DOI: https://doi.org/10.12700/btsz.2025.7.3.129

RELIABLE AND SAFE COMMUNICATION FOR CONTEMPORARY RAILWAY SYSTEMS

MEGBÍZHATÓ ÉS BIZTONSÁGOS KOMMUNIKÁCIÓ A KORSZERŰ VASÚTI RENDSZEREKBEN

KÚN Gergely[1] – WÜHRL Tibor[2]

Abstract

Digital communication technologies play an important role in the data networks that support modern railway transport. Contemporary railway systems—especially those employing automated train control solutions—place strict requirements on the underlying communication infrastructure. These include high reliability, deterministic behavior, and rapid recovery in the event of connection failures. This paper examines both the operational conditions, technologies, and protocols applied in railway communication infrastructures, and the most important safety-related risks. It provides an in-depth, component-level analysis of latency as a critical hazard. By identifying the different causes of communication delay, it becomes possible to establish clear technical requirements and protocol-level solutions aimed at enhancing reliability and safety. The approaches presented support future network design and contribute to the sustainable development of railway transport.

Keywords

telecommunication, railway, ETCS, safety-critical, digital, reliability

Absztrakt

A digitális kommunikációs technológiák a korszerű vasúti közlekedést kiszolgáló adathálózatokban is meghatározó szerepet töltenek be. A modern vasúti rendszerek, elsősorban az automatizált vonatbefolyásoló megoldások, szigorú követelményeket támasztanak a kommunikációs hálózatokkal szemben. Alapvető elvárás a magas megbízhatóság, a determinisztikus viselkedés, valamint kapcsolati hiba esetén a gyors helyreállás. A cikk egyrészt a vasúti infokommunikációs infrastruktúrák működési feltételeit, alkalmazott technológiáit és protokolljait vizsgálja, másrészt elemzi a biztonságkritikus szempontból felmerülő legfontosabb veszélyforrásokat is. A késleltetést, mint veszélyforrást részletesen, összetevőire bontva tárgyalja. A késleltetésre ható tényezők feltárása lehetőséget teremt konkrét követelmények meghatározására, valamint olyan technológiai és protokollszintű megoldások kidolgozására, amelyek a megbízhatóság és a biztonság növelését szolgálják. A bemutatott megközelítések támogatják a jövőbeli hálózattervezést, és hozzájárulnak a vasúti közlekedés fenntartható fejlődéséhez.

Kulcsszavak

telekommunikáció, vasút, ETCS, biztonságkritikus, digitális, megbízhatóság

[1] kun.gergely@kvk.uni-obuda.hu, kun.gergely@kti.hu | ORCID: 0000-0003-0572-5177 | assistant lecturer, Óbuda University | egyetemi tanársegéd, Óbudai Egyetem | technical expert, Institute for Transport Sciences | megfelelőségértékelési szakértő, Közlekedéstudományi Intézet

[2] wuhrl.tibor@kvk.uni-obuda.hu, wuhrl.tibor@kti.hu | ORCID: 0000-0002-7522-3511 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem | technical expert, Institute for Transport Sciences | megfelelőségértékelési szakértő, Közlekedéstudományi Intézet

INTRODUCTION

The reliable and safe operation of critical infrastructure is very important at the national level, as failures can lead to serious social and economic consequences. The railway system—including tracks, control equipment, and communication networks—is also considered as critical infrastructure [1]. The role of railway transport is continuously increasing, as it is becoming increasingly important in both passenger and freight transportation.

Modern railway systems increasingly rely on computer-based, automated monitoring and control solutions, where communication networks play a key role. Automatic Train Control (ATC) systems [2] are based on continuous data exchange between the train and the trackside control systems. For these systems in order to function reliably, it is essential that the transmitted information should reach its destination in a secure manner, on time, , and without distortion.

With the rise of digital communication technologies, new challenges have emerged for industrial and safety-critical systems—including the railway sector. Traditionally long life cycle and static systems are increasingly being replaced by rapidly evolving solutions, many of which were originally designed for commercial use. While these new technologies may offer cost advantages, their integration requires a fundamentally different design approach, particularly in the areas of reliability, availability, and risk management.

In railway communication networks, it is very important to classify information based on its criticality, to identify potential hazards accurately, and to apply appropriate protective actions. Technological advancements and standardization efforts jointly create new opportunities as well as new expectations. The goal is to align these aspects in order to implement a robust communication architecture that meets railway safety requirements over long term.

CONCEPTUAL BACKGROUND AND RELATED WORK

Initially, the key components of railway supervision systems are reviewed. In the early stages of railway supervision and control, signaling devices appeared first. Their function was limited to simple information transmission, without direct intervention in train operations.

Interlocking systems

The next major advancement was the introduction of interlocking systems, which established logical dependencies between the state of the railway infrastructure and control actions. Unlike basic signaling, interlocking systems do not only provide information but also implement active safety logic—for example, they prevent a switch from being moved if a train occupies the corresponding track.

The central unit of the interlocking system collects and evaluates data from trackside sensors. Based on the gathered information, it performs control actions in accordance with railway safety regulations. A railway infrastructure operator typically has multiple interlocking centers, each responsible for supervising a specific geographical area. These centers are connected via data network that enables information exchange between them [2] [3].

A Computer-Based Interlocking (CBI) system consists of a central server, associated trackside equipment, and the communication network. From the perspective of safe railway operations, it is considered the most critical system.

Centralized traffic supervision and control

Central traffic supervision enables the automated monitoring of larger traffic areas, junctions, or longer railway line sections from a central location [4]. In contrast, Centralized Traffic Control (CTC) allows remote supervision and control of train movements from a centralized control center. The centralized control is executed via local interlocking systems, which carry out the issued commands. The primary goal of CTC is to increase the efficiency and flexibility of railway operations.

Track circuits and axle counters

One of the fundamental components of railway interlocking systems is track occupancy detection, which reliably identifies whether a train is occupying a specific track or track section. The most common solutions include track circuits and axle counters. In modern railway networks, reliable track occupancy detection is essential for providing accurate track status information, which is required by ETCS (European Train Control System) or other onboard train control systems.

European Railway Traffic Management System

The ERTMS (European Rail Traffic Management System) aims to establish a unified train control and management system across national borders. It has three parts:

The ETML (European Traffic Management Layer) covers tasks related to traffic management and control. EIRENE (European Integrated Railway Radio Enhanced Network) provides the radio communication link between onboard and trackside equipment. This role is currently fulfilled by the GSM-R (Global System for Mobile Communications – Railway) system, which will be replaced in the future by the 5G-based FRMCS (Future Railway Mobile Communication System).

The third component is the European Train Control System (ETCS), the elements of which are presented in the following sections. The goal of ETCS is to provide a standardized automatic train protection system and a comprehensive train control solution across Europe, supporting cross-border interoperability.

The implementation of the ETCS system is progressing gradually, and it currently everywhere operates former national systems in parallel. ETCS offers three levels of service capability that will be detailed below. Nowadays Level 2 is the most widely deployed and used, primarily in Europe but increasingly all over the world [5] [6].

Components in ETCS - Balise

A balise is a passive device between the rails in a fixed position. It operates based on electromagnetic principles and transmits data by radio waves to a locomotive passing above it. The energy required for data transmission is supplied inductively by the balise transmission unit installed on the locomotive. The transmitted data may include information such as kilometer positions, movement authority, braking commands, or signal states.

In the ETCS system, two types of balises are present: fixed- and controlled balises. Controlled balises are capable of transmitting variable data, which are managed by the LEU (Lineside Electronic Unit). The LEU enables data flow between the interlocking system and

the controlled balise, allowing context-dependent, targeted information transmission based on the current traffic situation. It is applied in ETCS Level 1, and performs point-wise train control. In contrast, fixed balises can only transmit static data and are typically used to provide location reference information, especially in ETCS Levels 2 and 3.

Radio Block Center

At ETCS Levels 2 and 3, the Radio Block Center (RBC) is introduced as the central trackside control unit of the system. A railway infrastructure operator may use multiple RBCs. The number of RBCs depends on how many trains could be managed simultaneously by a single RBC (typically between 50 and 100). An RBC can communicate with adjacent RBCs and may have also interfaces to the local CBI systems, the CTC center, and other system components.

The tasks of the RBCs include managing movement authorities for trains and generating control commands based on information received from the interlocking system and trackside equipment. These instructions are transmitted to the onboard equipment by the GSM-R radio network.

Temporary Speed Restriction System

The Temporary Speed Restriction System (TSRS) is an optional supplementary function of the ETCS. Its purpose is to manage temporary speed restrictions in the event of maintenance work, track defects, or other temporary safety-related risks. The related control commands are transmitted via the RBC to the onboard units of the affected trains.

ETCS levels

ETCS Level 1 (L1) implements point wise train control and it is based on conventional interlocking systems. In this setup, information—such as the current state of a lineside signal—is transmitted to the trains typically via controlled balises managed by LEUs. This version does not use data communication solutions.

ETCS Level 2 (L2) is also based on conventional interlocking systems, meaning that train detection based on track circuits or axle counters. The interlocking system communicates with the RBC, which manages movement authorities within its control area and thereby automates traffic control. Movement authorities, as well as control and status information, are transmitted to the onboard unit by the GSM-R network. Accurate train positioning is very important in ETCS L2, and it is achieved by the onboard system using data received from passed balises. This research focuses specifically on systems operating at this level.

ETCS Level 3 (L3) represents the most advanced version of the system, offering the highest level of functionality. At this level, full radio-based train control is implemented, including continuous speed supervision and moving block operation, which allows dynamic train separation instead of traditional fixed blocks. ETCS Level 3 enables removing all of trackside signaling equipment, as all necessary information is transmitted to the onboard unit via radio communication. Thus, in theory, the role of the train driver could be reduced to a minimum.

A new feature in ETCS L3 that the responsibility of train integrity supervision is assigned to the onboard system. As a result, the vehicles coupled behind the locomotive become integrated into the onboard communication network and maintain a continuous data

transfer to the integrity monitoring unit. This introduces new requirements for the onboard architecture and communication systems.

Reducing the number of trackside devices can lead to significantly lower maintenance costs. Although ETCS L3 has not yet been deployed in regular operation, pilot projects are underway in several European countries [7].

Communication links among system components

Modern computer-based systems in railway supervision use information and communication technologies. They improve both infrastructure capacity and operational safety. The operation of such systems requires highly reliable, stable communication networks with continuously increasing transmission capacity. Figure 1 illustrates the interconnections between the components of an ETCS L2 system:

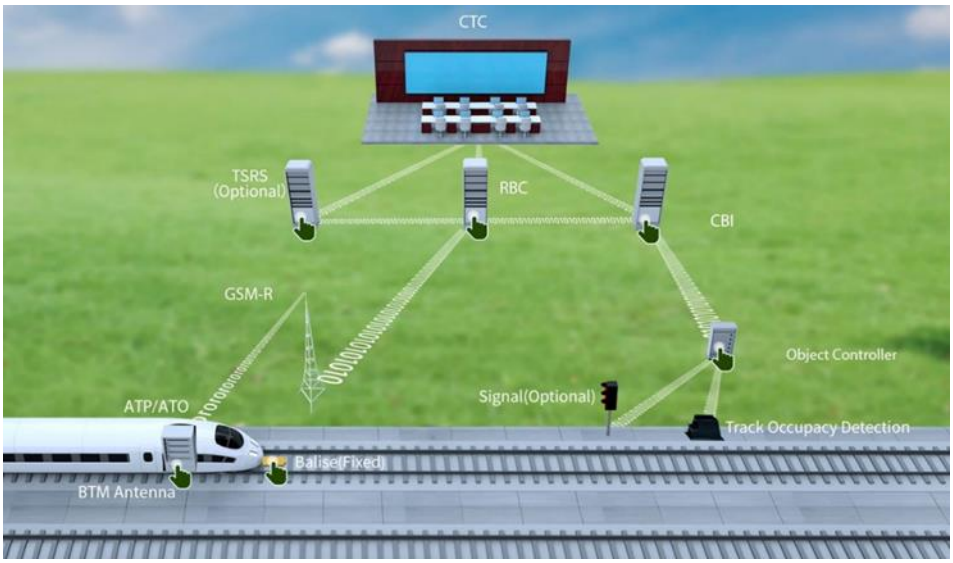

Figure 1: Communication links among functional components of ETCS L2 system [8]

From a functional view, the communication links between the system components can be classified based on their importance and safety-critical nature. The following sections present the properties of the connections shown in the figure.

Safety-critical communication networks

A safety-critical communication network refers to a type of communication infrastructure whose failure, outage, or performance degradation has a direct and severe impact on the operation and safety of the railway system—potentially posing a direct threat to human life. These networks must typically meet strict reliability, availability, and safety requirements, and are generally required to comply with SIL4 (Safety Integrity Level 4) certification, issued by an independent assessment body. To fulfill the relevant standards, such networks commonly incorporate redundancy, latency optimization, and various error correction or signaling mechanisms.

The CBI–RBC interface (in ETCS Level 2 and Level 3 systems) is responsible for enabling the RBC to calculate and transmit movement authorities and other train operation-

related information in real time. The necessary trackside data—such as the status of switches, signals, and other interlocking elements—is provided by the CBI system through this interface.

The RBC–GSM-R (and in the future, FRMCS) interface facilitates communication between the RBC and the onboard ETCS units via the GSM-R mobile network. This connection ensures the continuous transmission of movement authorities and other operational data to the trains.

The purpose of the radio link between the GSM-R network and the onboard equipment is to ensure continuous data communication between the ETCS onboard unit—namely the Automatic Train Protection (ATP) system and the Automatic Train Operation (ATO) system—and the Radio Block Center (RBC) via the radio channel.

The purpose of the connection between neighboring RBCs is to ensure the seamless handover of ETCS L2 trains from one control area to another, maintaining the continuity of movement authorities and uninterrupted train control.

CBI–Trackside equipment controller connection ensure continuous data flow from track occupancy detection devices (such as track circuits and axle counters) to CBI. The CBI processes data received and controls the associated trackside equipment. Since this communication affects the safety-critical layer of railway control, the interface must meet strict safety requirements and is vital for system operation.

The TSRS–RBC connection allows the RBC to send up-to-date temporary speed restriction information to trains running under ETCS L2 and L3, using data from the TSRS.

Non-safety-critical communication networks

A non-safety-critical communication network, in contrast to the previous one, is a network whose failure, temporary outage, or performance degradation does not significantly affect core operational processes. These networks are typically subject to less stringent requirements in terms of reliability, availability, and latency.

The purpose of the CTC–RBC connection is to provide the RBC with operational and time schedule-related data from the CTC system. This information can be taken into account when issuing movement authorities. In case of an interface failure, the RBC can continue to function based on trackside data from the CBI, but traffic management becomes significantly more difficult and may require manual intervention.

The purpose of the CTC–CBI connection is to enable the CTC system to monitor remotely the status of the CBI and, when necessary, to control switches and signals. Although the CBI can operate independently via local control, a loss of the central connection may significantly reduce traffic management efficiency.

The purpose of the TSRS–CTC connection is to allow the CTC system to monitor and manage temporary speed restrictions via this interface, which are stored and maintained by the TSRS. This connection enables the CTC to query, update, or modify speed restrictions, for example in cases of track maintenance or adverse weather conditions. If the interface fails, the CTC can no longer directly manage or verify temporary speed restrictions; however, basic railway operations can still continue.

In addition for normal operation of the system several other non-safety-critical connections are included, which are not shown in the diagram. These are maintenance and diagnostic interfaces, as well as operational communication links, which are present at each

system component. Although these interfaces are not part of the real-time safety chain of train control, they are essential for sustainable operation and for ensuring long-term system reliability.

Challenges of technological advancement

To establish the connections between the system components introduced earlier, reliable network solutions are applied. Following the emergence of digital data transmission, synchronous transmission technologies—particularly SDH (Synchronous Digital Hierarchy)—served as the basis of backbone network infrastructures over a long period. These systems were primarily used over optical transmission media, though earlier implementations included copper-based and microwave links as well.

SDH technology provides real-time fault detection and automatic switching to redundant paths, ensuring highly reliable data transmission. It also served as an underlying transport backbone for classical E1 and ATM (Asynchronous Transfer Mode) systems, and later for IP-based networks. Although its use is gradually declining, SDH still plays an active role in many existing railway communication infrastructures.

One of the key features of SDH technology is that the containers transmitted at the data link layer are transferred according to a strictly timed, synchronous system. All transmission nodes are synchronized to a central clock, enabling highly precise timing and deterministic data transfer. As a result, SDH is particularly well suited for serving delay-sensitive applications, such as critical railway communication systems.

A clear trend can be observed today: communication networks are increasingly built on Ethernet-IP foundations. This development is not limited to office and home environments but is also evident in industrial systems, including railway communication networks. The use of Ethernet-IP networks in the railway sector offers several advantages, such as higher data transfer capacity, cost-effective operation, and the use of standardized and widely available equipment. However, this approach also raises significant technical and security challenges, particularly in terms of reliability and protection of safety-critical systems.

Compared to the synchronized communication systems, Ethernet-IP packet-switched networks are fundamentally based on a best-effort transmission model. This means by default, there is no guarantee on the delivery, integrity, or latency of data packets. From a timing perspective, such networks inherently lack the precision required for critical applications. However, significant advancements in network capacity have enabled the introduction of compensating mechanisms that improve the reliability and accuracy of time synchronization. In the future, the role of timing and synchronization will become even more important, especially with the emergence of next-generation standards such as Time-Sensitive Networking (TSN). TSN integrates precise traffic scheduling into Ethernet-based systems, aiming to provide deterministic, predictable, and latency-controlled data transmission—an essential requirement for safety-critical railway applications.

The railway context imposes very strict safety requirements on communication systems. These regulations typically do not prescribe specific technologies, but rather define performance indicators, functional requirements, operational parameters, as well as recommended procedures and solutions.

A similar approach can be observed in other industrial sectors, where standardized requirement frameworks have been developed to ensure the reliability and stable operation of equipment and systems, as well as to protect human health and safety. Depending on the sector, these standards may contain mandatory or optional provisions, and they play a fundamental role in ensuring the compliance of products supplied by manufacturers and vendors.

The IEC 61508 international standard [9], issued by the International Electrotechnical Commission (IEC), provides a general framework for the design, application, maintenance, and operation of electrical, electronic, and programmable electronic safety systems. It covers the entire lifecycle of a product. The standard defines the required input information and expected output results for each lifecycle phase.

Furthermore, it mandates the identification of hazardous events and the assessment of associated risks, taking into account their probability, frequency, and the severity of potential consequences. The application of IEC 61508 is recommended or required in cases, where the operation involves risks that could endanger human life, health, or environmental safety.

Functional safety standards based on IEC 61508 adopt a risk-based approach to achieve the required level of process and system safety. Safety targets are defined using quantitative metrics derived from risk assessments. One such metric is the THR (Tolerable Hazard Rate), which indicates the maximum acceptable probability of occurrence for a hazardous event. In contrast, the TFFR (Tolerable Functional Failure Rate) specifies the acceptable frequency of functional failures.

These standards define four Safety Integrity Levels (SIL), where SIL1 represents the lowest, and SIL4 the most stringent safety requirements. SIL0 is not covered by the standard, as it does not provide formally recognized functional safety. Devices corresponding to each SIL level are classified into two categories by the standard, based on the nature of their usage:

- For low-demand devices, safety performance is characterized by the probability of failure. These systems are typically activated only occasionally—for example, a monitoring system in a power plant that engages only when an operational parameter deviates from the allowed range. If such a system is classified as SIL1, its allowable probability of failure must fall between 0.01 and 0.1.
- For high-demand or continuously operating devices, performance is measured by the frequency of failure occurrence, typically expressed in hours^{-1} (1/h). An example of this would be a route-setting system in railway operations, where the acceptable failure frequency for SIL1 ranges between 10^{-6} and 10^{-5} failures per hour.

The MSZ EN 50159:2011 standard [10] defines the IT and safety requirements that communication networks supporting railway applications must meet. These networks can be categorized as either closed or open and may interconnect both safety-critical and non-safety-critical system components.

The primary goal of the standard is to ensure the reliability, data security, and resilience of railway communication systems. To this end, it prescribes the use of various security mechanisms, such as encryption, authentication, data integrity checks, redundancy, and fault tolerance. Additionally, the standard specifies documentation requirements that ensure

traceability and transparency, which are essential for the auditability and safety compliance of communication systems.

RESEARCH RESULTS

A reliable and secure design of communication networks requires a thorough understanding of the potential hazards and failure sources associated with the system. The MSZ EN 50159:2011 standard [10] specifically addresses the identification of risks relevant to communication. Given the broad scope of the topic, present study focuses exclusively on communication and technological aspects.

The standard identifies numerous potential events that may pose a threat to the operation of the transmission system and determines which "basic message errors" they can cause. The most typical of these errors are as follows:

- repetition;
- deletion;
- insertion;
- re-sequencing;
- corruption;
- delay;
- masquerade.

The network infrastructure of safety-critical railway systems must meet strict timing, reliability, and synchronization requirements. A network is considered deterministic primarily if its data transmission times are predictable and guaranteed—this is essential for critical applications.

The delay, which the standard classifies as a "basic message error", should be analyzed by breaking it down into components. This approach allows the various causes of delay to be linked to specific entities involved in the communication process. As a result, the direct effects of these delays can be identified, and corresponding prevention strategies can be defined.

For instance, in Hungary, in case of ETCS L2 implementation, the communication between the onboard equipment and the trackside system may not be interrupted for more than 18 seconds. If the time elapsed since the last valid received message exceeds this threshold, the onboard system automatically initiates a predefined safety action—such as braking or emergency braking. Within this time window—assuming the worst-case scenario—the communication system must be capable of reestablishing the transmission channel. During this process, the GSM-R system must ensure the availability of the radio channel and maintain the connection toward the RBC through the aggregation network.

Regarding latency, several factors contribute to the overall delay, with the following being the most significant:

- connection establishment time or delay;
- transmission delay;
- congestion-induced delay;
- recovery time in case of link or network failure;
- mobility-related delays (e.g., handover).

In the following sections, proven methods and practical recommendations are reviewed to mitigate the effects of these latency components.

Reduction of call establish time

The time required to establish a communication path can be minimized by using static IP address allocation, TSN-based preconfigured network schemes, MPLS (Multiprotocol Label Switching) label-based routing, or equivalent solutions. It is strongly recommended to avoid dynamic IP allocation—such as the use of the DHCP (Dynamic Host Configuration Protocol)—because this method introduces uncertainty in both the connection setup time and the recovery time in case of failure. DHCP address allocation is handled by a dedicated server. However, even with redundant configurations, network issues can make the servers unreachable, which may cause unstable network operation.

Minimizing transmission delay

Transmission delay refers to the time it takes for a message to travel from the sender to the receiver. This quality parameter is one of critical importance in train control systems, and therefore strict limits apply. It is closely linked to the requirements of real-time operation and is one of the most important factors in the design of deterministic networks. Consequently, not all commonly used network protocols are suitable for application in such a demanding environment.

In wired communication systems, from the perspective of access to the transmission medium, protocols that allow shared medium access are not permitted. In such cases, a competition may arise between frames attempting to transmit simultaneously, which introduces random delays. This excludes the possibility of deterministic operation, as it cannot be guaranteed how long it will take for a given frame to pass through the network segment.

Based on this, it can be stated that in safety-critical networks, the use of shared access protocols (such as Carrier Sense Multiple Access with Collosion Detection or Avoidance - CSMA/CD, CSMA/CA) at Layer 2 is not allowed. Although these access methods are still technically available at the device level, they can—and should—be effectively avoided through appropriate network design, such as the use of point-to-point links, star topologies, and Layer 2 switched paths.

When using a radio channel, access to the shared medium cannot be avoided, so a different approach is required to achieve deterministic operation. A proven solution to this challenge is the use of a strictly time-division-based access method, known as Time Division Multiple Access (TDMA), which assigns predefined time slots to each communicating party. This enables collision-free and predictable data transmission and ensures that time-critical information is delivered reliably and within the required timeframe.

At the network level, the use of Network Address Translation (NAT) should be avoided, as address translation not only slows down and complicates the transmission of data packets but also hinders error detection and traffic tracing—issues that are particularly critical in safety-related systems. The use of VPN-based solutions should also be carefully considered, as they can significantly increase both connection setup time and transmission latency, especially when multi-level encryption or complex tunneling mechanisms are involved. (In non-closed networks, their use may be necessary to ensure adequate data security; in such cases, the increased latency must be taken into account.)

Increasing availability and reducing recovery time

To ensure high availability, a proven method is the redundant design of communication networks, such as implementing duplicated networks or using ring or dual-ring topologies. These solutions allow data transmission to continue via alternative paths in the event of a network failure.

In commonly used Ethernet networks, early solutions relied on various spanning tree-based protocols, which could handle redundant paths but typically required several seconds for recovery in failure scenarios. However, in safety-critical applications, the recovery time of redundancy-handling protocols must not exceed the millisecond range. Therefore, in Layer 2 switched networks, Spanning Tree Protocol (STP) [11], Rapid STP (RSTP) [12], and Multiple STP (MSTP) [13] are not suitable, as their recovery times are too long for these stringent requirements.

At the network level, when using MPLS technology, it is also possible to define redundant paths using the MPLS Fast Reroute (FRR) mechanism. FRR allows a preconfigured backup Label Switched Path (LSP) to be automatically activated if a failure occurs at any point on the primary route. This switchover typically happens within 50 milliseconds, making MPLS suitable even for latency-sensitive, safety-critical applications. One major advantage of MPLS is that routes can be preplanned, eliminating the need for route calculation during failure, thereby reducing network convergence time in case of a disruption.

While the recovery time provided by MPLS is sufficiently low for most applications, redundancy solutions implemented at lower protocol layers—such as PRP (Parallel Redundancy Protocol) and HSR (High-availability Seamless Redundancy) [14], along with certain vendor-specific implementations [15]—can achieve near-zero (0 milliseconds) recovery time. The key principle of these approaches is that Ethernet frames are sent in duplicate from the sender along diverse paths. On the receiver side, the first-arriving frame is processed, while the second is discarded.

One of the main advantages of these solutions is that they are fully transparent to higher protocol layers. This means that no changes are needed in the upper-layer communication systems when the underlying transport network is replaced by these redundancy mechanisms.

Acceleration of routing

The timing issues of route selection can be effectively mitigated by implementing the mechanism at lower protocol layers and using simplified algorithms. One of the most widely used solutions today is MPLS, which uses predefined label-switched paths to forward packets, thereby reducing decision-making time. In addition, MPLS enables the integration of Quality of Service (QoS) functions, such as priority-based traffic management, theoretically allowing both critical and non-critical traffic to be handled appropriately over the same physical network. When combined with Ethernet–IP-based infrastructure, this approach provides a fast and reliable route selection mechanism that meets the demands of modern railway communication systems.

CONCLUSIONS

The fast evolution of communication technologies has become a key factor in the context of railway communication. Modern railway communication systems are required to

meet strict performance requirements, including high reliability, safe operation, and deterministic network behavior, along with extremely fast recovery capabilities.

In analyzation of the communication links between train control systems, interlockings, and other trackside elements, I examined both current and potential technologies and protocols. Based on this, it can be concluded that while Ethernet–IP-based technologies are widely adopted, they cannot fully meet the specific requirements of the railway environment on their own. Their application must therefore be supplemented with additional mechanisms, furthermore, non-deterministic protocols must be entirely avoided in networks that carry safety-critical information.

Through a review of standards for safety-critical systems and communication networks, I identified common risk factors, with a particular focus on latency. The analysis shows that a detailed breakdown of latency components is essential to define precise requirements for the entities and protocols involved in communication. In addition, I have provided recommendations and best practices—based on both literature and personal experience—for mitigating the impact of these risks. The purpose of this analysis was to enhance the reliability of safety-critical communication systems and to support the planning and design of future railway networks.

SUMMARY

Digital technologies used in railway communication networks enable efficient and automated operation. However, the adoption of new technologies and protocols requires a different perspective on safety, reliability, and performance expectations. Ensuring deterministic network behavior, error-free and secure information delivery, and the integration of appropriate redundancy mechanisms are essential for both current and future railway systems. The reliability of railway communication systems depends on the choice of appropriate technologies and protocols, the careful design of network architecture, and the consistent application of relevant standards. The harmonized implementation of these factors ensures that the systems remain compliant with increasing traffic demands, expanding service requirements, and tightening safety regulations over the long term.

REFERENCES

[1] Z. Haig, B. Hajnal, L. Kovács and Z. Muha, “A kritikus információs infrastruktúrák meghatározásának módszertana,” Budapest, Hungary: ENO Avisory Kft., 2009. Accessed: Feb. 28, 2024. [Online]. Available: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

[2] P. Baczoni, “Vonali biztosítóberendezések,” Budapest, Hungary, MÁV Szolgáltató Központ Zrt. Baross Gábor Oktatási Központ, 2019.

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

[4] G. Tarnai, “Távvezérlés, KÖFE, KÖFI,” Budapest, Hungary, BME Közlekedésautomatikai Tanszék, 2012, Accessed: Jan. 7, 2025. [Online]. Available: https://kjit.bme.hu/images/Tantargyak/Bsc_(2016_elott)_targyak/Vasuti_ir._es_komm._rendsz._I/kfe_kfi_2012_februr_ltalnos_rsz.pdf

[5] *MÁV Feltétfüzet - Az ETCS L1 és L2 pályamenti alrendszerére vonatkozó alkalmazási követelményeire*, MÁV P-5600, 0.1.1. verzió, 2008.
[6] D. Kurhan, M. Kurhan and N. Hmelevska, "Development of the High-Speed Running of Trains in Ukraine for Integration with the International Railway Network," Acta Polytechnica Hungarica, vol. 1/3, pp. 207-218, March. 2022, DOI: 10.12700/APH.19.3.2022.3.16
[7] E. Kretschmer, "ETCS Hybrid Level 3," in *ETCS in Deutschland*, Hamburg, Germany, Eurailpress, 2020, pp. 351–360.
[8] HolySys. "ERTMS/ETCS LEVEL 1/2 Solution." HolySys, Accessed: 6/23/2024 Nov. 11. 2024. [Online.] Available: https://www.hollysys.com/industries/industries/transportation/main-line-railway/railway/22
[9] *Functional safety of electrical / electronic / programmable electronic safety-related systems, International Electrotechnical Commission*, IEC 61508, 2010.
[10] *Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems*, MSZ EN 50159:2011, 2011.
[11] *Local Area Network MAC (Media Access Control) Bridges*, IEEE 802.1D, 1998.
[12] *Local and metropolitan area networks—Common specifications, Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration*, IEEE 802.1w, 2001.
[13] *Local and Metropolitan Area Networks - Amendment to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees*, IEEE 802.1s, 2002.
[14] M. Ostertag, "Seamless Redundancy with PRP and HSR", Accessed: Feb. 1. 2024. [Online.] Available: https://www.zhaw.ch/en/engineering/institutes-centres/ines/communication-network-engineering/seamless-redundancy-with-prp-and-hsr
[15] Moxa Inc., "Redundancy Technologies Application Note", Moxa Inc., Accessed: Jan. 17. 2025. [Online.] Available: https://www.moxa.com/en/literature-library/redundancy-technologies-application-note