DATACOM INDUSTRY ASSOCIATION

Cyber security for the evolving FRMCS deployment in the European Railway Sector

DIA Railway Working Group

Authors: Omar Benjumea, Daniele Bozzolo, Martin Reed, Paolo Volpato

datacom-ia.eu

Executive Summary

The evolution from the Global System for Mobile Communications – Railway (GSM-R) to the Future Railway Mobile Communication System (FRMCS) represents a foundational transformation in European railway communications. FRMCS brings the benefits of 5G's service-based architecture into the rail domain, offering enhanced bandwidth, deterministic latency, and built-in cyber security mechanisms derived from the 3GPP framework. However, the migration introduces new dependencies on virtualized architectures, digital identities, and cross-domain trust models that must be carefully governed in particular with regard to cyber security requirements.

This paper examines the cyber security dimensions of FRMCS within the broader context of the European railway digitalisation agenda. It explores how railway-specific standards (particularly CLC/TS 50701 and the forthcoming IEC 63452) interlock with the 3GPP trust and authentication model to create a layered defence across radio, core, and operational domains. Together, these layers support a vision of a resilient, secure, and interoperable European railway communications ecosystem that complies with the forthcoming EU Cyber Resilience Act, ensuring that connected railway systems meet modern product-level cyber security requirements, while simultaneously contributing to the broader sustainability and interoperability goals set out under the European Green Deal.

Key elements and findings include:

- *Identity and Confidentiality*: FRMCS replaces the GSM-R IMSI with a concealed identifier (SUCI/SUPI), mitigating tracking and impersonation risks.
- *Mutual Authentication and Key Hierarchies*: 5G-AKA procedures and hierarchical key derivation maintain continuous protection as trains move between cells.
- *Cross-Domain Security via SEPP*: Inter-operator signalling is validated, encrypted, and policy-enforced at the Security Edge Protection Proxy (SEPP), supporting both home-routed and visited-routed roaming scenarios.
- *Railway Trust Framework (RTF)*: An extended model, analogous to automotive Public Key Infrastructure (PKI) federations, allowing certificate-based assurance across European infrastructure managers.
- *Zero-Trust Integration*: Applying cloud-derived zero-trust principles to safety-certified operational technology is essential for long-term resilience.
- *Longevity and Lifecycle Assurance*: Cyber security must remain maintainable and verifiable across technology generations, ensuring continuity beyond 5G and 6G.
- *Cryptographic Agility*: The system must anticipate the integration of new and post-quantum cryptographic algorithms, compatible with evolving standards.

The paper concludes by recommending that the rail sector should focus on coordinated actions to formalise a European Railway Trust Framework for cross-border trust and certificate management, to validate FRMCS security in zero-trust contexts, to accelerate the adoption of standards within national certification regimes, and to include continuous observability as a core design principle. Through these combined measures, FRMCS can become a strategic enabler of secure, interoperable, and sustainable railway operations, forming a core component of Europe's broader digital and environmental transformation.

Table of Contents

List of Abbreviations

AMF – Access and Mobility Management Function
ATO – Automatic Train Operation
ATP – Automatic Train Protection
CA – Certification Authority
CCS TSI – Control Command and Signalling Technical Specification for Interoperability
CER – Critical Entities Resilience Directive
CENELEC – European Committee for Electrotechnical Standardization
CLC/TS – CENELEC Technical Specification
CRA – Cyber Resilience Act
CRL – Certificate Revocation List
DPI – Deep Packet Inspection
EC – European Commission
ECC – Electronic Communications Committee
EN – European Norm (European Standard)
ERA – European Union Agency for Railways
ERTMS – European Rail Traffic Management System
ETB – Ethernet Train Backbone
ETCS – European Train Control System
ETSI – European Telecommunications Standards Institute
FRMCS – Future Railway Mobile Communication System
GFM – Ground Fixed Means
gNB – 5G base station (gNodeB)
GoA – Grade of Automation
GPRS – General Packet Radio Service
GSM-R – Global System for Mobile Communications – Railway
IEC – International Electrotechnical Commission
IM – Infrastructure Manager
IMSI – International Mobile Subscriber Identity
IMU – Inertial Measurement Unit
IP – Internet Protocol
ITU – International Telecommunication Union
MCX – Mission Critical Services
MNO – Mobile Network Operator
MS – Member State
NIS2 – Network and Information Security Directive (Version 2)
OCSP – Online Certificate Status Protocol
OT – Operational Technology
PKI – Public Key Infrastructure
PLMN – Public Land Mobile Network
PTC – Positive Train Control
RAMS – Reliability, Availability, Maintainability and Safety

RBC – Radio Block Centre
RMR – Railway Mobile Radio
RTA – Root Trust Authority
RTF – Railway Trust Framework
SEPP – Security Edge Protection Proxy
SERA – Single European Railway Area
SIEM – Security Information and Event Management
SMF – Session Management Function
SOAR – Security Orchestration, Automation, and Response
SUCI – Subscriber Concealed Identifier
SUPI – Subscriber Permanent Identifier
TCN – Train Communication Network
TEN-T – Trans-European Transport Network
TS – Technical Specification
UDM – User Data Management
UIC – Union Internationale des Chemins de fer (International Railway Union)
UPF – User Plane Function
VBS – Voice Broadcast System
VGCS – Voice Group Call System
WTB – Wire Train Bus

1 Introduction to the evolving Rail management systems

1.1. Background

The European Railway EU-27 network covers over 202,000 Km of lines. Around 57% of the network is electrified, an increase of 2,410 km since 2015 (+2.2%). The EU's high-speed rail network stretched to over 15,600 km by the end of 2023, an increase of 14.5% since 2015. Should the current trend to extend the network continue over the next decades, the length of the high-speed network would see an increase of about 50% for 2020-2030 and by a factor of 2.5 for 2020-2050. The EU Sustainable and Smart Mobility Strategy (1) has set ambitious targets for high-speed rail traffic, which should double traffic volumes by 2030 and triple by 2050 compared to 2015 figures.

The EU has one of the densest railway networks in the world, however national railway systems across the EU vary. The process of improving the compatibility of EU member states' national railway systems started in the 1990s with the end goal of developing an efficient and competitive EU-wide railway network – the Single European Railway Area (SERA). Rail policy is part of the EU's transport policy which aims to achieve connected, sustainable, inclusive, safe and secure mobility across the EU.

The expansion and harmonisation of the EU's rail sector has faced a number of challenges over the years, which have slowed down the process of EU integration in the sector. This is mainly due to traditional fragmentation of the European railways due to complex stand-alone national systems and low efficiency, flexibility and reliability of the service, in particular for freight. To strengthen EU rail policy, the EU has adopted in recent years four railway strategies which aimed to open the railway market to competition, increase the interoperability of national railway systems and define a framework for a single European railway area.

In the broader framework of the EU's transport policy, the Trans-European Transport Network (TEN-T) (2) seeks to establish an integrated system of nine core corridors linking railways with roads, inland waterways, maritime routes, ports, and airports across the Union. As part of this effort, the co-legislators have agreed on key measures to enhance interoperability and operational efficiency within the extended core and comprehensive network. These include the deployment of the European Rail Traffic Management System (ERTMS) (3), the transition to a European standard nominal track gauge, the facilitation of 740-metre freight trains, and the achievement of a minimum line speed of 160 km/h for passenger services. Collectively, these provisions are designed to ensure sufficient capacity and uninterrupted rail transport operations across the entire TEN-T network. In addition, the provisional agreement integrates operational requirements for rail freight corridors into the revised TEN-T regulation, recognising that such operational parameters are inseparable from the underlying infrastructure requirements.

European Rail Train Management System

Before the conception of ERTMS, almost every European country operated its own Automatic Train Protection (ATP) system, the vital equipment on board the train that would

guarantee that the train driver would never exceed the authorised maximum speed on the line. Normally these systems were not compatible with each other and thus crossing a signalling area border meant that trains needed to implement several onboard ATP devices, each of which was self-functioning. Due to the increase in international rail services, a harmonised ATP system was needed for the European context. Thus, the aim of ERTMS was (and is) to gradually replace the different national ATP systems in European countries.

The ERTMS is composed of two main subsystems. The first is the European Train Control System (ETCS), which provides a standardised ATP mechanism. The second is the GSM-R, a dedicated communication system tailored to the specific needs of railway operations. Together, these two pillars form a unified European train control framework intended to progressively replace the numerous incompatible national systems currently in use across Europe.

ETCS has been designed encompassing 3 different levels:

ETCS Level 0

Level 0 applies when an ETCS-fitted vehicle is used on a non-ETCS route. The train-borne equipment monitors the maximum speed of that type of train. The train driver observes the trackside signals. Since signals can have different meanings on different railways, this level places additional requirements on the training of drivers. If the train has left a higher-level ETCS, it might be limited in speed globally by the last balises encountered.

ETCS Level 1

Level 1 is a cab signalling system that can be superimposed on the existing signalling system, leaving the fixed signalling system (national signalling and track-release system) in place. Eurobalise radio beacons pick up signal aspects from the trackside signals via signal adapters and telegram coders (Lineside Electronics Unit – LEU) and transmit them to the vehicle as a movement authority together with route data at fixed points. The on-board computer continuously monitors and calculates the maximum speed and the braking curve from this data.

ETCS Level 2

Level 2 is a digital radio-based system. Movement authority and other signal aspects are displayed in the cab for the driver. Apart from a few indicator panels, it is therefore possible to dispense with trackside signalling. However, the train detection and the train integrity supervision still remain in place at the trackside. Train movements are monitored continually by the RBC using this trackside-derived information. The movement authority is transmitted to the vehicle continuously via GSM-R or GPRS together with speed information and route data. The Eurobalises are used at this level as passive positioning beacons or "electronic milestones". Between two positioning beacons, the train determines its position via sensors (axle transducers, accelerometer and radar). The positioning beacons are used in this case as reference points for correcting distance measurement errors. The on-board computer continuously monitors the transferred data and the maximum permissible speed.

The Control Command and Signalling (CCS) Technical Specification for Interoperability

(TSI) 2023 [4] redefines ETCS Level 2 to incorporate the functionality previously described as Level 3 in earlier specifications. This enhanced form of Level 2 extends beyond traditional train protection to enable full radio-based train spacing. In this configuration, ground fixed means (GFM) such as track circuits or axle counters are no longer required. Instead, trains determine their own position through onboard sensors and data fusion combining inputs from positioning beacons, axle transducers, inertial measurement units (IMUs), gyroscopes, accelerometers, and radar. Each train must also reliably determine its train integrity onboard.

By transmitting this position and integrity information to the Radio Block Centre (RBC), the system can continuously identify the exact point on the track that the train has safely cleared. This enables a following train to be granted a new movement authority up to that cleared position, removing the need for fixed block sections. Consequently, train separation becomes dynamic rather than segmented, approaching a moving block principle in which line-clear authorisation is effectively continuous, limited only by braking distance. At present, movement authorities are still transmitted via GSM-R, while the train reports its position and integrity to the ground system to confirm when it is safe to issue the next movement authority.

1.2. Global System for Mobile Communications - Railway

The GSM-R, derived from second-generation GSM technology, has served as the digital backbone of European railway radio communications for over two decades. Developed under the EU-funded MORANE programme and deployed across all Member States, GSM-R provides secure, prioritised voice and data connectivity between trains and control centres, forming the mandatory radio bearer for the European Train Control System (ETCS) Level 2 [5].

Through continuous communication supporting train control, dispatching, and emergency coordination, GSM-R significantly enhanced interoperability and operational safety compared with the fragmented analogue systems it replaced. However, as a 2G-based technology, it now faces end-of-life challenges including diminishing vendor support, spectrum constraints, and limited capacity to meet modern performance and cyber security requirements.

In response to the growing demand for higher data rates, deterministic latency, and integration with digital and automated services, the Future Railway Mobile Communication System (FRMCS) — based on 4G/5G architectures — has been designated as the long-term successor to GSM-R within the European railway digitalisation roadmap.

Further detail on the historical context, system architecture, and operational functions of GSM-R is provided in the Appendix: GSM-R historical context.

1.3. Functional Safety and Cyber security in Railways

Functional safety ensures that risks arising from hazards caused by the malfunction or failure of systems are reduced to an acceptable level. These risks are growing in the rail industry as systems become increasingly complex, with hardware and software interacting in diverse ways and components sourced from multiple global suppliers.

In the railway domain, functional safety is governed internationally by the CENELEC EN 5012x series (and their equivalent IEC standards):

- EN 50126 (IEC 62278) – Reliability, Availability, Maintainability and Safety (RAMS)
- EN 50716 (formerly EN 50128, IEC 62279) – Software lifecycle processes
- EN 50129 (IEC 62425) – System safety

While functional safety focuses on ensuring that systems remain safe and reliable in the event of internal faults or failures, cyber security addresses protection against external threats such as unauthorised access, cyberattacks, and data breaches.

To bridge these two domains, CENELEC TC 9X issued the Technical Specification TS 50701 "Railway Applications – Cyber security" in 2023. This document establishes a consistent approach for managing cyber security across the railway sector, providing operators, system integrators, and suppliers with practical guidance on integrating security within the EN 50126 RAMS lifecycle.

Building on this foundation, IEC TC 9 is currently developing IEC 63452 "Railway Applications – Cyber security", a full international standard that will replace TS 50701. It is expected to be published in 2026, providing a comprehensive global framework for cyber security in railway applications.

2 The new standard for Rail signalling communications: FRMCS

FRMCS is the next-generation railway telecommunications system designed to meet two complementary objectives: on the one hand, to replace GSM-R in the communications between trains and ground due to its expected technical obsolescence within a decade; on the other, to lay the foundation for enhanced railway applications, enabling rail transport digitalization. FRMCS is designed to follow future evolutions of the 3GPP standards thus *future-proofing* railway telecommunications in a manner that was not possible with GSM-R. This evolutionary strategy meets the objectives of the European Commission's Green Deal (6) and their Sustainable and Smart Mobility Strategy (1).

A high-level comparison between the functionalities in GSM-R and FRMCS immediately exposes the differences between the two technologies as shown in Figure 1.

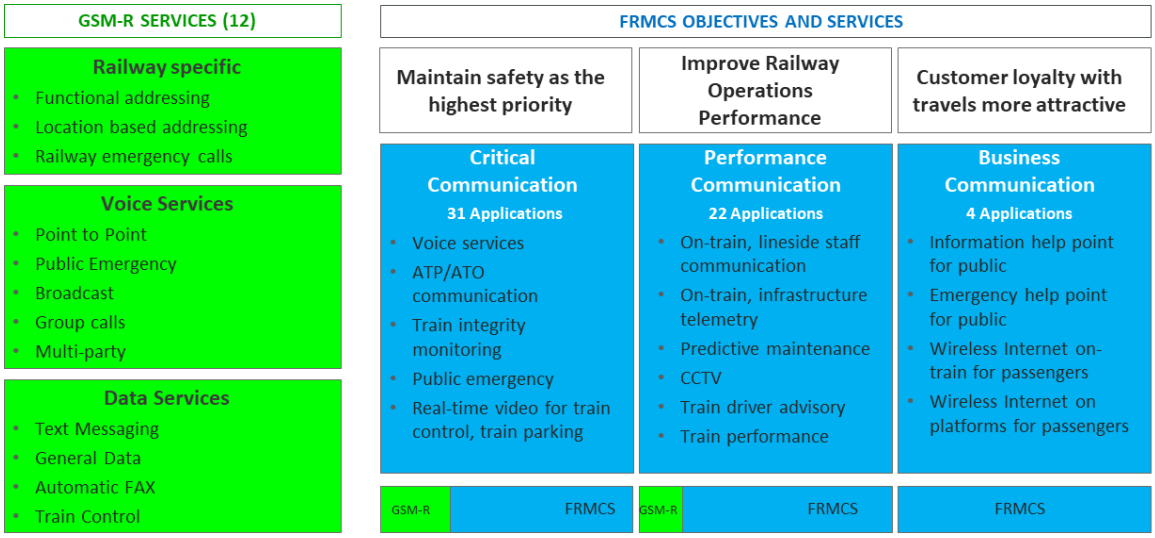

Figure 1 Comparison between GSM-R and FRMCS functionalities

GSM-R was conceived to support a limited number of railway services in support of control and train management (12 services). On the other hand, FRMCS expands the number of services (called applications in the UIC User Requirement Specification (7)), grouped in three main classes:

- Critical communication (31 applications) for driver/staff/ground communication, advanced control and safety, expanding the previous set of control applications introducing video and data capabilities.
- Performance and operational efficiency communication (22 applications), to support non mission-critical communication, telemetry, maintenance and other operational tasks, defining new functions barely available with GSM-R.
- Business communication (4 applications) directed mainly to passengers to enhance their quality of the travel experience, something not even foreseen in GSM-R.

At the time of writing, the UIC already delivered Version 2.1 of their user, functional and

system specifications. ETSI TC RT completed the so-called Phase 1 of FRMCS, which is a set of technical specifications describing the different aspects of the FRMCS architecture. ETSI TS 103 765-1 [8] provides the description of the FRMCS transport layer (termed the "transport stratum"). Several architectures are potentially applicable, depending on whether the radio access and the mobile core functions are performed by the Infrastructure Manager, the Mobile Network Operator, or both.

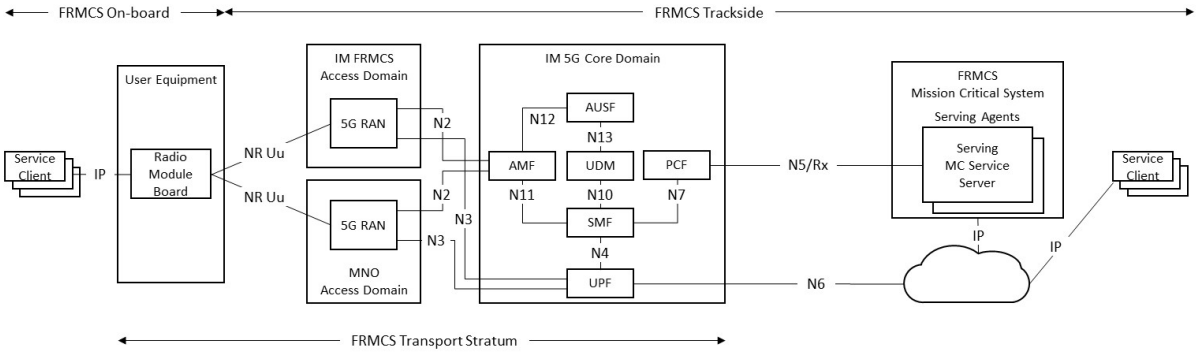

Figure 2 FRMCS Standalone Transport Domain Architecture, derived from ETSI TS 103 765-1

The FRMCS Standalone Transport Domain Architecture (non-roaming) [8] is depicted in Figure 2 which provides an overview of the key FRMCS technology components. 5G, the wireless system defined by 3GPP, provides radio connectivity to the train on-board equipment allowing the communication to the trackside applications. The transport of the services between the radio towers and the core network is performed by an IP backbone.

The all-data nature of the FRMCS services is enabled through the 3GPP MCX, defined in 3GPP TS 23.280 [9], TS 23.289 [10] and relevant specifications; these are highlighted by the box named "FRMCS MC System" on the right of Figure 2. The Electronic Communications Committee (ECC) allocated, in November 2020, the paired frequency bands 874.4–880.0 MHz and 919.4–925.0 MHz, and the unpaired frequency band 1900–1910 MHz for Railway Mobile Radio (RMR) use while the EC later mandated that these frequencies are made available for railway applications by the EU Member States (MS).

As for the immediate future, these are the envisioned next activities around FRMCS:

- The Horizon Europe FP2-MORANE-2 project, driven by Europe's Rail Joint Undertaking [11], will validate the current specifications of FRMCS through simulations and in-field testing. The project will last until 2027 and is expected to provide important feedback to both UIC and ETSI's work.
- Both the UIC and ETSI will continue working on their specifications. For UIC the version 3 of their functional specifications is expected by 2027. The same can be said for ETSI FRMCS Phase 2.
- All of the above will become input to the new version of the CCS TSI of ERA in 2028, where FRMCS is addressed as the communication framework to support both the existing applications (such as ETCS, critical voice-based communication) and the new applications such as Automatic Train Operations (ATO), data and video services, and other essential telecom applications requiring enhanced quality, flexibility and capacity.

As the cornerstone of Europe's next-generation rail signalling and control infrastructure,

FRMCS will underpin every layer of digital railway operation, from train control and automation to passenger information and maintenance systems. Its role as the primary communication bearer for safety-critical and operational data makes it an essential service whose reliability and trustworthiness directly affect rail safety and network integrity. Consequently, cyber security is not merely an adjunct to FRMCS deployment but a fundamental design requirement, ensuring that this vital system remains resilient against evolving threats and maintains the confidence of operators, regulators, and passengers alike. The rest of this white paper will consider the cyber security of railways and FRMCS.

3 Cyber security today in Rail

Railway cyber security is unlike cyber security in almost any other vertical because it directly intertwines with passengers' physical safety, national mobility, and complex operational technology (OT) that is designed to be deterministic and to run for decades. Trains, interlockings, wayside equipment and traffic management systems must maintain precise timing and integrity; a misconfiguration or delay is not merely a service quality issue but a potential safety hazard. As railways digitize, with wide deployment of ERTMS/ETCS, communications-based train control, and increasingly connected traffic management platforms, the sector's risk surface expands across onboard, wayside, and back-office systems. In Europe, the industry has converged on a "zones and conduits" approach—partitioning railway systems into security zones and tightly controlling flows between them—grounded in the CENELEC Technical Specification CLC/TS 50701 and aligned to the industrial/OT family IEC 62443. This gives operators a shared lifecycle language to integrate security into design, procurement, validation and maintenance, rather than bolting it on after commissioning.

What makes rail different from more conventional IT environments is the collision of safety and security lifecycles. Rolling stock and signalling assets have life expectancies measured in decades; patch windows can be narrow and require safety re-validation, and components often come from multi-tier global supply chains whose software provenance is opaque. Consequently, the sector's frameworks emphasize systematic risk assessment, segregation, authenticated maintenance access, secure update processes, and supplier development practices. The CLC/TS 50701 explicitly maps rail safety engineering concepts to cyber security controls and references IEC 62443, while the broader EN 50126/9 and EN 50716 remains the foundation of the safety case. The result is a pragmatic blueprint: manage zones and conduits, define security levels for safety-related functions, and require evidence that suppliers build and maintain products securely.

Recent incidents illustrate why these distinctions matter and why the topic is urgent. In Denmark in late 2022, trains were halted for hours when a software subcontractor shut down servers following a cyberattack; although infrastructure was not directly compromised, the ripple effects across operational dependencies forced nationwide disruption. The case is now a staple example of supply-chain concentration risk in transport. In Poland in 2023, saboteurs used cheap analogue radios to broadcast unauthorised "radio-stop" signals on an unencrypted frequency, triggering emergency brakes on more than 20 trains—an attack vector that bypassed IP networks entirely yet still produced meaningful operational disruption. In San Francisco in 2016, ransomware on SFMTA systems disabled ticketing and forced open faregates, rapidly translating a classic IT incident into service degradation and revenue loss. These cases, spanning IT ransomware to exploitation of sector-specific wireless and safety behaviours, demonstrate that cyber security incidents cascade quickly into safety and societal effects.

There are structural reasons that railway cyber security is a hot topic now. First, digitalization is accelerating. The sector is preparing to migrate from GSM-R to the 5G-based FRMCS, a multi-year program that will coexist with GSM-R and introduce a new radio core, spectrum and supplier stack to secure. FRMCS is positioned as both the successor to GSM-R and a key enabler of rail digitalization; coexistence into the next decade makes

secure-by-design engineering non-negotiable. Second, the threat environment has intensified, with critical infrastructure increasingly targeted for disruption, coercion or political signalling — raising the bar for baseline resilience and incident readiness in transport.

Regulatory developments are reshaping obligations — particularly in Europe. The NIS2 Directive overhauls the EU's cyber security framework for essential and important entities, explicitly covering rail infrastructure managers and railway undertakings. Member States were required to transpose NIS2 by October 2024; the directive mandates risk management controls, incident reporting, and supply-chain due diligence, and empowers authorities to supervise and impose fines. In parallel, the Critical Entities Resilience (CER) Directive addresses physical and organizational resilience across eleven sectors, including transport, with timelines that interlock with NIS2 and require Member States to identify critical entities and ensure risk-management and resilience planning. Together, NIS2 and CER push operators to treat cyber and physical resilience as a cohesive obligation rather than separate silos.

A second European regulatory development with major implications for rail suppliers is the Cyber Resilience Act (CRA) — a horizontal regulation that establishes cybersecurity requirements for all products with digital elements. The CRA entered into force in December 2024, with its main obligations applying from December 2027. For rolling stock, signalling, and telecommunications components within the EU, it places greater accountability on manufacturers to ensure secure-by-design principles, robust vulnerability management, and ongoing post-market monitoring. As a result, procurement frameworks and supplier assurance processes across the rail sector are expected to evolve significantly to reflect these new obligations.

Internationally, sector-specific regulators are moving in step. In the United States, the Transportation Security Administration has issued and updated rail cyber security directives since 2022, and these are now performance-based and periodically extended. The directives maintain requirements for incident reporting, network segmentation, access control, monitoring and testing, and explicitly bring Positive Train Control (PTC) components into scope for identification as critical cyber systems. The agency continues to refine and codify these measures through updates and related rulemaking.

Modern rail cyber security also hinges on one foundational capability: sustained visibility into the operational networks that actually move trains. In architectures shaped by zones and conduits, the most meaningful signals of risk appear at the interfaces among traffic management, interlockings and RBCs, onboard train networks, and telecom domains. Instrumenting those conduits, rather than relying solely on perimeter logs, turns otherwise opaque control flows into measurable telemetry that engineering and security teams can act on. Guidance developed with CLC/TS 50701 in mind provides a practical blueprint for where to observe and how to contain so anomalies are caught early and safely isolated.

Because critical rail systems are safety-certified and often carry tight warranty constraints, the method of observing them matters as much as the fact of observation. Passive network monitoring, via taps or SPANs, avoids the scheduling, re-validation and fragility concerns associated with active scans or host agents on signalling and rolling-stock assets. Contemporary OT security guidance recommends monitoring approaches that are ICS/OT-focused, capable of continuous network inspection, and fluent in control-

system protocols, with deep-packet inspection (DPI) to analyse protocol semantics rather than just headers and ports. In practice, that means tools that can build behavioural baselines, detect deviations, and integrate with SOC tooling—without interfering with train operations.

Generic IT sensors are not enough; rail uses its own stacks and timing behaviours. The Train Communication Network (TCN) family in IEC 61375 shapes traffic within and between vehicles (such as Wire Train Bus and Ethernet Train Backbone), while ETCS/ERTMS brings specific messaging flows around RBCs, balises, and train-to-ground exchanges. DPI that genuinely understands these environments — able to parse TCN/ETB/WTB and interpret RBC handover semantics — will reveal issues that payload-agnostic tools miss, from unexpected function activations to policy-breaking inter-zone flows or malformed command sequences. As FRMCS rolls out, protocol awareness must extend to 3GPP-based railway services and their failure modes on the radio path. In short, rail-specific visibility in critical OT is no longer a luxury; it is a prerequisite for trustworthy detection and safe response.

Recent disruptions underline why this visibility layer belongs inside the OT network, not just at enterprise perimeters. Denmark's nationwide stoppage in 2022 — triggered by a compromise at a software subcontractor — propagated through operational dependencies rather than classic north-south ingress; the ability to baseline and alert on abnormal application-to-operations relationships would have accelerated safe response. Poland's 2023 radio-stop sabotage, while not IP-borne, still produced observable knock-ons in connected systems, from unexpected stop sequences to management alarms; correlating network and operational telemetry helps distinguish nuisance from coordinated disruption. Even the San Francisco Muni ransomware incident showed how quickly passenger-facing IT failures can force railways into degraded operating modes; continuous OT-side monitoring gives operators independent confirmation of what remains safe to run.

For procurement and governance, the practical upshots are straightforward:

- prioritize monitoring capabilities that are passive by default
- provide DPI for control-system protocols with rail-specific decoders
- auto-discover assets and build baselines across wayside, onboard, and telecom segments
- detect east-west policy violations between zones
- integrate via open formats with SIEM/SOAR
- and, support threat-intel workflows and compliance reporting.

Guidance for ICS/OT monitoring explicitly calls for technologies built specifically for ICS assets that understand OT communications (including via DPI), generate alerts on baseline deviations, and support standards-based information sharing; capabilities that map cleanly to TS 50701 and IEC 62443 and help satisfy incident-handling expectations under modern regimes.

The policy arc reinforces the business case. In Europe, NIS2, CER and the CRA now make explicit what many rail leaders already understood: cyber resilience in rail is inseparable from safety and service continuity, and accountability is spreading across the ecosystem—from operators to suppliers. In the United States and other jurisdictions, performance-based regulatory instruments are evolving in similar directions, emphasizing

outcomes over checklists and expecting demonstrable visibility, segmentation, access control and testing in critical rail systems. Operators and suppliers that internalize CLC/TS 50701 and IEC 62443, design with zones and conduits, and hold the supply chain to verifiable, lifecycle-oriented practices will be best placed to keep trains moving safely in the face of modern threats. The cases from Denmark, Poland, and San Francisco show the stakes are not hypothetical: they rest on avoided stoppages, protected revenue, and preserved public trust.

In conclusion, rail is different because safety-critical OT, long asset lifecycles, and cross-border operations make conventional IT playbooks insufficient. It is urgent because, even as regulation raises expectations, digitalization is expanding attack surfaces and there is a heightened threat environment. The operationally sound answer is sustained visibility into critical networks using passive monitoring with rail-aware DPI, anchored in zones-and-conduits designs and backed by supplier assurance. Paired with evolving regulatory frameworks in Europe and abroad, this approach enables operators and manufacturers to reduce risk pragmatically while preserving safety, availability, and public trust.

4 Cyber security and FRMCS

The Future Railway Mobile Communication System (FRMCS) inherits the security foundations of the 3GPP 5G architecture, which provides strong, standardised mechanisms for confidentiality, integrity, authentication, and authorisation. The 5G architecture is complex with many core components and as it uses a service-based architecture these components are virtualised and vary from implementation to implementation. The key components associated with FRMCS security functions are shown in Figure 3, this figure does not include the media functions and MCX services. Core functions such as the *Access and Mobility Management Function* (AMF), *User Data Management* (UDM), and the *Security Edge Protection Proxy* (SEPP) create an end-to-end trust framework within both national and cross-border railway domains.

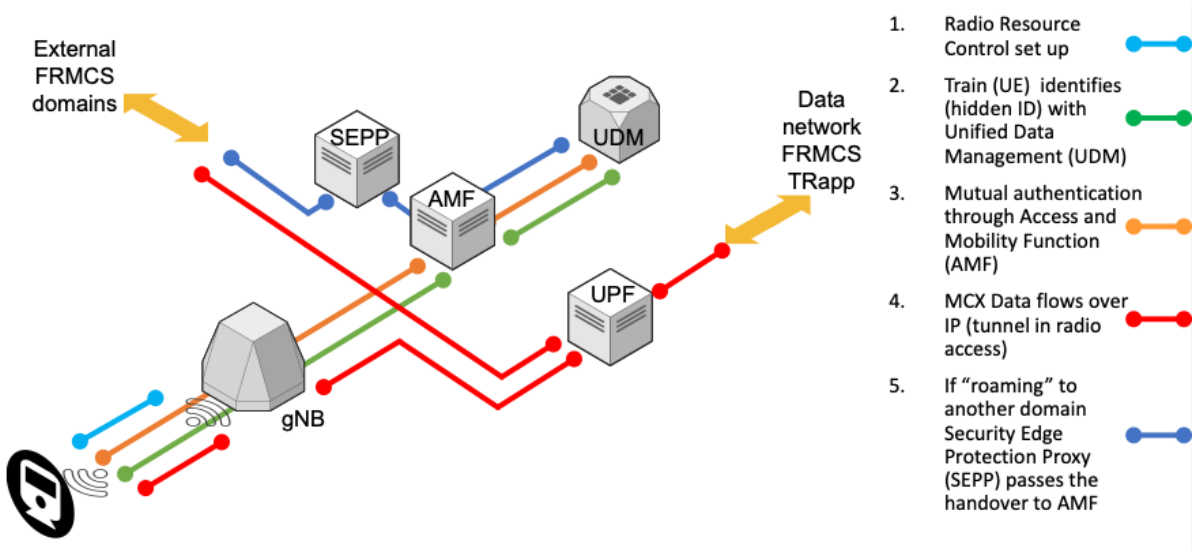

Figure 3 The 5G components forming the key parts of FRMCS security

At the radio and identity layers, there are two stages to registration of a new device: first the subscriber ID is validated; then mutual authentication follows as described below.

At the radio layer, the Subscriber Permanent Identifier (SUPI) is concealed by the Subscriber Concealed Identifier (SUCI) during the registration process, protecting user identities, such as those of trains or trackside terminals, even from passive interception. This mechanism replaces the clear-text International Mobile Subscriber Identity (IMSI) used in legacy systems like GSM-R, which was vulnerable to eavesdropping and spoofing. In FRMCS, the SUPI is never transmitted over the air; instead, the user equipment (UE) (the train onboard equipment) encrypts it using the public key of the home network's UDM before sending the SUCI to the AMF. Only the home network can decrypt this value, ensuring that even a compromised or malicious visited network cannot learn the permanent identity of the subscriber. The resulting temporary identifiers, gNB-allocated and session-specific, further reduce tracking risk by frequently refreshing during mobility events. Together, these measures provide a major advance in privacy and identity assurance, establishing the foundation for mutual authentication and secure key exchange in the subsequent stages of FRMCS session setup.

Once the subscriber's concealed identity has been validated, the network and the onboard

equipment establish trust through the 5G Authentication and Key Agreement (5G-AKA) procedure. This process enables mutual authentication: the UE verifies the network's legitimacy while the network confirms the subscriber's credentials using authentication vectors derived from the Authentication Server Function (AUSF) and UDM. Successful authentication results in the derivation of a hierarchy of cryptographic keys, beginning with the primary K_SEAF key, which is distributed to the AMF and subsequently used to generate further session-specific keys for signalling and user-plane protection. These keys underpin encryption and integrity verification between the UE (train on-board equipment) and the network, ensuring that both control messages and user data remain confidential and tamper-resistant across the air interface. In the FRMCS context, this mechanism guarantees that only trusted railway devices (e.g., certified onboard units, driver consoles, or maintenance terminals) can access the network, while simultaneously protecting the network infrastructure from rogue or spoofed endpoints. This mutual authentication stage thus forms the cryptographic foundation upon which all higher-level FRMCS applications, including mission-critical voice and data services (MCX), securely operate.

The registration process above is relatively slow and, while acceptable when a train first connects to the FRMCS domain, it would cause too much latency when moving between the trackside gNBs. Consequently, following mutual authentication, FRMCS relies on a hierarchical key-derivation structure to sustain secure connectivity as trains move rapidly between radio cells. The master key K_SEAF, generated during the 5G-AKA exchange, remains valid for the current serving network and is used by the AMF to derive a series of subordinate keys. From the K_SEAF, the AMF creates K_AMF, which governs the overall security context for that registration area. When a handover occurs to a new gNB, a further key (K_gNB) is derived locally to protect the user plane and radio-resource control signalling. These keys are chained and refreshed hierarchically: as long as the train stays within the same AMF or Public[1] Land Mobile Network (PLMN), the AMF securely transfers the context and new K_gNB values to successive gNBs without repeating the full 5G-AKA procedure. This mechanism preserves encryption and integrity protection while enabling sub-second handovers, a prerequisite for maintaining uninterrupted FRMCS service continuity at high train speeds.

Security is further reinforced at the inter-domain level by the SEPP, which validates and encrypts all control-plane signalling exchanged between railway operators' PLMNs. This mechanism is essential when trains roam between infrastructure managers or national operators, providing confidentiality and policy enforcement equivalent to public-mobile roaming. Acting as a secure border gateway between administrative domains, the SEPP ensures that only authorised and integrity-protected service requests traverse the inter-operator boundary, while hiding the internal topology of each network. This function becomes particularly critical when trains cross national borders or move between infrastructure managers, where the onboard equipment must attach to a visited FRMCS network while maintaining logical continuity with its home network. Two principal roaming modes support this operation. In home-routed roaming, the user plane remains anchored

[1] Note the "public" in PLMN is derived from a historic use by 3GPP from the GSM era, there is no implication that an FRMCS PLMN domain is likely to be public, although it might be possible for a PLMN to make use of a *slice* from an existing public 5G network.

in the home network's core, meaning that mission-critical traffic, such as MCX voice, data, or train-control signalling, is tunnelled securely back through the home operator's UPF. This arrangement maximises policy control and ensures that all data flows remain within the home domain's security perimeter, but at the cost of increased latency caused by the longer routing path. By contrast, visited-routed roaming (termed as *local breakout*) allows the user plane to terminate within the visited PLMN, enabling local access to edge applications and lower latency for real-time services. This model delivers better performance but requires a stronger, policy-driven trust framework between domains so that service quality, assurance levels, and isolation policies remain consistent. In both cases, the SEPP provides the cryptographic trust anchor, enforcing confidentiality, integrity, and policy validation across the inter-operator interface, and thereby guarantees that cross-border FRMCS signalling achieves a security posture equivalent to that of trusted intra-domain communication.

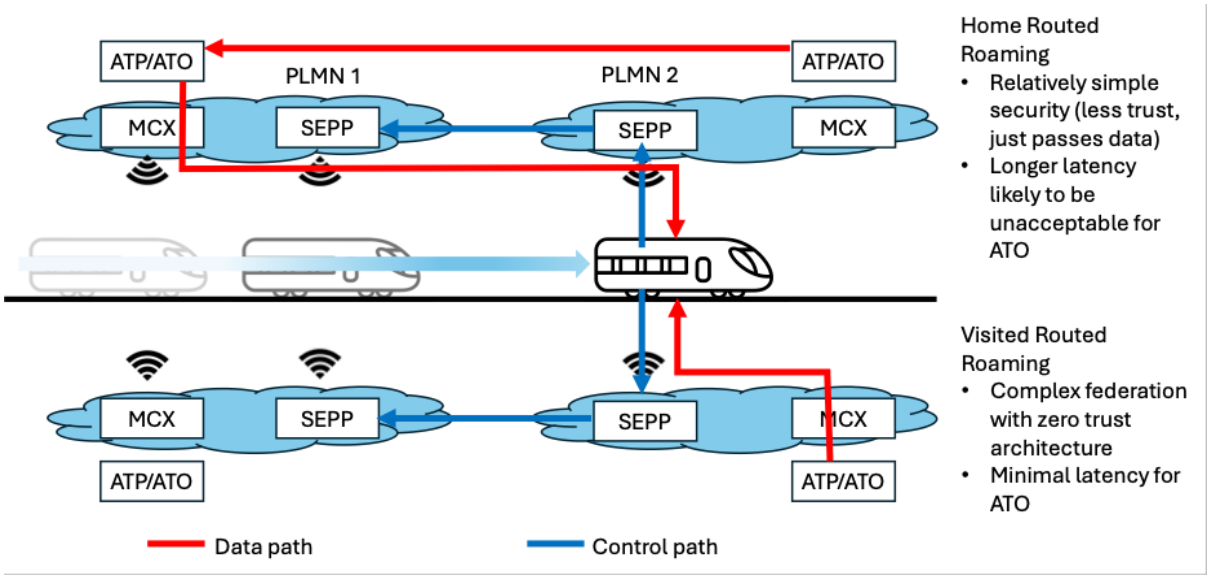

Figure 4 SEPP-mediated inter-domain connectivity in FRMCS

Figure 4 illustrates how the SEPP secures the exchange of control-plane signalling between two PLMNs, such as those operated by neighbouring infrastructure managers; the diagram assumes a train has just left PLMN 1 and is moving to another domain such as PLMN 2, this might be the case when a train moves from one country to another, or even between two infrastructure management domains in a single country. Only one of either *home-routed* or *visitor-routed* is likely to be used in a single case, but both are shown on the same diagram. In the *home-routed* configuration, both the control and user planes (data path) are tunnelled through the home FRMCS core, with the SEPP pair providing end-to-end encryption and topology hiding across the federation boundary. In the *visited-routed* configuration, the control plane continues to pass through the SEPPs for policy enforcement and authentication, while the user plane is locally terminated in the visited PLMN's UPF to achieve minimal latency. In both scenarios, SEPP-to-SEPP trust, mutual certificate validation, and policy synchronisation ensure that inter-domain connectivity preserves the same integrity and confidentiality guarantees as within a single FRMCS domain.

From a lifecycle perspective, IEC 63452 defines the overarching cyber security framework for railway operations, complementing FRMCS's technical safeguards by prescribing governance, risk assessment, and certificate-management processes. Whereas 3GPP focuses on network-layer defences, IEC 63452 addresses the operational deployment context including: key management, patching policy, and supplier assurance. Both perspectives are essential: FRMCS ensures secure transport and authentication, while IEC 63452 ensures that these capabilities are embedded within organisational processes.

Nevertheless, FRMCS security cannot be viewed in isolation. It forms one component of the wider ERTMS ecosystem, which includes signalling, interlocking, and train control systems with diverse legacy interfaces. Each interworking point, for example between the onboard EVC, the RBC, and the FRMCS gateway, introduces a potential vulnerability. Adopting a zero-trust philosophy is therefore essential: every connection must be authenticated and authorised, data must be integrity-checked at each boundary, and continuous monitoring should detect anomalous behaviour. Indeed, the service based architecture of the 3GPP 5G architecture is itself essentially a zero-trust architecture that requires systems that use it to also embrace this security philosophy.

Finally, long-term resilience will depend on the agility of railway cyber security governance. As threats evolve, from quantum-computing risks to AI-driven attack automation, the assurance methods used in railway safety must adapt. Formal verification, explainable AI for threat detection, and cryptographic agility should form part of the future FRMCS security roadmap.

5 Security for the future of Rail and FRMCS

Although FRMCS provides a robust and standardised foundation for secure communications, its practical deployment across the European rail network will expose a number of complex challenges. Chief among these is the question of *inter-domain trust and federation*. As trains move across borders, they must authenticate and exchange data through multiple operators' domains, each governed by distinct regulatory and operational frameworks. The current SEPP-based federation model, inherited from 3GPP, secures inter-operator signalling but remains largely static and bilateral. To achieve true pan-European interoperability, a more dynamic and policy-driven trust infrastructure will be needed: one capable of automating certificate exchange, verifying service assurance levels, and enforcing cross-domain security policies in real time.

A practical approach to establishing cross-domain trust within FRMCS would be the creation of a Railway Trust Framework (RTF), analogous to the federated PKI architectures already in use across the automotive sector [12]. At its apex, a Root Trust Authority (RTA)—governed at a European or pan-railway level—would define the overarching certificate policy, audit procedures, and cryptographic standards. Each national infrastructure manager or railway operator would act as a subordinate Certification Authority (CA), cross-certified with the RTA to ensure mutual recognition of credentials between domains. Beneath these, equipment-level subordinate CAs would issue certificates to onboard units, trackside devices, and gateway systems during the provisioning phase, using limited certificate lifetimes to reduce long-term exposure. Revocation and status checking would be handled through lightweight OCSP or delta certificate revocation lists (CRLs) distributed efficiently via the FRMCS control plane, ensuring that compromised identities can be invalidated quickly. Service access decisions would be enforced through the existing 5G control functions—SEPP, SMF, and AMF—which would validate certificate attributes such as assurance level, operator domain, and permitted service class before establishing a session. To preserve low-latency performance, especially during cross-border operations, edge nodes in visited domains could cache validated certificates and perform local verification, enabling seamless re-authentication without repeatedly querying the central authority. Together, these mechanisms would create a layered and policy-driven trust ecosystem, capable of supporting secure interoperability among the many stakeholders in the European rail network.

A second area of difficulty lies in integrating legacy systems with the new FRMCS environment. Signalling and control subsystems that pre-date IP networking will continue to operate for many years. Gateways that bridge these environments must provide rigorous isolation and protocol validation while maintaining the latency and determinism demanded by safety-critical control. This integration problem is not merely technical: it requires new governance models to manage risk across organisational boundaries and life-cycle stages.

Moving toward a *zero-trust architecture* will also test existing operational practices. While IEC 63452 introduces important measures for certificate management and supplier assurance, it does not yet provide a full framework for continuous authentication and authorisation between operational domains. Extending zero-trust principles to railway operations will require both architectural change and cultural adaptation within infrastructure managers and train operators; for example, they will need to implement

systems that provide: identity-centric access control, micro-segmentation, and continuous verification.

Zero-trust architectures have emerged from cloud-based systems which are closely related to the service-based architecture of 5G. However, adopting a zero-trust architecture within railway OT environments presents unique challenges compared with cloud or enterprise IT systems (13). Traditional OT networks are built around deterministic control loops, fixed topologies, and long equipment lifecycles, often exceeding twenty years. Their devices (interlockings, signalling controllers, and train control units) were never designed for continuous authentication, dynamic policy enforcement, or micro-segmentation. Implementing zero-trust principles therefore demands careful retrofitting of identity, monitoring, and policy layers without compromising real-time performance or safety certification. Many OT systems also rely on proprietary or legacy protocols that lack native encryption or mutual authentication, making it difficult to integrate them into an identity-centric access model. Furthermore, the cultural shift required is significant: security boundaries in OT have historically been physical and organisational rather than logical. Moving toward zero-trust means re-architecting both the technology and the governance model so that every transaction, whether between sensors, gateways, or operators, is verified, logged, and continuously evaluated within stringent safety and availability constraints.

Another future issue is the evolution of cryptographic standards. The prospect of quantum computing demands migration toward quantum-resistant algorithms, affecting both 3GPP and IEC ecosystems. Achieving crypto-agility, the capacity to update algorithms and keys without service disruption, will be critical for long-term resilience and regulatory compliance.

Finally, assurance and organisational readiness remain cross-cutting themes. As safety and cyber security assurance converge, new methods such as formal verification and explainable AI will help validate that FRMCS components meet both security and safety requirements. Yet technical assurance must be complemented by well-rehearsed incident-response coordination, training, and shared situational awareness across national borders.

In summary, FRMCS security is not a single technological problem but a systemic endeavour. It demands that the railway sector blend 5G's technical safeguards with the governance and assurance frameworks of IEC 63452, establishing a resilient foundation capable of evolving with both the threat landscape and the ambitions of a connected, pan-European railway.

6 Conclusion and future actions

Cyber security within FRMCS is both an engineering and governance challenge. While the adoption of 5G technologies provides a robust cryptographic foundation, true resilience depends on embedding these mechanisms into the operational and regulatory frameworks that govern the European railway system. The introduction of FRMCS extends beyond technological renewal; it requires the creation of a trusted ecosystem that balances safety, interoperability, and security assurance across national and operational boundaries.

Inter-domain trust must evolve from bilateral SEPP peering relationships to a federated, policy-driven trust model such as a Railway Trust Framework (RTF) as proposed in this white-paper. This would enable consistent assurance and authentication policies across infrastructure managers, operators, and suppliers, creating a shared basis for digital identity and credential validation. Likewise, zero-trust principles (continuous authentication, micro-segmentation, and verification of every transaction) must be adapted to the constraints of railway operational technology, ensuring that functional safety and deterministic performance are not compromised by added security controls.

Legacy integration remains a critical factor. The coexistence of FRMCS with signalling and control systems such as ETCS and interlockings demands strong isolation and protocol validation at every interface. This layered defence model should be complemented by continuous monitoring and passive inspection capabilities, giving operators real-time visibility into network behaviour and enabling rapid detection of anomalies without interfering with safety-certified systems.

The long operational lifecycle of railway systems also necessitates cryptographic agility. FRMCS deployments will span multiple technology generations, and the underlying security architecture must be able to evolve to accommodate emerging and post-quantum cryptographic algorithms. In parallel, European harmonisation efforts such as the IEC 63452 standard and the EU Cyber Resilience Act will define baseline assurance requirements, reinforcing the need for consistent certification and supplier governance across Member States.

Looking forward, the rail sector should focus on several coordinated actions. The first is to formalise a European Railway Trust Framework that extends federated PKI principles, ensuring cross-border trust and certificate management. The second is to continue the cross-domain testbeds for validating FRMCS security in roaming, SEPP, and zero-trust contexts (as with MORANE-2). The third is to accelerate the adoption of IEC 63452 within national certification regimes, aligning procurement and compliance practices. Finally, continuous observability should become a core design principle, supported by AI-driven, explainable monitoring tools that strengthen both operational awareness and safety assurance.

Through these combined measures, FRMCS can move beyond being a technical successor to GSM-R. It can become a strategic enabler of secure, interoperable, and sustainable railway operations, forming a core component of Europe’s broader digital and environmental transformation.

Appendix: GSM-R historical context

GSM-R is built on 2G-based GSM technology, and benefits from the economies of scale of its GSM technology heritage, aiming at being a cost-efficient digital replacement for existing incompatible in-track cable and analogue railway radio networks.

The standard is the result of over ten years of collaboration between the various European railway companies, with the goal of achieving interoperability using a single communication platform. GSM-R carries the vital signalling information (on ETCS Level 2 and Level 3) directly to the train driver, enabling higher train speeds and traffic density with a high level of safety.

The specifications were finalized in 2000, based on the European Union-funded MORANE (Mobile Radio for Railways Networks in Europe) project. GSM-R is fully defined in ETSI standards.

GSM-R has been selected by 38 countries across the world, including all member states of the European Union and countries in Asia, Eurasia and northern Africa.

GSM-R is a secure platform for vital signalling data as well as voice communication between railway operational staff, including drivers, dispatchers, shunting team members, train engineers, and station controllers. It delivers features such as group communication, location dependent addressing, priority levels, railway emergency calls, shunting communication. This supports applications such as cargo tracking, video surveillance, and passenger information services.

GSM was chosen at the beginning as the best technology because it was widely proven, highly interoperable and finally, a hugely successful global standard.

Key Features and Functions of GSM-R are:

- Digital, Secure, and Dependable: it uses modified GSM technology to provide a robust and secure platform for critical railway communications.
- Voice and Data: supports both voice calls and data services, which are essential for operational messaging and control.
- Integrated in ERTMS: acts as the mandatory radio bearer for the ETCS, specifically for ETCS level 2 (including the extensions that were previously termed ETCS 3), allowing for seamless integration with advanced train management functions.
- Interoperability: as a global standard that ensures trains and railway staff can communicate across national borders without issues, fostering greater safety and operational efficiency.
- Prioritized Communications: incorporates processes and features to prioritize urgent communications, such as alerting signallers when a train is stopped at a red signal.

Benefits are then the following:

- Improved Safety and Performance: it enhances safety and performance by providing a standardized, reliable communication system for all railway operations.
- Standardization: replaces a multitude of non-interoperable national systems with a

single, international standard.
- Enhanced Capacity: contributes to a more modern, digitally enabled railway network with increased capacity.
- Operational Efficiency: streamlines communication processes between drivers, control centres, and other staff, leading to more efficient operations.

GSM-R is typically implemented using dedicated base station masts close to the railway, with tunnel coverage effected using directional antennae or 'leaky' feeder transmission. The distance between the base stations is 7–15 km. This creates a high degree of redundancy and higher availability and reliability. In areas where the ETCS Level 2 or 3 is used, the train maintains a circuit switched digital modem connection to the train control centre at all times. This modem operates with higher priority than normal users (eMLPP). If the modem connection is lost, the train will automatically stop.

GSM-R uses a specific frequency band, which can be referred to as the "standard" GSM-R band:

- Uplink: 876–880 MHz used for data transmission
- Downlink: 921–925 MHz used for data reception

GSM-R permits new services and applications for mobile communications in several domains:

- Transmission of Long Line Public Address (LLPA) announcements to remote stations down the line
- Control and protection (Automatic Train Control/ETCS) and ERTMS
- Communication between train driver and regulation centre
- Communication of on-board working people
- Information sending for ETCS
- Communication between train stations, classification yard and rail tracks

It is used to transmit data between trains and railway regulation centres with level 2 and 3 of ETCS. When the train passes over a Eurobalise, it transmits its new position and its speed, then it receives back agreement (or disagreement) to enter the next track and its new maximum speed.

New GSM-R features for mobile communication are based on GSM, and are specified by EIRENE project. Call features are:

- PtP Call: Point-to-Point Call, the same type of call as a normal GSM call
- VGCS: Voice Group Call System, quite similar to walkie-talkie communication but with a single uplink handled by the network (only one person can speak at a time)
- VBS: Voice Broadcast System, like a VGCS but only the call initiator can speak (the other are only listeners)
- REC: Railways Emergency Call, is a special VGCS defined as 299 with the highest priority possible (0)
- SEC: Shunting Emergency Call, is a special VGCS defined as 599 with the highest priority possible (0)
- Priority control of all the different calls (PtP, VGCS, VBSm, REC and SEC calls)

There are other additional features:

- Functional Addressing, alias system to call someone registered on the GSM-R network, only by knowing the temporary function user (engine driver of train such-and-such, ...)
- Location Dependent Addressing, routing system to call the most appropriate train controller regarding the current train position by dialling a pre-defined short code
- Shunting mode, when users work on the tracks

The involved suppliers have indicated that they will support GSM-R technology and GSM-R products at least until 2035. The industry is also starting to suffer from skills gaps, with fewer engineers available with the right skills to support GSM-R.

On top of the problem of GSM-R being about to reach the end of its lifetime, Railway applications are becoming more demanding in terms of performance and features required from their future telecommunication system.

In Europe, the current GSM-R based rail communication system is unable to support the demand of these new applications and services that GSM-R cannot satisfy completely.

New list of such needs is grouped into four main categories:

- signalling for safe train control,
- critical voice,
- critical video for obstacle detection and monitoring doors inside trains,
- critical data for communications among trains and trackside.

The Rail community is actively studying, designing, developing and testing the proposed alternative to GSM-R: the Future Rail Transportation Communication System (FRMCS). This is a radio system based on current 4G and 5G technologies to mitigate the risk of GSM-R obsolescence with the addition of extra features and functions capable to properly support the current effort for the digitalization of railways. This new journey to the new FRMCS system was led by the Union Internationale des Chemins de fer (UIC, or International Railway Union) with an early analysis in mid-2010s that eventually brought to the UIC FRMCS program in 2018 [ref. 4]. The FRMCS program provided major feedback to the European Union Agency for Railways (ERA) in their system definition for the evolution of railway radio communication eventually incorporated into Regulation 2023/1695 of the European Commission (EC) [ref. 5]. The EC also mandated the Technical Committee “Railways Telecommunications” (TC RT) of the European Telecommunications Standards Institute (ETSI) to begin the standardization work program for FRMCS.

References

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Sustainable and Smart Mobility Strategy – putting European transport on track for the future. 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0789

[2] Regulation (EU) 2024/1679 of the European Parliament and of the Council of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and repealing Regulation (EU) No 1315/2013 (Text with EEA relevance). 2024. [Online]. Available: http://data.europa.eu/eli/reg/2024/1679/oj/eng

[3] E. U. A. for Railways, 'European Rail Traffic Management System (ERTMS) | European Union Agency for Railways'. [Online]. Available: https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms_en

[4] Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 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. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2023/1695/oj/eng

[5] UIC ERTMS/GSM-R Operators Group GSM-R Industry Group, ERTMS/GSM-R Quality of Service Test Specification for EIRENE QoS requirements. v2.0.0, 23 Nov. 2017.

[6] European Commission, 'The European Green Deal', Brussels, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2019) 640 final, Dec. 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0640

[7] UIC, FRMCS System Requirements Specification v2.1.0, Apr. 25, 2025.

[8] ETSI TS 103 765-1, Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Building Blocks and Functions; Part 1: Transport Stratum, v1.0.0, 10 July 2025.

[9] 3GPP TS 23.280, 'Common functional architecture to support mission critical services; Stage 2'.

[10] 3GPP TS 23.289: 'Mission critical services using 5GS; Stage 2'.

[11] https://rail-research.europa.eu/rail-projects/fp2-morane-2/.

[12] A. C. H. Chen, C. -K. Liu, C. -F. Lin and B. -Y. Lin, 'V2X Credential Management System Comparison Based on IEEE 1609.2.1 and ETSI TS 102 941', presented at the 2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon), Bagalkote,

India (Online). Available: https://ieeexplore.ieee.org/document/10774595

[13] M. Lyu and J. Farooq, 'Zero Trust in 5G Networks: Principles, Challenges, and Opportunities', in 2024 Resilience Week (RWS), Dec. 2024, pp. 1–8. doi: 10.1109/RWS62797.2024.10799354.

