthatók.

III. Hipotézis

Feltételezem, hogy a felderített veszélyforrások ellen megelőző védelmi intézkedések tehetők, mellyel növelhető a működésbiztonság.

Kutatási módszerek

Az értekezés tématerületet áttekintő részében már létező és publikált tudományos eredményeket ismertetek, melyekre alapozva keresem a korszerű kommunikációs technológiák és a magas megbízhatóság közös halmazát, melyek rendszerezése és kategorizálása vasúti kontextusban a kitűzött cél. Kutatómunkám során a kapcsolódó szakterületeket kvalitatív, kvantitatív és empirikus módszerekkel térképeztem fel. Az általam meghatározott kutatási célok eléréséhez tudományos cikkek, szabványok, esettanulmányok, valamint saját tapasztalataim és vizsgálataim eredményeit használtam fel.

A kutatómunka meghatározóbb módszerei:

- Kutatómunkám kezdetén a témát érintő alapinformációk gyűjtését és rendszerezését végeztem a hazai és nemzetközi szabványok, rendeletek, esettanulmányok és szervezetek nyilvánosan elérhető publikált adataiból.
- Irodalomkutatást végeztem a vasúti kommunikációt megvalósító rendszerekről nyílt forrásból elérhető hazai és idegennyelvű publikációk, szabványok, rendszerdokumentációk és a vonatkozó jogszabályok tekintetében.
- Interjúkat készítettem, konzultáltam a kutatásom témakörét érintő szervezetek munkatársaival, többek között a vasúti biztosító berendezéseket üzemeltető és tanúsító kollégákkal és a távközlési és informatika hálózat tervezéséért és kivitelezéséért felelős szervezetek képviselőivel.
- Munkám során a tanúsított vasúti berendezések kommunikációinak, alkalmazott interfészeinek kialakításával kapcsolatos tapasztalatokat gyűjtöttem és használtam fel kutatásomban.
- Áttekintettem gyártóspecifikus megoldásokat a magas megbízhatóságot megvalósító kommunikációs hálózatokra.
- A napi oktatói, mérnöki, kutatói és ellenőrző, irányító és jelző (CCS) szakterületen tanúsítói munkám során folyamatosan figyelem az aktuális trendeket, mellyel a kutatási témám aktualitásának fenntartását biztosítottam.

Alaki és formai megjelenés

A disszertációmban felhasznált szakirodalmi forrásokat, ábrákat és képeket a törzsszövegben, az előfordulásuk sorrendjében, a műszaki szakirodalmi hivatkozások szabványának megfelelően [szögletes zárójelben], arab számokkal jelölve hivatkoztam, A hivatkozásokat az „Irodalomjegyzék" fejezetben rendszereztem sorszámuk alapján. Az értekezésben szereplő ábrákat a források feltüntetésével az „Ábra jegyzék" fejezetben, míg a táblázatokat a „Táblázat jegyzék" fejezetben soroltam fel, szintén a források megjelölésével. Az értekezéstervezet végén a szövegben található rövidítéseket ábécé sorrendben a „Rövidítés jegyzék" alatt tüntettem fel. Kutatási munkámat 2025. március 31-én zártam le.

1 INFOKOMMUNIKÁCIÓS HÁLÓZATOKKAL KAPCSOLATOS ELVÁRÁSOK, SZABVÁNYOK, IRODALOMKUTATÁS

A technológiai fejlődés a vasúti közlekedést támogató rendszerek területén is folyamatos. Az új technológiák bevezetésével szemben elvárás, hogy javítsák az addig elért biztonsági mutatókat, mivel a közlekedés minden ágazatában, így a vasútnál is elsődleges prioritás a biztonság. A vasúti rendszerekben a biztonságkritikus funkciók megvalósítását a biztosítóberendezések [5] látják el, amelyek még az egyszerűbb funkciók esetében is számítógépek vagy beágyazott vezérlőjű számítógépek hálózatát alkotják.

A vasúttársaságok általában országok szerint szerveződnek. A nemzeti vasúthálózat az adott ország teljes területét lefedi, ezért azt kiszolgáló kommunikációs hálózatoknak is szükséges lefednie az egész országot, vagy az üzemeltető szolgáltatási területét, biztosítva a megbízható kommunikációs szolgáltatásokat.

A vasutak kommunikációs rendszerei két fő kategóriába sorolhatók: a fedélzeti és a pályamenti rendszerek [9]. Kutatásom a pályamenti kommunikációs rendszerek kialakításának kérdéseire összpontosít, azonban figyelembe véve a két csoport együttműködésének alapvető fontosságát, a fedélzeti eszközökre vonatkozó főbb jellemzőket és kapcsolódási pontokat is vizsgálom a szükséges mélységben.

1.1 Vasúti előírások, szabványok áttekintése

Az ipar számos területén használt eszközöknek, berendezéseknek szükséges bizonyos biztonsági elvárásoknak megfelelni, a stabil, megbízható működés, vagy az emberi egészség, épség megóvásának érdekében. Iparágak szerint a tipikus elvárásokat szabványokba foglalták, amelyek a gyártók és beszállítók eszközeinek tekintetében kötelezően betartandó vagy opcionális elvárásokat fogalmaznak meg.

A Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission) által kiadott IEC 61508 [10] nemzetközi szabvány általánosságban tárgyalja az automatikus biztonságtechnikai rendszerek tervezésének, alkalmazásának, karbantartásának és működési módjainak elvárásait.

Az IEC 61508 szabványon alapuló funkcionális biztonsági szabványok négy, úgynevezett SIL szintet (Safety Integrity Levels) határoznak meg. Az egyes szinteknek megfelelő eszközök, meghibásodási valószínűségben különböznek. A meghibásodás valószínűségét alkalomszerűen használt eszköz esetén évre vonatkoztatva, vagy folytonos üzem esetén, órán belüli időegységre vonatkoztatják. Például egy SIL1-es szintnek megfelelő eszköz meghibásodási valószínűsége 0,01..0,1 között kell lennie éves szinten. Órára vetítve ez az érték $10^{-6}..10^{-5}$ közötti lesz folytonos üzemű rendszerek esetén. A SIL1 követelményei a leggyengébbek, a SIL4 követelmények a legszigorúbbak. A SIL 0 biztonságintegritási szint nem tartozik a szabvány hatálya alá. Az alábbi táblázat összefoglalja az egyes szintekhez tartozó, szabványban rögzített, meghibásodási valószínűségeket éves és órás skálára vetítve. A kockázat csökkentési tényező az éves meghibásodásból számítható reciprokképzéssel, ez a mutatószám indikálja, hogy adott szint alkalmazása hányad részére csökkenti a kritikus rendszerekben a hiba valószínűségét.

Biztonsági szint	**Hiba átlagos valószínűsége**		**Kockázat csökkentési tényező**
Safety Integrity Level (SIL)	**évente**	**óránként**	
SIL 4	10^{-5} … 10^{-4}	10^{-9} … 10^{-8}	10^{5} … 10^{4}
SIL 3	10^{-4} … 10^{-3}	10^{-8} … 10^{-7}	10^{4} … 10^{3}
SIL 2	10^{-3} … 10^{-2}	10^{-7} … 10^{-6}	10^{3} … 10^{2}
SIL 1	10^{-2} … 10^{-1}	10^{-6} … 10^{-5}	10^{2} … 10^{1}
SIL 0	10^{-1}	10^{-5}	10^{1}

1. táblázat. SIL szintek mutatószámai [10]

SIL	**Hiba a kontrolálhatóság szempontjából**	**Hiba a veszélyesség szempontjából**
4	Nem kontrolálható	Tömegkatasztrófa
3	Nehezen, csak bizonyos körülmények között kontrolálható	Több ember halála, súlyos sérülése
2	Kontrolálható, de csak kellően gyors emberi reakcióval	Súlyosabb sérülések, egy ember halála
1	A rendszer funkcionalitása csökken, de normál reakcióval közel veszélytelen marad	Kisebb sérülések
0	Meghibásodás esetén, csak bosszantó eredmény van, veszély nincs	Nincs sérülés, esetleg horzsolások

2. táblázat. SIL szintek a hibák kontrolálhatósága és veszélyessége alapján [10]

Az IEC 61508 (magyar változata az MSZ-EN 61508) csak általános célokat, iparágtól független előírásokat fogalmaz meg. A szabvány csak elektronikus vagy szoftveres biztonságorientált rendszerekre vonatkozik és a termék teljes életciklusát felöleli az igény megfogalmazásától, a kiépítésen keresztül, a leselejtezésig. Alkalmazása akkor célszerű,

vagy kötelező, ha üzem közben emberi élet lehet veszélyben, vagy egészségkárosodás, környezeti kár lehetősége áll fenn.

Vasúti alkalmazások esetében a fenti szabvány specifikus változatai szakterületenként az alábbiak:

- MSZ-EN 50126-1:2018 (IEC 62278-1) „Vasúti alkalmazások. A megbízhatóság, az üzemkészség, a karbantarthatóság és a biztonság (RAMS - Reliability, Availability, Maintainability and Safety) előírása és bizonyítása. 1. rész: Az általános RAMS-folyamat” [11]. (Ez a vasútspecifikus változata az általános, bármely iparági MSZ-EN 61508-1 szabvány első részének [10].) A szabvány célja a vasúti rendszerek biztonságának garantálása, a RAMS kezelési folyamatának alapelveit és általános követelményeit határozza meg. Elősegíti a vasúti rendszerek megbízhatóságának és rendelkezésre állásának növelését, ami a szolgáltatások zavartalan működéséhez, a rendszerek egyszerű és hatékony karbantartásához szükséges. Alkalmazásával minimalizálható az állásidő és a fenntartási költségek.
- MSZ-EN 50126-2:2018 (IEC 62278-2) „Vasúti alkalmazások. A megbízhatóság, az üzemkészség, a karbantarthatóság és a biztonság (RAMS) előírása és bizonyítása. 2. rész: Rendszerek biztonsági megközelítése” [11]. Az első részhez képest ez a biztonság gyakorlati megvalósítására fókuszál szintén a vasúti környezetben. A szabvány részletes útmutatást nyújt a vasúti rendszerek RAMS folyamatának gyakorlati megvalósítására a teljes rendszerfejlesztés és jóváhagyás során.
- Az MSZ-EN 50128:2011 (IEC 62279) „*Vasúti alkalmazások. Távközlési, biztosítóberendezési és adatfeldolgozó rendszerek. Szoftverek vasúti vezérlő- és védelmi rendszerekhez*” szabvány a vasúti vezérlő és biztonsági rendszerekhez kapcsolódó szoftverekre vonatkozik, melyek a kommunikációs, adatfeldolgozó és biztonsági eszközökben kerülnek alkalmazásra. A szabvány követelményei nagyon fontosak a vasúti rendszerek biztonságos és megbízható szoftverfejlesztése szempontjából. Alkalmazása biztosítja a szoftverek megbízhatóságát és működőképességét, a szoftverhibák minimalizálásával növeli a vasúti közlekedés biztonságát. A szabvány foglalkozik a szoftverrendszerek kockázati szintje alapján a különböző SIL-

szintek meghatározásával is, valamint útmutatást ad a fejlesztési és tesztelési módszerekhez minden SIL-szinten. [12].

- Az MSZ-EN 50129:2019 (IEC 62425) „*Vasúti alkalmazások. Távközlési, biztosítóberendezési és adatfeldolgozó rendszerek. Biztonsági elektronikai rendszerek biztosítóberendezésekhez*” szabvány témája az elektronikus biztosítóberendezések (vonatvezérlési rendszerek, vasúti kommunikációs, adatfeldolgozó és biztonsági eszközök, jelzőrendszerek és más vasúti biztonságkritikus rendszerek, amelyek elektronikus vagy programozható elektronikus technológiákat használnak) minősítésének és jóváhagyásának folyamata. A szabvány meghatározza a biztonsági vonatkozások bizonyításához szükséges követelményeket és eljárásokat, amelyek alapját képezik a biztonsági igazolásoknak. [16]
- Az MSZ-EN 50159 (IEC 62280) „Vasúti alkalmazások. Távközlő-, jelző- és adatfeldolgozó rendszerek. Biztonsági távközlés átviteli rendszerekben.” [17] E szabvány biztosítja, hogy a vasúttal kapcsolatos alkalmazásokat kiszolgáló kommunikációs hálózatok milyen informatikai és biztonsági követelményeknek kell megfelelniük. A szabvány megkülönbözteti a zárt (class A), a nyitott, nyilvános (class B) és a vegyes, hibrid (class C) hálózatokat. A szabvány célja, hogy a vasúti kommunikációs rendszerek megbízhatóságát, adatvédelmét, hibatűrését biztosítsa (pl. hibadetektálás, helyreállás, adatvesztés, késleltetés kibertámadások kezelése). E cél elérése érdekében a szabvány különböző biztonsági megoldások alkalmazását írja elő (titkosítás, hitelesítés, adatintegritás-ellenőrzés, redundancia, hibatűrés biztosítása. A szabvány tartalmazza a nyomon követhetőséget és átláthatóságot biztosító dokumentáció készítésének követelményeit is.
- Az MSZ-EN-50701 szabvány az IEC 62443 ipari kiberbiztonsági szabványra épül, de a vasúti infrastruktúrák sajátosságaihoz igazították. A szabvány célja a biztosítóberendezések, forgalomirányító rendszerek, kommunikációs rendszerek és vasúti járművek védelme a kibertámadások ellen. E cél érdekében a szabvány meghatározza hozzáférés-kezelés, titkosítás és hálózati szegmentáció elveit, továbbá a támadások észlelésének és kezelésének módszereit. E mellett kitér az egyes vasúti alrendszerek biztonsági szintjeinek meghatározására is.

- Az EN 63452 szabvány jelenleg még nem véglegesített szabvány, tervek szerint az EN-50701 szabvány műszaki specifikációit váltja fel, kibővítve annak fókuszát. A szabvány szintén az IEC 62443 sorozat követelményeit alkalmazza a vasúti környezetre, de az IEC 62278 sorozatban tárgyalt megbízhatóság, rendelkezésre állás, karbantarthatóság és biztonság (RAMS) témakörét is magába foglalja. A szabvány célja, hogy a vasúti rendszerekre veszélyes kockázatokat azonosítsa, és kezelésükre, felügyeletükre eljárásokat adjon meg. Ezzel a vasúti üzemeltetők és infrastruktúra-kezelők számára biztosítson elvárt biztonsági szintet, szinteket.

Néhány további fontos szabványt is megemlítek, melyek a vasúti rendszerekbe telepített elemekre vonatkoznak:

- Az MSZ EN 50121 szabványsorozat az elektromágneses összeférhetőséggel (EMC - Electromagnetic Compatibility) foglalkozik vasúti alkalmazások tekintetében. A szabványsorozat célja, hogy biztosítsa a vasúti rendszerek és berendezések zavarmentes működését, valamint a környezetre gyakorolt elektromágneses hatások minimalizálását. A szabványsorozat öt részből áll, melyek az általános és a rendszerszintű követelményeken túlmenően specifikusan tartalmaznak a járművekre, a járművek segédberendezéseire, a jelző- és telekommunikációs eszközökre és a telephelyekre vonatkozó EMC előírásokat. Fő célkitűzések, hogy maguk az eszközök kellő mértékben zavartűrőek legyenek és ne okozzanak más rendszerekben zavarokat elektromágneses hatásokkal, minimalizálják a környezetre gyakorolt hatást, és csökkentsék a elekromágneses zavarokból eredő üzemi hibákat. [13]
- Az MSZ EN 50155 szabvány a vasúti járművekbe beépítendő elektronikai eszközök beépítésével, szigetelésvizsgálattal, eszközök immunitásának vizsgálatával foglakozik: hőmérséklet, rázkódás, ütődés, páratartalom, tápellátás bizonytalansága, EMC, egyéb környezeti hatások – por és vízbehatolás – tekintetében. A szabvány előírja a különböző tesztelési módszereket (megbízhatósági vizsgálatokat, működési teszteket és egyéb ellenőrzési eljárásokat), amelyek biztosítják és igazolják a berendezések megfelelőségét [14].

1.2 Nemzeti szabályozások

Minden országban a nemzetközi szabályokon, szabványokon felül nemzeti szabályok, rendeletek vonatkoznak a vasút üzemeltetésnek minden szegmensére. Ezeket európai szinten évek óta igyekeznek egységesíteni, és a nemzeti előírások közötti különbségeket csökkenteni, elsősorban az európai szintű átjárhatósági szempontok miatt, de még valószínűleg évekig együtt kell élnünk ezekkel az egyre csökkenő számú különbségekkel.

Magyarországon a vasúti kommunikációs rendszerekre vonatkozó előírásokat sok éven át a hagyományos vasúti rendszerek kölcsönös átjárhatóságáról szóló 103/2003 (XII.27) GKM rendelet tartalmazta. E rendelet része Az Országos Vasúti Szabályzat I. kötete. Ebben a kötetben a „B" fejezet (A hagyományos vasúti rendszer strukturális alrendszere) 3. részének (Ellenőrző-, irányító-, jelző- és biztosítóberendezések) két fejezete szól a távközlő és informatikai rendszerek megvalósításáról. (3.2 - Vasúti távközlő berendezések - és a 3.3 - Vasúti informatika). [15]. Az európai vasúti közlekedés harmonizálásának érdekében e rendelet 2024 októberében hatályát vesztette és a nemzeti szabályozások teljesen új alapra kerültek.

A Vasúti Műszaki Előírások (VME) 2024 év végétől a nemzeti sajátosságokat rögzíti. A Vasúti Műszaki Bizottság [63] elsődleges feladata az volt, hogy tisztán és átláthatóan rögzítse az elengedhetetlen fontosságú nemzeti sajátosságokat, és a lehető legnagyobb teret biztosítsa az ÁME-k érvényesülésének.

1.3 Üzemeltetői szabályozások

Üzemeltetői szinten speciális kézikönyvek (helyi szabványok) határozzák meg az adott vállalat specifikus elvárásait. Ezek a MÁV és a GySEV esetében az ún. Feltétfüzetek.

A feltétfüzetek fontos szerepet játszanak a vasúti közlekedés biztonságának, hatékonyságának és szervezett működésének fenntartásában. Ezek a dokumentumok átfogó és specifikus előírásokat és szabályokat tartalmaznak, amelyek biztosítják, hogy a vonatok a megfelelő paraméterek szerint közlekedjenek, a személyzet pedig az előírt szabályok szerint végezze munkáját. A feltétfüzetek egy-egy területre fókuszálnak, és – hasonlóan a szabványokhoz – időről-időre átdolgozáson és frissítésen esnek át. Kutatásom témájában áttekintettem a biztonsági előírásokkal, kivitelezésekre vonatkozó műszaki paraméterekkel és megoldásokkal, a karbantartással és a kommunikációval továbbá a jelzési rendszerekkel foglalkozó füzeteket.

Az OVSZ I. megszűnése nyomán a feltétfüzetek funkcióját – az eredeti elgondolás szerint – a VME veszi át, hogy az előírások az üzemeltető vállalattól függetlenek legyenek.

1.4 Megfelelőség értékelés és tanúsítás szerepe

Vasutak esetében a vonatkozó követelményeknek való megfelelést – a beruházás jellegétől függően – legkésőbb a normál üzem megkezdése előtt, de legtöbb esetben még a tervezés és kivitelezés során is igazolni kell.

A tanúsítás fontos szerepet játszik a vasútépítésben, biztosítva, hogy az építési és üzemeltetési folyamatok megfeleljenek a vonatkozó biztonsági, műszaki, és minőségi elvárásoknak. A tanúsítás során független szervezetek igazolják, hogy a vasútépítéshez kapcsolódó berendezések, rendszerek és eljárások összhangban vannak a nemzetközi, nemzeti szabványokkal, üzemeltetői előírásokkal és jogszabályi kötelezettségekkel. [8]

1.4.1 Eszköz és rendszerszintű vizsgálat

Biztonsági szempontból a megvalósított rendszerek és elemeik eszközszinten és rendszerszinten is értékelendők.

1.4.1.1 Eszközszintű vizsgálat

Gyártói oldalon az eszközszintű tanúsítás történik legtöbb esetben. Ezzel igazolni tudják, hogy az általuk gyártott rendszerelemek teljesítik-e a vonatkozó szabványok előírásait, esetleg a nemzeti és üzemeltetői elvárásokat is, hogy egy adott térség vasúti rendszerében egyáltalán alkalmazható-e az eszközük.

Ha egy gyártó egy üzemeltető projektjébe beszállító lesz, vagy akar lenni, a rendszerintegrátor elsőként ellenőrzi, hogy eszközszinten az integrációhoz rendelkezésre álló eszközök teljesítik-e a vonatkozó követelményeket. Ezeket a gyártó a korábban már megszerzett tanúsítványokkal tudja legegyszerűbben igazolni. A rendszertervezés kezdeti fázisában fontos szerepe van, hogy az eszközök tanúsítványai tartalmaznak-e limitációkat, mert esetleg épp ezek a nem megvalósított funkciók miatt nem alkalmazható az adott eszköz egy projektben.

1.4.1.2 Rendszerintegráció

Rendszerintegrációnál fontos tény, hogy a leggyengébb láncszem elve mindig teljesül. Akár egy darab rendszerelem, ami alacsonyabb szintet teljesít a kiépített rendszer elemeihez képest, a teljes rendszer biztonsági szintjét lerontja a saját szintjére. Rendszerintegráció esetén olyan eshetőség is felmerülhet, hogy bár az egyes elemek

azonos eszközszintű biztonsági szinttel rendelkeznek, de az általuk létrehozott rendszer nem teljesíti ugyanazt a szintet.

Az egyes elemek összekapcsolását biztosító kommunikációs interfészek és eszközök kialakításának olyan biztonsági szinttel kell rendelkeznie, amely teljesíteni tudja az elvárt szintet. Ezért nagyon fontos és elkerülhetetlen, hogy az egyes elemek külön vizsgálata mellett a belőlük összeállított rendszer vizsgálata, ellenőrzése, tesztelése és tanúsítása is elvégzésre kerüljön.

Összetett rendszer esetén már a tervezés során meg kell határozni a műszaki és üzembiztonsági jellemzőket és elvárásokat, amik a kivitelezés különböző fázisaiban folyamatosan ellenőrizhetők és ellenőrzendők.

1.5 Vasúti rendszerek és kommunikációjuk

Ebben a részben áttekintés olvasható a jelenlegi vasúti biztosítóberendezési rendszerek legfontosabb elemeiről.

1.5.1 Vasúti biztosítóberendezések elemei

A vasúti biztosítóberendezések fejlesztésének és alkalmazásának elsődleges célja mindig is a vasúti közlekedés biztonságának és hatékonyságának növelése. Ezt a célt kizárólag úgy lehet elérni, hogy a tervezés első lépésétől kezdve folyamatosan figyelembe vesszük a biztonsági elvárásokat [6].

Az alábbiakban röviden bemutatom a vasúti biztosítóberendezések fejlődésének főbb mérföldköveit jelentő generációkat.

1.5.1.1 Mechanikus, manuális rendszerek

A 19. század elején a vasúti forgalomirányítás kézi jelzésekkel és mechanikus váltó- és jelzőállítással történt. A jelzőőrök zászlókkal vagy lámpákkal adtak jelzéseket a vonatoknak. Az első távvezérlésű váltókat és jelzőket erős huzalokon (vonóvezetékkel) keresztül kézzel állították az állomásokról. Ezek állomástól való távolsága igencsak korlátos volt a kialakítás nehézségei miatt. Az alapvető biztonsági követelmények teljesítését mechanikus reteszeléssel oldották meg.

1.5.1.2 Elektromechanikus biztosítóberendezések

A 19. század végén megjelentek az első elektromechanikus biztosítóberendezések, amelyek elektromos árammal működtették a váltókat és jelzőket. Ez jelentősen növelte a vasúti közlekedés biztonságát és csökkentette az emberi hibák lehetőségét. Ebben a

korszakban került bevezetésre a pálya szakaszok blokkrendszerbe szervezése, amihez szükséges feltétel volt a jelzők hatékonyabb kezelése és a vonatok mozgásának ellenőrzése is.

1.5.1.3 Jelfogós biztosítóberendezések

A 20. század első felében a relék alkalmazása a biztosító berendezésekben új lehetőségeket nyitott meg a vonatfelügyelet és vezérlés terén. A relék és a rákapcsolt pályamenti ezközök segítségével automatikusan lehetett ellenőrizni a vonatok helyzetét és biztosítani a kizárásos elvet, hogy ne történjenek összeütközések. Ez a technológiai szint tette lehetővé a nagyobb pályaudvarok és összetettebb vasúthálózatok létrejöttét és hatékony és biztonságos irányítását.

1.5.1.4 Elektronikus és számítógépes rendszerek

A 20. század második felében az elektronikus rendszerek megjelenése tovább növelte a vasúti közlekedés megbízhatóságát, rugalmasságát és kapacitását. Az 1960-as évektől kezdve a relés rendszereket fokozatosan felváltották az első elektronikus, majd számítógépes biztosítóberendezések, amelyek lehetővé tették komplex forgalomirányítási algoritmusok alkalmazását. [20,35]

1.5.1.5 Számítógép alapú biztosítóberendezés

A számítógép alapú biztosítóberendezés (Computer Based Interlocking - CBI) rendszere a biztosítóberendezési funkciókat megvalósító központi szerverből, a terepi eszközökből és az ezeket összekötő hálózatból áll. A leggyakrabban CBI-nek nevezett szerver az adott területet kiszolgáló biztosítóberendezés rendszer központja. A biztonságos vonatközlekedés szempontjából ez a legfontosabb rendszer.

A számítógépes biztosítóberendezések általában két részből állnak: az egyik rész a biztonsági funkciókat valósítja meg, rájuk vonatkozó követelmények közel hibamentes működést írnak elő (SIL4 szint) [10]. A másik rész az úgynevezett „nem létfontosságú” funkciókat valósítja meg, mint például a kézi beavatkozó eszközök, állapotjelzők, visszajelző monitorok üzeme.

A biztosítóberendezés központjában a pályamenti biztosítóberendezések információinak gyűjtése, kiértékelése történik, amelyek alapján beavatkozásokat hajtanak végre az előírt és biztonságos vonatközlekedési követelményeknek megfelelően.

Egy vasúttársaságnak rendszerint több biztosítóberendezés központja van, melyek egy-egy terület ellátásért felelősek. Az egyes területek biztosítóberendezéseinek szerverei össze vannak kötve egymással információcsere céljából, de elsődleges feladatuk a saját régiójuk biztonságának és folyamatos üzemének biztosítása. [9,20]

1.5.2 Központi Forgalomirányitás

A Központi Forgalomirányítással (KÖFI, vagy CTC - Centralized Traffic Control) lehetővé válik a vasúti járművek mozgásának távoli felügyelete, irányítása egy központi vezérlőhelyről. A központi forgalomirányító rendszer (KÖFI) az általa felügyelt területen belül irányítja a vonatközlekedést és a tolatási műveleteket. A rendszer a CBI-on keresztül biztosítja a központi vezérlést. A KÖFI elsődleges célja a vasúti közlekedés hatékonyságának és rugalmasságának növelése.

A KÖFI rendszer egy központi forgalomirányító központból áll, ami összeköttetésben áll tipikusan az állomási biztosítóberendezésekkel. A forgalomirányító személyzet számítógépes felületen keresztül figyelemmel kíséri a vonatok mozgását, módosíthatja azokat a biztosítóberendezéseken keresztül a jelzők és váltók állapotának változtatásával. Az információátvitel történhet többféle fizikai közegen és technológiával. Jelenleg a korszerű IP-alapú rendszerekre való áttérés a jellemző és ez a kutatásom fő irányvonala.

A KÖFI rendszer decentralizált és autonóm tervezési elvekre épül, elosztott számítási és vezérlési technológiát alkalmaz. Ennek köszönhetően képes térben és időben azonosítani a vonatközlekedés és a tolatási műveletek során fellépő problémákat, valamint a szükséges műveleti korrekciókat a tervezett ütemezéshez igazítva végrehajtani. Ezáltal biztosítja a közlekedési és tolatási folyamatok hatékony és összehangolt vezérlését.

1.6 Egységes Európai Vasúti Közlekedésirányítási Rendszer

Az ERTMS (European Rail Traffic Management System), azaz Egységes Európai Vasúti Közlekedésirányítási Rendszer célja, hogy megvalósítsa az országhatárokon átívelő egységes vonatfelügyeletet és irányítást minden aspektusból.

Az ERTMS egyik része az ETML (European Traffic Management Layer), mely a forgalommenedzsment és forgalomirányítási feladatok megoldását jelenti.

A másik rész az EIRENE (European Integrated Railway Radio Enhanced Network), ami a rádiós kapcsolat megoldását jelenti a fedélzeti és a pályamenti eszközök között. Ez jelenleg a GSM-R rendszert jelenti, a távlati tervek szerint az 5G alapú FRMCS.

A harmadik része az ETCS, amiről a következőkben lesz szó.

1.7 Európai egységes vonatbefolyásoló rendszer

Az egy rendszerbe integrált rendszerelemek komplex szolgáltatásokat nyújtanak a vonatirányítás számára. Ezt igyekszik megvalósítani Európában az ETCS (European Train Control System) automatikus vonatbefolyásoló rendszer, ami jelenleg is kiépítés alatt áll. Ennek a rendszernek az elsődleges feladata legkülönfélébb üzemi helyzetekben a vonatforgalom felügyelete és biztonságának garantálása.

Az ETCS rendszer bevezetése fokozatosan történik, mindenhol a korábbi, különböző nemzeti rendszerek mellett működik. Az ETCS rendszernek szolgáltatási képességei szerint három szintje van. Jelenleg a kettes szint használata és kiépítése zajlik a legtöbb helyen. Európában – és országokon belül is – vannak vonalak, ahol már kiépítésre került a rendszer valamelyik szintje és vannak vonalak, ahol még nem. [21,22] A következő részekben összefoglalom az egyes szintek főbb tulajdonságait.

1.7.1 Az ETCS szintjei

1.7.1.1 1. szintű ETCS

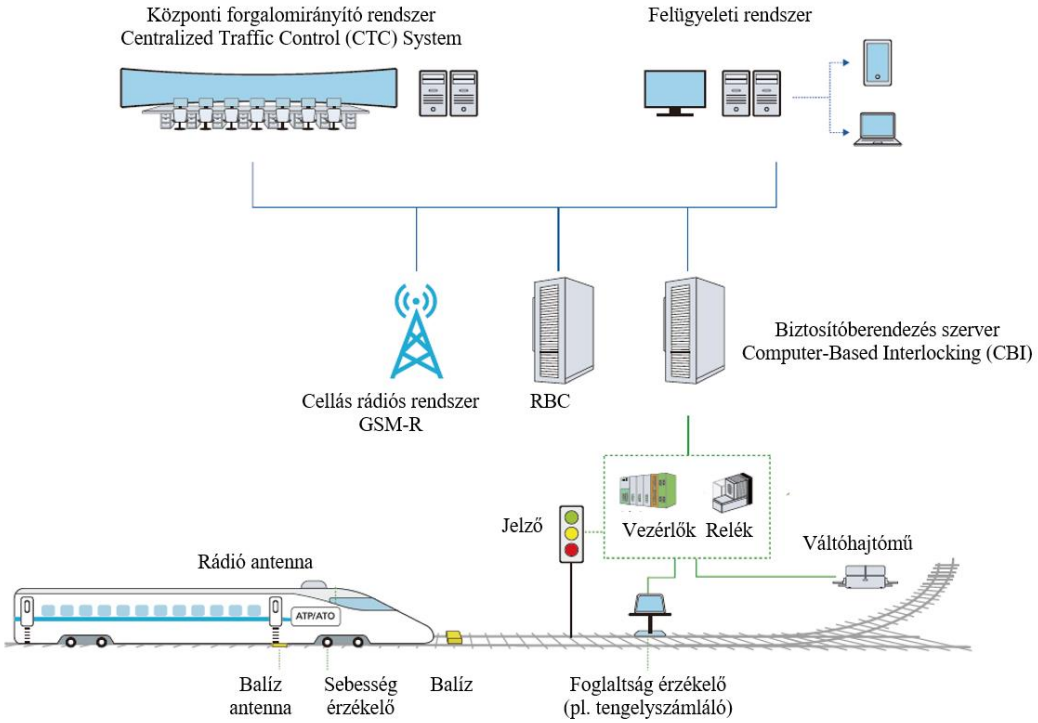
Az ETCS rendszer 1. szintje (L1 – Level 1) csak úgynevezett pontszerű vonatvezérlést tud megvalósítani, ez a szint a hagyományosnak mondható biztosítóberendezéseken alapul. Az 1. ábrán látható egy példa. Itt egy lokálisan megvalósított kommunikáció során jut el a vonatra az éppen aktuális jelzőkép. Ebben a változatban korszerű kommunikációs adatátviteli módok nem alkalmazottak, így ezzel a változattal nem foglalkozok a továbbiakban. Az ábrán látható LEU és balíz, mint ETCS rendszerelemek az 1.8 részben kerülnek bemutatásra.

1. ábra. Az 1-es szintű ETCS csak pontszerű vonatvezérlést valósít meg [23]

1.7.1.2 2. szintű ETCS

A 2. szintű ETCS (ETCS L2) is a hagyományos biztosítóberendezéseken alapul, azaz a vonatérzékelést továbbra is sínáramkörökkel vagy tengelyszámlálókkal valósítják meg.

A biztosítóberendezés kapcsolatban áll az RBC-vel, ami működési területén belül kezeli a vonatok menetengedélyeit, automatizálva a közlekedésüket. A menetengedélyek, vezérlési- és állapotinformációk a GSM-R hálózaton keresztül jutnak el a szerelvények mozdonyaihoz, ahogy a 2. ábra is szemlélteti. Állapotinformációk terén a legfontosabb a vonatok helyzete. Az ETCS L2 képes mozdony részben a meghaladott balízokból kiolvasott adatokból állapítja meg a helyzetét és továbbítja az RBC felé. (A mozgásparamétereket a balízokból kinyert helyinformációk mellett a mozdonyban található odométer, GPS vevő, gyorsulásmérő, giroszkóp is szolgáltatja.)



2. ábra. 2-es szintű ETCS rendszer blokkvázlata [24]

1.7.1.3 3. szintű ETCS

Az ETCS 3. szintje a jelenlegi legmagasabb szintű szolgáltatásokkal bíró változat. Ezzel a rendszerrel a rádiós vonatvezérlés teljes mértékben megvalósul: a folyamatos sebességfelügyelettől kezdve, az elméletben jó ötletnek tűnő mozgó blokkos rendszerig (fix térközös megoldás helyett). Ezen a szinten lehetőség van a jelzőberendezések teljes elhagyására is (a mozdonyvezető is elméletileg feladat nélkül marad). A fedélzeti elemek számára új feladatként jelenik meg a vonatintegritás ellenőrzése, ezzel új követelményszint jelenik meg a fedélzeti kommunikáció terén, mivel a mozdonyra kapcsolt vagonok is belépnek a fedélzeti kommunikációba. és folyamatos

kommunikációs kapcsolatban állnak a mozdonyban kialakított integritást felügyelő rendszerelemmel. Ezzel a pályamenti eszközök száma csökken, így a fenntartási költségek terén is jelentős megtakarítás érhető el. Jelenleg ez a szint még nem került üzemszerű alkalmazásba sehol. Legnagyobb kihívás véleményem szerint ennél a szintnél a vonatintegritás infrastruktúrájának kialakítása, továbbá a pályamenti-vonat kommunikációs hálózat olyan szintű megbízhatósága, hogy a pályamenti eszközök elhagyása és ezzel együtt az emberi felügyelet megszüntetése ne okozza a biztonsági színvonal csökkenését. Pilot projektek e téren vannak Európa szerte. [36]

1.8 ETCS kiszolgáló rendszerelemek

Az ETCS L2 bevezetésével folyamatos kommunikációs szükséglet jelent meg a vonat és a pályamenti eszközök, központok között.

1.8.1 GSM-R

Az ETCS L2 megjelenésével szükség volt egy megbízható, robosztus rádiós technológiára, mely nagy területek lefedésére képes. Akkor egyértelmű volt a választás, hogy a polgári környezetben már bizonyított GSM technológia alkalmas erre. A GSM-R (Global System for Mobile Communications – Railway) speciálisan vasúti célú cellás földi mobil rádiórendszer, melynek szolgáltatási területe lefedi a kiépített ETCS 2-es és 3-as szintű vonalszakaszok teljes hosszát. Ez a rendszer a GSM (Global System for Mobile Communications) mobiltelefon-technológia vasúti adaptációja, célja, hogy akár világszinten egységes, megbízható és biztonságos kommunikációs csatornát biztosítson a vasúti személyzet és a vasútirányítás részére. Jelenleg elsősorban az European Train Control System (ETCS) rendszer kommunikációs hordozószolgáltatása, mivel biztosítja az adatátviteli csatornát a vonat és a földi infrastruktúra közötti kommunikációhoz, amely elengedhetetlen a vonat pozíciójának követéséhez, az automatikus sebességszabályozáshoz, menetengedélyek kiadásához és további biztonsági funkciókhoz.

A GSM-R alapvető célja volt, hogy helyettesítse a korábbi, nemzetközi szinten nem egységes és általában inkompatibilis vasúti rádiórendszereket. Ennek köszönhetően lehetővé teszi az egységes kommunikációt a különböző országok vasúti hálózatai között. Alkalmazása az európai országokban kötelező a főbb nemzetközi vonalakon TEN-T (Trans-European Transport Network), de találunk GSM-R rendszert Európán kívül Kínában, Indiában, Dél-Afrikában, Ausztráliában és a Közel-Keleten is. [37,38,41]

A GSM-R fokozott biztonsági protokollokkal rendelkezik, amelyek biztosítják, hogy a kommunikáció megbízható és zavartalan maradjon, még nagy sebességű vonatok esetében is. A rendszer támogatja a folyamatos és valós idejű kommunikációt egyrészt a vonatok (mozdonyok) és a pályamenti biztosító és vonatvezérlő rendszerek, másrészt a vasúti személyzet között. [3]

Rádiós lefedettségnek szakadásmentesnek kell lenni, mert a rádiós rendszer feladata, hogy az adott területet kiszolgáló RBC központ és a közlekedő, ETCS képes vonatok között folyamatos adatkapcsolatot tartson fent. A kapcsolat megszűnése esetén – rögzített időzítés letelte után – vészfékezésre kényszerítik a vonatot.

A GSM-R rádióhálózat RBC-kből, bázisállomás-vezérlőkből és bázisállomásokból áll. Ez a pályamenti és a fedélzeti berendezések közötti kommunikáció hordozószolgáltatása.

1.8.1.1 A GSM-R utódai

A GSM-R az 1990-es évek technológiájára épül, és bár robosztus és megbízható kezd már elavulni. Adatátviteli képességei (kis adatsebesség és viszonylagosan magas késleltetés) korlátozzák az újabb vasúti alkalmazások támogatását.

Jelenleg már egyértelműen az 5G-alapú FRMCS (Future Railway Mobile Communication System) tekinthető a jövő vasúti mobilkommunikációs rendszerének, amely a GSM-R rendszer helyébe lép. Az FRMCS átviteli képességei jelentősen meghaladják a GSM-R technológia képességeit. Az EU tervei szerint hamarosan kezdődhet a bevezetése [39,40]. A szabványosítás már elért egyféle készültségi fokot és a rendszer tesztelését már több helyen megkezdték, ugyanakkor véleményem szerint továbbra is kihívást jelent a vasúti kommunikációra jellemző, magas megbízhatósági követelmények maradéktalan teljesítése.

Átmeneti fejlesztési irányvonalnak vehetjük a 4G alapú megoldás, azaz az LTE-R (Long Term Evolution – Railway) rendszerét, ami rádiós szempontból részben kompatibilis a későbbiekben megvalósuló 5G alapú hálózatokkal. [34]

1.8.2 Rádiós irányítóközpont

Az ETCS (European Train Control System) 2-es és 3-as szintjében (1.7.1 rész) jelenik meg a rádiós irányítóközpont (Radio Block Center – RBC), ami a vasúti automatikus vonatbefolyásoló rendszer pályamenti központi berendezése. Egy vasúttársaságnak több

RBC-je is van (hasonlóan a CBI-khez), számuk az RBC-k kapacitásának függvénye, hogy mennyi vonatot képesek egy időben nyilván tartani (tipikusan 50-100, de ez sok tényezőnek a függvénye). Egy RBC kapcsolatban van a szomszédos RBC-kkel, az adott területért felelős biztosítóberendezés szerverével (CBI), a központi forgalomirányítással (CTC – Centralized Traffic Control) és esetleg más elemekkel.

Az RBC-k feladata többek között a szerelvények menetengedélyeinek kezelése, vezérlőparancsok generálása a biztosítóberendezés és a pályamenti eszközök információinak felhasználásával, és ezek rádiós továbbítása a GSM-R hálózaton keresztül a fedélzeti berendezés felé.

1.8.3 Bázisállomások és bázisállomás vezérlők

A GSM-R hálózatban a bázisállomás vezérlők (BSC – Base Station Controller) és a bázisállomások (BTS – Base Transceiver Station) kulcsszerepet játszanak a rádiós infrastruktúra működésében.

A bázisállomás felelős a rádiós kapcsolatok létrehozásáért és fenntartásáért a vonatok és a hálózat között. A BTS-ek biztosítják a lefedettséget, továbbítják a hang- és adat információkat, valamint a vezérlőjeleket az RBC és a fedélzeti berendezések között. Az ETCS megköveteli a duplikált lefedettséget az ETCS képes vonalszakaszokon.

A bázisállomás vezérlők a BTS-ek vezérléséért felelősek. A BSC-k kezelik a hívásokat, vezérlik handover folyamatokat és az erőforrás-menedzsmentet. A GSM-R hálózatban a a lefedettség optimalizálása is a BSC feladata, továbbá folyamatos kapcsolatot biztosít a hozzá tartozó BTS-ek között, miközben interfészt biztosít a kapcsoló központ felé (MSC – Mobile Switching Center) és azon keresztül a vasúti alkalmazások felé.

1.8.4 Balíz, LEU

A balíz egy olyan eszköz, amely elektromágneses elven működik, és adatokat továbbít a felette elhaladó mozdony számára. A balízok a sínek között, fixen vannak elhelyezve. A kiolvasást tekintve teljesen passzív eszközök, a bennük eltárolt információ továbbításához szükséges energiát az elhaladó mozdony balíz olvasó egysége szolgáltatja induktív módon. Az átadott adatok többek között lehetnek például kilométerszelvényre, haladási adatokra, fékezési parancsokra, jelzőképekre vonatkozó adatok.

A balízok a pontszerű vonatbefolyásolás alapvető elemei, ld. ETCS Level 1.

Alapvetően kétféle balíz létezik: fix és vezérelt balízok:

- A fix balízok csak statikus adatokat tudnak továbbítani. Általában a pontos helymeghatározáshoz szükséges információk továbbítására használják őket.
- A vezérelt balízok változó adatokkal dolgoznak, melyeket a LEU, avagy pályamenti elektronikus egység (Lineside Electronic Unit) vezérli. A LEU a biztosítóberendezés és a vezérelt balíz közötti információcserét valósítja meg. Pl. térköz határon a jelzőképet és az új menetengedélyt a szerelvény számára. Jellemzően az ETCS 1-es szintjén használják, mivel ez a működési mód kizárólag pontszerű vonatbefolyásolást valósít meg.

  Az ETCS 2-es és 3-as szinteken a GSM-R hálózaton keresztül juttatható el a vonatbefolyásoláshoz szükséges fix és változó információk a járművekre. A balízok feladata ettől fogva már nem a változó jelzési képek átvitele, ellenben a pontos helymeghatározásban veszik ki a részüket, mint egyfajta stabil, fix kilométerkövek.

1.8.5 Ideiglenes sebességkorlátozási rendszer

Az ideiglenes sebességkorlátozási rendszer (TSRS – Temporary Speed Restriction System) egy opcionális kiegészítő rendszerelem az ETCS rendszerben. A rendszer célja, hogy karbantartási munkák, pályahibák vagy más időleges biztonsági tényezők miatt ideiglenes sebességkorlátozásokat kezeljen és az ezzel kapcsolatos parancsokat továbbítson az RBC-n keresztül az érintett vonatok számára.

Logikailag forgalomvezérlési feladatkörbe sorolható ez a funkció, de több tényező miatt érdemes dedikált rendszerként implementálni:

- az ideiglenes sebességkorlátozásokra vonatkozó igény az infrastruktúra felől érkezik és azt valós időben kell továbbítani az érintett vonatok számára. Ez magas biztonsági követelmények teljesülését igényli. A központi forgalomirányítási rendszer nem igényel ilyen magas biztonsági szintet.
- Az előző pontot technológiailag úgy lehet megtámogatni, ha közvetlen interfésszel rendelkezik a TSRS jellemzően az RBC felé.
- Más szabályozási logika szerint működik, mint a KÖFI.
- A KÖFI a vasútüzemeltető speciális igényeire szabott. A TSRS különálló fejlesztése és később üzemeltetése lehetővé teszi, hogy eltérő szabványokat és technológiákat alkalmazó vasúti rendszerekhez is illeszkedni tudjon.

1.9 Összegzés

Jelen fejezet célja a vasúti infrastruktúrát kiszolgáló kommunikációs eszközök, rendszerek elemeinek áttekintése, és a kapcsolódó szabályozások és szabványok rendszerezése és bemutatása. A fejezet első részében áttekintettem azokat az ipari szabványokat melyek a magas megbízhatósággal rendelkező rendszerekre vonatkoznak, majd ismertettem a legfontosabbakat azok közül, amik ezeknek a vasúti alkalmazásokra vonatkozó részhalmaza. Megemlítettem a magyarországi nemzeti és üzemeltetői szabályozások rendszerét is.

A következő szakaszban általános összefoglalót adtam a vasúti biztosítóberendezés főbb generációiról, és a központi forgalomirányítás rendszeréről. Ezután rátértem az Egységes Európai Vasúti Közlekedésirányítási Rendszer és azon belül az egységes európai vonatbefolyásoló rendszer bemutatására. Az ETCS rendszer különböző szintű szolgáltatásokat nyújthat, jelenleg az ETCS 2. szint az, aminek kiépítése a legtöbb helyen zajlik és jelen munka alapját is ez a szint jelenti. Ebben a részben tehát általánosan bemutatom az ETCS L2 rendszer kiszolgálásához szükséges rendszer elemeket, melyek közötti kommunikációt biztosító hálózatok kialakítása a kutatásom fókusza.

2 MEGOLDÁSOK MEGBÍZHATÓ HÁLÓZATOK LÉTREHOZATALÁRA

Vasúti alkalmazások esetében sok, egymástól elkülönülő rendszer együttműködése valósítja meg a különböző feladatokat. Ennek oka, hogy az egyes funkciók fontossága, a rájuk vonatkozó követelmények különbözőek, rendszerint eltérő biztonsági követelményekkel is rendelkeznek.

Az eltérő igényű rendszereket általában külön rendszerként, alrendszerként kell megvalósítani, ezzel biztosítható, hogy a különböző biztonsági szintek megvalósulása is teljesüljön rendszerenként. Ezt a korábban említett nemzeti szabályozás is kimondja [15].

Az interfészeket és a köztük lévő kommunikációs technológiákat tekintve meg kell különböztetni, hogy az egyes kommunikációs alrendszerek mennyire létfontosságúak a teljes rendszer biztonsági elvárásainak szempontjából. Ez főként a korábban már áttekintett vonatkozó szabványokon túlmenően a kiszolgálandó alkalmazások szerint is kategorizálható.

Létfontosságú kategória a biztosítóberendezés kommunikációjának folyamatos biztosítása, ezért ezeket a hálózatokat magas megbízhatóságúra kell tervezni, esetenként hibatűrő, redundáns megoldásokat kell alkalmazni [33]. Ennek megoldásait tekintem át a következőkben.

Napjainkban a leggyakrabban alkalmazott második rétegbeli kommunikációs technológiák Ethernet protokollon alapulnak. Az Ethernet hosszú múltra tekint vissza. Kezdetben tiltott volt az adatkapcsolati rétegben hurkokat tartalmazó topológiát kialakítani a protokoll alapvető működési elvei miatt. (Nem volt séma az esetleg hibásan továbbított és végtelen hálózati hurokban rekedt keretek észlelésére és eldobására.) Ezt a problémát többféle feszítő fa struktúra alapján működő protokoll kiegészítéssel oldották meg, amelyek már képesek voltak kezelni a hálózatban lévő hurkokat [26,27,28]. Az így kialakított hálózatok redundanciájuk révén ugyan hibatűrőek voltak, de a linkhiba kezelés sajátosságai miatt több másodperces nagyságrendbe esik a helyreállítási idejük.

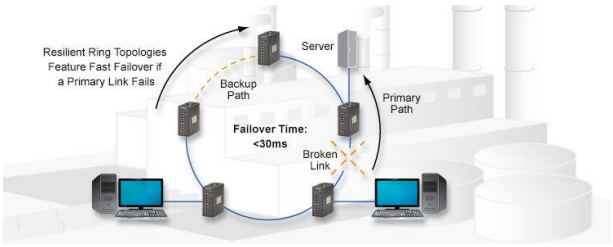
2.1 Redundáns adatátvitel megvalósítása

Kommunikációs téren, ha folyamatos és megbízható adatátvitelt szeretnénk biztosítani, bizonyos fokú redundancia lesz a kézenfekvő megoldás. Hasonlóképpen az

adatfeldolgozás és az automatikus döntéshozatal esetén is ezzel találkozhatunk [25]. Ezekkel a megoldásokkal egy meglévő rendszer megbízhatósága is jelentősen növelhető.

Vasúti környezetben is elsőrendű a megbízhatóság. Biztosítóberendezések terén – a megbízható relé áramkörök alkalmazása után, illetve mellett – elsősorban különböző típusú UART (Universal Asynchronous Receiver/Transmitter) kommunikációs módok szolgálták a megbízható átviteli adatkapcsolatokat, szükség szerint duplikáltan. Jelenleg még sok esetben találkozhatunk ilyen megoldásokkal, rendszerint végponti kommunikáció megvalósításában kapnak még szerepet. Azonban nagyobb távolságok esetén, több entitás összekapcsolásakor az Ethernet alapú megoldások az elterjedtebbek. A vasúti adathálózatokban a jövőben az Ethernet alapú kapcsolatok még szélesebb körű elterjedésére lehet számítani.

A redundancia nem feltétlenül jelenti az adott eszközök duplikációját. Hálózati kommunikáció esetében a duplikáció kiváltható a legtöbb esetben gyűrű topológiával, ami nagymértékben képes emelni a rendelkezésre állást és költséghatékony megoldás is. Gyűrűs szerkezet esetén, ha a gyűrűben egy kapcsolat megszakad, az adott csomópont a másik irányban továbbra is elérhető marad. Bár a hibásan működő kapcsoló és a hozzá kapcsolódó eszközök persze kiesnek a kommunikációból, de a hálózat többi része és eszközei tovább működhetnek és kommunikálhatnak. A gyűrűs topológiákban az alkalmazott kapcsolási protokollnak képesnek kell lennie a hálózatban lévő hurok kezelésére, és hiba esetén a megfelelő és gyors helyreállítási képessége a fontos.



3. ábra. Gyűrű topológia link hibával [32]

Ethernet esetében több feszítő fa alapú protokoll jelent meg kezdetben a hurkokkal rendelkező topológia kezelésére: STP (Spanning Tree Protocol) [26], RSTP (Rapid Spanning Tree Protocol) [27], MSTP (Multiple Spanning Tree Protocol) [28]. Ezek legnagyobb hátránya, hogy lassúak, hibaelhárító sebességük másodperc nagyságrendbe esik, ami irodai környezetben elfogadható, de kritikus infrastruktúrák kommunikációjában nagyon kedvezőtlen nagyságrend.

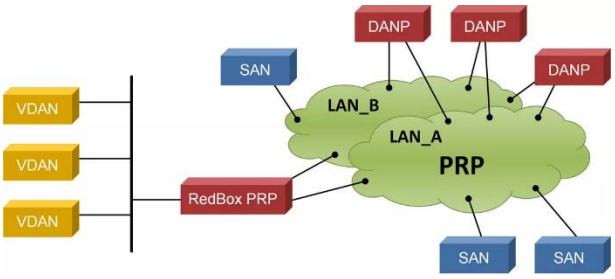
2.1.1 Korszerű redundáns kommunikációs protokollok

Biztonságkritikus rendszerekben, milliszekundum nagyságrendben, vagy az alatt kell a helyreállítási időnek maradni. A PRP (Parallel Redundancy Protocol) és a HSR (High-availability Seamless Redundancy) protokollok [29,30] ezt az elvárást maradéktalanul teljesítik, valójában zéró helyreállítási időt produkálnak.

PRP

PRP esetén két független – nevéből adódóan „párhuzamosan működő redundáns" – hálózat képezi a redundanciát, amikhez két Ethernet porttal rendelkező speciális hálózati csomópontok kapcsolódnak. Az Ethernet keretek két példányban kerülnek kiküldésre az adó oldalon a két, független hálózatba. Vevő oldalon az elsőként érkező példány kerül továbbításra a felsőbb rétegek felé, a második eldobásra kerül. Ez a megvalósítás tisztán második rétegbeli, teljesen transzparens a felsőbb rétegek felé, alkalmazásukhoz a felsőbb rétegekben semmilyen változtatás nem kell. Felsőbb rétegek felől a második rétegbeli hálózat egy nagy megbízhatóságú hálózatként látszik. A duplikált keretküldés biztosítja, hogyha keletkezik egy hálózati hiba, a másik keret ettől még célba ér, azaz nem szakad meg a kommunikáció. Máshogy fogalmazva ennek a megoldásnak a helyreállítási ideje zéró. Ezen túlmenően a duplikált keretek átvitele felhasználható a két hálózat állapotának, minőségi paramétereinek felügyeletére is (pl. hamarabb lehet hibára gyanakodni, ha csak az egyik hálózat esetében növekszik meg a késleltetés vagy a bithiba arány – egy optikai interfész „elfáradása" esetén).

PRP alkalmazása esetén az összes hálózati elemet meg kell duplázni. A PRP csomópontok (PRP-t megvalósító kettős csatlakozású csomópontok - DANP) két Ethernet porttal rendelkeznek, amelyek két független, különálló, de hasonló topológiájú hálózathoz kapcsolódnak (2. ábra). A két hálózatnak nincsenek közös kapcsolatai, így hibafüggetlennek tekinthetők. A két Ethernet interfész ugyanazt a MAC-címet használja, ami megengedett, mivel a két csatlakoztatott hálózat egymástól független és teljesen szeparált. Egy PRP csomópontnak továbbra is csak egy IP-címre van szüksége, és az ARP protokoll megfelelően társítja a MAC-címet az IP-címmel további kiegészítések nélkül.



4. ábra. PRP redundáns hálózati strutúra [30]

A forrás csomópont (DANP) két másolatot küld egy keretről egyidejűleg a két hálózati portján keresztül. A két keret két különböző hálózaton keresztül halad, amíg elérik a célcsomópontot (DANP). A két keret érkezési ideje között bizonyos időbeli különbség lesz. A célcsomópont az elsőként beérkező keretet fogadja el, és elveti a másodikat (ha megérkezik). A célalkalmazás (felső réteg) mindig csak egy keretet kap, amíg legalább az egyik hálózat működik. A PRP nulla időtartamú helyreállítást biztosít, és egyidejűleg lehetővé teszi a redundancia folyamatos ellenőrzését a másodikként beérkező keretek feldolgozásával (például a két hálózat állapota folyamatosan monitorozható az érkezési időkülönbség és a keretveszteségi arány figyelésével).

A duplikált keretek felismerése a keretek forráscímén és egy hozzáadott sorszámon alapul, amely minden egyes PRP protokoll szerint küldött keret esetében növekvő értéket mutat. A sorszámot, a keret méretét, az útvonal azonosítóját és az Ethertype mezőket közvetlenül az Ethernet ellenőrző összeghez adják hozzá egy extra 6 oktet hosszúságú PRP mezőként. Ez a kiegészítés figyelmen kívül marad minden olyan csomópont esetében, amely nem ismeri a PRP protokollt. Emiatt a csatlakozó hálózatokban nem kritikus csomópontok is lehetnek, amelyek csak az egyik hálózathoz csatlakoznak egyetlen interfésszel (SAN - Single Attached Node).

Az egyetlen hálózati interfésszel rendelkező kritikus eszközök mindkét hálózathoz csatlakoztathatók egy RedBox segítségével. A RedBox mögötti csomópontokat virtuális DAN-oknak (VDAN) nevezzük, mivel a többi csomópont számára ugyanúgy jelennek meg, mint egy DAN(P).

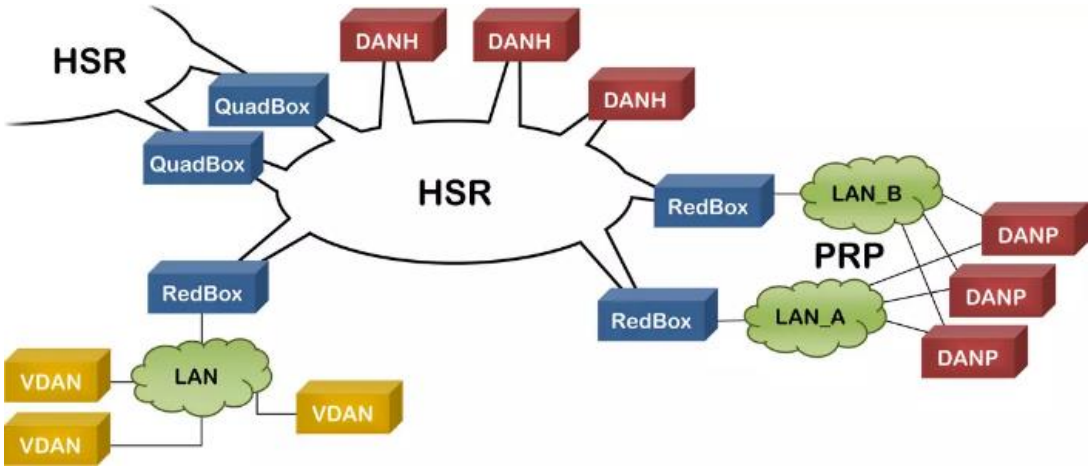
HSR

HSR használata esetén a hálózat topológiája gyűrű, neve nyomán magas megbízhatóságú kapcsolatot biztosít „zökkenőmentes helyreállással”. A csomópontok itt is szintén két Ethernet porttal rendelkeznek és csatlakoznak a szomszédos csomópontokhoz a gyűrű

vonalán. Az adó csomópont két keretet küld el egyidőben az ellentétes irányokba, és amelyik keret hamarabb ér a célállomásra, az kerül továbbításra a felsőbb rétegek felé, a másikat eldobja a csomópont. Költség szempontjából ez a megoldás a gyűrű topológia miatt kedvezőbbnek mondható, a többi mutatója pedig a PRP-hez hasonlóan alakul. [29]

A HSR csomópontok szintén két porttal rendelkeznek, de hálózati hídként működnek, amely lehetővé teszi a redundáns hálózat működését gyűrű vagy háló topológiában dedikált kapcsolók nélkül.

Az HSR alkalmazás esetében a többletköltséget a protokoll hardvertámogatásának megvalósítása jelenti a csomópontok számára (FPGA vagy ASIC alapú), mivel szükséges a csomópontokon áthaladó keretek továbbítása vagy elvetése mikrosekundumokon belül. Ezt a költséget ellensúlyozza az a tény, hogy ebben a hálózatban nincs szükség további Ethernet kapcsolókra.



5. ábra. HSR redundáns hálózati strutúra [30]

Egy HSR hálózati csomópont (DANH) szintén legalább két Ethernet porttal rendelkezik, amelyek mindegyike egy szomszédos HSR csomóponthoz csatlakozik, így mindig két élő kapcsolat van két csomópont között (3. ábra). A felső réteg, azaz a célalkalmazás, mindig csak egy keretet kap, mert a duplikált keretek közül a második elvetésre kerül a második rétegben. A HSR csomópontok azonban folyamatosan ellenőrizhetik a redundancia állapotát, hogy rejtett hibákat észleljenek.

A HSR és PRP hálózatok RedBoxokon keresztül összekapcsolhatók egymással.

2.2 A késleltetés problémái

Az egyre nagyobb sebességű vasutak esetén a kommunikációs hálózat késleltetésének nagysága egyre fontosabb kérdés. Létfontosságú, hogy a valós pályainformációk, sebességadatok és menetengedélyek időben a fedélzeten legyenek, mert egy vonat egy másodperc alatt akár több 10 métert is haladhat. A szükséges adatok késedelmes megérkezése felesleges vészmegállításhoz, rosszabb esetben balesethez is vezethet.

Napjaink kihívása, hogy a korábban alkalmazott szinkronizált időosztásos hálózatok helyett az összes kommunikációs hálózat tekintetében csomagkapcsolt hálózatok kerülnek kiépítésre. Csomagkapcsolt környezetben az átviteli késleltetés nagysága nem nyilvánvaló, mivel az a csomagok változó kezelési időigényein alapulnak. Ezzel szemben a régi szinkron rendszerekben ez a paraméter csak egy egyszerű konstans érték volt. A vasúti kommunikációs hálózatok esetében kulcsfontosságú tényező, hogy olyan hordozó szolgáltatások és protokollok kerüljenek kiválasztásra, amelyek képesek kielégíteni és folyamatosan biztosítani az időzítési követelményeket.

(ETCS 2 esetén az alapértelmezett T_NVCONTACT értéke 30 másodperc, ez Magyarországon szigorított értékű: 18 másodperc.) [21]

2.3 Szinkronizáció

A csomagkapcsolt kommunikációs hálózatok szinkronizációja sem egyértelmű jelenleg, összehasonlítva a szinkronizált időosztásos hálózatokkal, ahol ez a hálózat jellegéből eredendően adódott.

Csomagkapcsolt hálózatokban a csomagtovábbításnak nem feltétlenül kellene szinkronizáltan működni, hiszen egy hálózati csomópontba megérkező csomag a memóriában tárolást követően egy másik ütemezéssel továbbítható lehet a szomszédos rendszerelemnek. A hálózatokban működő berendezések interfészei viszont egyre magasabb adatátviteli sebességet tesznek lehetővé, ez egyben azt is jelenti, hogy egységnyi idő alatt jelentős mennyiségű adat érkezhet az eszközbe, amit belső memóriában átmenetileg tárolni kell. Egymással szinkronizálatlan eszközök esetén a belső memória kihasználtsága pulzáló, jitteres lesz. A pillanatnyilag nagymértékben feltöltött, esetleg túlcsordult memória adatvesztést is eredményezhet.

A fenti negatív hatások csökkenthetők a hálózati építőelemek precíz szinkronizálásával. Csomagkapcsolt hálózati építő elemek hatékony szinkronizálására a Precision Time Protocol (PTP) szolgál.

Az első verziójú PTP-t az IEEE publikálta, majd megjelent ennek a szabványnak a második, javított verziója is. 2019-ben megjelenő újabb, módosított időszinkron eljárás [51] már felülről kompatibilis a korábbi kiadással. Korunk hálózati kihívásait jobban kielégítő adaptáció az IEEE802.1AS szabványként (IEEE, 2019b) jelent meg, elsősorban az Audio, Video bridging és az időkritikus hálózati alkalmazások elvárásainak kielégítésére, részletezve még a következő részben. [52]

A PTP úgynevezett Master – Slave architektúrát követ, ahol a referenciát a „Grandmaster" (Root Timing Reference) adja. A szinkronizálás, és így a működés alapgondolata az, hogy a szinkronizáló üzenetekben található időbélyegek (time stamp) és az üzenet beérkezési időbélyegei alapján az egyes eszközök órája (órajel frekvenciája, esetenként fázispontossága is) korrigálható, szinkronizálható.

2.3.1 Időkritikus kommunikáció

A TSN (Time-Sensitive Networking) időkritikus Ethernet alapú kommunikációs technológia, ami alacsony késleltetéssel és determinisztikus adatátviteli jellemzők biztosításával járul hozzá a magas megbízhatóságú kommunikációhoz. Az ilyen kialakítású kommunikációk egyik elvárása a precíz időszinkron kialakítása a hálózaton belül.

A TSN technológiát megtaláljuk már több ipari és közlekedési területen, és a vasúti szektorban is elindult a bevezetése és tesztelése. A TSN egy szabványcsoport (IEEE 802.1 szabványcsalád), amelyek különféle képességeket biztosítanak a kialakítandó hálózat képességeihez igazodva.

TSN szabványcsalád tagjai:

- IEEE 802.1AS: Precíziós időszinkronizációt valósít meg, PTP-alapon, amely mikroszekundumos vagy annál jobb időpontosságot biztosít. Jelenleg is már alkalmazásban van pl. az automatizálásban gyártósorokon. Protokoll alapja az IEEE 1588v2 (PTP – Precision Time Protocol) aminek ez egy szűkített, precízebb változata. Vasúti alkalmazásban a helyzetjelentések és vonatengedélyek időbélyeggel vannak ellátva, ezek szinkronizált időt igényelnek. Kritikus és a

nemkritikus adatfolyamok szétválasztása ezzel a módszerrel elvileg lehetséges. Vasúti alkalmazás jelenleg tesztfázisban van [55].

- IEEE 802.1Qbv: Időalapú ütemezést, forgalomszabályozást (Time-Aware Shaper) valósít meg. Célja, hogy meghatározott időablakokban kizárólag egy adott forgalomtípus haladhasson, ezzel ütközésmentes és determinisztikus adatátvitelt biztosítva. Kizárja a versenyhelyzetet az adatfolyamok között, úgy, hogy a kritikus adatok mindig időben haladhassanak át a hálózaton. A kritikus forgalmak (pl. vezérlőparancsok, időérzékeny adatfolyamok) számára előre meghatározott időablakok (transmission gates) kerülnek lefoglalásra, így az ütközések elkerülhetők és a késleltetés kiszámíthatóvá válik. Ipari Ethernet hálózatokban jelenleg is már alkalmazzák, a vasúti alkalmazásai tesztfázisban vannak [56].

- IEEE 802.1Qci: Bejövő forgalom szűrését és hozzáférésszabályozást valósít meg, ezzel megakadályozza, hogy egy hibás vagy feltört eszköz túlterhelje a hálózatot. Mielőtt foglalkozna a beérkezett csomaggal igyekszik kiszűrni a nem megfelelő példányokat. Segít izolálni a különböző alrendszerek forgalmát, és prioritást adni a biztonságkritikus adatfolyamoknak (pl. ETCS parancsok, járműdiagnosztika, vagy FRMCS hívások). Támogatja a QoS-mechanizmusokat, amelyek a késleltetésérzékeny alkalmazásokhoz elengedhetetlenek [57].

- IEEE 802.1CB: célja röviden a megbízhatóság növelése, keretismétléssel és az átviteli hibák kiszűrése és eliminálása a duplikált keretek összevetésének segítségével. Tesztelés és implementáció jelenleg folyamatban. A korábban bemutatott HRP és PRP protokollokkal ellentétben ez elvileg bármilyen topológiájú hálózattal működik, csak a szabvány szerinti képességű switch-ek kellenek a hálózatba [58].

- IEEE 802.1Qcc: Centralizált konfigurációs vezérlés, ami az ipari TSN menedzsment rendszerekbe integrálható. Fő célja a TSN hálózatok konfigurációjának és erőforrás-foglalásának automatizálása és leegyszerűsítése, különösen nagyméretű vagy dinamikus hálózatok esetén. Vasúti kommunikáció terén rengeteg időkritikus adatfolyam lehet jelen (pl. vezérlőjelek, videóadatok, diagnosztika), amihez a statikus kézi konfiguráció nem elég hatékony, mivel a hatékony átvitelhez az erőforrásokat csak az adott adatfolyam aktualitásának

idejéig kell foglalásban tartani. Az ETCS Level 3-ban például a vonatintegritás ellenőrzését a szerelvénynek kell biztosítani, tehát az ETCS kommunikációba, még ha nem is közvetlenül, de a szerelvény összes vagonja be fog kapcsolódni. A szerelvény integritását biztosító hálózat kezelésének dinamikusnak kell lenni, mert ilyen módon tudja rugalmasan és automatikusan kezelni a szerelvény vagonjainak szándékos, üzemszerű fel- és lecsatlakozásait és üzemhiba miatti integritás sérüléseket [59].

- IEEE 802.1Qch/Qcr: szabványok célja, hogy a korábbi megoldásokhoz képest fejlettebb sorbanállás-kezelést (queue scheduling) és erőforrás-foglalást (resource reservation) biztosítsanak az Ethernet-alapú hálózatokban, kifejezetten illeszkedve az időkritikus (determinisztikus) kommunikációhoz [60,61].

Az FRMCS aggregációs és gerinchálózatában a TSN szerepe mindenképpen domináns lesz, mert az 5G hálózatok esetében a pontos időszinkron a rádiós interfész hibátlan működéséhez is elengedhetetlen [47,48,49].

Fontos megemlíteni azonban, hogy a vasúti alkalmazásokban a szigorú biztonsági követelmények miatt lassú az új technológiák bevezetése. A trend viszont egyértelműen a TSN irányába mutat, egyaránt a fedélzeti és pályamenti Ethernet hálózatok esetén.

2.4 Gyártóspecifikus megoldások

A magas működésbiztonság redundáns hálózati kialakításokkal valósítható meg, melyek gyakran gyártótól függő megvalósítások [31]. Ezek hátránya, hogy csak az adott beszállítótól származó eszközök kompatibilisek egymással és az üzemeltetési és szervizelési támogatást is csak az adott gyártó szolgáltat. Az alábbi példa a MOXA egyik magas megbízhatóságú ipari Ethernet eszközeiből megvalósított termék, mely rendkívül gyors helyreállási képességgel rendelkezik a redundáns kialakítás kétféle módját megvalósítva és rugalmasan alkalmazható többféle hálózati konfiguráció, vagy földrajzi elhelyezkedés esetén is.

A Moxa Turbo Ring olyan redundáns Ethernet hálózati technológia, amelyet magas megbízhatóságot igénylő ipari alkalmazásokhoz fejlesztettek ki. Gyors helyreállítási képességgel rendelkezik (20ms körüli idő), hogy minimálisra csökkentse a hálózati hibák miatti kiesések idejét. A gyűrűbe kapcsolt Ethernet alapú switch-ek hálózati hiba esetén alternatív útvonali továbbításra térnek át. Turbo Ring kialakítása a gyártó ajánlása szerint

akkor ideális, ha kritikus üzemű hálózati kommunikációt kell megvalósítani, fix gyűrűs topológiával.

A Ring Coupling funkció lehetővé teszi több, kisebb Turbo Ring hálózat összekapcsolását oly módon, hogy bár fizikailag elkülönülnek, de továbbra is tudnak kommunikálni egymással (például két telephely között).

A Turbo Chain akkor hasznos megoldás, ha rugalmas hálózatbővítés lehetőségre van szükség minimális kábelezéssel, például moduláris rendszerekben, ahol gyakori új eszközök hozzáadása. Topológia szempontjából a Turbo Chainben a hálózati eszközök láncban kapcsolódnak egymáshoz, és a lánc két vége csatlakozik, független linkeken egy már meglévő hálózathoz. Ezzel rugalmas és skálázható topológiák hozhatók létre, melyek szintén redundanciával rendelkeznek és a Turbo Ringgel egyező értékű helyreállítási gyorsasággal rendelkeznek.

2.5 Vasúti biztonsági protokoll

Railway Signal Safety Protocol (RSSP) egy alkalmazásrétegbeli biztonsági protokoll, ami a vasúti jelzőrendszerek biztonságos kommunikációját kezeli. Az RSSP-1 és RSSP-2 protokollok különböző szintű biztonsági követelményeket elégítenek ki a vasúti rendszerekben és illeszkednek az EN 50159 által meghatározott hálózati biztonsági szintű hálózatok jellegéhez.

- RSSP-1: Ez a protokoll a zárt átviteli rendszerekben (Class A) alkalmazott biztonsági kommunikációra összpontosít, ahol a jelzőberendezések közötti üzenetátvitel hibamentessége és biztonsága kiemelten fontos.
- RSSP-2: Ezt a protokollt a nyílt átviteli rendszerekben (Class B) történő biztonságos kommunikációra fejlesztették ki, ahol a kommunikációs csatornák nyitottabbak és emiatt potenciálisan sebezhetőbbek.

A digitális átvitel megjelenésével E1 (2Mbit/s) vonalak (G.703 szabvány) voltak a vasúti biztosítóberendezések, forgalomirányító rendszerek és jelzőrendszerek közötti kommunikáció fő átviteli csatornái. A nagyobb, trönkvonali forgalmak multiplexeléssel SDH vagy PDH vonalakon kerültek továbbításra. A biztosítóberendezéseket és a kommunikációban résztvevő elemeket soros kommunikáció (V.24, X.21, RS-232, RS-485) segítségével csatlakoztatták az E1 interfészhez.

Ebben az időben az E1 csatornákat szigorúan zártnak lehetett tekinteni, közvetlenül csatlakoztak az RSSP protokollt futtató eszközök rá. A vasúti központok, állomások és biztosítóberendezések közötti kommunikáció ezekre a dedikált vonalakra épült. Az E1 vonalakon általában PCM-alapú (Pulse Code Modulation) átvitel történt, amely lehetővé tette az adatok és hangkommunikáció együttes kezelését az időosztásos multiplexelésnek köszönhetően.

Jelenleg az E1/SDH rendszerek kifutóban vannak, az IP/MPLS technológia elterjedése lehetővé tette az RSSP Ethernet-IP feletti alkalmazását. Az újabb rendszerek (pl. ETCS Level 2/3) már IP-alapú infrastruktúrát használnak, amely Ethernet-alapú átvitelre épül.

2.6 Összegzés

A második fejezet a magas megbízhatóságú hálózatok létrehozatalára alkalmas technikai megoldásokat tekinti át. Bemutattam a redundáns átviteli megoldásokat, és azok továbbfejlesztett, korszerű változatait, melyek például gazdaságosabb topológiai kialakítással nyújtanak ugyanolyan megbízhatósági szintet és gyors helyreállást, mint ha teljes duplikációt alkalmaznánk.

A következő témaköröm az időtényező volt. A kritikus kommunikációs hálózat működésének determinisztikusnak kell lenni, ami megköveteli a hálózati szinkronizáció szigorú fenntartását. Korábbi, szinkron átviteli adathálózatok esetén ez adódott a hálózat alaptulajdonságából, de a jelenlegi Ethernet/IP alapú hálózatok alapvető aszinkron tulajdonsága miatt erre külön figyelmet kell fordítani. Áttekintettem a szinkronizációra vonatkozó szabványokat és az időkritikus hálózatok kialakítását támogató ajánlásokat is.

Egy gyártó termékein keresztül bemutattam annak lehetőségét is, hogy a nyílt szabványok, ajánlások paramétereihez képest a gyártók saját eszközeik között, egyéni módszerekkel gyakran érnek el jobb teljesítménymutatókat, de ezek a legtöbb esetben csak az adott gyártó termékei közötti kommunikációban valósul meg.

A fejezet végén kitértem az RSSP vasúti biztonsági protokollokra is, amelyek a vasúti jelzések biztonságos és zavartalan működését hivatottak biztosítani többféle hálózattípus felett.

3 PÁLYAMENTI VASÚTBIZTONSÁGOT MEGVALÓSÍTÓ ÉPÍTŐELEMEK

3.1 Bevezetés

Napjaink vasúti infrastruktúrájának növekvő igényeket kell kiszolgálni mind a teher mind a személyszállítás területén. Egy korszerű, meglévő vasúti hálózattól elvárható, hogy képes legyen a kapacitását növelni a meglévő infrastruktúra felhasználásával anélkül, hogy a megbízhatósága vagy a biztonsága csorbát szenvedne. A modern, automatizált biztosító-, és forgalomirányító rendszerekkel mindez megvalósítható.

A klasszikusnak nevezhető biztosítóberendezések mechanikus, relés vagy elektronikus alapáramkörök használatával biztosították és biztosítják még sok helyen jelenleg is a megbízható vonatközlekedést, de bővíthetőségük, rugalmasságuk már rég nem tudja kiszolgálni a megnövekedett forgalmi igényeket. Ezzel szemben a modern, számítógép-alapú megoldások, amelyek az információs és kommunikációs technológiát (Information and Communication Technology – ICT) alkalmazzák, nagymértékben javítják nemcsak a meglévő infrastruktúra kapacitását, hanem a vasúti biztonságot is. Ezek a rendszerek egy, de inkább több, magas megbízhatóságú, stabil és egyre nagyobb átviteli képességű kommunikációs hálózatot igényelnek.

Jelenleg egyértelmű tendencia, hogy a kommunikációs hálózatok egyre inkább TCP/IP alapúak és valamilyen Ethernet technológiát használnak. Ez nemcsak az irodai és otthoni környezetben figyelhető meg, hanem ipari alkalmazásokban is, így a vasúti kommunikációs hálózatok sem kivételek ez alól. A TCP/IP alapú Ethernet hálózatok használata a vasúti kommunikációban számos előnyt kínál, például nagyobb sávszélességet, költséghatékonyságot és szabványos, széles körben elérhető eszközöket. Ugyanakkor komoly technikai és biztonsági kihívásokat is felvet.

A vasúti környezet magas biztonsági követelményszintek teljesítését várja el a kommunikációs rendszerekkel szemben.

A korábbi, szinkronizált adatkommunikációs rendszerekhez képest a TCP/IP csomagkapcsolt hálózatok alaptulajdonsága a best-effort (legjobb szándékú) adattovábbítási képesség, ami röviden annyit jelent, hogy alapértelmezés szerint nincs garancia az adott adatcsomag megérkezésére, sértetlenségére vagy késleltetésére. Emiatt

a TCP/IP és Ethernet technológiák csak megfelelő kiegészítésekkel, specifikált változataik alkalmazhatók vasúti környezetben.

Csoportosítás szükségessége

A megfelelő interfészazonosítás, az alkalmazott protokollok, a berendezések csatlakozási módjának megválasztása a hálózat tervezésének és megvalósításának kritikus pontja. Ezek a hálózati kapcsolatok különböző szintűek a létfontosság tekintetében és ennek tükrében kell a rendelkezésre állóságot biztosítani.

Az interfészek és a köztük lévő kommunikációs technológiák kapcsán szükséges megkülönböztetni, hogy az egyes alrendszerek milyen mértékben járulnak hozzá az egész rendszer biztonságához, megbízhatóságához. Ez elsősorban a vonatkozó szabványokon alapul és a szolgáltatások, funkcionalitások alapján kerülnek kategorizálásra. A következőkben biztosítóberendezési rendszer interfészei és kommunikációs kapcsolatai kerülnek fókuszba és fontosságuk szerinti csoportokba.

3.2 Kritikus és nem kritikus hálózatok

Kritikus

A kritikus vagy létfontosságú hálózat (vital-network) olyan hálózati infrastruktúra, amelynek meghibásodása, leállása vagy teljesítménycsökkenése közvetlen és súlyos hatással van a vasúti rendszer működésére, biztonságára, akár követlen életveszélyt is jelenthet. Ezek a hálózatok tipikusan szigorú megbízhatósági, rendelkezésre állási és biztonsági követelményeknek kell megfeleljenek, általában SIL4-es [10] besorolást független tanúsító által kell kapjanak. A vonatkozó szabványok teljesítése végett rendszerint alkalmaznak redundanciát, késleltetés-optimalizációt, és különböző hibajavító, vagy jelző eljárásokat.

Nem kritikus

A nem kritikus, vagy nem létfontosságú hálózat (non-vital network) ezzel szemben olyan hálózat, amelynek meghibásodása, időleges leállása vagy teljesítménycsökkenése nem befolyásolja jelentősen az alapvető működési folyamatokat. Ezeknél a hálózatoknál a megbízhatósági, rendelkezésre állási és késleltetési követelmények általában kevésbé szigorúak. Nem feltétlenül kell redundanciát és hibakezelési mechanizmusokat alkalmazni esetükben.

Csak elkülönített megvalósítás

A digitalizáció hatására a vasúti kommunikációban is egységesedés figyelhető meg, azaz a kommunikációs hálózatok egyformán digitális adatokat kezelnek. Ha a vállalati vagy internetszolgáltatói hálózatokra szolgáltatásokra gondolunk, az IP-alapú átvitel felé történő konvergencia egyértelmű és ugyanez a tendencia a vasúti szektorban is egyre meghatározóbbá válik.

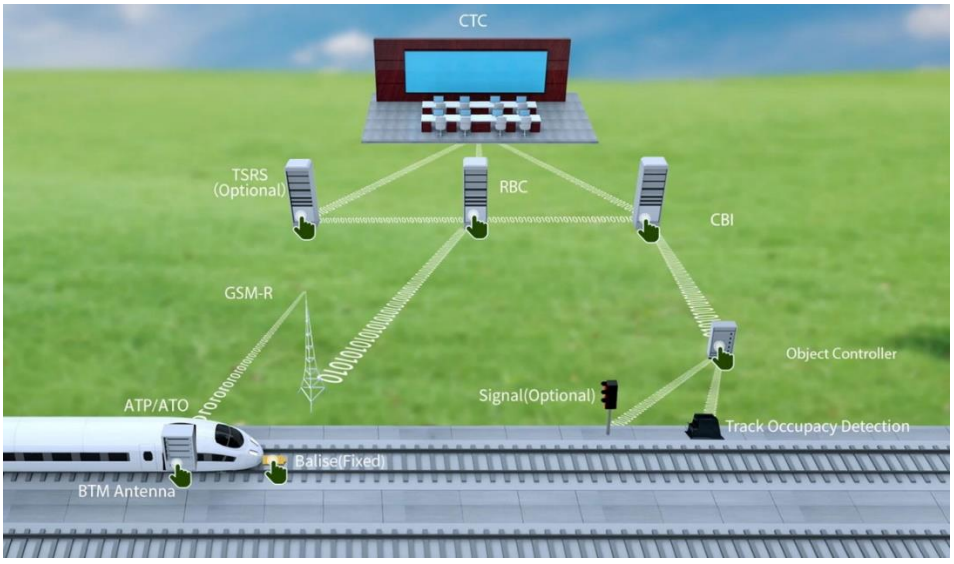
Napjainkban már lehetőség van arra, hogy egy megfelelő kapacitású és megbízható közös hordozóhálózaton belül olyan virtuális hálózatokat és alhálózatokat hozzunk létre, amelyek egymástól teljesen elkülönítve működnek, különböző minőségi mutatókkal rendelkeznek, prioritásokat képesek kezelni. Ezek a megoldások csökkentik a kommunikációs infrastruktúra szükséges mennyiségét, és gazdaságosabb üzemeltetést tesznek lehetővé.

Elméletileg ez a megközelítés a vasúti kommunikációban is alkalmazható lehetne, azonban a biztonsági, megbízhatósági és fokozott rendelkezésre állási követelmények miatt jelenleg nem megengedett – és remélhetőleg a jövőben sem válik megengedetté.

A kritikus és a nem kritikus hálózattípusnak merőben eltérő követelményeket kell teljesíteniük, megvalósításuk csak elkülönítetten valósítható meg.

3.2.1 Kritikus hálózatok, kapcsolatok, interfészek

A 2. szintű ETCS rendszerelemek kapcsolatait szemlélteti az alábbi ábra funkcionális szempontból:



6. ábra. ETCS2 funkcionális elemei [42]

- CBI – RBC interfész. Funkciója: az ETCS Level 2 és 3 rendszerben az RBC valós időben számítja ki és továbbítja a vonatok számára a menetengedélyeket más haladással kapcsolatos adatokat. A számítások alapjául szolgáló pályainformációk (váltók és jelzők állapota, további biztosítóberendezési információk) ezen az interfészen érkeznek a CBI felől. Kritikussága: Magas, Az interfész meghibásodása esetén a vonatok nem kapnak menetengedélyt, ami leálláshoz vezet. Ezen létfontosságú hálózati kapcsolatoknak és a kiszolgáló berendezéseknek rendszerszinten meg kell felelniük a SIL 4 [10] követelményeinek.
- RBC – GSM-R (jövőben FRMCS) hálózati interfész. Funkciója: az RBC a GSM-R mobilhálózaton keresztül kommunikál a fedélzeti ETCS egységekkel, biztosítva a menetengedélyek és más menetadatok továbbításának folytonosságát. Kritikussága: Magas – Ha például a GSM-R kapcsolat megszakad, a vonatok nem kapnak menetengedélyt, ami vészfékezést vált ki, ha a kapcsolat egy meghatározott időn belül (TNV_CONACT) nem képes helyreállni,.
- RBC – RBC interfész. Funkciója: a szomszédos RBC-k biztosítják az ETCS Level 2 vonatok zökkenőmentes átadását egyik RBC kiszolgálási területéről a másikra. Kritikussága: Magas – ha az interfész hibás, a vonatok nem léphetnek be az új RBC területére, a szerelvény megállásra kényszerül.
- CBI – pályamenti rendszerelemek vezérlője közötti interfész. Funkciója: a CBI a foglaltságérzékelő eszközökből (pl. sínáramkörök, tengelyszámlálók) származó adatokat dolgozza fel. A pályamenti információk összegyűjtése és a pályamenti eszközök vezérlése a legmagasabb szintű biztonságot igényli, ezért ezek a kommunikációs kapcsolatok létfontosságúnak számítanak. Kritikussága: Magas – Ha a foglaltságérzékelés információi nem jutnak el a CBI-hez, akkor a biztosítóberendezés hibát jelez és megállítja a közlekedést. (Rossz esetben hibás információkat adhat a vonathelyzetekről, de ennek előfordulási esélye igen csekély a kötelezően betartandó legmagasabb biztonsági integritási szint miatt ezen eszközök és hálózatok esetében.
- TSRS-RBC interfész. Funkciója: az RBC felelős azért, hogy az ETCS Level 2/3 rendszerekben a vonatok mindig érvényes sebességkorlátozási információkat kapjanak. Az RBC a TSRS-ből kapott adatokat továbbítja a vonatok fedélzeti

ETCS rendszerének a GSM-R mobilhálózaton keresztül. Például egy pályahiba vagy karbantartás miatt új ideiglenes sebességkorlátozás (TSR) lép életbe, azt a TSRS közvetíti az RBC felé, ami továbbítja az érintett szerelvények felé. Ha az interfész meghibásodik vagy az információ jelentősen késik, a vonatok nem kapják meg időben a frissített sebességkorlátozásokat, ami veszélyes helyzetet teremthet, de az alkalmazott biztonsági protokollok miatt az ETCS-fedélzeti egység egy konzervatívabb megközelítést alkalmazhat és pl. alacsonyabb sebességen engedi a vonatot haladni. Ettől függetlenül a teljes rendszer megbízhatósága csökken, tehát az interfész kritikussága magas.

- CTC – RBC interfész. Funkciója: ezen az interfészen a központi forgalomirányítás elsődlegesen üzemi és menetrendi adatokat szolgáltat az RBC számára. Például az RBC a menetengedélyek kiadásánál figyelembe vehet olyan vonatút-beállítási információkat, amelyeket ezen az interfészen kap meg a CTC-től. Ennek az interfésznek a kiesése esetén az RBC továbbra is tud működni a CBI által szolgáltatott adatok alapján, de a forgalomirányítási folyamatok jelentősen megnehezedhetnek és szükség lehet manuális beavatkozásra is. Ilyenkor a CBI-RBC a saját kiszolgálási területükön belül hozzáférnek azokhoz az adatokhoz, amik a biztonságos vasúti közlekedés feltétele, de a teljes vonali forgalomirányítás nem működik teljes értékűen. Kritikussága: Mérsékelt (nem kritikus, de fontos)

- CTC – CBI interfész. Funkciója: A CTC és a CBI közötti kapcsolat lehetővé teszi a központi forgalomirányítás számára, hogy távolról felügyeljék a biztosítóberendezés állapotát és szükség szerint állítsák a váltókat és a jelzőket. A A CBI önállóan képes önállóan is működni helyi vezérléssel, de a központi forgalomirányítással való kapcsolat elvesztése esetén a forgalomirányítás hatékonysága csökken. Kritikussága: Fontos, de nem feltétlenül biztonságkritikus

- TSRS – CTC interfész. Funkciója: A TSRS (Temporary Speed Restrictions – TSR) tárolja és kezeli az ideiglenes sebességkorlátozásokat. A forgalomirányítás ezen az interfészen keresztül ellenőrizheti és menedzselheti (lekérdezheti, frissítheti vagy módosíthatja) az időleges sebességkorlátozásokat, pl. pálya-karbantartás, időjárási viszonyok miatti korlátozások.

Az interfész működésképtelensége esetén a CTC nem tudja közvetlenül frissíteni vagy ellenőrizni az ideiglenes sebességkorlátozásokat, de ettől még a vasúti közlekedés alapvetően tovább működik. Ebben az esetben szükség esetén manuális beavatkozás kell, ami az információ késését okozza. Ez a forgalomirányítás hatékonyságát csökkentheti, de a vonatok közlekedése folyamatos maradhat a korábban érvényes TSR-ek alapján. Kritikussága: Nem biztonságkritikus, de fontos.

3.2.2 Kezelői interfészek csatlakozásai

A kezelői interfész (HMI – Human-Machine Interface) olyan hardveres és szoftveres rendszerelem, amely lehetővé teszi az ember és az irányítási vagy valamilyen technológiai rendszer közötti interakciót. A kezelői interfészek a vasúti rendszerekben kulcsszereppel rendelkeznek a biztonságos és hatékony üzemeltetésben, mivel a forgalomirányítók, diszpécserek karbantartók, fejlesztők és további más szakemberek ezeken keresztül figyelhetik meg, vezérelhetik és konfigurálhatják a különböző rendszereket.

Különböző funkcionális célú kezelői interfész minden rendszerelemhez csatlakozik vagy csatlakoztatható, így a korábbiakban bemutatott rendszerelemek mindegyike rendelkezik üzemeltetési, karbantartási, diagnosztikai vagy egyéb célú kezelői interfésszel, vagy interfészekkel.

3.2.2.1 Üzemeltetési interfészek

Ezek a szokványos, mindennapi forgalomirányítási és üzemi működtetéshez szükséges interfészek. A kezelők ezeken keresztül végzik a rendszer felügyeletét és vezérlését. Funkciók szerint:

valós idejű adatmegjelenítés passzív vagy aktív interakciókkal. Pl. KÖFI, CBI HMI felületei a vonathelyzetek, jelzőállapotok, váltóállások megjelenítésére vagy kezelésére. Mozdonyvezetői kijelzők és beavatkozók a menetkezelésre vonatkozóan.

3.2.2.2 Karbantartási, diagnosztikai interfészek

Üzemeltetési naplók, riasztások és figyelmeztetések megjelenítése, letöltése. A kezelői interfészek két fő módon csatlakozhatnak az adott rendszerelemhez: helyileg és távolról.

Helyi hozzáférés (Local Access)

A helyi kezelői interfész közvetlen, hardveres kommunikációs kapcsolatban áll az irányított vagy felügyelt rendszer kezelői interfészével. A kezelői felületet megvalósító munkaállomás vagy érintőképernyős panel közvetlenül csatlakozik a vezérlőrendszerhez, például Etherneten, soros vonalon (RS-232, RS-485) vagy akár egyéb ipari protokollokon (PROFINET, CAN busz, stb.) keresztül.

Speciális, dedikált terminálok: vasúti környezetben a munkaállomások mellett a forgalomirányító és a vonali biztosítóberendezések saját kezelőpultokkal (pl. grafikus, nagyképernyős megjelenítő) is rendelkezhetnek, amelyek a rendszer belső interfészein keresztül kapcsolódnak a vezérlőegységhez.

Távoli hozzáférés (Remote Access)

A távoli kezelői interfésszel lehetővé válik az adott rendszer felügyelete és irányítása akár nagy távolságból is. Legjellemzőbb csatlakozási mód új kiépítéseknél, általában IP-alapú hálózatokon keresztül történik. Ekkor a kezelői felület a távoli munkaállomásról vagy a központi forgalomirányítási rendszerből (KÖFI) elérhető, jellemzően adott biztonsági szintet teljesítő kommunikációs csatornán (pl. VPN, MPLS vagy egyéb hálózati megoldások alkalmazásával), vagy elkülönített, dedikált hálózaton.

3.2.3 Összegzés

- Kritikus interfészek: Azok az interfészek, amelyek közvetlenül befolyásolják a vonatok biztonságát és működését: magas SIL besorolást igényelnek.
- Nem kritikus interfészek: Az üzemi és információs interfészek, amelyek kiesése nem befolyásolja közvetlenül a vonatok biztonságát: alacsonyabb SIL követelmények vonatkoznak rájuk.

A 3. táblázat összegzi a korábbiakban bemutatott interfészek csoportosítását biztonsági és megbízhatósági szempontok szerint. A fenti csoportosítás alapja az EN 50126, EN 50129 és EN 50159 szabványokban megfogalmazott funkciók és az azokhoz kapcsolódó a Safety Integrity Level (SIL) és a RAMS követelmények.

Interfész	Kritikus?	SIL besorolás (EN 50129)	RAMS követelmények (EN 50126)
RBC – CBI	Igen	SIL4	Nagyon magas
RBC – GSM-R	Igen	SIL4	Nagyon magas
RBC – RBC	Igen	SIL4	Nagyon magas
CBI – tengelyszámlálók	Igen	SIL4	Nagyon magas
TSRS – RBC	Igen	SIL2-SIL3	Közepesen magas
TSRS – CTC	Nem kritikus	SIL1 vagy „SIL0”	Alacsony/közepes
CTC – CBI	Nem kritikus	SIL1-SIL2	Közepes
CTC – TSRS	Nem kritikus	SIL1 vagy „SIL0”	Alacsony
HMI – Kritikus rendszerek	Igen	SIL3-SIL4	Magas
HMI – Diagnosztika	Nem kritikus	SIL1 vagy SIL0	Alacsony

3. táblázat. Interfészek kritikussága

3.3 Infokommunikációs interfészek - Fizikai közegek

Az alkalmazott kommunikációs interfészeket és azok kategóriáit az ISO-OSI rétegezettség mentén tekintem át.

3.3.1 Rádiós interfész

A vonat (mozdonyok) és a pályamenti eszközök között csak rádiós, azaz levegő (air), interfész található, mivel fix és mozgó elemek vesznek részt a kommunikációban.

3.3.1.1 Balíz (Eurobalise) interfész:

A pályán elhelyezett balízok és a vonaton található balíz-olvasó (Balise Transmission Module, BTM) közötti kommunikációt biztosítja. Kevés adat szállítására optimalizált, de robosztus interfész. Feladata, hogy nagy sebességgel közlekedő vonat is biztosan ki tudja olvasni a tárolt információt. A balízok mozdony irányába való adattovábbításához nem szükséges tápellátás, a kiolvasáshoz szükséges energiát a mozdonyban lévő olvasó biztosítja induktív módon.

Vezérelt balízok esetén a dinamikus információk betöltése a balízba vezetékes úton történik a LEU felől, de az teljesen független interfész ettől.

3.3.1.2 GSM-R interfész:

A GSM-R (Global System for Mobile Communications – Railway) vasúti alkalmazásokra optimalizált mobil kommunikációs rendszer. A Radio Block Center (RBC) és a vonaton található EVC (European Vital Computer) közötti adatkommunikáció használja a GSM-R interfészt e mellett beszédátvitelre is alkalmas. Feladata, hogy kétirányú, folyamatos

kapcsolatot tartson fenn a vonat és a pályamenti hálózat között. A GSM-R rádióhálózat RBC-kből, bázisállomás-vezérlőkből és bázisállomásokból áll. Ezen az interfészen többek között a vonat valós idejű pozíció adatai, menetengedélyek, sebességgel kapcsolatos utasítások kerülnek továbbításra. Csak nagyon magas szintű szemlélet esetén beszélhetünk GSM-R interfészről, mivel maga a vonat-pályamenti rádiós interfész a mozdony és a bázisállomások közötti levegő interfész szigorúan véve. A bázis állomások és az RBC között számos más technológia (elsősorban vezetékes optikai) és protokoll alkalmazása valósítja meg a kommunikációt.

A rádiós interfész (Um interfész) kétirányú kommunikációt valósít meg. Frekvenciasávban a full-duplex átvitel Downlink irányban: 921–925 MHz, míg Uplink irányban: 876–880 MHz között találjuk. Mivel kritikus infrastruktúráról van szó, ezek a sávok Európában a vasút számára kizárólagosak, így alacsony interferencia és kontrollálható telítettség jellemzi. A nyilvános GSM-hez hasonlóan a többszörös hozzáférést TDMA 8 időréses struktúrával biztosítja alapvetően. A digitális adatok átvitelére a robosztus GMSK modulációt használja.

A vasúti kommunikáció speciális jellege miatt optimalizált megoldásokkal találkozunk: hosszabb, hosszúkás cellák kialakításának lehetősége, akár 70km-es hosszig, szemben a GSM 35km-es limitjével. Nagy sebességű mozgás támogatása: biztos adatátvitel 500 km/h sebességig, speciális kézbesítési prioritások érvényesítése a kommunikációban mind adat, mind beszédcélú hívások esetén.

3.3.1.3 Jövőbeli megoldás az FRMCS

Bár a vasúti kommunikáció adatmennyiség igényét jelenleg a GSM-R korlátozott átviteli képessége maradéktalanul ki tudja szolgálni, de a fejlesztési irányok és a növekvő szolgáltatási igények miatt ez a korlát hamarosan akadályozná a fejlesztéseket. E mellett a gyártók oldaláról is van folyamatos nyomás, hogy a régebbi technológiák támogatását megszüntessék. Gazdaságilag nem kifizetődő több tízéves támogatást nyújtani olyan elemekre, részegységekre, vagy komplett rendszerekre, amelyek rendelési darabszáma viszonylagosan alacsony. Ráadásul a gyártási folyamatot az is drágítja, hogy biztonságkritikus eszközök lévén SIL és egyéb tanúsítási minősítéseket is meg kell szerezni rájuk.

A Future Railway Mobile Communication System (FRMCS) a GSM-R utódja lesz Európában és várhatóan a világ sok más részén is. 5. generációs földi cellás mobilhálózati

szabványon alapul, mely az UIC (International Union of Railways) és a 3GPP közös fejlesztése (3GPP Release 17 és későbbi verziók). Egységes IP alapú adatátviteli platformot nyújt a vasúti kommunikáció minden szegmenséhez, beleértve a biztonságkritikus adatkapcsolatokat, hanghívásokat – ahogy a GSM-R-ben is volt. Ezen felül mozgógépek továbbítása és nagyszámú IoT eszközök kezelésére is alkalmas, ami új szolgáltatások megjelenését jelenti.

Az FRMCS a GSM-R-hez képest sok új szolgáltatást és magasabb KPI értékeket teljesít: nagyobb adatátviteli sebességet, alacsonyabb késleltetést, QoS-alapú forgalomszabályozást, natív forgalmi prioritáskezelést.

Az FRMCS szabványosított funkciói, mely alapvető fontosságúak a jövőbeli hordozóhálózat szolgáltatási között:

- Mission-Critical Services (MCX), IP-alapú csoportos és vészhelyzeti kommunikáció
- Ultra-Reliable Low Latency Communications (URLLC): Nagyon alacsony késleltetésű kommunikáció (<5–10 ms) rendkívül magas megbízhatósággal párosítva (>99.999%)
- Network Slicing: Logikai „hálózatszeletek” kialakításának lehetősége különböző szolgáltatásoknak, melyek egymástól teljesen elkülönülten működhetnek, akár különböző képességekkel, paraméterekkel. pl. ETCS L3-at kiszolgáló „szelet”
- QoS osztályok széles skálája, vagyis garantált sávszélesség és késleltetés szolgáltatási teljeskörűen és dinamikus kialakítási lehetőséggel. (Ez korlátozottan a GSM-R-ben az eMLPP).
- Massive IoT & Sensor támogatás: Nagy számú végponti eszköz kapcsolatának fenntartása, jellemzően alacsony adatátviteli igényekkel. Szenzorok rendszerbe integrálása karbantartási, üzemeltetésoptimalizálási célból.

Néhány jövőbeli funkcionalitáshoz, alkalmazáshoz rendelve az FRMCS fentebb felsorolt képességeit:

- Az ETCS L3 lehetőségeit csak egy megbízható és a GSM-R-hez képest alacsonyabb késleltetésű hálózat biztosíthatja, amit az FRMCS URLLC képes teljesíteni a stabil, alacsony késleltetésű adatkapcsolatával.

- Automatikus vonatvezetés (ATO) megvalósításához URLLC kapcsolat, Mission Critical Szolgáltatások és pontos időszinkron (PTP/TSN) szükséges.
- Vészhelyzeti videóhíváshoz, Misson Critical Video hívási szolgáltatás szükséges.
- Szenzorok által szolgáltatott adatok alapján a prediktív karbantartás megvalósításához a Massive IoT támogatás a megoldás.
- Előnyben részesített diszpécseri utasítás: MCPTT és QoS prioritás, hasonlóan a GSM-R eMLPP-jéhez, csak dinamikusabb és szélesebb paraméterezéssel.

3.3.1.4 Műholdas kommunikáció, mint lehetőség

A földi cellás rádiós lefedettség mellett technológiailag indokolt megemlíteni a műholdas kétirányú kommunikáció lehetőségét is és annak vasúti alkalmazását.

A műholdas kommunikációnak a vasút tekintetében az igen gyéren lakott, infrastruktúrában szegény területeken lehet a jövőben szerepe. Jelenleg is vannak nagy kiterjedésű lakatlan, infrastruktúra nélküli területeken vasútvonalak (pl. Ausztrália északi részén lévő vasútvonalak, Kanada, Oroszország és Afrika egyes részein.) Ezeken a területeken hatalmas költség lenne kialakítani a cellás lefedettséget biztosító földi infrastruktúrát.

Jelenleg is léteznek már kétirányú kommunikációt biztosító LEO műholdhálózatok, melyek a távolabbi jövőben alkalmazhatók lehetnek vasúti környezetben is. A műholdas rendszerek vasúti célú kritikus infrastruktúraként való alkalmazásának legjelentősebb korlátja a késleltetés. Ezért is egyedül a LEO pályán keringő műholdak jöhetnek számításba, ahol 20-50ms körüli értéken lehet tartani a fizikai réteg kétirányú késleltetését, a körül-fordulási időt. Az alábbi szolgáltatók műholdas rendszerei jelenleg is biztosítanak kétirányú adatkommunikációt:

- OneWeb (Eutelsattal egyesülve): együttműködésben van több távközlési vállalattal és globális szélessávú lefedettséget igyekszenek kialakítani az infrastruktúráktól távol eső területeken LEO műholdakkal. Pl. Ausztráliában és Új-Zélandon. Ez az infrastruktúra alkalmas lehet vasúti kommunikációra cellás földi hálózat mobilhálózat helyett. [62]
- Az Iridium műholdas távközlési szolgáltató globális lefedettséget biztosít már évtizedek óta. Az Iridium NEXT műholdak fellövésével elérhetővé vált az Iridium Certus szolgáltatás [44], amely IP-alapú adatátvitelt és közvetlen internet-

hozzáférést kínál. Az Iridium már tapasztalt kritikus kommunikációs alkalmazásokban is, pl. rendelkezik a Globális Tengeri Vészhelyzeti és Biztonsági Rendszer (GMDSS) szolgáltatás biztosításához is tanúsítvánnyal. (Azelőtt csak az Inmarsat volt jelen ezen a területen). Alacsony sávszélesség jellemző a rendszerre, a megbízhatóságra és a biztos lefedettség biztosítására optimalizálták.

- Telesat Lightspeed – Kanadai távközlési szolgáltató, műholdas hálózatát alacsony késleltetésűre és a korábbi rendszerekhez képest nagyobb kapacitásúra tervezték. Felhasználási körét elsősorban ipari (akár kritikus) alkalmazások teszik majd ki (pl. légiközlekedés, hajózás, hadsereg vagy a vasút is a jövőben). Üzembe állítása legkorábban 2027-re várható. [46]

- Starlink (SpaceX) – Nagy adatátviteli sebesség, alacsony késleltetés jellemzi, ezek alapján alkalmas lehetne vasúti kritikus kommunikáció hordozószolgáltatásának is, de a determinisztikus átvitel jelenleg még nem garantált, a szükséges KPI elvárások nem teljesülnek. Hasonlóan a GSM-R-hez dedikált frekvencia tartomány és a nyilvános hálózattól, nyilvános forgalmaktól elkülönített működés szükséges, ez sem teljesül jelenleg. Jelenleg néhány vasúttársaság az utasélmény növelésére célozta meg ezt a szolgáltatást internetelérésre használja [45].

- Az Inmarsat jelenleg GEO pályán lévő műholdakkal szolgál ki kommunikációs igényeket, köztük tengeri alkalmazásban tanúsított vészhelyzeti kommunikációs alkalmazás is található. A biztos lefedettség az egyik fő szempont, de a GEO műholdaknál a magasabb keringési pályák tipikusan 500–700 ms körülfordulási idejű késleltetést eredményeznek. Ez már túl sok valós idejű biztonságkritikus kommunikációhoz, például az ETCS Level 2 vonat – RBC kapcsolatban. Ezt orvosolandó az Inmarsat tervezi egy hibrid GEO+LEO+5G földi mobil hálózat kombinált rendszer bevezetését a jövőben, ennek a projektnek a neve „Orchestra”. A különböző technológiák előnyeit igyekszik ez a projekt ötvözni és a hátrányokat az együttműködés révén elnyomni. Globális és stabil lefedettség a GEO műholdaknak köszönhetően. Nagyobb forgalmú területeken kapacitásnövelés lehetősége, kisebb késleltetéssel a LEO műholdak segítségével. Magas forgalmi igényeket támasztó területeken pedig együttműködés a földi 5G cellás mobilhálózatokkal. Ezek koordinált együttműködése (a technológiák közötti észrevétlen handover) biztosítja majd a zökkenőmentes kommunikációt. E mellett

a hálózat központi és útválasztói elemeinek terheltségét decentralizált mesh technológiával igyekszenek csökkenteni, ami a műholdakon keresztüli közvetlen routolást vagy akár a kommunikációs partnerek közötti közvetlen kapcsolat felépítésére is képes.

Összességében elmondható, hogy a rádiós interfész esetén a műholdas kommunikációban van potenciál, de a jelenleg is sűrűn lakott, kellő infrastruktúrával ellátott területeken gazdaságilag nem kifizetődő ilyen rendszerek alkalmazása. Európa több részén már kiépített a GSM-R hálózat van az ETCS kommunikációhoz, ennek továbbfejlesztése az indokolt és kifizetődő.

Az átállás egy teljesen új kommunikációs hordozóra jelentős költséggel és szabványosítási kihívásokkal járna. A LEO rendszerek nem nyújtanak nagy előnyt olyan területeken, ahol a földi cellás lefedettség már eleve jó. Továbbá a műholdas kétirányú kommunikáció esetén, az oda vissza irányú késleltetés, mint minőségi paraméter mindig is magasabb marad, mint egy hasonló képességű és kapacitású földi hálózatban. Ezen kívül az elvárt redundáns, duplikált lefedettség biztosítása, a műholdak gyors mozgása és a gyors mozgásuk miatti gyakori handoverek további kihívást jelentenek egy ilyen hálózat megfelelő stabilitású és biztonságú szintjének kivitelezésében. Kiegészítő rendszerként, tartalék kommunikációs lehetőségnek viszont van esély, hogy hamarabb alkalmazásba kerülnek. Kutatásomban ezzel a kommunikációs lehetőséggel mélyebben nem foglalkozom.

3.3.2 Vezetékes közegek – optika

Az optikai szálas kommunikáció kulcsfontosságú szerepet tölt be napjainkban a modern kommunikációs rendszerek minden területén így a korszerű vasúti rendszerekben. Nagy sávszélességet, alacsony késleltetést és kiváló elektromágneses zavartűrést biztosít. Ez utóbbi kiemelten fontos a vasúti környezetben, mivel az esetek többségében a vasúti pálya mentén haladnak az optikai szálak nyomvonalai, az oszlopokra rögzítve, vagy föld alatti kábelcsatornákban. Ezek az optikai hálózatok megbízható gerinchálózatot biztosítanak a különféle kommunikációs, vezérlési és biztonsági rendszerek számára.

A vasúti távközlési és vezérlési hálózatokban jelenleg a single-mode száloptikai kábelek a legelterjedtebbek. Ezek a kábelek kis csillapítással és alacsony diszperzióval rendelkeznek így különösen alkalmasak nagytávolságú és nagy megbízhatóságú adatátvitelre.

A WDM (Wavelength Division Multiplexing) technológia, különösen annak „sűrített” változata (DWDM), lehetővé teszi, hogy egyetlen szálon több független adatfolyam legyen jelen különböző hullámhosszokon. Ezzel a módszerrel jó esetben egy már meglévő optikai kapcsolat kapacitása megnövelhető anélkül, hogy további fizikai kábelezésre lenne szükség. A jövőben várhatóan még tovább nő a WDM-alapú megoldások szerepe, az ETCS Level 2 és 3-hoz kapcsolható kritikus kommunikációval kapcsolatban vagy a jövőbeli FRMCS mobil rendszerek pályamenti oldalán.

A kritikus rendszerek számára alapvető fontosságú az alacsony késleltetésű kommunikáció és időszinkron fenntartása, amely szintén jól illeszkedik az optikai infrastruktúrához (pl. PTP over fiber). Ez alapján kijelenthető, hogy az optikai szálak szerepe kritikus jelentőségű technológiai alapot képez a jövő vasúti kommunikációs rendszereiben.

3.3.2.1 Alkalmazás kritikus kommunikációs rendszerekben

ETCS/ERTMS kommunikáció: az ETCS Level 2 és 3 rendszerben az RBC-k és további alrendszerek közötti kommunikációhoz szükséges megbízható IP-hálózat gerincét legtöbb esetben, napjainkban optikai kapcsolat biztosítja.

GSM-R háttérhálózata: a GSM-R-ben a rádiós interfész pályamenti oldalán a BTS – BSC – MSC, MSC – RBC kapcsolatok jellemzően optikai szálon történnek.

A központi forgalomirányítás és biztosítóberendezések hálózatai magas megbízhatóságát szintén az optikai hálózatok képesek teljesíteni. Ezekhez a rendszerekhez rendelt SIL biztonsági szinteknek megfelelő redundancia, gyors helyreállási idők kialakítására kifejezetten alkalmasak az optikai szálak.

Biztonságkritikus adatátvitel esetén a késleltetés és az időszinkron fenntartása alapvető fontosságú, pl. PTP (Precision Time Protocol – IEEE 1588), MPLS, TSN – ehhez az optikai átvitel megbízhatósága és alacsony késleltetése alapvető fontosságú.

3.3.2.2 Alkalmazás nem kritikus rendszerekben

Vagyonvédelmi és videómegfigyelő rendszerek esetében a nagyfelbontású kamerák, kamera rendszerek hatalmas mennyiségű adatainak átvitelére gyakran csak az optikai hálózatok képesek.

Utas-tájékoztató és jegyértékesítő rendszerek, azaz az utasok kiszolgálását szolgáló rendszerek is megnövekedett adatmennyiséggel dolgoznak, ezek csatlakoztatása is szintén optikai hálózaton keresztül történik.

3.3.3 Vezetékes közegek – rézvezeték

Az elektromos áram megjelenéséhez köthető a rézvezeték alkalmazása, jó áramvezetőképessége és kedvező mechanikai tulajdonságai alapján.

A vasúti távközlési és vezérlési rendszerek fejlődése során a rézvezetékes kommunikációs kapcsolatok hosszú időn át – az optikai átvitel megjelenéséig – kizárólagos szerepet töltöttek be. A rézvezetékek előnyei közé tartozik a viszonylag egyszerű telepíthetőség, kedvező ára, valamint az energiaátvitel lehetősége.

A korszerű vasúti infrastruktúrában ma is található számos terület, ahol a rézvezeték maradt a célszerű megoldás, ilyenek például a szervertermekben és kapcsolóhelyiségekben kialakított kommunikációs kapcsolatok, ahol tipikusan a lokális Ethernet-alapú adatátvitel (pl. UTP CAT5e/CAT6 kábelek segítségével) rézvezetéken történik. Ezeken a rövid és jellemzően zavarvédett távolságokon belül a réz gyors, olcsó és megbízható kapcsolatot biztosít hálózati eszközök, szerverek vagy kezelőpanelek között.

A rézvezetékeket a vasúti infrastruktúrában mind a mai napig alkalmazzák, különösen olyan rendszerekben, ahol lokális vezérlésre, alacsony vagy középfeszültségű betáplálásra, illetve régi rendszerelemek fenntartására van szükség.

3.3.3.1 Rézvezetékek klasszikus alkalmazásai

Rövid áttekintés keretében összefoglalót adok a régebben, klasszikus alkalmazásokhoz köthető rézvezetékes alkalmazásokról. Sok esetben előfordul, hogy ezek korszerű elemekre való lecserélése nem egy időben valósul meg, viszont az új digitális alapú megoldásoknak illeszkedni, együttműködni kell ezekkel az öröklött (legacy) rendszerekkel, rendszerelemekkel. Ezekben az esetekben sokszor egyedileg készül egy-egy interfész-illesztő áramkör, ami megvalósítja az információ átalakítását, ha kell két irányban.

Analóg vagy digitális távbeszélő rendszerek rézvezetéken kommunikálnak. Az analóg jeleket digitalizálni szükséges, általában PCM jelekké alakították, hogy utána digitális trönkvonalakon lehetséges legyen a digitális multiplexelésük. Az ISDN digitális

készülékek PCM jelekkel üzemeltek. Ezek illesztése a korszerű VoIP (Voice over IP) hálózatokhoz probléma mentes, mivel a távközlési szolgáltatóknak már évtizedek óta bevált eszközeik vannak a klasszikus beszédcélú távközlő berendezések jeleinek VoIP rendszerekbe való átalakítására.

Elektromechanikus és később az elektronikus biztosítóberendezések és az ahhoz kapcsolódó eszközök, mint pl. jelzők, váltók, foglaltságjelző áramkörök, sorompók, vezérlései közvetlen vezetékezéssel, relés áramkörökkel, vagy alapáramkörökkel valósították meg a vezérlést és a helyes működés ellenőrzését való visszajelzéseket. Ezeken az egyszerűnek mondható interfészeken meghatározott feszültség jelenléte, vagy előírt áram nagysága volt az információ, ami a vezérlést vagy a helyes működést igazolta. A vezetékeken kommunikáció jellemzően nem volt, vagy csak igen korlátozottan, ha többféle visszajelzési, vagy vezérlési információ továbbítása volt a cél az rendszerint további erek, vagy érpárak jelenlétét jelentette.

A hangos utastájékoztatás hangrendszerének vezetékei is rézkábeleken futottak az állomáson belül, vagy az állomások között, a hangot analóg módon továbbítva.

Központi órahálózatok vezetékei, az állomási órák, sőt az üzemeltető összes órájának szinkronban tartása régen is és most is alapvető fontosságú. Régen a szinkronban tartást elősegítő impulzusok rézvezetékeken keresztül érkeztek egy központi óráról.

3.3.3.2 Rézvezetékek alkalmazása napjainkban

Bár egyre több helyen digitális az átviteli technika, sokszor fordul elő, hogy régebbi berendezések illesztése megköveteli a rézvezetékes csatlakozást. Jellemzően végpontokon, rövidebb távolságokon, az adott készülék közelében a kommunikáció rézkábeles jelekre épül (pl. jelző és váltómotor vezérlés, vágány foglaltság visszajelzések, egyéb állapot-visszajelzések).

Régi telepítésű analóg telefonvonalak tartalékként való fenntartása, vagy az átépítés idejére előfordul.

Karbantartás, telepítés, konfigurálás esetén az esetek többségében réz alapú kapcsolat a leggyakrabban alkalmazott összeköttetés.

Energiaellátás

Kis és középfeszültségű táplálások (pl. 24V, 48V, 230V 400V) a biztosítóberendezés végberendezéseihez, továbbá a kommunikációt megvalósító eszközök táplálásához mindenképpen réz alapú vezetékeken történnek.

Kommunikáció és táplálás egyben

A rézvezetékes megoldások nemcsak régen, de jelenleg is lehetővé teszik az energiaellátást és a kommunikáció megvalósítását akár egy érpáron is.

A Power over Ethernet (PoE) [53] technológia egyszerre teszi lehetővé az adatátvitelt és az áramellátást egy közös Ethernet-kábelen keresztül, így különösen hasznos olyan helyeken, ahol a tápkábel kiépítése nehézkes – például mozgó vasúti járműveken vagy korlátozott hozzáférésű telepítési pontokon. Ezzel az eszközök csatlakoztatása jelentősen leegyszerűsödik, vagyis gyorsabb és olcsóbb lesz a telepítés és a fenntartás is

Egy másik módszer a PLC (Power Line Communication) technológia. Váltakozó áramú betáplálás esetén az alapfrekvencia (jellemzően 50Hz) fölé, nagyfrekvenciás jeleket (tipikusan kHz–MHz tartományban) szuperponálnak, az információ továbbítása ebben a frekvencia tartományban történik. Kétirányú kommunikáció is kialakítható így.

Két alapvető csoportja létezik:

- Broadband PLC (BB-PLC): 1–30 MHz közötti frekvencia tartományban valósul meg a gyorsabb adatátvitel, ami pl. lakossági internethozzáférésre alkalmazható, ipari környezetben nem jellemző, zavarérzékenysége, zavarsugárzási szintje miatt. Hatótávolsága is relatíve alacsony.
- Narrowband PLC (NB-PLC): 3–500 kHz közötti frekvencia tartományban hordozza az információs jeleket. Ez alkalmas hosszú távú adatátvitelre kis sávszélességgel, általában elektromos szolgáltatók az okosmérők leolvasására használják. Vasúti környezetben való alkalmazhatósága korlátozott, biztonságkritikus eszközök kommunikációjára inkább külön vezetéken működő, iparban már jól bevált kommunikációs módokat használnak (pl. RS-485, RS-422, CAN).

Amennyiben a redundáns kapcsolat kialakítása követelmény ez a mód nem alkalmazható, hacsak nem a táplálás kialakítását is duplikálva kell megoldani. Kevés információ, pl. csak néhány állapot visszajelzésére alkalmazható. Felügyeleti elektronikával rendelkező

jelzők esetén alkalmazható a jelző fényforrás állapotának visszajelentésére a biztosítóberendezés felé [7]. Hatótávolság km-es nagyságrendben van.

Szempont	**Rézvezeték**	**Optikai szál**
Átviteli adatsebesség	Alacsony, közepesen magas	Nagyon nagy
Zavarérzékenység	Magas (EMI érzékeny)	Alacsony (EMI mentes)
Hatótáv (erősítés nélkül)	Korlátozott	Több tíz-száz km (monomódus esetén)
Alkalmazhatóság	Lokális kommunikáció, Régi rendszerek, Energiatáplálás	Gerinchálózat, IP-rendszerek

4. táblázat. Vezetékes közegek jellemzői

3.4 Infokommunikációs interfészek – Adatkapcsolati réteg

Az OSI rétegmodel második rétegében történik meg a keretszervezés és az alacsony szintű „kapcsolás”, keret irányítás. A layer-2 hálózatok nagy jelentőséggel bírnak a hozzáférési technikák, illetve a nagy megbízhatóságú ipari hálózati kialakítások terén.

3.4.1 SDH szinkron hálózatok

Elsőként az igen kifutóban lévő szinkron hálózatokat említem meg, mert ezen kommunikációs hálózatok hosszú időn keresztül teljesítettek és – bár csökkenő számban – de teljesítenek szolgálatot mind a mai napig. A SDH (Synchronous Digital Hierarchy) gerinchálózati digitális átviteli technika. Jelenleg elsősorban optikai fizikai közegen találkozhatunk vele, de rezes és mikrohullámú közegen is használták. Biztos átvitelt biztosít valós idejű hibaérzékeléssel, és automatikus átváltással a redundáns útvonalakra hiba észlelése esetén. Hordozó hálózatként volt használatos a klasszikus E1, ATM kapcsolatok számára, majd a megjelenő IP hálózatokat is szolgálta.

A legfontosabb jellemzője viszont, hogy az adatkapcsolati szinten megjelenő konténerek időzítése szigorú szinkron szerint kerültek továbbításra. Az összes átviteli csomópont egy központi órához igazodott, így nagyon precíz időzítést és determinisztikus adattovábbítást tett lehetővé. Ennek eredményeképpen kiválóan alkalmazható késleltetés-érzékeny alkalmazásokhoz, mint pl. vasúti vezérlés.

3.4.2 Ethernet hálózatok

Ethernet (Fast Ethernet, Gigabit Ethernet, 10G Ethernet) és az ipari Ethernet (pl. PROFINET, EtherCAT, további gyártó specifikus változatok is) a vasúti központokban, állomásokon és a járművekben is használatos.

3.4.3 WLAN szabványok

WLAN szabványok 802.11 (pl. 802.11ac, 802.11ax) változatai biztonságkritikus rendszerekben nem használatosak, jellemzően utas élmény növelésére általában a fedélzeti Wi-Fi kialakítása terén kerül terítékre.

3.4.4 MPLS

Bár valójában az MPLS 3. rétegbeli csomagtovábbítást valósít meg cimkéivel, jelen esetben funkcionálisan ebbe a részbe soroltam, mert a többletszolgáltatásai révén válnak az IP/Ethernet hálózatok valóban alkalmassá a szinkron hálózatok leváltására.

A jelenlegi hálózati technológiák körében gerinchálózati szinten a Multiprotocol Label Switching (MPLS) egy széles körben alkalmazott megoldás, különösen az olyan esetekben, ahol magas rendelkezésre állás, alacsony késleltetés és forgalmi prioritások kezelése kiemelt követelmény, mint például a vasúti környezetben a kritikus infrastruktúrák kommunikációs igényeinek kiszolgálása. Az MPLS működése az OSI-modell szempontjából az adatkapcsolati réteg felett, a hálózati rétegben működik (az IP címzések alatt), és lehetővé teszi, hogy az IP-csomagok útvonalát előre meghatározott címkék (label-ek) alapján irányítsák gyorsabban, a klasszikus IP útválasztási módszerekhez képest.

Az MPLS alkalmazása igen előnyös például optikai gerinchálózatokban, ahol a redundáns topológia, az útvonalak gyors újrakiosztása, valamint a forgalmi osztályok szerinti prioritáskezelés fontos szerepet játszanak a megbízható, hatékony és gyors helyreállási képességű hálózati működésben. Ez a technológia tehát nemcsak a telekommunikációs szolgáltatói környezetben elterjedt, hanem a vasúti kommunikációs rendszerekben is (például az ETCS Level 2 és 3 hálózati infrastruktúrájában is helye van).

A vasúti IP-alapú alkalmazások – mint például a RBC–fedélzeti kapcsolat, vagy a valós idejű diagnosztikai adatátvitel – eltérő követelményeket támasztanak a hálózattal szemben. Az MPLS lehetővé teszi ezek logikai elkülönítését egyazon fizikai infrastruktúrán belül, miközben támogatja a különböző késleltetés- és rendelkezésre állási igényekkel bíró szolgáltatások egyidejű kiszolgálását is. Emellett jól kombinálható

különböző hálózat szinkronizációs technológiákkal (PTP, TSN), így egyfajta technológiai hídként szolgál a hagyományos IP-alapú és a determinisztikus hálózati megközelítések között.

3.5 Alacsony szintű UART kommunikáció

Az UART (Universal Asynchronous Receiver/Transmitter) nem igazán illeszthető az OSI modellbe, mivel adatkapcsolati és fizikai szintű funkciókat is ellát.

Az UART egy egyszerű, soros kommunikációs protokoll, célja két eszköz közötti aszinkron adatátvitel megvalósítása. Az UART maga a kommunikációs logika, míg a fizikai réteg (pl. TTL, RS232, RS422 vagy RS485) határozza meg a feszültség-, áramszinteket és az elektromos jellemzőket. Egyszerűsége és alacsony erőforrásigénye miatt az UART jelenleg is népszerű mikrokontrollerek, szenzorok, diagnosztikai eszközök és különféle beágyazott rendszerek közötti kommunikációban, ha nincs nagy adatátviteli sebesség igény.

Vasúti rendszerekben jelenleg elsősorban a rendszerelemeken belül találunk különböző UART interfészeket, melyek célja a részegységek közötti kommunikáció, vagy külső interfészként biztosítani a karbantartás, konfigurálás lehetőségét. Üzem közbeni kommunikáció céljára a jelentősége egyre inkább csökken, ennek ellenére még sok új eszközben is előfordul, mert kis távolságra megbízható és egyszerű kommunikációs csatorna biztosítható vele.

Bár az UART egyszerűsége miatt továbbra is népszerű az alacsony szintű kommunikációban, egyre több vasúti rendszer tér át fejlettebb soros kommunikációs protokollokra, mint például fedélzeti buszrendszerek esetén a CAN (Controller Area Network), mely több eszköz egyidejű kommunikációjára is alkalmas. RS-485 (differenciális soros kommunikáció), mely szintén több csomópont között képes kommunikációra és akár nagyobb távolságok esetén is alkalmazható (akár 1 km).

3.6 Következtetések, összegzés

A vasúti kommunikációval és biztonsággal kapcsolatos általam korábban áttekintett szabványok általában nem konkrét technológiákat írnak elő, hanem teljesítménymutatókat, követelményeket, működési paramétereket és javasolt eljárásokat határoznak meg. Ebben a részben egymásnak megfeleltettem az egyes előírásokat a jelenlegi és a jövőben várhatóan alkalmazott technológiákkal, protokollokkal.

Találhatók azonban bizonyos szabványok, előírások, melyek javasolják, vagy preferálják konkrét technológiák alkalmazását. Ennek oka, hogy – vasúti kontextusban – nagyobb területeken lehessen együttműködő hálózatokat kialakítani, más szóval biztosítani az interoperabilitást és az egységes biztonsági szintet.

3.6.1 Konkrét technológiát előíró szabványok, előírások

Erre jelen esetben példa a GSM-R rendszer kötelező alkalmazása a vonat és a pályamenti ETCS rendszer közötti kommunikációra, melyet az ETCS/ERTMS rendszerhez kapcsolódó előírások írják elő. Az ehhez kapcsolódó legfontosabb előírások és szervezetek az alábbiak:

Az Európai Unió műszaki előírásai – TSI-k (Technical Specifications for Interoperability), melyek meghatározzák a fedélzeti és pályamenti rendszerek interoperabilitását, használható kommunikációs szabványokat, előírják a kötelezően használandó EIRENE (European Integrated Railway Radio Enhanced Network) specifikációkat.

EIRENE specifikációk definiálják a GSM-R rendszer szolgáltatásait, interfészeit, protokolljait és működési paramétereit (frekvenciák, prioritások stb.).

Az Európai Unió vasúti interoperabilitási irányelvei, például a „Directive (EU) 2016/797 on the interoperability of the rail system within the European Union”, mely előírja, hogy a tagállamok kötelesek az interoperábilis rendszerek bevezetésére, amelyhez a GSM-R is hozzátartozik. [4]

Jövő tekintetében elmondható, hogy a CCS TSI 2023-as kiadása [39,40] tartalmaz hivatkozást a FRMCS-re, mint a GSM-R utódjára, és megnyitja az utat annak fokozatos bevezetésére.

Az ERA és az EU által meghatározott átállási ütemterv a következő:

Év	
2023	A CCS TSI 2023-as kiadásában megjelenik az FRMCS alkalmazása a jövőben.
2025	Várhatóan véglegesítik az FRMCS Release 2-t, ami a teljes funkcionalitást tartalmazza LTE és 5G támogatással.
2026–2027	A tagállamok elkezdhetik a FRMCS tesztelését és kísérleti bevezetését.
2030 után	FRMCS válik a kötelező rendszerré új vonalak, nagyobb felújítások esetén. A GSM-R fokozatos kivonása ekkor indul el.

5. táblázat. GSM-R FRMCS átállási ütemterv

Összegezve Európában a vasúti kommunikáció egyik legfontosabb, levegő interfészét tekintve a kötelező előírások miatt biztos, hogy a földi cellás GSM-R és FRMCS rendszer lesz alkalmazásban. Jelenleg épp a példáját láthatjuk annak, hogy az előírt technológia elavulttá válik. Ebben az esetben a szabályozás változik, de a jövőbeli interoperabilitás biztosítása érdekében szintén egy meghatározott technológia előírása szükséges.

Áttekintettem más technológiákat is e téren, de az európai szintű átjárhatóság biztosítása miatt ebben az esetben szükség van olyan előírásokra, ami a konkrét technológiát írja elő.

Az alábbi táblázatban összefoglaltam a műholdas technológiák és a földi cellás technológiák jellemzőit és műszaki szempontú alkalmazhatóságát.

	Alkalmazhatóság	Késleltés	Lefedettség	Alkalmazhatóság
Földi cellás	Sűrűn lakott területeken, cellás rendszer kiépítése gazdaságos	Alacsony	cellamérettől függő, csak az érdekelt területen	Sűrűn lakott területeken, cellás rendszer kiépítése gazdaságos
Műholdas GEO	Ritkán lakott területeken	nagyon magas	nagy területű, globális	Nem alkalmas
Műholdas LEO	Ritkán lakott, cellás infrastruktúra nélküli területeken	kontrolálható	sok műholddal globális	Elvi alkalmazhatóság

6. táblázat. Műholdas és földi cellás technológiák összevetése

3.6.2 Technológia váltás

Az alábbiakban összefoglalom a szinkron SDH hálózatokról csomagkapcsolt IP hálózatokra történő váltás esetén milyen különbségek adódnak a kommunikációs hálózat jellegében.

	Szinkron átviteli hálózat SDH	Csomagkapcsolt hálózat IP
átviteli mód	szinkron (vonalkapcsolt)	aszinkron (csomagkapcsolt)
statisztikus multiplexelés	nincs	van
sávszélesség kihasználás hatékonysága	rugalmatlan, rögzített értékek	rugalmas, hatékony
skálázhatóság	limitált	magas
determinált átvitel	igen (állandó értékű késleltetés, fix adatsebesség)	nem (változó késleltetés)
időérzékeny alkalmazások támogatása	igen	nem, csak kiegészítő technológiákkal (TSN, MPLS)
Hibatűrés	beépített redundancia	nincs, vagy szoftveresen valósítható meg
Hálózati szinkronizáció	SDH órajelosztás alapján van	nincs, csak kiegészítő technológiákkal (PTP)

7. táblázat. Szinkron aszinkron váltás jellemzői

3.6.3 Interfészek és technológiák összerendelése

3.6.3.1 Teljesítmény és késleltetés mutatók

- A késleltetés (latency) azaz amennyi idő alatt célba ér egy üzenet. Ez a paraméter egy fontos és kritikus érték vonatbefolyásolásnál. Szigorú határértékek vannak meghatározva rájuk, szorosan összefügg a valós idejű működés támogatásával. A determinisztikus hálózat kialakításához a legfontosabb paraméter.
- Átviteli sebesség (sávszélesség, throughput), mekkora adatátviteli kapacitás áll rendelkezésre az adott rendszer vagy kapcsolat esetén. Jellemzően a vonatbefolyásolás, vezérlés megvalósítása nem igényel nagy adatátviteli kapacitást, de a felhasználási igények, az egyre szélesebb körű alkalmazások miatt eljutottunk mostanára arra a pontra, hogy pl. a GSM-R kapacitása már szűknek bizonyul.
- QoS (Quality of Service) támogatás, azaz a forgalmak prioritásainak kezelése. Ez abban az esetben fontos, amikor a hordozó hálózat különböző fontosságú adatokat továbbít.

- Rendelkezésre állás kritikus hálózatoknál nagyon magas érték legyen.
- Szinkronizációs képesség, a hálózat támogatja-e az eszközök időszinkronban tartását.

Kritikus hálózatok esetén ezen paraméterek megfelelő szintű biztosítása az alábbi táblázat szerinti technológiákkal biztosítható:

Kritikus hálózatok	Jellemző érték	Technológia
Időkritikusság	<10ms	TSN, PTP
Determinisztikus hálózat	igen	TSN, (SDH)
szinkronizációs igény	van (micro- nanosec)	PTP, GPS
átviteli sebesség	alkalmazás függő	MPLS/IP/Ethernet
rendelkezésre állás	magas	redundáns kialakítás

8. táblázat. Kritikus hálózatokra jellemző technológiák

Nem kritikus hálózatok esetén a fenti paraméterek enyhébb szinten tartása megfelelő, az alábbi táblázat szerinti technológiákkal biztosítható:

Nem kritikus hálózatok	Jellemző érték	Technológia
Időkritikusság	100ms	IP/Ethernet
Determinisztikus hálózat	nem	IP/Ethernet
szinkronizációs igény	nincs / sec	- / NTP
átviteli sebesség	alkalmazás függő	IP/Ethernet, best effort
rendelkezésre állás	választható	-

9. táblázat. Nem kritikus hálózatokra jellemző technológiák

4 VASÚTI INFOKOMMUNIKÁCIÓS HÁLÓZATOK VESZÉLYFORRÁSAI

A kommunikációs hálózatok megbízható és biztonságos kialakításának feltétele, hogy tisztában legyünk a felmerülő hibák és veszélyforrások lehetőségeivel. Az infokommunikációs szempontból felmerülő veszélyforrásokat azonosítottam és kategorizáltam őket vasúti hálózatok kontextusában A téma igen szerteágazó, esetemben csak a kommunikációs és technológiai aspektust elemzem, míg a kibertámadást, a fizikai hálózatvédelmi és eszközvédelmi témákat csak érintem. A berendezések megbízhatósága függ a működés közben felmerülő hibák előfordulásától, azok gyakoriságától. E szempontból az eszközök és rendszerek a korábban bemutatott szabványokban rögzített módon minősíthetők (SIL1-4 [10]), de sok esetben a rendszerben való minősítés igen nehézkes és nem vezethető le az azt alkotó rendszerelemek megbízhatóságából. A működésbiztonság az adathálózat külső támadásoknak való ellenállásának is a függvénye, a hálózati rendszerek és protokollok támadhatósági vizsgálata is e témakörbe tartozik.

4.1 Technikai, technológiai eredetű veszélyforrások

Kutatásomban csak a technikai, technológiai eredetű veszélyforrásokkal foglalkoztam, amiket ebben a részben tárgyalok.

4.1.1 Időzítési és késleltetési problémák

Magas késleltetés értékek problémát jelentenek a valós idejű alkalmazáskor, ahol a haladó vonat számára fontos menetengedélyek, forgalmi utasítások időben kell, hogy megérkezzenek.

Késleltetés ingadozás (jitter) a csomagalapú IP hálózatok alapvető tulajdonsága, ha csak hálózati réteg alap funkcionalitását tekintjük. A best-effort jellegű csomagátvitel esetén nincs garancia a csomagok időbeli kezelésére, időben egyenletes továbbítására.

Időszinkron hibák, azaz a hálózati elemek közötti időszinkron megszakad, az eszközök eltérő időt látnak, emiatt az időkritikus műveletek, prioritáskezelés nem megfelelően működik.

A kifutóban lévő SDH hordozó hálózatok ezekre a problémákra mind megoldást nyújtottak, de az IP-Ethernet alapú hálózatok többletszolgáltatásai, rugalmas konfigurálhatósága miatt kiszoruló félben vannak. Az SDH hálózatok elemei szigorú időszinkronban voltak egymással, központi óra ütemében dolgozott a hálózat összes

eleme, ezzel megbízható alapot adott az időkritikus alkalmazásoknak. Stabil hálózati kapcsolatot biztosított redundanciával, gyors helyreállítással, alacsony késleltetéssel és jitterrel, amik miatt még a fentiek ellenére speciális esetekben nem kerültek leváltásra.

Az IP-Ethernet hálózatok időzítésben igen gyengék, de mivel ezen technológiák kapacitás növekedése és terjedése magas, már jó ideje folyamatosan megjelennek a gyengeségeit kompenzálandó eljárások.

Nagy késleltetéseket a torlódások, az útválasztás magas protokoll rétegbeli megvalósítása, az algoritmusok lassúsága okozhat. Hálózati hiba esetén a redundáns útvonal kiépítése miatti késlekedés lehet számottevő.

Ezekre a problémákra mind vannak egyre fejlődő megoldások, melyeket a korábbi részekben áttekintettem.

Az útválasztás időbeli problémáit alacsonyabb rétegbeli megvalósítással, és egyszerű algoritmusokkal lehet gyorsítani. Erre az MPLS címkék alkalmasak, melyek egyúttal QoS funkciókat is el tudnak látni, azaz prioritáskezelés is megvalósul egyben. (Korábban az ATM hordozóhálózatok esetén is az egyik fontos tervezési szempont volt, hogy megfelelő prioritású és előre definiált útvonalak legyenek a hálózatban, a minél gyorsabb cellatovábbítás érdekében.) Az MPLS gyakorlatilag ezen a filozófián alapulva valósítja meg ezt a fajta forgalomkezelést az IP-Ethernet hálózatokkal ötvözve.

Az MPLS esetén is definiálhatók redundáns útvonalak (MPLS Fast reroute), de még jobb, hogyha ezt lentebbi réteg valósítja meg. Az Ethernet széleskörű elterjedése folytán ezekre a hálózatokra is született sok megoldás. Gyűrűs, dupla gyűrűs topológia, duplikált hálózati topológiát kezdetben nem kezelte a klasszikus Ethernet hálózat, de a jelenlegi megvalósítások támogatják (pl. HRP, PRP). Ezek előnyei, hogy ezeket a protokollokat megvalósító eszközök transzparensen működnek a fentebbi rétegek számára, azokon semmilyen változtatást nem kell eszközölni a hordozó hálózat ilyen jellegű cseréje esetén, viszont sokkal megbízhatóbb mutatókkal rendelkezik a teljes kommunikációs rendszer.

Az időszinkron kezelése nagyon fontos probléma az IP-Ethernet alapú hálózatokban, mert alapvetően a hálózat jellege aszinkron, viszont a determinisztikus működéshez fontos az időszinkron megléte, ami egyébként a korábbi generációs szinkron SDH hálózatokban meg is volt. Ha időszinkronizációs hiba van jelen, az eszközök nem ugyanazt az időt „látják”, eltérnek a belső órájuk, így rosszul időzítik az üzeneteket. Erre

a Precision Time Protocol (IEEE 1588v2) a most már klasszikusnak mondható megoldás, amivel fent lehet tartani az eszközök közötti időszinkront. A szinkronhibák okai gyakran a PTP Grandmaster hibája, kiesése, esetleg hálózati konfigurációs probléma, hogy a PTP üzenetek nem továbbítódnak megfelelően, amire megoldás a redundancia kialakítása PTP Grandmaster fallback mechanizmussal.

A jövőben viszont még nagyobb fókuszt kap az időzítés újabb szabványok megjelenésével, melyek a Time Sensitive Networking alapú forgalomtervezésbe tartoznak. Ezek egy része már el is érhető és alkalmazásban van.

Az időszinkron megléte az FRMCS esetében alapvető fontosságú. Ez az 5G alapú mobil hálózati technológia rádiós időosztásos rendszere precíz időszinkron nélkül képtelen működni [47,48,49].

A hálózat determinisztikus viselkedését azaz az átviteli idő előre kiszámíthatóságát a kritikus hálózatok esetén biztosítani kell. Ez elvileg már rendelkezésre áll a forgalmi osztályok kialakításával és a megfelelő prioritáskezeléssel.

4.1.2 Adatátviteli hibák, fizikai rétegben

Szimbólum hibák és az abból eredő bithibák, a fizikai réteg, azaz az átviteli út zavarai miatt léphetnek fel, pl elektromágneses zavar, vagy kábelhiba miatt. Ennek okai az elektromágneses interferencia (EMI), gyenge minőségű kábelezés, vagy kivitelezés, optikai, vagy villamos csillapítás, rosszul beállított fizikai szintű paraméterek. Nagy hőingadozás is hatással lehet az optikai vagy réz alapú adatátvitelre.

Ezekre kidolgozott előírások, szabványok vannak [54], azok betartásával lehet ezeknek a hibáknak az előfordulását minimalizálni, mind a pályamenti, mind a fedélzeti környezetben.

Fizikai rétegként a rádiós csatornára vonatkozó veszélyek áttekintése is fontos. Megbízható vezeték nélküli kapcsolat elengedhetetlen a pályamenti rendszer és a vonat közötti kommunikációhoz, hogy minimalizáljuk a rendszer leállásának idejét és maximalizáljuk a rendszer rendelkezésre állását. A rádiós (vezeték nélküli) csatorna megszakadásának vagy minőségromlásának.

4.1.3 Csomagvesztés

Csomagvesztés történhet adathiba esetén, ekkor a csomagot fogadó útválasztó fedezi fel az adathibát a csomagban lévő ellenőrző összeg alapján és dobja el a hibás csomagot. A hálózat túlterheltsége miatt is kerülhetnek csomagok eldobásra az útválasztókban.

A csomagvesztés elkerülésére az egyik legalapvetőbb megoldás a hálózat kapacitásának megfelelő méretezése [K4]. Kritikus hálózatok esetén megfelelő nagyságú biztonsági kapacitás tartalékot kell képezni, ezekben az esetekben nem a hálózat kihasználtságának a maximalizálása a cél.

Amennyiben a hálózat többféle prioritású forgalommal dolgozik, a kritikus forgalmakat minden esetben előnyben kell részesíteni, mely MPLS címkézés alapon, vagy virtuális hálózatok megvalósításával oldható meg.

A csomagvesztés szorosan összefügg a hálózati hibák kialakulásával, linkszakadás esetén tömeges csomagvesztés várható, míg a közvetítő link minőségromlása esetén szórványos veszteségek fordulnak elő. Ezekre korszerű megoldás az alacsony rétegbeli (Layer2) megoldások [29], melyek egyrészt képesek biztosítani a hibás csomagok eldobását és a redundáns átvitelnek köszönhetően az ép csomag azonnali továbbítását. Linkszakadás esetén pedig a duplikált csomag a redundáns útvonalon egy példányban még mindig képes megérkezni.

A klasszikus IP átvitel során a csomagvesztés magasabb rétegben (TCP esetén a szállítási) került csak detektálásra, és szükség esetén újraküldéssel javításra (TCP), ami jelentős késlekedést vitt az átvitelben. Rádiós csatorna esetén rossz vételi viszonyok között a kapcsolat megszakadását is eredményezheti, ha nem alacsony rétegben kerül a csomagvesztés detektálása, és a hibajavítás vagy újraküldés implementálása.

4.1.4 Redundancia

A kritikus rendszereket a kapcsolódó szabványok alapján [12,14] redundánsan kell kialakítani. Ez eszközszinten az összes, kommunikációban résztvevő elem duplikációját jelenti.

Topológia szinten a gyűrűs topológia a gazdaságos megoldás a legtöbb esetben, mert ebben egy link szakadása, vagy egy útválasztó leválása esetén a hálózat többi része működőképes marad. Ezt lehet fokozni a dupla gyűrűs kialakítással.

4.1.5 Monitoring és hibakezelés hiányosságai

A vasúti kommunikációs és vezérlőrendszerek állapotának felügyeletével, hibadetektálásával a monitoring rendszerek és operátorok foglalkoznak.

Nagyon sokféle hibának vannak jellemző előjelei, amiket időben detektálva sok esetben megelőzhetők a komolyabb hálózati hibák, leállások. Ezeknek az információknak az értéke igen magas, mivel megelőzhetők vele az információ hiányból eredő súlyosabb problémák. Amennyiben a kommunikációs hálózat működésének folytonosságát garantálni akarjuk, fontos hogy a hálózat összes elemére kiterjedő felügyeleti rendszert alakítsunk ki, ne legyenek ún. vakfoltok.

Ezen felül a hibadetektálás és kezelés sebessége is fontos paraméter. Itt már az emberi tényező is szerepet játszhat, amennyiben detektálás és lekezelése az operátor feladata. A tipikus jellemzőkkel rendelkező, és tipikus műveletet igénylő hibákat érdemes automatizáltan kezelni, ezzel egyrészt emberi erőforrást lehet spórolni, másrészt a hiba kezelésére, kijavítására nyerhetünk több időt.

A monitoring szerepe és a beavatkozások automatizáltsága nem kizárólagosan központosítottan működhet. A csomagokat továbbító útválasztók felruházhatók olyan képességekkel, mellyel a továbbított forgalmak jelenlétének jogosultságát is ellenőrizhetik validációs módszerekkel. Ezzel az illetéktelen, vagy esetleg a rendszerben ragadt forgalmakat képesek kiszűrni, a hozzájuk tartozó csomagokat eldobni és megelőzni, hogy az adott eszköz terheltsége feleslegesen megnőjön.

4.1.5.1 Szoftverfrissítés és konfigurálás veszélyei és megoldásai

Vasúti környezetben a szoftverfrissítések kritikus jelentőségűek, mert a rendszerek hosszú élettartamra készülnek (20-30 éves nagyságrend), és működésük során folyamatosan alkalmazkodniuk kell a változó technológiai és biztonsági követelményekhez. Egy rosszul kezelt szoftverfrissítés üzemzavart, kompatibilitási problémákat vagy akár biztonsági kockázatokat is okozhat. Jelenleg a szoftveres frissítéseket többféle módon lehet telepíteni attól függően, hogy milyen eszközről és mennyire kritikus rendszerről van szó.

- Kézi frissítés (offline, helyszíni telepítés) a preferált frissítési mód a nagyon magas megbízhatóságot igénylő rendszerek esetén, mint pl. biztosítóberendezések, vasúti forgalomirányító központok, fedélzeti vezérlőrendszerek. A frissítés helyszínre érkező szakember által történik,

fizikailag kell az eszközhöz férnie, és rácsatlakozni, tipikusan USB meghajtóval, memória kártyával, vagy a laptopjával USB, vagy UART csatlakozással. Nagyon fontos, hogy csak előzetesen hitelesített személyzet végezheti a műveletet. Ez a szoftverfrissítési mód a legkörülményesebb, nagy idő és erőforrásráfordítási igénnyel rendelkezik. A biztonságkritikus rendszerek esetén jellemzően előfordul, hogy csak karbantartási időszakokban frissíthetők. Az emberi tényező kulcsfontosságú ebben a műveletben: a személyzet hitelesítése és a tevékenység naplózása alapvető fontosságú, mert egy fertőzött szoftver rendszerbe jutása komoly kockázatot jelent.

- Hálózati frissítés, központi szerverről. Ebben az esetben a frissítés távolról, automatikusan, vagy félautomatikusan történik. A kliens eszközök letöltik a frissítést ellenőrzött, hitelesített csatornákon keresztül (pl. VPN-es kapcsolaton) és telepítik. Fontos, hogy a központi szerveren lévő frissítés megbízható legyen, biztosítani szükséges, hogy ahhoz a géphez ne férjen hozzá illetéktelen személy. A frissítés szoftver tartalma is hibátlan kell, hogy legyen, előzetesen tesztkörnyezetben minden esetben validálni szükséges, mert az egész flottát megbéníthatja egy inkompatibilis, vagy hibás frissítési csomag. Ez a módszer jellemzően nem kritikus rendszerekben kerül alkalmazásra pl. jegyértékesítő, utastájékoztató, karbantartási, diagnosztikai rendszerek.
- Vezeték nélküli OTA (Over-the-Air) frissítés, a nevéből következően rádiós hozzáférés esetén alkalmazható, főként a jövőben várható elterjedése, bár több komoly kockázatot is felvet használata, emiatt kritikus rendszerek esetén nem valószínű, hogy a közeljövőben gyakorlatba is kerül a használata vasúti környezetben. Mobil hálózathoz kapcsolódva a 4G és 5G rendszerekre alapuló FRMCS alapú fedélzeti rendszerek frissítése képzelhető el ilyen módon. A nyilvánvalóan kényelmes és gazdaságos megoldással szemben az áll, hogy a frissítés hitelességét robosztus rendszerrel kell védeni és ellenőrizni, telepítés csak akkor történhet, ha a forrás hitelessége igazolt. Végpont-végpont közötti titkosított frissítési csatornán történhet a csomag letöltése. Frissítés közben a kapcsolat megszakadása ne okozza az eszköz használhatatlanságát, ami biztosítható, hogy a letöltés és a telepítés ne egyszerre történjen.

Mindegyik módszer esetén a frissítési folyamatnak kellően védettnek kell lenni, ezzel elsősorban az emberi tévedések veszélyét lehet nagyon alacsony szinten tartani, de a szándékos károkozás (például kibertámadások) esélyét, mértékét is lehet mérsékelni, vagy előírt valószínűségűre csökkenteni. Adathordozós frissítésnél plug-and-play jellegű automatikus csatlakoztatást és telepítést el kell kerülni.

Erős hitelesítési mechanizmusokat kell használni, a kezelő személyzet és a telepítendő programkódra is. Csak meghatározott személyek hajthatnak végre szoftverfrissítést. Ezek naplózása szintén alapvető követelmény és a naplókat védetten és visszakereshető módon kell tárolni.

Programkód azonosításra, hitelesítésre digitális aláírás, vagy kriptográfiai hash használandó. Telepítés előtt a rendszer ellenőrzi, hogy a gyártó által megadott hitelesítési azonosítóval ellátott programkódot akarnak-e telepíteni. Ezzel biztosítható, hogy véletlenül megsérült fájlok, vagy szándékosan megváltoztatott fájlok kerüljenek telepítésre. A telepítendő fájlok csak verifikált forrásból érkezhetnek, letöltés során VPN, vagy más titkosított csatorna használata szintén előírás lehet. [12,17,18,19]

4.2 Fizikai és emberi tényezőkön alapuló veszélyforrások

A vasúti kommunikációs rendszerek megbízhatóságának magas szintű biztosítása nem csupán a hálózati és protokollszintű technikai megoldások függvénye. Ezen rendszerek megbízhatóságának vizsgálatakor figyelembe kell venni a fizikai hozzáféréssel, az emberi mulasztásokkal vagy a szándékos károkozással járó veszélyeket is. Bár jelen kutatásom elsősorban a technikai aspektusokra fókuszál, a teljes körű biztonsági kép megértéséhez röviden áttekintem fizikai és emberi tényezőkön alapuló a veszélyforrásokat is.

4.2.1 Felhasználói interfészek hibás kialakítása

Ezek a tényezők nem minősülnek közvetlen támadásnak, hanem a kezelői felületek (HMI Human-Machine Interface) nem megfelelő ergonómiai tervezéséből fakadó felhasználói hibák következményei. A rosszul kialakított kezelőfelületek megtéveszthetik a kezelőt, megnehezítik a helyes döntéshozatalt, vagy előidézhetnek nem szándékos műveleteket, amelyek viszont potenciálisan veszélyeztethetik a rendszer biztonságát vagy megbízhatóságát (pl. hasonló ikonok vagy gombok, nem egyértelmű visszajelzések, megerősítő kérdés nélküli műveletek, vagy éppen a nem lokalizált nyelvek).

4.2.2 Fizikai és emberi tényezőkön alapuló fenyegetések

4.2.2.1 Belső támadó

Szervezeten belüli jogos hozzáféréssel rendelkező személyek (pl. alkalmazottak, alvállalkozók, vagy adminisztrátori jogkörrel rendelkező személyek) szándékos károkozása, ami lehet tudatos vagy gondatlan adat-, eszköz-vagy rendszerkompromittálás. Kiváltó okok sokrétűek lehetnek, pl. elégedetlenségből, kényszerítés hatására vagy pénzügyi motiváció által.

Belső támadók, hozzáférhetnek olyan interfészekhez, ahol az egyébként kellően védett adatforgalom titkosítatlan formában kerül továbbításra. Ezeken a pontokon lehetőség van a továbbított információk lehallgatására. Ha nem csak információszerzés a cél, hanem beavatkozás is, akkor egy ilyen felületen megvalósítható egy Man-in-the-Middle (MITM) támadás is, ahol a támadó aktívan módosítja vagy átirányíthatja a kommunikációt.

A szoftverfrissítés szintén érzékeny és nagy odafigyelést igénylő művelet kritikus rendszerek esetén. Megfelelő jogkörrel rendelkező belső támadók esetén rosszindulatú kód, vagy vírusok, trójai programok telepítése is megtörténhet.

4.2.2.2 Jogosulatlan személyek általi fizikai hozzáférés

Hozzáférés adatkapcsolati berendezésekhez, szerverekhez vagy karbantartási interfészekhez olyan személyeknek, akiknek nem lenne joguk elérni ezeket az eszközöket, interfészeket. A hozzáférés megakadályozásának egyik lehetősége az objektum megfelelő védelme, ezzel megakadályozható a vezetékes becsatlakozások, adathordozóról kártékony szoftverek bejuttatása a rendszerbe. Sok esetben viszont mindez kiegészíthető technikai megoldásokkal is, amikor a fizikai hozzáférés nem elegendő a manipulációhoz, mert további jogosultság, igazolások szükségesek, hogy valóban hozzáférjenek a rendszerhez (pl. jelszavak, hardverkulcsok).

A rádiós interfészek fizikai védelme nem lehetséges, hiszen éppen az a céljuk, hogy az adott területen bárki számára elérhető legyen az adás és vétel szempontjából. Ebben az esetben csak technikai megoldásokkal – például titkosítási és hitelesítési eljárásokkal – biztosítható az illetéktelen hozzáférés. Jó példa erre a GSM-R rádiós interfésze, aminek biztonságát a GSM szabványban rögzített eljárások biztosítják [50].

4.2.2.3 Zavarás és külső beavatkozás:

Vezeték nélküli kommunikáció ellehetetlenítésére a rádióinterferencia alkalmazása egy bevált módszer. Megfelelő sávszélességű, teljesítményű és helyzetű zavaró jel

sugárzásával megszakítható a kapcsolat adó és vevő között. A rádiós kommunikáció zavarérzékenységét lehet csökkenteni alkalmas jelfeldolgozási eljárásokkal, redundáns vivők kialakításával.

Amennyiben a hálózati kapcsolathoz hozzáfértek valamilyen szinten (akár rádiós, akár vezetékes mód esetén) akkor a behatolóknak lehetőségük van DoS (Denial of Service) támadások indítására. A vasúti vezetékes kritikus kommunikációs hálózatok fizikailag és logikailag is elkülönítettek és kellően védettek (ismertetett szabványok szerint), tehát itt kis eséllyel valósul meg ilyen jellegű támadás. A rádiós interfész ismét a könnyebben hozzáférhető, de a GSM-R vagy az FRMCS mobil rendszerhez csatlakozni adatkapcsolati szinten is igen komoly kihívás.

4.2.3 Jogosultságkezelési és konfigurációs hibákból eredő fenyegetések

Rosszul konfigurált jogosultságok lehetővé tehetik az illetéktelen belépést fizikailag és logikailag is kritikus rendszerekhez. Alapvető hiba egy nem izolált vagy nyílt karbantartási port használata, jelszavas védelem nélkül. Távmenedzsment esetén a hibásan konfigurált (pl. VPN vagy egyéb védelem nélkül), vagy túl nyitott protokollok használata (pl. SNMP).

Kritikus rendszerek esetén szoftverfrissítést nem végezhet egy személy önállóan, kell egy második fél általi jóváhagyás (pl. ellenőr vagy mérnöki vezető).

4.3 Következtetések, összegzés

A fizikai réteg szintjén jelentkező bitszintű adatátviteli hibák (például megnövekedett bithibaarány (BER)) jellemzően hibás csomagok vagy azok újraküldésének formájában észlelhetők. Ezek a hibák megnövelhetik a késleltetést, valamint adatvesztéshez is vezethetnek, különösen akkor, ha hibajavításra nincs lehetőség. Hatása azonnal jelentkezik.

Egy tipikus példa erre a GSM-R alapú rádiós összeköttetésben előforduló átviteli csatorna minőségének romlása, amely CRC hibás csomagokat eredményez, és újraküldésre kényszeríti a rendszert.

Az ebből származó késleltetés proaktív megoldással küszöbölhető ki, vagy csökkenthető jelentősen. A bithiba észlelést és a reakció megvalósítását minél alacsonyabb protokoll szinten kezelni kell. Ez vezetékes, főleg optikai hálózatokban kevésbé fontos, az alacsonyabb zavartatás miatt, de rádiós csatornán viszont kezelendő és állandó probléma.

Az FRMCS-ben az LDPC (Low-Density Parity-Check Codes) hatékonyan képes detektálni és javítani egyes bithibákat a fizikai csatornán. Adatkapcsolati szintén található megoldás erre az FRMCS-ben a HARQ, amely ötvözi az FEC (Forward Error Correction) és az ARQ (Automatic Repeat reQuest) megközelítéseket.

A hálózati és szállítási rétegben a csomag, vagy szegmensvesztés hatása – főleg, ha IP/UDP vagy más nem megbízható protokollt használnak – szintén azonnal vagy nagyon rövid idő alatt jelentkezik. A hibát a hiányzó üzenet (ez jellemzően felsőbb rétegbeli feldolgozással derül ki) vagy időtúllépés (watchdog mechanizmusok) alapján lehet észlelni. Kritikus vezérlési vagy biztonsági protokollok működése válhat instabillá. Ha pl. az RBC-től egy menetengedély nem érkezik meg a mozdonyhoz a vonat nem indulhat el. Emiatt az ilyen kritikus kapcsolatok és üzenetekre mindig nyugtázással kell válaszolni, ha ez időben nem érkezik meg ismét elküldhető az üzenet. E mellett persze más mechanizmusok folyamatosan monitorozzák a link állapotát és ha a kapcsolattal van baj, áttérnek a redundáns átviteli csatornára.

A hálózati elemek szinkronizációs eltérései fokozatosan alakulhatnak ki, ha az időalap lassan, de folyamatosan egyre inkább eltér a referenciaértéktől. Ez az időbélyegek eltolódását, jitter növekedést vagy más időzítési inkonzisztenciákat (idő offset) okozhat. Az ilyen eltérések különösen az időkritikus kommunikációs és vezérlési folyamatokban veszélyesek. Ezért volt jó a klasszikus SDH rendszerekben, hogy a szinkronitást a hálózat működőképessége magában hordozta. Jelenleg ezt a PTP, és egyre inkább a TSN megoldások szolgáltatják az alapból aszinkron jellegű IP átvitel felett.

A hálózati architektúrában jelentkező redundancia hiánya rejtett kockázatot hordoz, amely csak akkor válik nyilvánvalóvá, ha hiba történik, és nincs aktív tartalékút. Ennek hatására egyetlen pont meghibásodása is teljes szolgáltatáskieséshez vezethet, akár a hálózat nagyrészét megbénítva. Például ha egy MPLS-alapú hálózatban megszűnik egy Label Switched Path (LSP) és nincs előre konfigurált alternatíva, akkor a mozdony és az RBC közötti kommunikáció teljesen megszakadhat.

A monitorozás hiánya – különösen a menedzsment és felügyeleti szinteken – olyan fokozatos, vagy akár hirtelen bekövetkező hibákat eredményezhet, amelyek nem kerülnek időben lekezelésre. Ilyen esetekben a hiba hatása csak akkor válik nyilvánvalóvá, amikor az már a rendszer működésében is zavarokat okoz. Tipikus példa lehet, amikor a QoS paraméterek romlása miatt fokozatosan csökken a kommunikációs

kapcsolat minősége, de a kapcsolat nem szakad meg. A monitorozás hiánya, vagy gyenge képessége nem detektálja ezt a romló tendenciát időben, nem történik beavatkozás, majd váratlan üzemzavar lép fel emiatt.

A hálózatok típusa szerinti bontást az alábbi táblázat tartalmazza. Kritikus hálózatok esetén az áttekintett biztonsági tényezők láthatóka az alábbi táblázatban:

Kritikus hálózatok	Jellemző érték	Technológia
Biztonsági követelmény	titkosítás, hitelesítés, naplózás kötelező	szeparált hálózat, IPSec, tűzfal alkalmazása
Frissítés / rollback támogatás	csak digitálisan aláírt, verziókövetett, verifikált frissítés személyzet hitelesítése	Secure Boot, rollback mechanizmus, digitálisan aláírt frissítés
Redundancia	Kötelező (interfészek és linkek és tápellátás tekintetében)	Dual ring, failover switch, bypass port

10. táblázat. Kritikus hálózatok biztonsági jellemzői

Nem kritikus hálózatok esetén pedig az alábbiak:

Nem kritikus hálózatok	Jellemző érték	Technológia
Biztonsági követelmény	egyszerű védelmek, naplózás opcionális	jelszavak
Frissítés / rollback támogatás	Egyszerű szoftver csere mechanizmus elegendő	-
Redundancia	opcionális	kettős interfész, hideg tartalék

11. táblázat. Nem kritikus hálózatok biztonsági jellemzői

5 INFOKOMMUNIKÁCIÓ BIZTONSÁGÁT NÖVELŐ IRÁNYELVEK

Információbiztonsági irányelvekre a vasúti kommunikációs hálózatok esetében elsősorban a magas rendelkezésre állás és a közel hibamentes működés biztosítása érdekében van szükség. Jelen fejezet célja olyan módszerek és eljárások bemutatása, amelyek alkalmasak az információbiztonsági kockázatok csökkentésére, illetve bekövetkezésük esetén az időbeli lefutás minimalizálására. A karbantartási és javítási idők kiemelt fontosságúak egy ilyen rendszer üzemeltetése során, mely irányelveket a tervezési szakaszban (RAMS dokumentumban) kell lefektetni, de ez nem része a kutatásaimnak. Vizsgálataim kizárólag protokolláris megközelítésben és redundáns, hibatűrő rendszerek kialakítása gondolatmenetén végeztem.

Ez a fejezet szorosan kapcsolódik az előző kettőhöz: a feltárt technikai hibák és biztonsági problémák elkerülésére gyakorlati megoldásokat és irányelveket fogalmaz meg. A cél nem csupán a biztonsági kockázatok mérséklése, hanem a meghibásodások időtartamának csökkentése, a helyreállítási folyamatok gyorsítása, ezáltal a teljes rendszer megbízhatóságának növelése. Ebben a részben megfogalmazott ajánlások hozzájárulhatnak a jövőbeli vasúti kommunikációs hálózatok megbízhatóbb és rezisztensebb kialakításához.

5.1 Bevezetés – Az irányelvek célja

Az előző részekben bemutattam, hogy az előírások és szabványok a legtöbb esetben nem konkrét technológiák használatát írják elő, hanem minőségi mutatókat, tervezési irányelveket adnak meg. Napjainkban a technológia gyors változása fejlődése miatt, a minőségi biztonsági irányelveket megfogalmazó szabványokba sok esetben nem is érdemes konkrét technológiákat belevenni, mert hamar elavulttá válhatnak. Erre példa a GSM-R előírása az európai tagországoknak, ami jelenleg módosítás alatt áll és következőként az FRMCS-t írja elő a vasúti rendszerek kötelezően használandó rádiós hordozószolgálataként. Persze erre abból a szempontból volt szükség, hogy Európa szerte a globális átjárhatóságot biztosan meg lehessen valósítani. Először áttekintettem, hogy mely jelenlegi és jövőbeli technológiák képesek megfelelni az egyre szigorúbb elvárásoknak, viszont a technológiaváltás időnként olyan problémákat is felvet, amelyekkel korábbi, egyszerűbb megoldások, esetén nem is kellett foglalkozni.

Másodikként a kommunikációs hálózatokra vonatkozó veszélyforrásokat vettem lajstromba, két csoportra bontással: a technikai és a fizikai, emberi eredetű veszélyforrások. Csak a technikaival foglalkoztam részletesen. Célom a vasúti infokommunikációs rendszerek műszaki veszélyforrásainak azonosítása és rendszerezése volt, tekintettel azok időbeli lefutására és a rendszer működésére gyakorolt hatására. A megközelítés célja a hibatípusok időbeli viselkedésének feltárása és a kritikus rendszerelemekre gyakorolt kockázatok jobb megértése, amely hozzájárulhat a nagy megbízhatóságú vasúti kommunikációs architektúrák tervezéséhez.

5.2 Az információbiztonsági irányelvek rendszerezése

A vasúti kommunikációs hálózatokkal szemben támasztott magas rendelkezésre állási és információbiztonsági követelmények teljesítése nem valósítható meg kizárólag technológiai fejlesztésekkel, hanem rendszerszintű irányelvek alkalmazása is szükséges.

Jelen szakasz célja az előző fejezetekben feltárt műszaki veszélyforrások, hiányok orvoslására információbiztonsági ajánlások rendszerezett bemutatása. Ezek segítségével az összetett, heterogén vasúti infokommunikációs rendszerekben csökkenthető a hibák miatti üzemidőkiesés időtartama, gyorsítható a helyreállítás és növelhető a hálózat rendelkezésre állása, megbízhatósága.

Az irányelvek kialakításakor a jelenlegi ipari szabványokat, a jövőbeli technológiai trendeket, valamint a vasúti környezet sajátos követelményeit egyaránt figyelembe vettem.

Az irányelveket három fő szempont köré építettem:

- időtényezők, hibaészlelés és reagálás;
- kommunikációs és információbiztonsági kérdések;
- hálózattervezés és hardveres megvalósítás.

Az itt bemutatott ajánlások technológiafüggetlenül alkalmazhatók, ugyanakkor figyelembe veszik a már jól bevált és a legújabb ipari gyakorlatokat is.

5.2.1 Hibák időtényezői

A vasúti kommunikációs hálózatok megbízhatóságának növelése szempontjából fontos a meghibásodások megelőzése, vagy a bekövetkezett hibák hatásainak időbeli minimalizálása, azaz a gyors és hatékony felismerés és az optimalizált helyreállítási

folyamatok végrehajtása. Az alábbiakban három fő terület mentén foglalok össze olyan technikai és rendszerszintű ajánlásokat, amelyek hozzájárulnak az időtényezők csökkentéséhez.

Gyors hibaészlelés

A hiba korai felismerése elengedhetetlen feltétele a gyors beavatkozásnak. A korszerű kommunikációs rendszerekben egyre nagyobb szerepet kapnak az automatizált monitoringeszközök, valamint az adatalapú diagnosztikai megoldások, melyek a rendszer viselkedésének mintázataiból képesek előre jelezni a lehetséges meghibásodásokat vagy teljesítményromlásokat. Az ilyen predikciós elven működő modellek alkalmazása segítik a proaktív karbantartást, így a kritikus hálózati komponensek állapotának folyamatos felügyelete nemcsak a hiba bekövetkezésének kockázatát csökkenti, hanem annak időbeli lefolyását is jelentősen lerövidítheti.

A protokollrétegezettség alacsony szintjén megvalósított bithiba észlelés és megfelelő kódolással megvalósított javítás szintén megoldás lehet komolyabb kommunikációs hibák megelőzésére. Rádiós csatornán mindig mostohább környezettel kell számolni. Itt robosztusabb csatornakódolások és hibadetektálási és javítási, újraküldési módszerek alkalmazásával, fentről nézve stabil kommunikációs csatornát lehet létrehozni akkor is, ha vételi viszonyok kedvezőtlenek.

A hibadetektálás és a hiba lokalizálásának gyorsítására egyik eszköz a mikroszegmentált hálózati architektúra. Ez a kezelt hálózati incidensek, hibák előfordulását szűk szegmensen belül képes tartani, hogy az incidensek lokalizáltan maradjanak, így a többi hálózati szegmens zavartalanul képes tovább működni. Az áttekintett TSN szabványok alapján adatkapcsolati szinten megvalósíthatók ilyen hálózati architektúrák.

Helyreállítás gyorsítása

A hibahatások időbeli hosszának csökkentésében meghatározó szerepe van a gyors helyreállítás lehetőségének.

Kommunikációs csatornák esetén ennek egyik legfontosabb eszköze a redundáns infrastruktúra, amely lehetővé teszi egy, vagy akár több, hibás elem automatikus kiváltását működő tartalékokkal. A gyakorlatban ez megvalósítható duplikált adatútvonalakkal, interfészekkel.

A GSM-R hálózatokban a redundancia több szinten is jelen van, mivel ez a kommunikációs csatorna biztonságkritikus szerepet játszik.

Rádiós átvitel biztosítása terén a cellák kialakításában (a kiszolgálási terület kétszeresen átlapolt lefedésével) duplikációt valósítanak meg, amivel elérhető, hogy ha az egyik cella jele gyengül vagy megszakad, a rendszer automatikusan átkapcsol a másik, átfedésben lévő cellára. Frekvencia redundanciával pedig a rádiós csatorna minőségi problémáinak nagyrésze kiküszöbölhető. Ha egy adott vivőfrekvencián külső hatások miatt az átvitel minősége bizonyos határ alá csökken (tipikusan fading jelenségek), akkor a bázisállomás zökkenőmentesen át képes állni más vivőfrekvenciára a kapcsolat megszakítása nélkül.

Fedélzeti szinten duplikált fedélzeti rádiókkal vannak a mozdonyok általában ellátva, ami lehetővé teszi, hogy ha az egyik rádió meghibásodik, a másik továbbra is biztosítja a kommunikációt.

Pályamenti oldalon duplikált bázisállomások segítségével biztosítják, hogy ha egy bázisállomás meghibásodik, egy másik bázisállomás átvegye a szerepét (melegtartelékként üzemelve), minimalizálva a kapcsolat megszakadásának esélyét. A központi elemek (Mobile Switching Center (MSC) és a Base Station Controller (BSC)) és a közöttük lévő kapcsolatok is redundáns kialakításúak, ami szintén szükséges a hálózat előírt rendelkezésre állásának és megbízhatóságának biztosítására.

A redundáns adatátvitel nem feltétlenül jelenti az összes hálózati eszköz fizikai megkettőzését. A gyakran alkalmazott gyűrűs topológiák például lehetővé teszik a költséghatékony, mégis nagy megbízhatóságú rendszerek kialakítását.

A nagy megbízhatóságú eszközök általában redundáns tápbemenetekkel rendelkeznek. Ha az eszközök egy nagy megbízhatóságú rendszert szolgálnak ki, vagy ilyen rendszer részét képezik, az áramellátás redundanciája is elengedhetetlen. Ez két módon valósítható meg: a szerverhelyiségben legalább két független áramforrás van, így biztosítva a folyamatos áramellátást, vagy magának az eszköznek van két bemenete az áramcsatlakozásokhoz, lehetővé téve független áramforrások csatlakoztatását (pl. normál üzemi és akkumulátor). A második esetben az egyik bemenetről a másikra történő megszakítás nélküli átkapcsolás feladatát magának az adott eszköznek kell elvégezni áramkimaradás esetén. Ideiglenes áramforrás esetén (aggretátor vagy akkumulátor telep) a fő tápellátás kiesése esetén limitált a helyreállási idő a lokális forrás kapacitásának függvényében.

A szoftverfrissítések önmagukban is komoly kockázatot jelenthetnek, ha nem megfelelően menedzselik őket. Ezért szükséges az ilyen frissítések során a digitálisan aláírt csomagok használata.

Hibás szoftverfrissítések, vagy hibás konfiguráció esetén a helyreállítás automatizálása kiemelt szerepű lehet. Az automatikus visszaállítás (rollback) mechanizmusok alkalmazása esetén egy hibás frissítés vagy konfiguráció esetén a hiba észlelése után a rendszer képes önmagától visszatérni az utolsó stabil állapothoz, visszaállítva a helyes működést.

Reakcióidő csökkentése

A detektált hibákra adott válaszreakció gyorsasága jelentős hatással van a teljes hibaidőre. A reakcióidő minimalizálásának egyik eszköze – a korábbiakban már említett – mikroszegmentált hálózati architektúra, ez nemcsak az incidenskezelés hatékonyságát, hanem a hálózat általános robusztusságát is növeli.

További lépésként alkalmazható a zero-trust modell, amely minden kommunikációs műveletet ellenőriz, még a belső hálózati forgalmat is. A gyors reakció ezzel úgy valósul meg, hogy a csomópontok a kommunikáción túlmenően, a továbbítandó adatok épségével, hitelességével is foglalkoznak és incidens esetén rögtön közbeavatkoznak és jeleznek.

Hálózatterhelés-tervezés

A vasúti közlekedést támogató rendszereknél az új technológiák bevezetésével együtt alapvető elvárás, hogy a biztonsági mutatók még tovább javuljanak. A vasúti biztosítóberendezések kommunikációs hálózatának technológiai fejlődése viszont kihívásokat is tesz a fejlesztők elé, mert az újabb technológiák alkalmazása adott esetben néhány mutató romlását is hozhatja a sok előny mellett. Erre legjobb példa a csomagkapcsolt adattovábbítás és az ebből következő késleltetés ingadozás, illetve a hálózat eredendő aszinkronitása. Magasfokú biztonságot és rendelkezésre állást megkövetelő kommunikációs hálózat megvalósításakor már tervezéskor figyelembe kell venni ezeket a kedvezőtlen tulajdonságokat.

A vasúti kommunikációs hálózatok sajátossága, hogy azok nem csupán a mindenkori forgalmi terhelésnek kell megfeleljenek, hanem a hirtelen megnövekedett igénybevétel esetén is garantálniuk kell a megbízható működést. Ezért a hálózati kapacitást gyakran

jelentősen túl kell méretezni – rendelkezésre álló modell és modellszámításokkal alátámasztottan – egy azonos terhelésű, de nem biztonságkritikus infrastruktúrához képest.

Emellett figyelembe kell venni a csomagkapcsolt technológiákból adódó késleltetés-ingadozást is, különösen az ETCS Level 2 és 3 típusú rendszerek esetén, ahol a determinisztikus kommunikáció kiemelten fontos. A forgalom pontos modellezése és a várható késleltetések előzetes becslése segít a tervezés során az időkritikus viselkedésű hálózati komponensek kiválasztásában.

5.2.2 Az információbiztonsági szint növelése

A magas megbízhatóságú vasúti kommunikációs rendszerek alapvető követelménye nemcsak a magas rendelkezésre állás, hanem az információbiztonság szigorú biztosítása is. Az alábbi ajánlásokkal a rendszer egészére nézve lehet az információ integritását, hitelességét és bizalmasságát garantálni.

Fizikai és logikai szegmentáció

Az egyik leghatékonyabb védelmi megközelítés a különböző célú hálózatok fizikai vagy logikai elkülönítése, amivel elválaszthatók egymástól a különböző funkciójú alrendszerek és eszközök. A fizikai szétválasztás a legbiztosabb, ez a módszer lehetővé teszi, hogy a kritikus rendszerek teljesen izoláltan működhessenek, de ennek gazdasági vonatkozása is van, teljesen külön álló hálózatot kell kiépíteni és fenntartani. A logikai szétválasztással jobb hálózatkihasználtságot lehet elérni, de igen nagy hangsúlyt kell ebben az esetben fektetni az egy hordozón továbbított adatok prioritására és mennyiségére. Jelenleg a kritikus hálózatok fizikailag elkülönítetten kerülnek kialakításra, mert így biztosíthatók és ellenőrizhetők a magas biztonsági követelmények. A logikai felosztásnak ott van jogos tere, ha az átviteli csatorna szűknek mondható, és ez mindig a rádiós interfész. A GSM-R-ben az adatok továbbítása terén is már van prioritáskezelés, ami az utódrendszerben (FRMCS) még szofisztikáltabb megvalósítással rendelkezik. A pályamenti hálózatok kialakításánál a jövőben is érdemes a fizikai elkülönítést választani, bár a technológiák fejlődése egyre ígéretesebb e téren.

Titkosítás és digitális aláírás alkalmazása

A vasúti kommunikációs rendszerekben minden kritikus kommunikációs csatornán javasolt a titkosítás és a digitális aláírás alkalmazása. A titkosítással biztosítható az adatok

bizalmassága, míg a digitális aláírás révén garantálható az üzenetek eredetisége és integritása. Ezek különösen fontosak az olyan vezérlési vagy vészjelzési funkciókat ellátó kommunikációs utak esetében, ahol már egyetlen hamis vagy manipulált csomag is súlyos következményekkel járhat.

Távoli hozzáférés szabályozása

A távoli elérés lehetősége megkerülhetetlen a modern vasúti infrastruktúrákban, azonban különösen szigorú információbiztonsági szabályozást igényel. Minden távoli hozzáférés esetében többszintű hitelesítést (pl. kétfaktoros azonosítást) kell megkövetelni.

Naplózás, eseményfigyelés

Helyi, vagy távoli hozzáférés esetén, karbantartási, diagnosztikai, konfigurálási, vagy szoftverfrissítési, vagy csak az üzemszerű használat során végzett tevékenységekkel kapcsolatban elengedhetetlen fontosságú a naplózás. Az elvégzett műveleteket személyhez és időponthoz kötve kell tárolni, visszakereshető módon, úgy hogy bizonyító erejű legyen.

5.2.3 Tervezési és technológiai szempontok

Fizikai kialakítás

A vasúti kommunikációs hálózatok megbízható és hosszú távon fenntartható működéséhez elengedhetetlen a megfelelő hardverszintű, ipari gyakorlatokon és szabványokon alapuló tervezési elvek betartása.

A vasúti eszközök üzemeltetése gyakran extrém hőmérsékleti, páratartalmi és elektromágneses zavartatású környezetben történik. Ezért kulcsfontosságú, hogy a használt komponensek megfeleljenek az EN 50155 szabvány előírásainak, amely többek között számos környezeti tényezőre fogalmaz meg követelményeket, amiket az adott eszköznek vagy rendszernek el kell tudni viselni üzemszerű működése közben: hőmérséklet-tűrés (-40 °C – +70 °C), EMC- és ESD-védelem, mechanikai igénybevétel (rezgés, rázkódás), nedvesség- és porállóság.

A nagy vibrációnak és mechanikai igénybevételnek kitett környezetekben – például mozdonyokon vagy pályamenti szekrényekben – standard RJ45 csatlakozók helyett M12 vagy M23 típusú ipari csatlakozók alkalmazása javasolt. Ezek rezgésállóak, stabil elektromos kontaktust biztosítanak, víz- és poralló kivitelben is elérhetők (pl. IP68, IP69, vagy hermetikus típusok).

5.2.4 Fedélzeti szempontok – kiegészítő megfontolások

Bár a kutatásom fókusza a pályamenti kommunikációs infrastruktúrákra irányul, ebben a részben a fedélzeti elemekről ejtek pár szót. A fedélzeti kommunikációs hálózatok szintén hozzájárulnak az utasbiztonsághoz, vagy épp a szolgáltatások minőségéhez.

Az itt tárgyalt fedélzeti rendszerek nem, vagy nem közvetlenül vesznek részt a biztonságkritikus adatátviteli folyamatokban, ugyanakkor a megfelelő utazási élményt, a megbízható működést szolgálják, így ezek biztonságos és üzembiztos hálózati kiszolgálása sem mellőzhető.

A modern vonatok, szerelvények fedélzetén egyre több olyan kommunikációs hálózatot igénylő rendszer található, amely nem biztonságkritikus, de üzembiztos működésük elvárás a vasúttársaságok és az utasok részéről is. Ilyenek például:

- utasok számára elérhető WLAN rendszerek,
- utastájékoztató kijelzők és hangos bemondók,
- CCTV és videómegfigyelő rendszerek,
- klíma-, fűtés- és világításvezérlés,
- tűzjelző és ajtóvezérlő rendszerek.

Ezek a rendszerek eltérő sávszélesség- és válaszidő-igénnyel rendelkeznek: az I/O-alapú vezérlési feladatok alacsony sávszélességű, de determinisztikus viselkedésű kapcsolatot igényelnek, a videós vagy utasinformációs rendszerek viszont gyakran nagy sávszélességet igényelnek, és burst-ös forgalmi jellegük van.

Napjainkban már a fedélzeti hálózatok kialakításánál az alábbi szempontokra kell figyelni:

- Gigabites hálózati gerinc kiépítése a nagyobb sávszélességű rendszerek kiszolgálására,
- útválasztók, switch-ek gyűrű-topológiába szervezése, ami a redundanciát és a magas rendelkezésre állást szolgálja,
- Bypass megoldások, eszközhiba esetére. A reléalapú bypass porttal rendelkező kapcsolók biztosítják a hálózati kapcsolat fennmaradását még akkor is, ha maga a kapcsoló meghibásodik.

- A Power over Ethernet (PoE) technológia lehetőséget nyújt arra, hogy perifériás eszközök – például IP-kamerák, szenzorok, kijelzők – egyetlen kábelen keresztül kommunikációs csatornát és tápellátást is kapjanak [53]. Ez különösen előnyös lehet mozgó járműveken vagy nehezen hozzáférhető helyeken.
- Ajánlott továbbá az eszközök kialakítása ventilátor nélkül, a hőleadást passzív módon megoldani. Ezzel a megoldással jobban is illeszkednek a fedélzeti telepítési környezethez (korlátozott hely, por, vibráció), és csökkenti a karbantartási igényt és növeli a rendszer élettartamát.
- M12 típusú csatlakozók alkalmazása a rezgésállóság biztosítása érdekében,
- EN 50155 és egyéb vasútspecifikus szabványok betartása (hőmérséklet, EMC, rázás, páratartalom).

5.3 Következtetések, összegzés

Ebben a részben olyan információbiztonsági irányelveket fogalmaztam meg, amelyek hozzájárulhatnak vasúti infokommunikációs rendszerek megbízhatóságának és rendelkezésre állásának növeléséhez. A bemutatott ajánlásaim rendszerszintű megközelítést követnek: figyelembe veszik a hibák időbeli lefutását, a kommunikációs hálózatok tervezési szempontjait, valamint az ipari gyakorlatban bevált megoldásokat, technológiai példákkal alátámasztva. A protokollszintű védelmi mechanizmusoktól a fizikai megvalósításig terjedő javaslatok célja, hogy a kritikus infrastruktúrák működése kiszámítható, determinisztikus, hibatűrő és hosszú távon fenntartható legyen. A javasolt irányelvek nemcsak a meglévő rendszerek továbbfejlesztésére alkalmasak, hanem a jövőbeli, például FRMCS-alapú megoldások tervezését is megalapozhatják. Kiegészítésképpen – bár a fókusz a pályamenti rendszerekre irányult – néhány fedélzeti megoldás, javaslat is megemlítésre került.

A következő táblázatban összefoglaltam a legfontosabb ajánlásokat jelen fejezetből.

Művelet	Javaslat	Módszer
Gyors hibaészlelés	alacsony protokollszinten	kódolással
Gyors hibajavítás	alacsony protokollszinten	hibajavító kóddal, vagy újraküldéssel
Késleltetést elviselő hibajavítás	magasabb protokoll szinten	újraküldési mechanizmusok pl. TCP
Hiba lokalizálás	szegmentált hálózat	TSN alkalmazás
Gyors helyreállítás	redundáns infrastruktúra	duplikált adatküldés
tápellátás biztosítása	redundáns táplálás	automatikus átkapcsolás
Szoftverfrissítések	hitelesített szoftver használata hitelesített személyzet	digitális aláírás, jogosultságok ellenőrzése
Reakció idő csökkentése	szegmentált hálózat	hálózatrészek elkülönítése, áthaladó forgalom ellenőrzése alacsony protokoll szinten
Funkciók szétválasztása	fizikai szétválasztás	külön hálózat építése
Reakció idő csökkentése	zero-trust model	csomópontok ellenőrzik a forgalmat
Hálózat terhelés	indokolt mennyiségű tartalékképzés	tesztüzem, előzetes forgalom becslése
Kommunikáció titkosítása, hitelesítése	titkosítási, hitelesítési algoritmusok használata	protokoll rétegezésbe titkosítási réteg
Távoli hozzáférés	kétfaktoros azonosítás, titkosított csatorna	VPN kötelező alkalmazása
Eseményfigyelés	Automatikus naplózás előírása	események rögzítése azonosítható módon
Fizikai kialakítás	környezeti tényezők figyelembe vétele	szabványok alkalmazása, gyakorlati megfontolások

12. táblázat. Infokommunikáció biztonságát növelő ajánlások

ÖSSZEGZETT KÖVETKEZTETÉSEK

A témaválasztásomat a kommunikációs technológiák gyors ütemű fejlődése, a vasúti infokommunikáció folyamatos korszerűsítése, valamint az ezekkel szorosan összefüggő szabályozási, biztonsági és működésbiztonsági kihívások indokolták.

A kommunikációs technológiák gyors ütemű fejlődése a vasúti infokommunikációban is szükségszerűen megjelent. Szakmai tapasztalataimra építve kutatásom keretében a korszerű vasúti infokommunikációs hálózatokkal szembeni elvárásokkal, a megbízható és biztonságos működés feltételeivel és az ezeket teljesíteni képes műszaki-technológiai megoldásokkal foglalkozom. Munkám célja az volt, hogy bemutassam, hogyan lehet a technológiai, szabványosítási és biztonsági szempontokat összehangolva olyan jövőálló rendszereket kialakítani, amelyek megfelelnek a vasúti közlekedés egyre szigorodó biztonsági és hatékonysági elvárásainak.

Az értekezéstervezet első fejezetében elsőként áttekintettem a vasúti infokommunikációs hálózatokra vonatkozó szabványokat és előírásokat, beleértve az európai és nemzeti szabályozásokat is. Ezek a legtöbb esetben nem konkrét technológiát, hanem teljesítménykritériumokat és működési paramétereket határoznak meg, amivel lehetővé válik az egyre korszerűbb technológiák alkalmazása. Komplex rendszerek esetén viszont nagyon fontos, hogy a különböző technológiák együttműködésének biztosítása rendszerszintű szemléletet is megkövetel. Ugyanakkor bizonyos esetekben az átjárhatóság érdekében konkrét technológiák alkalmazása kötelező (mint például a GSM-R, FRMCS és az ETCS rendszerek esetén). A későbbi fejezetek érthetősége miatt ebben a részben áttekintettem a vasúti kommunikációban és az ETCS rendszerben résztvevő rendszerelemeket és főbb jellemzőiket is.

A második részben bemutattam a megbízható hálózatok létrehozására alkalmas technológiákat. A megbízhatóság szintjének növelése több tényező megfelelő kialakításán múlik, így foglalkoztam a redundáns adatátvitellel, az időzítési és késleltetési problémákkal, valamint a szinkronizáció és gyártóspecifikus megoldásokkal is. Az időkritikus kommunikációs hálózatokra vonatkozó követelmények teljesítése csak olyan topológiákkal és protokollokkal lehetséges, amelyek képesek a determinisztikus működésre.

A harmadik fejezetben részletesen elemeztem a pályamenti infokommunikációs elemek különböző interfészeit és azok jellemzőit, melyeket rendszereztem és megfeleltettem a jelenlegi és jövőbeni technológiákkal alkalmazhatóságuk függvényében.

A negyedik fejezet célja a vasúti kommunikációs rendszerek veszélyforrásainak összegyűjtése és rendszerezése, hatásaik elemzése. Vizsgálataim a műszaki jellegű hibákra és azok időtényezőire fókuszáltak, melyek közül a legfontosabbak a késleltetések, a csomagvesztés, az adatátviteli hibák és a monitoring, azaz a felügyelet hiányosságai. Ezek mellett érintőlegesen foglalkoztam a felhasználói és emberi tényezőkön alapuló veszélyforrásokkal is.

Az ötödik fejezetben olyan információbiztonsági irányelveket foglaltam össze, amelyek célja a vasúti kommunikációs rendszerek megbízhatóságának és rendelkezésre állásának növelése. Az ajánlott irányelveim figyelembe veszik a hibák időbeli lefutását, a technológiai és üzemeltetési szempontokat és a fizikai védelmi lehetőségeket. Időállóság és megbízhatóság szempontjából azok a megoldások a megfelelők, amelyek már beváltak ipari környezetben, és kellő rugalmasságuk révén alkalmazhatók a jövőbeli rendszerekben is.

Az egyes fejezetek mondanivalóját három új tudományos eredménybe soroltam. Elsőként rendszereztem és egymásnak megfeleltettem a vasútbiztonsági szempontból releváns interfészeket és az ezekhez kapcsolódó technológiákat. Másodszor kategorizáltam a potenciális műszaki veszélyforrásokat káros hatásaik és időbeli viselkedésük szerint is. Elhárításukra összefoglaltam a gyakorlatban bevált módszereket. Végül pedig olyan irányelveket fogalmaztam meg, amik a két előző tézisben feltárt összefüggések alapján ajánlanak magas megbízhatóságot biztosító kommunikációs megoldásokat, melyek alkalmasak lehetnek rendszertervezési feladatokban a vasúti infokommunikációs hálózatok megbízhatóságának és biztonságának növelésére és technológiai váltások kezelésére is.

ÚJ TUDOMÁNYOS EREDMÉNYEK

I. Tézis

Rendszereztem és egymásnak megfeleltettem a vasútbiztonsági szempontból releváns kommunikációs interfészeket, kapcsolataikat és az alkalmazható technológiákat. [K1,K3,K4,K5]

II. Tézis

Igazoltam, hogy a rendszerbe sorolt vasútbiztonsági szempontból releváns interfészek potenciális veszélyforrásai beazonosíthatók. [K3,K6]

III. Tézis

Igazoltam, hogy a felderített veszélyforrások ellen megelőző védelmi intézkedések tehetők, mellyel növelhető a működésbiztonság. [K2,K3,K4]

AJÁNLÁSOK, JAVASLATOK

Valós idejű monitoring- és hibaesemény-gyűjtő rendszer alkalmazása. Javasolom olyan központi felügyeleti rendszer bevezetését, amely képes a hálózati események valós idejű naplózására, egyes hálózati hibák előre jelzésére és automatikus reakciókra is.

A kommunikációs infrastruktúra fejlesztése mellett elengedhetetlen a karbantartó és üzemeltető személyzet képzése az újabb és újabb technológiák megfelelő használatára, a megváltozott működési jellemzők ismeretére és a hálózati hibák felismerésére és megfelelő kezelésére.

Disszertációm felhasználását javaslom az oktatásban, illetve vasúti CCT rendszerek, alrendszerek kommunikációs infrastruktúra tervezése során iránymutató dokumentumnak.

IRODALOMJEGYZÉK

[1] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor, „A kritikus információs infrastruktúrák meghatározásának módszertana”, ENO Avisory Kft., 2009

[2] Z. Rajnai, „A kritikus információs infrastruktúrák összetétele, biztonsági kérdései”, Nemzetközi Gépész és Biztonságtechnikai Szimpózium, pp. 15-22. 2012.

[3] D. Maros, D. Tokody, Zs. Tiszavölgyi, „A GSM-R rendszer jelene és jövője”, Vezetékek világa 2015, pp. 17-21. 2015.

[4] D. Tokody, D. Maros, G. Schuster, Z. Tiszavölgyi, „Communication-based Intelligent Railway - Implementation of GSM-R System in Hungary”, in SAMI 2016 - IEEE 14th International Symposium on Applied Machine Intelligence and Informatics - Proceedings, pp. 99–104. 2016.

[5] G. Szabó, „Elektronikus rendszerek funkcionális biztonsága és a biztonság elérésének egyes kihívásai”, Elektrotechnika 115/5-6, pp. 44-48. 2022.

[6] G. Szabó, „A biztonságintegritás és a biztonságorientált alkalmazási feltételek teljesítése a vasúti biztosítóberendezések tervezése és létrehozása során”, In: Stangl, Imre; Csilléry, Béla (szerk.) XVIII. Közlekedésfejlesztési és beruházási konferencia, pp. 25-27, 2017.

[7] G. Szabó, „LED-optika biztonságmenedzsment”, Vasúti vezetékvilág 2, pp. 3-6. 2018.

[8] G. Szabó, G; Tarnai, B.Sághi, G, Rácz, “Kijelölt és bejelentett megfelelésértékelő szervezetek tevékenysége biztosítóberendezési területen”, Vezetékek világa 18, pp. 3-7. 2013.

[9] B. Jóvér, “ETCS, Az Egységes Európai Vonatbefolyásoló Rendszer”, MÁV Szolgáltató Központ Zrt. Baross Gábor Oktatási Központ, Budapest, 2006

[10] IEC 61508, “Functional safety of electrical / electronic / programmable electronic safety-related systems”, Edition 2.0, April 2010.

[11] MSZ EN 50126, “Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).”, April 2018.

[12] MSZ EN 50128, “Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems”, November 2011.

[13] MSZ EN 50121-4, “Railway applications. Electromagnetic compatibility Emission and immunity of the signalling and telecommunications apparatus”, May 2019.

[14] MSZ EN 50155, “Railway applications. Rolling stock. Electronic equipment”, July 2021.

[15] 103/2003. (XII. 27.) GKM rendelet a hagyományos vasúti rendszerek kölcsönös átjárhatóságáról. Hatályos 2023.02.21-2024.11.30. https://njt.hu/jogszabaly/2003-103-20-0L (letöltve: 2024.12.06.)

[16] MSZ EN 50129, “Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling”, March 2019.

[17] MSZ EN 50159, “Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems”, January 2011.

[18] MSZ EN 50657:2017, “Railway applications – Software for rolling stock applications”, 2017

[19] MSZ EN 50716:2023, “Vasúti alkalmazások. Szoftverfejlesztésre vonatkozó követelmények”, 2023

[20] P. Baczoni, “Vonali biztosítóberendezések”, MÁV Szolgáltató Központ Zrt. Baross Gábor Oktatási Központ, Budapest, 2019, ISBN 978-963-9852-34-1

[21] MÁV Feltétfüzet, „Az ETCS L1 és L2 pályamenti alrendszerére vonatkozó alkalmazási követelményeire, 0.1.1. verzió, MÁV P-5600, 2008.

[22] D. Kurhan, et al., “Development of the High-Speed Running of Trains in Ukraine for Integration with the International Railway Network”, Acta Polytechnica Hungarica, Vol. 19, No. 3, pp. 207-218, 2022

[23] Kapsch, “European Railway Traffic Management System - ERTMS”, White paper, 2020.

[24] Hollysys whitepaper, “ERTMS/ETCS LEVEL 2 Solution”, Beijing, China, 2023. https://www.hollysys.com/cms/show-754.html (letöltve: 2024.06.23.)

[25] S. Rosić et al., “Analysis of the Safety Level of Obstacle Detection in Autonomous Railway Vehicles”, Acta Polytechnica Hungarica, Vol. 19, No. 3, pp. 187-205, 2022

[26] IEEE 802.1D, “Local Area Network MAC (Media Access Control) Bridges”, 1998.

[27] IEEE 802.1w, “Local and metropolitan area networks—Common specifications, Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration”, 2001.

[28] IEEE 802.1s, “Local and Metropolitan Area Networks - Amendment to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees”, 2002.

[29] IEC 62439-3:2021, “Industrial communication networks – High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)”, 2021.

[30] M. Ostertag, “Seamless Redundancy with PRP and HSR”, 2022.

[31] Moxa, “Moxa Redundancy Technologies”, 2023. https://www.moxa.com/en/spotlight/industrial-ethernet/redundancytechnology/technologies#turbo (letöltve: 2024.05.12.)

[32] Black Box Network Services, “Advantages of Ring Topologies in Networking”, 2021. https://www.black-box.eu/en-int/page/46882 /Resources/technical/Black-Box-Explains/lan/Advantages-of-Ring-Topologies-in-Networking (letöltve: 2024.05.12.)

[33] H. Song, E. Schnieder, “Development and Evaluation Procedure of the Train-Centric Communication-Based System”, IEEE Transactions on Vehicular Technology PP(99):1-1, September 2018 DOI: 10.1109/TVT.2018.2868881

[34] K. Smith, “Beyond GSM-R: the future of railway radio”, International Rail Journal. Simmons-Boardman Publishing Inc., 2017. https://www.railjournal.com/in_depth/beyond-gsm-r-the-future-of-railway-radio/ (letöltve: 2024.09.11.)

[35] M. Gadnai, „A biztosítóberendezések fejlődése, üzemi tapasztalatok”, MÁV Zrt. Pályavasúti Területi Igazgatóság Miskolc Biztosítóberendezési Főnökség,

[36] E. Kretschmer: „ETCS Hybrid Level 3”. In: Jochen Trinckauf, Ulrich Maschek, Richard Kahl, Claudia Krahl (Hrsg.): „ETCS in Deutschland”. 1. Auflage. Eurailpress, Hamburg 2020, ISBN 978-3-96245-219-3, S. 351–360.

[37] „GSM-R Frequencies India” Chapter 8 Mobile communications – GSM-R. Indian Railways. May 2012.

[38] Australian Railway Association, „Australian Rail Industry Submission to the Minister for Broadband, Communications and the Digital Economy 1800 MHz Spectrum Licenses”. March 2019.

[39] Európai Vasúti Ügynökség (ERA), „Interfaces between Control-Command and Signalling Trackside and Other Subsystems” ERA/ERTMS/033281

[40] Commission implementing regulation (EU) 2023/1695, on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919, 10 August 2023

[41] Lin Junting1, Dang Jianwu1 and Min Yongzhi. „NGCTCS: Next-generation Chinese Train Control System”, Journal of Engineering Science and Technology Review, pp. 122- 130, 2016.

[42] „ERTMS/ETCS LEVEL 1/2 Solution”, HolySys, https://www.hollysys.com/industries/industries/transportation/main-line-railway/railway/22 (letöltve: 2025.01.06.)

[43] „Sat One secures OneWeb capacity for Australia and New Zealand”, Eutelsat OneWeb, https://oneweb.net/resources/sat-one-secures-oneweb-capacity-australia-and-new-zealand (letöltve: 2025.01.06.)

[44] „Iridium Certus 700 FACT SHEET”, Iridium, https://www.iridium.com, (letöltve: 2025.02.08.) 2024.

[45] B. Clatworthy, „All aboard the Starlink Express, a marvel of wi-fi connectivity”, https://www.thetimes.com/uk/politics/article/high-speed-train-wifi-connection-germany-d67k3zx6w

[46] R. Lea, „SpaceX inks 14-launch deal to loft Telesat's 'Lightspeed' internet constellation”, https://www.space.com/spacex-telesat-lightspeed-constellation-launch-deal (letöltve: 2025.01.30.), 2023.

[47] K. Mészáros, T. Wührl, P. J. Varga, S. Gyányi, R. Kovács, M. T. Baross, and G. Kún, “RF kutatások a Kandón, kiemelten 5G vonatkozásában,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 53–53.

[48] R. Kovács, P. J. Varga, G. Kún, S. Gyányi, T. Wührl, and K. Mészáros, “5G hálózatok strukturáltsági vizsgálata” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 46–46.

[49] K. Gergely, J. V. Péter, W. Tibor, W. Dóra, G. Sándor, N. László, and K. Róbert, “ ‘Opened’ or ‘Closed’ RAN in 5G,” in IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022), 2022, pp. 347–351.

[50] 3GPP TS 43.020, „Security related network functions, 3rd Generation Partnership Project (3GPP)”, Technical Specification, Release 17, 2022.

[51] IEEE 1588-2019, „Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”, ISBN:978-1-5044-6341-6

[52] P802.1AS-Rev, „Local and Metropolitan Area Networks – Timing and Synchronization for Time-Sensitive Applications”, ISBN:978-1-5044-6430-7

[53] IEEE 802.3af/at/bt „IEEE Standard for Information Technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements … Power via Media Dependent Interface (MDI)” 2003, 2009, 2018

[54] EN 50173-3:2018, „Information technology – Generic cabling systems – Part 3: Industrial spaces”, 2018.[55] IEEE 802.1AS:2020, „Timing and Synchronization for Time-Sensitive Applications”, 2020.

[56] IEEE 802.1Qbv:2015, „Enhancements for Scheduled Traffic”, 2015.

[57] IEEE 802.1Qci:2017, „Per-Stream Filtering and Policing”, 2017.

[58] IEEE 802.1CB:2017, „Frame Replication and Elimination for Reliability”, 2017.

[59] IEEE 802.1Qcc:2018, „Stream Reservation Protocol (SRP) Enhancements and Performance Improvements”, 2018

[60] IEEE 802.1Qch:2017, „Cyclic Queuing and Forwarding”, 2017.

[61] IEEE 802.1Qcr:2020, „Asynchronous Traffic Shaping”, 2020.https://www.telesat.com/leo-satellites/ (letöltve: 2025.02.12.)

[63] Vasúti Műszaki Bizottság, https://vmb.kti.hu/ (letöltés: 2025.01.04.)

A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

[K1] G. Kún and T. Wührl, “Biztonságkritikus kommunikáció vasúti rendszerekben,” in KVK Habilitációs és PhD Workshop Minikonferencia, 2024, pp. 105–109.

[K2] G. Kún and T. Wührl, “Magas rendelkezésre állású kommunikációs hálózatok megvalósítása vasúti környezetben,” in XXXIX. Kandó Konferencia 2023, 2024, pp. 122–136.

[K3] G. Kún and T. Wührl, “Reliable Communication in Railway Systems”, in 2023 IEEE 6th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE), 2023, pp. 347–351.

[K4] G. Kún and T. Wührl, “Classification of Communication Interfaces in Railway Systems”, in IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023 : Proceedings, 2023, pp. 749–754.

[K5] G. Kún and T. Wührl, “Közlekedés és a mobilkommunikáció kapcsolata”, KÖZLEKEDÉS ÉS MOBILITÁS, vol. 2, no. 2, pp. 98–109, 2023.

[K6] G. Kún and T. Wührl, “Vasúti kommunikációs rendszerek biztonsági kérdései”, in KVK PhD Workshop Minikonferencia : Absztrakt kötet, 2023, pp. 6–7.

A SZERZŐ TOVÁBBI TUDOMÁNYOS KÖZLEMÉNYEI

[K8] M. T. Baross, G. Kún, T. Wührl, P. J. Varga, S. Gyányi, and R. Kovács, “5G gyakorlati oktatása a Kandón,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 57–57.

[K9] K. Gergely, J. V. Péter, W. Tibor, W. Dóra, G. Sándor, N. László, and K. Róbert, “ ‘Opened’ or ‘Closed’ RAN in 5G,” in IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022), 2022, pp. 347–351.

[K10] S. Gyányi, G. Kún, T. Wührl, P. J. Varga, M. T. Baross, and R. Kovács, “5G rádiós hozzáférési hálózati struktúrák,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 52–52.

[K11] R. Kovács, P. J. Varga, G. Kún, S. Gyányi, T. Wührl, and K. Mészáros, “5G hálózatok strukturáltsági vizsgálata,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 46–46.

[K12] G. Kún, T. Wührl, P. J. Varga, S. Gyányi, D. Wührl, and M. T. Baross, “Közlekedéstámogatás az 5G mobil hálózatokban,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 47–47.

[K13] K. Mészáros, T. Wührl, P. J. Varga, S. Gyányi, R. Kovács, M. T. Baross, and G. Kún, “RF kutatások a Kandón, kiemelten 5G vonatkozásában,” in XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet, 2022, pp. 53–53.

[K14] J. V. Péter, N. László, B. T. András, K. Eszter, W. Tibor, G. Sándor, K. Gergely, K. Róbert, B. Anna, and K. Miklós, “5G RAN research in Óbuda University,” in IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022), 2022, pp. 359–365.

[K15] K. Gergely, W. Tibor, J. V. Péter, D. Wührl, G. Sándor, and N. László, “Relationship between 5G and transportation,” in 2021 IEEE 4rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), 2021, pp. 153–158.

[K16] K. Gergely, R. Kovács, W. Tibor, K. Mészáros, N. László, G. Sándor, and J. V. Péter, “Introduction of 5G in education,” in 2021 IEEE 4rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), 2021, pp. 147–152.

[K17] G. Kún and T. Wührl, “Biztonságtechnikai vizsgálatok automatizálási rendszerekben,” in Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2021, 2021, pp. 30–30.

[K18] K. Róbert, K. Gergely, N. László, J. V. Péter, G. Sándor, W. Tibor, and M. Kristóf, “5G research in Kandó,” in 21th IEEE International Symposium on Computational Intelligence and Informatics (CINTI 2021), 2021, pp. 000217–000222.

[K19] T. Wührl and G. Kún, “Mobilkommunikáció és a közlekedés - biztonságtechnikai megközelítés,” in Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2021, 2021, pp. 35–35.

[K20] G. O. Kún, “IP forgalom analízis,” in XXXII. Kandó Konferencia 2016, 2016, pp. 1–13.

[K21] G. O. Kún, “IP traffic analysis,” in 30. Kandó Konferencia [K30th Kandó Conference], 2014, pp. 1–14.

[K22] G. Kún, “IP forgalom analízis,” in 29. Kandó Konferencia = 29th Kandó Conference, 2013.

[K23] G. Kún, D. Maros, P. Huber, J. Aromaa, and T. Viitaen, “2G, 3G mobil hálózat az egyetemi oktatásban,” in 28. Kandó Konferencia, 2012.

[K24] G. Kún, “Examination of IP Traffic based on Streaming Parameters,” in Science in practice, 2011, pp. 7–10.

[K25] G. Kún, “Discovering of Traffic Types based on Statistical Properties,” in 27th Scientific Electrotechnical Conference, 2009.

[K26] G. Kún, “Forgalmak azonosítása IP hálózatokban,” in XXIV. Nemzetközi Kandó Konferencia 2008, 2008.

[K27] G. Kún, “Identification of Traffic Types in IP Networks,” in Intertech 2008, 2008, pp. 287–290.

[K28] G. Kún and P. Varga, “Estimating Quality of Experience in IP Networks,” in MicroCAD 2007 International Scientific Conference, 2007, pp. 139–144.

[K29] G. Kún and P. Varga, “IP Traffic Characteristics in Case of Congestion,” in 6th International conference of PhD students = PhD hallgatók VI. Nemzetközi Konferenciája, 2007, pp. 299–303.

[K30] G. Kún, “Veszélyhelyzeti kommunikáció támogatása az IP hálózati forgalom osztályozásával,” in Veszélyhelyzeti kommunikáció 2007, 2007.

[K31] P. Varga, G. Kún, and G. Sey, “Towards Estimating Quality of Experience with Passive Bottleneck Detection Metrics,” in Advances in Information Systems Development, 2007, pp. 115–125.

[K32] G. Kún, “Detecting congestions in data networks,” in Kandó conference 2006 : in memoriam Kandó Kálmán, 2006.

[K33] G. Kún and P. Varga, “Utilizing MGR-PS Model Properties for Bottleneck Characterization,” in WTC 2006, 2006, pp. 1–8.

[K34] P. Varga, G. Kún, G. Sey, I. Moldován, and P. Gelencsér, “Correlating User Perception and Measurable Network Properties: Experimenting with QoE,” LECTURE NOTES IN COMPUTER SCIENCE, vol. 4268, pp. 218–221, 2006.

[K35] P. Varga, G. Kún, and I. Moldován, “Correlation of Advanced Bottleneck Metrics and Quality of Experience,” in APNOMS 2006, 2006, pp. 1–9.

[K36] P. Varga, G. Kún, and G. Sey, “A QoS mérőszámok és a felhasználói elégedettség közötti kapcsolatok,” in 15. Távközlési és Informatikai Hálózatok Szeminárium, 2006, pp. 1–10.

[K37] G. Kún and P. Varga, “Detecting congested links in internet service providers’ IP networks,” in Phd Hallgatók V. Nemzetközi Konferenciája., 2005, pp. 103–108.

[K38] P. Varga and G. Kún, “Utilizing higher order statistics of packet interarrival times for bottleneck detection,” in E2EMON’05, 2005, pp. 152–164.

[K39] G. Kún, Helyi számítógép-hálózatok. Budapest: Panem Kiadó, 2004.

[K40] B. J, H. Z, K. G, and M. M, “Advanced QoS Provision for Real-Time Internet Traffic,” in 13th IEEE Packet Video Workshop, 2003, pp. 153–159.

[K41] P. Varga, G. Kún, P. Fodor, J. Bíró, D. Satoh, and K. Ishibashi, “An Advanced Technique on Bottleneck Detection,” in Proceedings of 9th EUNICE Open European Summer School and IFIP WG6.3 Workshop on Next Generation Networks, EUNICE 2003, 2003, pp. 52–56.

[K42] K. G, L. D D, and B. J, “Bandwidth Estimation of Bottleneck Link,” in The Polish-Czech-Hungarian Workshop on Circuit Theory and Applications, 2002, pp. 46–51.

[K43] G. Kún, G. Szűcs, and J. Zátonyi, “Performance measurements to provide QoS in IP networks,” in TRANSCOM 2001, Proceedings of the 4th European Conference of Young Research and Science Workers in Transport and Telecommunications : Section 2. Electrotechnics, 2001.

[K44] G. Kún, D. D. Luong, and J. Bíró, “Bandwidth estimation of bottleneck link,” in Proceedings of Polish - Czech - Hungarian Workshop on Circuit Theory, Signal Processing and Telecommunication Networks, 2001, pp. 46–51.

RÖVIDÍTÉSJEGYZÉK

3GPP	3rd Generation Partnership Project
ÁME	Általános Műszaki Előírás
ARQ	Automatic Repeat reQuest
ATC	Automatic Train Control
BSC	Base Station Controller
BTM	Balise Transmission Module
BTS	Base Transceiver Station
CAN	Controller Area Network
CBI	Computer-Based Interlocking
CRC	Cyclic Redundancy Check
CTC	Centralized Traffic Control
CCS	Control Command and Signalling
DoS	Denial of Service
DWDM	Dense Wavelength Division Multiplexing
EIRENE	European Integrated Railway Radio Enhanced Network
EMC	Electromagnetic Compatibility
eMLPP	enhanced Multi-Level Precedence and Pre-emption.
ERTMS	European Railway Traffic Management System
ERTMS	European Rail Traffic Management System
ESD	Electrostatic Discharge
ETCS	European Train Control System
ETML	European Traffic Management Layer

EVC	European Vital Computer
FEC	Forward Error Correction
FRMCS	Future Railway Mobile Communication System
GEO	Geostationary Earth Orbit
GSM-R	Global System for Mobile Communications – Railway
HARQ	Hybrid Automatic Repeat reQuest)
HMI	Human-Machine Interface
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPSec	Internet Protocol Security
KÖFI	Központi Forgalomirányítás
LDPC	Low-Density Parity-Check Codes
LEO	Low Earth Orbit
LEU	Lineside Electronic Unit
LSP	Label Switched Path
LTE-R	Long Term Evolution – Railway
MCPTT	Mission Critical Push-To-Talk
MCX	Mission-Critical Services
MITM	Man-in-the-Middle
MPLS	Multiprotocol Label Switching
MSC	Mobile Switching Center
OVSZ	Országos Vasúti Szabályzat
PoE	Power over Ethernet

RBC	Radio Block Centre
RS-xxx	Recommended Standard xxx
SDH	Synchronous Digital Hierarchy
TEN-T	Trans-European Transport Network
TLS	Transport Layer Security
TSI	Technical Specification for Interoperability
TSRS	Temporary Speed Restriction Server
UART	Universal Asynchronous Receiver/Transmitter
UIC	Union Internationale des Chemins de fer (International Union of Railways)
URLLC	Ultra-Reliable Low Latency Communications
VMB	Vasúti Műszaki Bizottság
VME	Vasúti Műszaki Előírások
VPN	Virtual Private Network
WDM	Wavelength Division Multiplexing

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Köszönöm az Óbudai Egyetem Kandó Kálmán Villamos Karának, hogy kutatásaimat lehetővé tette és támogatta.

Köszönöm a KTI Tudományos Tanács kutatóinak támogatását, jobbító szándékú tanácsaikat és észrevételeiket. Köszönöm a Tanúsítási Igazgatóság CCS osztály munkatársainak segítségét.