Addressing Synchronization and Latency Challenges in Railway Communication Networks

Gergely Kún and Tibor Wührl

Obuda University, Kandó Kálmán Faculty of Electrical Engineering,
Institute of Electronics and Communication Systems,
Department of Telecommunications and Info-communications
Bécsi út 96/B, 1034 Budapest, Hungary

Institute for Transport Sciences
Than Károly utca 3-5., 1119 Budapest, Hungary

kun.gergely@kvk.uni-obuda.hu
wuhrl.tibor@kvk.uni-obuda.hu

Abstract: *The rapid advancement of information and communication technologies has a deep impact on transportation support systems, including the safety-critical networks of railway operations. The digital transition encompasses far more than the deployment of new technologies; it demands a fundamental shift in design principles, deployment strategies and operational practices. Traditionally, railway systems have relied on long-lifecycle, highly reliable, domain-specific equipment. Today, these are increasingly being replaced by rapidly evolving digital technologies originally developed for even commercial markets. These changes introduce significant challenges in ensuring the required levels of reliability, availability, and expected lifecycle performance. Due to the specific requirements of railway applications, many widely used communication technologies are either unsuitable or only partially applicable. This article highlights the key reliability considerations and conditions that determine how such technologies can be adapted to the railway environment. Additionally, it is essential to systematically analyze the technical hazards and risks affecting the networks, as this is the only way to identify solutions that meet strict performance requirements. While relevant standards address these risk factors, they are not comprehensive. This paper aims to examine and categorize the factors influencing data transmission latency within this context. This provides a solid foundation for determining which subsystem characteristics require attention during system integration, to ensure that end-to-end communication parameters meet the specified requirements.*

Keywords: railway, telecommunication, safety-critical, digital, reliability

1 Introduction

Modern railway interlocking systems and train control subsystems now primarily operate using digital information and communication technology infrastructures. Ensuring the operational safety and determinism of such high-reliability industrial networks is one of the major engineering challenges we face today.

The automation of railway operations and the enhancement of safety are facilitated by the development of Automatic Train Control (ATC) systems. These computer-based, integrated control and monitoring systems enable coordinated management of overall traffic including trackside elements and rolling stock. Various implementations of ATC are deployed worldwide, employing diverse technological solutions at different levels to support safe and efficient railway operations [1].

Modern railway infrastructures must accommodate increasing passenger and freight transport demands, which often necessitates expanding the capacity of existing networks, frequently through advancements in information and communication technology. Consequently, contemporary automated signaling and traffic management systems require highly reliable, high-capacity, and stable communication networks that enable real-time data exchange between trackside elements and rolling stock.

Alongside the evolution of communication systems, Ethernet and Internet Protocol (IP) based packet-switched data transmission has been introduced into railway networks, offering numerous advantages in terms of flexible configuration and higher throughput. However, this architecture is fundamentally asynchronous, requiring supplementary mechanisms to achieve the synchronization abilities that were natively present in earlier, classical Time Division Multiplexing-based (TDM) systems. This article reviews potential solutions addressing synchronization and timing challenges.

2 Background and Related Work

Recent and ongoing developments in information and communication technologies have accelerated our lives. Advances in modern digital devices, as well as in wired—primarily optical—and wireless transmission methods, now enable the transport of ever-increasing volumes of information every second. A few decades ago, generating and managing such amounts of data was unimaginable. Today, due to the continuous growth in technological capabilities and capacities, the increase in data volume has become a self-reinforcing process.

Digitalization of railway safety systems has similarly advanced. The initially employed, mechanical interlocking solutions, were followed by electrical and then

electronic circuit-based implementations. Today, digital communication technologies are increasingly used for interactions among railway devices and systems in a networked environment. This digital transition does not merely mean the introduction of new technologies; it also requires a fundamental shift in principles of design, deployment, and operation approaches for all safety-critical systems, including railway applications. Proper adaptation to this new paradigm is particularly important in railway networks, as rapidly evolving digital technologies—often originally developed for commercial purposes—are replacing traditionally durable, high-reliability systems. This shift introduces significant technical and system-level challenges regarding the maintenance of appropriate reliability and availability.

Advancement of technology in systems supporting railway operations is ongoing. New technologies are expected to improve safety, which remains the top priority in all types of transport, including railways. In railway systems, safety-critical functions are implemented by interlocking systems [2], which, even for relatively simple functions, consist of networks of computers or embedded controller-based devices.

Rail infrastructure operators are generally organized on a national basis. Since the railway network covers the entire area of a country, the supporting communication networks must also provide nationwide coverage, or at least cover the operator's service area, ensuring reliable communication services.

Railway communication systems can be divided into two main categories: on-board and trackside systems [3]. This article focuses on the design and implementation of trackside communication systems; however, considering the fundamental importance of the interaction between the two categories, the interfaces to on-board equipment and their key characteristics are also presented in the necessary detail.

2.1 Railway Regulations and Standards

2.1.1 Standards

Industrial equipment must comply with strict safety requirements defined by industry-specific standards. The international standard IEC 61508 [4] establishes the requirements for the entire lifecycle of electrical, electronic, and programmable electronic safety systems. It adopts a risk-based approach and provides an industry-independent framework for achieving functional safety, mainly in applications where human life, health or environmental protection is at stake.

For railway applications, specific adaptations of the above presented base standard, provide guidance. The standards reviewed below enable the identification and management of risks within railway systems. They ensure that operators can

achieve the required level of safety while prescribing standardized processes and documentation requirements, that cover the entire system lifecycle.

The MSZ EN 50126 (IEC 62278) [5] series aims to ensure the reliability, availability, maintainability, and safety of railway systems, detailing both the general principles of the processes and their practical implementation throughout system development and approval. MSZ EN 50128 (IEC 62279) [6] defines requirements for the software of railway control and safety systems, ensuring the proper design, documentation, and maintenance of communication, data processing, and safety devices. MSZ EN 50129 (IEC 62425) [7] specifies the safety certification and documentation requirements for safety-critical electronic systems.

The MSZ EN 50159 [8] standard for railway communication networks ensures that systems comply with both IT and safety requirements, whether operating over closed or open networks, and manage traffic between safety-critical and non-safety-critical devices. This standard includes fault detection, recovery, redundancy, and data security, as well as the necessary documentation and traceability requirements.

The industrial cybersecurity requirements for railway infrastructure and rolling stock are addressed by the CLC/TS 50701:2024 [9] standard, which adapts the principles of the IEC 62443 series. This standard defines the principles for access control, encryption, network segmentation, and intrusion detection, as well as the security levels of railway subsystems. The EN 63452 [10] standard, currently in draft form, is intended to replace the technical specifications of EN 50701, expanding its scope and integrating Reliability, Availability, Maintainability, and Safety (RAMS) considerations, thereby providing a comprehensive framework for the identification, management, and monitoring of risks in railway systems in the near future.

2.1.2 European Regulations

In Europe, the Technical Specifications for Interoperability (TSI) serve to standardize the technical requirements of railway systems. These specifications form a regulatory framework supporting the harmonization and interoperability of the EU railway network: EU Regulation 2016/797 provides the general framework for interoperability, while EU Regulation 2019/776 specifies the technical requirements for individual subsystems.

The European Union Agency for Railways (ERA) coordinates the practical application, interpretation, and technical support of the TSIs for Railways, which issues standards, specifications, and technical guidance. This includes ‘subset’ documents, detailing the requirements and technical specifications necessary for the implementation and operation of European Automatic Train Control systems.

2.1.3 National Regulations

In every country, in addition to international rules and standards, national regulations and decrees govern all aspects of railway operation. Efforts have been ongoing at the European level for years to harmonize these rules and reduce differences between national requirements, primarily to improve interoperability.

In Hungary, the legal framework for the National Railway Technical Specifications was introduced in 2020. From the end of 2024, these rules set out national requirements to ensure that railway infrastructure, vehicles, and systems meet European interoperability standards, while supporting safe and efficient operations. They also cover national-specific requirements in areas where EU regulations allow national regulations.

2.1.4 Regulations of Operators

Hungarian State Railways (Magyar Államvasutak, MÁV) and Gyor-Sopron-Ebenfurt Railway (Győr-Sopron-Ebenfurti Vasút, GySEV) are the main operators of railway infrastructure in Hungary.

At the railway infrastructure operator level, specialized manuals (local standards) define the specific requirements of each organization. In the cases of MÁV and GySEV, these are referred to as Constraint Manuals. These manuals are crucial for maintaining railway safety and efficient operations, as they set explicit rules for train movements and ensure that personnel follow proper procedures.

2.2 Railway Systems and Communication

This section provides an overview of the most important traditional components of current railway supervision systems.

2.2.1 Railway Interlocking Systems

The primary goal of developing and deploying railway interlocking systems has always been to enhance the safety and efficiency of railway operations. Today, mostly electronic and computer-based interlocking is used on high-traffic lines. A Computer-Based Interlocking (CBI) system consists of a central server implementing the interlocking functions, the trackside devices, and the network connecting them. The CBI server operates as the core of the interlocking system for a given area. CBI is the key component for ensuring safe train operations.

The CBI collects and evaluates information from the trackside interlocking devices, enabling interventions that ensure train operations comply with prescribed safety requirements. A railway operator typically has multiple interlocking centers, each responsible for a specific area. The servers of these interlocking systems are

interconnected to facilitate information exchange, but their primary role remains to maintain the safety and continuous operation of their respective regions [1][3].

2.2.2 Centralized Traffic Control

Centralized Traffic Control (CTC) enables the remote monitoring and management of rolling stock movements from a central control location. The CTC system directs train operations and shunting activities within its supervised area, providing central control through the interlocking systems. Its primary objective is to enhance the efficiency and flexibility of railway operations. The CTC system consists of a central traffic control center, typically connected to station interlocking. Traffic controllers monitor train movements via computerized interface and can modify operations by adjusting signals and switches through the interlocking systems.

Data transmission can be implemented over various physical media and technologies. Currently, the transition to modern IP-based systems is predominant, which is also the primary focus of this research. The Centralized Traffic Control system is built on decentralized and autonomous principles, using distributed computing and control. This allows the system to detect problems that occur during train operations and shunting. It can identify these issues, and perform the necessary corrections to keep operations on schedule. Consequently, it ensures efficient and coordinated control of train movements and shunting processes.

2.2.3 European Railway Traffic Management System

The European Railway Traffic Management System (ERTMS) aims to implement a unified cross-border train supervision and control framework in all aspects. ERTMS consists of three main components:

- First is the European Traffic Management Layer (ETML), which addresses traffic management and control functions.
- Second is the European Integrated Railway Radio Enhanced Network (EIRENE), which provides radio communication between onboard and trackside equipment. Its wireless communication link is supplied by the Global System for Mobile Communications – Railway (GSM-R) network, which is one of the most important subsystem of the whole system. Despite the GSM-R reliability and maturity, it is now considered outdated, and it will eventually be replaced by the Future Railway Mobile Communication System (FRMCS), which is based on 5G mobile communications [3][11].
- Third is the European Train Control System (ETCS), which will be discussed in the following section.

2.2.4 European Train Control System

The supervision and protection of train movements are achieved through an integrated train control framework composed of multiple system components.

Within the European railway domain, the European Train Control System provides this functionality, which is an Automatic Train Protection system under ongoing deployment. ETCS ensures safe train operation by continuously monitoring Movement Authorities (MA) and train dynamics across different traffic situations.

The deployment of the ETCS system is taking place gradually, and it operates in parallel with existing national systems everywhere. ETCS has three levels based on its offered services. At present, Level 2 is the one most deployed and used. Across Europe – and even within individual countries – some railway lines are already equipped with one of the ETCS levels, while others are not. [11][12] The following paragraphs give an overview of the main characteristics of each level.

The ETCS Level 1 (L1) system is based on conventional interlocking systems and only provides non-continuous train control. As such, it is outside the scope of this study.

ETCS Level 2 (L2) still relies on conventional railway interlocking systems, meaning train detection is performed by track circuits or axle counters. These wayside detection elements determine the location of trains and the occupancy status of track sections, forming the basis for issuing Movement Authorities. ETCS Level 2 introduces a significant innovation to the train supervision architecture by delegating the central decision-making function to the Radio Block Centre (RBC).

Figure 1 shows a typical ETCS Level 2 architecture and the connections between the RBC, interlocking system, trackside elements, the GSM-R network, and the train.

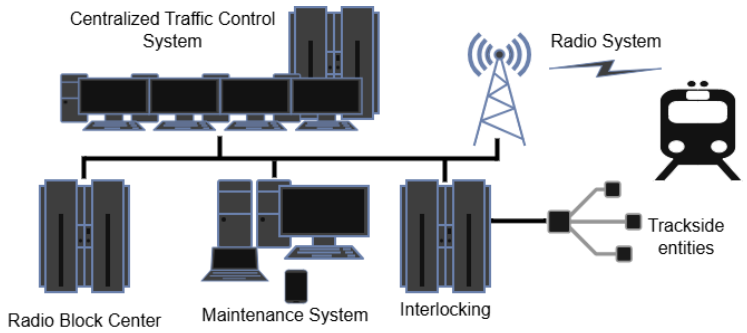

Figure 1
ETCS Level 2 architecture

The Radio Block Centre (RBC), continuously monitors train movements within its designated area, manages Movement Authorities, and determines the maximum speeds and section limits for each train. Its tasks include processing information received from the interlocking, tracking state changes, and generating the necessary

control and supervision data for the trains. As such, the RBC plays a key role in maintaining efficient railway operations and enabling automated train control.

The two-way communication between the RBC and the trains is provided by the GSM-R network, which enables high-reliability wireless data transmission for railway operations. Through the GSM-R network, trains receive operational instructions issued by the RBC. The locomotives also transmit their status data over the same channel, which is essential for the RBC to maintain continuous supervision. The latency and reliability of this communication channel are critical, and any disruption can directly affect train monitoring and control.

One of the most important data provided by the locomotives is the train position. In the ETCS Level 2 system, position determination primarily relies on balises that are fixed trackside devices. The trackside balises serve as reference points for the trains. A balise is queried by the locomotive's balise interface as it passes over, providing precise positioning information to the onboard system. Using the data read from the balises, the train's absolute position can be determined with high accuracy and reported to the Radio Block Centre.

In addition to balise-based positioning, the locomotive is equipped with several onboard sensor systems that operate continuously and provide relative positioning. These include the odometer, accelerometers, gyroscopes, and often GPS receivers also supply supplementary positional and motion-dynamic information. These data ensure continuous position tracking between the reference points defined by the balises, which the onboard ETCS unit—the European Vital Computer (EVC)—compiles and transmits to the Radio Block Centre.

ETCS Level 3 (L3) represents the highest level of service currently defined. This system level enables full radio-based train control, ranging from continuous speed supervision to a theoretically feasible moving-block operation, replacing fixed-block solutions. At this level, it is even possible to eliminate traditional signals entirely, potentially leaving the driver without operational tasks. A new task for onboard systems is the train integrity monitoring, introducing higher requirements for onboard communications, as the wagons connected to the locomotive also become part of the onboard communication network and maintain continuous contact to the integrity-monitoring system in the locomotive. This reduces the number of trackside devices, offering significant maintenance cost savings. Currently, this level has not yet been deployed in operational service anywhere. The main challenges at this level are the establishment of reliable train-integrity infrastructure and the development of a track-to-train communication network with sufficient reliability to allow the removal of trackside equipment and human supervision without compromising safety. Pilot projects addressing these issues are ongoing across Europe. [13]

2.2.5 ETCS Level 2 Communication in a Typical Operational Scenario

In the following an operational scenario is discussed, in which a train travels from an origin station to a destination while its movement is continuously supervised by the Radio Block Centre (RBC). Based on inputs from the interlocking system, the RBC sets the route, including point (switch) positions, signal aspects, and, where required, level crossing closures. At departure, the train receives a Movement Authority defining the permitted route up to the end of the next section.

After departure, the train transmits its position at predefined intervals to the RBC via the GSM-R network. These reports are derived from balise data and onboard sensors. Under normal operation, updates are received every few seconds, enabling the RBC to continuously revise the Movement Authority and ensure safe progression along the track.

In case of an exceptional event—such as an obstacle on the track or an unexpected slowdown of a preceding train preventing the release of the next section—the RBC performs immediate intervention. A modified or shortened Movement Authority is issued, possibly including commands for speed reduction or stop. These messages are highly time-critical, and communication delays directly affect system response.

From a timing perspective, the process includes position report generation, network transmission delay, RBC processing, and the delivery and onboard processing of the updated Movement Authority. The total end-to-end latency determines the system's responsiveness. Increased latency may lead to more conservative control decisions, such as reduced speed profiles or shorter movement authorities, negatively impacting capacity and operational efficiency while maintaining safety.

2.2.6 Communication Network Requirements

In railway applications, multiple isolated systems often operate in parallel, collaborating to accomplish the full range of operational tasks. The reason for this separation is that the criticality of individual functions and their corresponding requirements differ, including their safety and reliability levels. Ensuring the reliable operation of the previously described systems requires high-reliability, deterministic communication networks capable of transmitting time-critical messages in order, with guaranteed latency, and with high availability.

Deterministic communication networks are infrastructures that ensure predictable transmission time, correct packet delivery, and preserved data order, even when handling a large volume of non-time-critical traffic. In such systems, the outcome and timing of events are fully predictable under given initial conditions and inputs. This property is particularly important for safety-critical applications, where response times must be strictly defined in advance.

3 Synchronization and Latency Challenges on Communication Links

Currently, there is a clear trend toward newly deployed communication networks being increasingly IP-based and utilizing some form of Ethernet technology. In general, IP-based Ethernet networks offer higher data transfer capacity, cost efficiency, and the use of standardized, widely available devices. This shift is observed not only in office and home environments, but also in industrial applications. Consequently, newly implemented railway communication networks are also moving toward IP-based architectures; however, alongside these advantages, a significant number of technical and safety challenges arise.

3.1 Main Characteristics of Packet-Switched Networks

A key characteristic of IP packet-switched networks is their best-effort delivery, meaning there is no guarantee built-in that a data packet will reach its destination, remain intact, or experience a predictable delay. Network devices and protocols do their best to deliver packets, but if resources along the path are limited—such as a link with low bandwidth or insufficient buffer capacity—packets may be dropped. Even when packets are successfully delivered, the exact transmission delay cannot be determined in advance, as it depends on varying processing times. In complex network topologies, the correct order of segmented packets is also not assured. Overall, packet-switched networks provide asynchronous transmission and exhibit non-deterministic behavior.

3.2 Key Features of Traditional Synchronous Digital Networks

The Synchronous Digital Hierarchy (SDH) is a fundamental, traditionally used transmission technology in telecommunications networks, primarily developed for systems requiring high reliability and deterministic data transfer. SDH employs hierarchical Time Division Multiplexing, where data streams are transmitted in a synchronized structure based on a common clock. This strict synchronization enables predictable delay, minimal jitter, and extremely low error rates. Additionally, SDH provides high availability through stable, redundant network connections and fast recovery capabilities. For these reasons, SDH has long been considered a core technology for communication networks in critical infrastructures, such as railway, energy, and utility systems.

Notably, such networks are still in operation in applications where expanding services and capacity was never a priority, but stable, deterministic performance remained essential. Today, IP-based and packet-switched solutions are gradually taking over these roles, but the reliability and timing characteristics of SDH

continue to serve as a benchmark and are often used as a reference in the design of modern communication networks.

3.3 Latency Issues

In high-speed rail operations, the latency and response time of communication networks have become critical factors. For safe and efficient operation, it is essential that real-time trackside data, speed information, and Movement Authorities reach onboard systems as quickly as possible. Since a high-speed train can travel tens of meters every second, even a few hundred milliseconds of network delay can create a critical situation. Late delivery of necessary data may lead to false emergency stops or, in extreme cases, pose safety risks and hazards. Therefore, managing latency effectively and keeping it sufficiently low is not only a performance requirement, but also a safety-critical necessity in modern railway communication systems.

A critical performance parameter of network communication is the end-to-end delay, which results from a combination of several contributing factors. One of the dominant components is the queuing delay occurring at network nodes. Routers and switches use temporary buffer memory (queues) to store incoming packets until they can be forwarded to the outgoing link. While buffering is essential for absorbing traffic fluctuations, excessive network load may lead to significant delays. Under congested conditions, buffer overflow can occur, resulting in packet loss. The handling of lost packets at higher protocol layers may further increase overall delay, for example when retransmission is required at the receiver side.

The transmission delay of a link refers to the time required for a data packet to travel from one endpoint of a network connection to the other. This delay is primarily determined by the characteristics of the transmission medium and the physical distance between the communicating nodes.

Connection setup time, also referred to as connection establishment delay, is the time required to establish a communication channel between endpoints. It includes signaling exchanges, authentication procedures, and the allocation of required network resources. Although this delay does not affect already established connections, it becomes relevant for time-critical services in case of link failure and subsequent reconnection during ongoing communication.

Additional contributors to end-to-end delay include routing and traffic management mechanisms such as rate limiting, policing, and traffic shaping. While these functions are necessary to ensure Quality of Service and overall network stability, they introduce additional processing overhead, thereby increasing the total transmission time.

Due to the stack architecture of network protocols, processing delay increases significantly as more complex packet handling is performed at higher protocol

layers, such as encryption or deep packet inspection. For this reason, transmission and traffic management functions are best implemented at lower protocol layers. The IEEE 802.1 standard family and the widely used technology Multiprotocol Label Switching (MPLS) follows this principle, enabling faster packet processing and forwarding through functions implemented at lower layers.

Delays due to mobility, for example in case of a handover, occur when a locomotive's communication switches from one base station to another. This process partly involves establishing a new connection, which—if poorly implemented or under exceptional conditions—can lead to temporary packet loss or increased latency. Careful design of this process is crucial in time-critical systems.

In the event of a link or network failure, the recovery time is critical. The recovery time is the period during which the network detects the fault, switches to a backup path or device, and restores normal communication. In safety-critical systems, this duration directly affects service reliability, and effective redundancy management is required to minimize both the likelihood of occurrence and the time needed to recover.

3.4 Necessity of Network Timing and Synchronization

As discussed earlier, packet-switched networks inherently operate in an asynchronous manner. When a packet arrives at a network node, it is temporarily stored in a buffer and forwarded according to the device's scheduling process. In high-speed networks, memory management becomes a critical factor: interfaces capable of handling large data rates can receive bursts of traffic that must be processed and stored in the device's internal memory. Reading from and writing to these buffers consumes significant resources from the embedded controllers. In complex networks, data flow can be highly uneven between unsynchronized devices and their interfaces, which may necessitate larger buffers. Without proper timing and synchronization, these temporary traffic spikes can cause memory overflows, leading to packet loss and impacting the deterministic behavior required for critical network applications.

Managing time synchronization is a critical issue in Ethernet-IP networks, because although the network operates asynchronously by nature, deterministic behavior depends on precise timing. If synchronization errors occur, devices no longer share a common notion of time, and their internal clocks drift apart, which can cause time-critical tasks—such as priority handling—to fail. These synchronization deviations can accumulate gradually, as local clocks slowly drift from the reference time, leading to incorrect timestamps, increased jitter or other timing inconsistencies (time offsets), that directly affect the reliability and predictability of network communication.

IP-based networks are inherently asynchronous, so maintaining accurate timing and synchronization requires additional mechanisms. Nowadays, this is primarily achieved using the Precision Time Protocol (PTP) and increasingly through Time-Sensitive Networking (TSN) solutions, which can provide deterministic, time-based operation even over standard Ethernet infrastructure. TSN technology is already being deployed and tested in various industrial and transportation sectors, including railways. TSN is a set of standards (the IEEE 802.1 family) that offer different capabilities, so that networks can be configured to meet the required performance and functionality.

4 Solutions for Timing Issues

4.1 Implementing Deterministic Networks

Nowadays, the earlier widespread synchronous time-division networks are gradually being replaced by packet-switched, IP-based infrastructures across nearly all communication domains. The main reason for this shift is that Ethernet and IP technologies offer several advantages over conventional transmission systems, including high configurability, cost-effectiveness, and continuously increasing data rates and bandwidth, which enables support for modern high-traffic applications.

TDM-based systems previously played a fundamental role in telecommunications and railway communications due to their deterministic operation and precise timing. A current challenge is to make Ethernet-IP networks, which are naturally asynchronous, operate as predictably as time-division systems. This enables packet-switched networks to offer additional benefits—such as Quality of Service (QoS), flexible traffic management, and higher efficiency—even in critical infrastructure communication networks. To support these features, Ethernet-IP networks need to be equipped with essential synchronization capabilities, which are not inherent to packet-switched systems but were standard in traditional time-division networks.

4.2 Realization of Synchronization

To minimize latency and ensure deterministic data transmission, modern railway packet-switched communication networks employ multi-layer timing and traffic management mechanisms. Using the Precision Time Protocol (PTP) [14], network elements can be synchronized to a common time base, enabling precise scheduling and predictable processing of data. The adaptation of synchronization to meet the requirements of deterministic network operation is defined in the IEEE 802.1AS standard [15].

PTP follows a Master–Slave architecture, where the reference is provided by the Grandmaster (Root Timing Reference). A fundamental requirement for synchronization is that each device's clock can be adjusted based on the timestamps in the synchronization messages and the timestamps recorded when the messages are received. Synchronization primarily ensures correct clock frequency, but in certain cases, phase correction can also be achieved. An important condition for PTP to work correctly, is that the transmission delay between two devices should be the same in both directions, from sender to receiver and back.

The synchronization process is illustrated in Figure 2. The vertical time axis shows the progression of time from top to bottom. The left axis represents the clock of the "master" device that provides synchronization, while the right axis shows the clock of the "slave" device to be synchronized. The goal of synchronization is to align the slave's clock with the master's. To do this, the clock offset—the difference between the two clocks—must be determined.

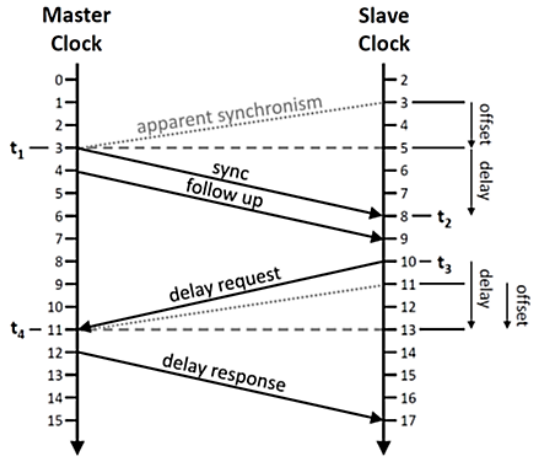

Figure 2
PTP synchronization process [14]

The process begins with the master sending a *sync* message, which leaves the interface at time t_1 according to the master clock. This t_1 timestamp must be included in the *sync* message itself. This step is not trivial, because the message is first assembled in the interface's memory, where the timestamp is inserted, and only then can the *sync* message be transmitted. Any potential inaccuracy in the *sync* message can be corrected using a *follow-up* message. The *follow-up* message can carry a much more precise t_1 timestamp, reflecting the actual moment the *sync* message was transmitted.

The *sync* message arrives at the slave at time t_2, according to the slave clock, while the t_1 timestamp, according to the master clock, can be read from the *sync follow-up* message. Shortly after, at time t_3 (slave clock), the slave sends a *delay_request*

message to the master, which is received at time t_4 (master clock). The t_3 timestamp is recorded by the slave but is not relevant to the master. However, the t_4 timestamp recorded by the master is important for the slave, so the master includes it in the *delay_response* message sent back to the slave. At the end of this synchronization process, the slave has the t_1, t_2, t_3, and t_4 values available. Using these timestamps, the transmission delay can be calculated with equation (1).

$$delay = \frac{(t_2 - t_1) + (t_4 - t_3)}{2} \quad (1)$$

In railway applications, train position reports and Movement Authorities issued by the RBC always include precise timestamps. These safety-critical messages can only be correctly interpreted if every system element relies on a common, high-precision time reference. The Precision Time Protocol (IEEE 1588) enables sub-microsecond synchronization in asynchronous IP-based networks regardless of the underlying physical transmission medium.

The standardized use of PTP in railway environments is currently in the testing phase [55], as interoperable deployment still requires further experiments, validation procedures, and reliability assessments. In the future, PTP is expected to form an elementary element of deterministic communication for ETCS and other railway systems, working in conjunction with Time-Sensitive Networking technologies.

In 5G-based FRMCS systems, synchronization and precise timing are important for the correct operation of the 5G radio interface. [16-18].

4.3 Traffic Policy and Shaping

In networks, the key tools for achieving deterministic and reliable data transmission are Quality of Service and Traffic Class (TC) mechanisms. These mechanisms allow for prioritizing data packets within the network, ensuring that safety-critical messages—such as Movement Authorities or precise position information—are handled with higher priority, enabling them to reach their destination more quickly and reliably.

The network synchronization discussed earlier also plays a critical role in this process. Providing a unified, precise time reference allows for the temporal separation of critical and non-critical data flows. Based on this common time reference, network devices can implement prioritized, scheduled, or time-gated traffic management. This is especially important in critical infrastructures—such as railway systems—where delays in position data or movement authority information directly affect operational safety and efficiency. In addition, delay and jitter (delay variation) can be further reduced through buffer optimization and traffic-shaping techniques, which help prevent network congestion and packet loss.

Time-Sensitive Networking technologies are increasingly being adopted in safety-critical industrial and railway infrastructures, enabling deterministic scheduling and time-based traffic management at the Ethernet level. Such networks can guarantee a maximum latency for critical messages, even in the presence of high volumes of non-critical background traffic.

Using a Time-Aware Shaper enables time-based scheduling and traffic control. The method works by opening and closing time windows (time gates) for transferring different types of traffic. This eliminates contention between data flows, giving dedicated, collision-free time slots for critical data transmission. This approach ensures deterministic data delivery and predictable latency [19]. Additional techniques exist to increase network flexibility and the number of deterministically managed data flows, which implement advanced queue scheduling and resource allocation [20][21]. The relevant standards are widely applied in industrial Ethernet networks, while railway implementations are currently in the testing phase.

4.4 Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) [22][23] is widely used at the backbone network level in scenarios where high availability, low latency, and traffic prioritization are critical. In the OSI model, MPLS operates above the data link layer and below the network layer, effectively acting as an intermediate ‘underlay’ layer. MPLS allows IP packets to be routed based on pre-assigned labels, enabling faster forwarding compared to the traditional, and relatively slow, IP routing methods.

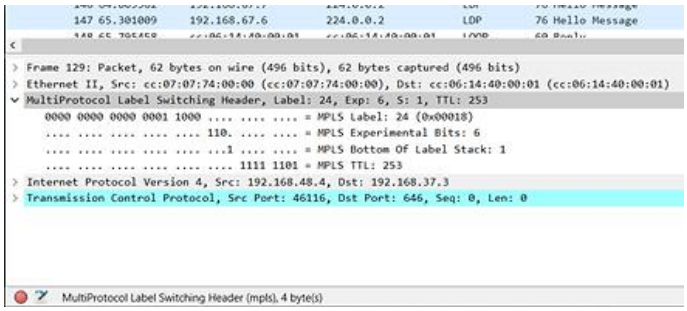

Figure 3
MPLS label insertion viewed in WireShark

Figure 3 shows the content of a packet captured in an MPLS network using the Wireshark [24] program. From an encapsulation perspective, the MPLS header is located between the data (Ethernet) and network (IP) layers. The MPLS header itself is relatively small, with the first field representing the MPLS label, which is used to quickly forward the packet to the next hop in the MPLS core network.

The use of MPLS is highly advantageous in optical backbone networks, where redundant topologies, fast rerouting of paths, and priority handling based on traffic classes play a key role in ensuring reliable, efficient, and quickly recoverable network operation. This technology is therefore not only widely adopted in telecommunication environments but is also increasingly applied in railway communication systems, including the network infrastructures supporting ETCS Level 2 and Level 3.

Railway applications—such as the RBC-to-onboard connection or real-time diagnostic data transfer—place different demands on the carrying network. MPLS allows these services to be logically separated over the same physical infrastructure while simultaneously supporting services with varying latency and availability requirements.

Furthermore, the combination of MPLS with network synchronization technologies such as PTP and TSN provides a technological bridge between traditional IP-based networks and deterministic networking architectures.

Although not strictly related to timing, it is important to highlight that MPLS networks can also define redundant paths by features such as “MPLS Fast Reroute”. The advantage of this approach is that it operates transparently to higher network layers, so no changes are needed in the communication architecture when the core network is upgraded. This allows the entire communication system to achieve significantly higher availability and reliability.

4.5 Reducing the Occurrence of Overload and Congestion

Network delay often arises from congestion at nodes, which can be triggered by malfunctioning or even intentionally generated traffic. In such cases, router buffer capacity can quickly become overloaded, causing significant delays in the transmission of normal data flows. The low-level ingress policing and resource access control defined by IEEE 802.1Qci addresses this issue. The node inspects and filters out inappropriate or congestion-causing packets before they reach the processing stage, thereby reducing delays caused by queuing. This mechanism also enables traffic isolation between different subsystems and prioritization of critical data flows, which is particularly important in safety-critical applications [25].

Another approach to reducing network delays is the early detection and handling of transmission errors, preferably at lower protocol layers. The Frame Replication and Elimination for Reliability (FRER) mechanism—part of IEEE 802.1CB—implements redundant frame transmission, allowing the receiver to quickly detect and eliminate transmission errors and packet loss by comparing duplicate frames.

This method avoids delays associated with higher protocol layers, since corrupted or lost frames are immediately discarded, while only valid frames are forwarded without retransmission [26].

4.6 Transition from Legacy Requirements to Deterministic Networking

The current phase of railway communication system evolution is characterized by hybrid network architectures, where legacy dedicated communication systems coexist with emerging IP-based infrastructures. This transitional configuration is driven by the gradual migration from physically separated, function-specific communication links to unified, multi-service packet-switched networks.

While IP-based technologies enable higher flexibility and integration of multiple services over shared infrastructure, they do not inherently satisfy the strict deterministic and safety-related requirements of railway applications. As a result, hybrid deployment models are currently required, in which safety-critical functions are still supported by dedicated communication paths, while less critical services are migrated to shared IP-based networks. This ensures compliance with existing safety standards while allowing incremental adoption of new technologies.

Current period can be considered transitional, where traditional requirement frameworks and emerging technologies coexist. Until newer, more efficient solutions are fully validated and widely deployed, safety-critical functions must continue to rely on separated, dedicated communication systems to ensure compliance with existing standards.

5 Conclusions and Future Work

This paper examines the impact of digitalization on critical communication networks, especially on railway systems, highlighting the resulting requirements, challenges, and engineering considerations. It begins with an overview of relevant standards and regulations, followed by a summary of the key components and characteristics of contemporary railway communication systems.

The European Train Control System receives special emphasis, focusing on the operation of ETCS Level 2, its elements, and the requirements of the underlying network architecture. Overall, modern railway communication requires deterministic network operation to ensure that time-critical data reaches its destination predictably and reliably.

While earlier synchronous networks exhibited deterministic behavior by design, Ethernet/IP technologies require additional protocols and mechanisms to realize comparable determinism. The inherently asynchronous nature of packet-switched networks creates challenges for achieving deterministic operation.

From the perspective of deterministic operation, delay stands out as a critical risk factor. The paper examined in detail the components of the end-to-end delay, highlighting the factors that influence its overall value, as well as the most

standardized methods and procedures available to minimize it. The analysis addressed the latency contributions of connection setup, routing, packet processing, error handling, and network congestion. Device synchronization was also highlighted as a key factor, closely tied to efficient, predictable traffic management and packet handling.

While many of the solutions discussed are already well-established in industrial contexts, their railway-specific deployment largely remains a challenge for the near future. Timing and synchronization technologies are essential for achieving deterministic, safe, and reliable operation in modern railway communication systems. Their full deployment is still pending, highlighting directions for further research. The discussed network developments pave the way for next-generation railway control systems built on fully deterministic, robust and secure communication platforms. These advances support higher train speeds, reduced infrastructure requirements, and the gradual introduction of fully autonomous train operation.

Acknowledgement

We thank Obuda University and the Institute for Transport Sciences for supporting our research and providing the opportunity to publish this paper.

References

[1] G. Theeg, et al., Railway Signalling and Interlocking, TZ-Verlag & Print GmbH, Hamburg, 2019, ISBN 978-3-96245-169-1

[2] G. Szabó, Challenges of Achieving Functional Safety in Electronic Systems, in Electrotechnics 115/5-6, pp. 44-48. 2022.

[3] L. Schnieder, European Train Control System (ETCS), Springer Vieweg, Berlin, 2024, ISBN 978-3-662-68969-1

[4] IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, Edition 2.0, April 2010

[5] MSZ EN 50126-1,2:2018, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[6] MSZ EN 50128:2011, Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems

[7] MSZ EN 50129:2019, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling

[8] MSZ EN 50159:2011, Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems

[9] CLC/TS 50701:2024, Railway applications - Cybersecurity

[10] EN 63452, Railway applications - Cybersecurity

[11] MAV Technical Requirements Specification for ETCS Level 1 and Level 2 Trackside Subsystems, Constraint Manuals, Version 0.1.1, MAV P-5600, 2008.

[12] 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. https://doi.org/10.12700/APH.19.3.2022.3.16

[13] E. Kretschmer, ETCS Hybrid Level 3. In: J. Trinckauf, et al., ETCS in Deutschland, 1. Auflage. Eurailpress, Hamburg 2020, ISBN 978-3-96245-219-3, pp. 351–360.

[14] IEEE 1588:2019, Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems https://doi.org/10.1109/IEEESTD.2020.9120376

[15] IEEE 802.1AS:2020, Timing and Synchronization for Time-Sensitive Applications, 2020. https://doi.org/10.1109/IEEESTD.2020.9121845

[16] K. Mészáros, et al., RF research at Kando, focusing on 5G applications, in XXXVIII. Kando Conference 2022 – Abstract proceedings, 2022, pp. 53–53.

[17] R. Kovács, et al., Structural analysis of 5G networks, in XXXVIII. Kando Conference 2022 - Abstract proceedings, 2022, pp. 46–46.

[18] G. Kún, et al., 'Opened' or 'Closed' RAN in 5G, in IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022), 2022, pp. 347–351. https://doi.org/10.1109/SAMI54271.2022.9780667

[19] IEEE 802.1Qbv:2015, Enhancements for Scheduled Traffic, 2015. https://doi.org/10.1109/IEEESTD.2016.8613095

[20] IEEE 802.1Qch:2017, Cyclic Queuing and Forwarding, 2017. https://doi.org/10.1109/IEEESTD.2017.7961303

[21] IEEE 802.1Qcr:2020, Asynchronous Traffic Shaping, 2020. https://doi.org/10.1109/IEEESTD.2020.9253013

[22] Bocci, M. et al., RFC 5921, A Framework for MPLS in Transport Networks. IETF, 2010. https://doi.org/10.17487/RFC5921

[23] Kompella K. et al., RFC 7274, Allocating and Retiring Special-Purpose MPLS Labels, IETF, 2014. https://doi.org/10.17487/RFC7274

[24] WhireShark website: https://www.wireshark.org/

[25] IEEE 802.1Qci:2017, Per-Stream Filtering and Policing, 2017. https://doi.org/10.1109/IEEESTD.2017.8064221

[26] IEEE 802.1CB:2017, Frame Replication and Elimination for Reliability, 2017. https://doi.org/10.1109/IEEESTD.2017.8091139