

RAIL PULSE

FREQUENTIS PUBLIC TRANSPORT NEWS



Thomas Karl, Vice President
Public Transport, Frequentis AG

Dear Reader!

The rail industry is moving towards a more connected, data-driven future. With FRMCS advancing from research and standardisation into implementation, the focus is shifting from defining capabilities to delivering them in real-world operations.

As networks become more connected and data-rich, cybersecurity, interoperability and operational intelligence are becoming essential to railway performance.

In this edition, we explore the technologies, partnerships and innovations supporting this transition.

Together with our partners FRAFOS, Control Center Apps, CNS Solutions & Support and Mission Embedded, we look at how railways can strengthen security, improve decision-making and unlock the value of next-generation communications.

We also share the latest market developments and industry perspectives.

I hope you enjoy this edition and find inspiration in how our industry is turning vision into operational reality. Wherever you are on your route to FRMCS, our Frequentis experts look forward to continuing the conversation.

More Information
[www.frequentis.com/
public-transport](http://www.frequentis.com/public-transport)



Thomas Preissner & Markus Myslivec

Until now, FRMCS has been shaped through research, standardisation and industry collaboration. Which capabilities are essential for railway operators to manage the shift from definition to real world operations?

Capability one: Operating between worlds

FRMCS will not replace GSM-R overnight. Forward-looking railway operators are already preparing for a long-term period where current and future communication environments must coexist.

- Successful operators need:**
- seamless interoperability between GSM-R and FRMCS
 - migration paths that avoid operational disruption
 - the ability to introduce new capabilities gradually

What it requires
A transition strategy built around coexistence and parallel operation rather than replacement and silo networks. Railway operators need communication architectures that allow current and future systems

to interwork, enabling a controlled migration at a pace that reflects operational priorities, infrastructure readiness and national rollout plans.

Frequentis perspective
This approach is reflected in Frequentis' FRMCS service layer architecture, which enables interworking between GSM-R and FRMCS environments through components such as the Interworking Function (IWF), guaranteeing interoperability.

Capability two: Keeping people at the centre of change

FRMCS will change the tools available to railway operations teams, but successful migration depends on maintaining confidence and usability in the control room.

- Successful migration requires:**
- continuity of dispatcher workflows
 - intuitive, adaptable and unified user interfaces
 - solutions that evolve alongside operational needs

Why involve people
A human-centred approach to technology adoption ensures new capabilities enhance operations not complicate them.

Frequentis perspective
With decades of safety-critical control room experience, Frequentis understands that communication technology must be designed around operational needs, providing a flexible environment that supports today's GSM-R operations while preparing for FRMCS capabilities.

Capability three: Building flexibility for the future

FRMCS will not be a one-time technology change. As standards mature, operational requirements evolve and new capabilities emerge, railway operators will need communication systems that can adapt.

- Successful migration requires:**
- open, standards-based architectures
 - freedom to evolve within a multi-vendor ecosystem
 - software-driven systems that can adapt over time

Why flexibility matters
A technology foundation built around interoperability and flexibility. Railway operators need solutions aligned with open standards such as ETSI, 3GPP and UIC, enabling them to integrate different technologies and avoid dependency on a single supplier.

Frequentis perspective
Frequentis designs its FRMCS solutions for multi-vendor ecosystems, based on open standards and modular architectures, as well as integration of legacy systems. This ensures flexibility to evolve while protecting past investments.

Different starting point, same destination

FRMCS migration is different for every railway. Network infrastructure, operational priorities, spectrum availability and investment cycles will all shape the path forward. Successful

strategies adapt to new capabilities when ready while maintaining reliable operations at every step.

Planning your FRMCS journey
As FRMCS testing accelerates across Europe the industry is proving the technology works. The challenge is ensuring it works at scale, in live operations, and throughout a migration period of many years. Success will be defined by technical validation, but also the ability to maintain continuity. The organisations best positioned for success will start planning early, build a flexible migration strategy, and prepare for coexistence from day one. Start your route to FRMCS here. <<

Migration stories

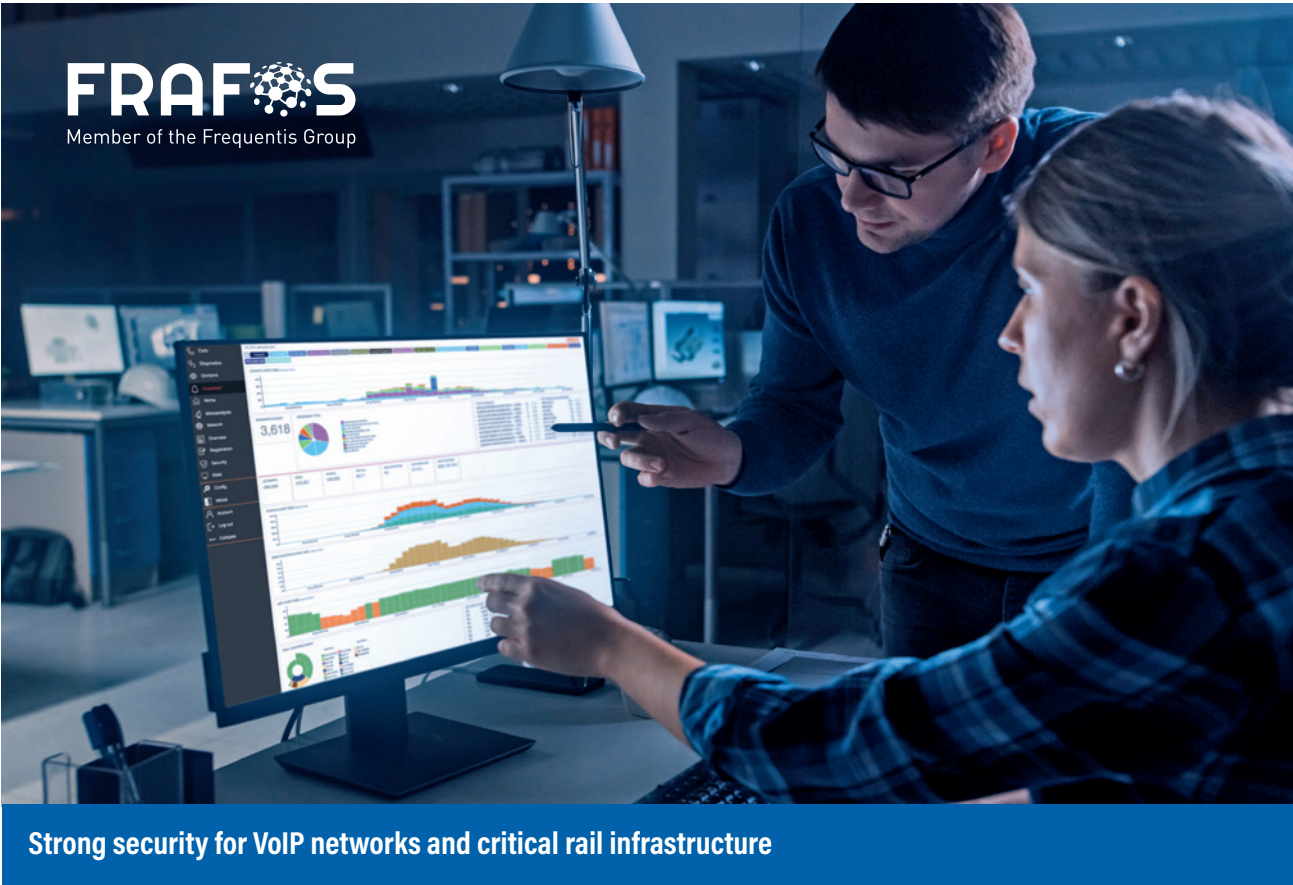
- Austrian Federal Railways (ÖBB):** Trials and validation activities to explore the technologies and operational concepts needed.
- Swiss Federal Railways (SBB):** Focusing on dispatcher evolution and interoperability using FRMCS-ready architecture. Showing importance of preparing the control room alongside the communication network.
- Lower Austrian Transport Company (NÖVOG):** Demonstrating how mission-critical communication services are delivered over public mobile networks, opening new possibilities for regional operators.
- Queensland Rail:** Highlighting how FRMCS principles support incremental adoption, with data capabilities introduced as an early step.

As railway communication networks transition to IP-based and cloud-enabled architectures, securing real-time communications becomes critical. Session Border Controllers (SBCs), developed by Frequentis' partner FRAFOS, play a vital role in safeguarding these environments.

Acting as a secure gateway between network domains, SBCs protect signalling and media traffic while enabling central control of routing, monitoring, and management across internal and partner

Advancing rail cybersecurity at the network edge

Dorgham Sisalem



networks. They ensure that only authorised sessions are established and shield critical infrastructures from external threats.

FRAFOS SBCs provide multi-layered protection against cyberattacks such as denial-of-service and fraud, using continuous traffic monitoring and filtering. Built-in redundancy and intelligent routing ensure high availability and uninterrupted mission-critical communications.

The FRAFOS Monitor complements this by offering an aggregated, near real-time view of user activity, based on data from the SBC, the FRAFOS Probe, and third-party VoIP components. This enables operators to analyse trends, detect irregular behaviour, verify policies, and troubleshoot efficiently.

Available for on-premises, virtualised, and cloud environments, FRAFOS SBCs ensure interoperability between legacy and next-generation systems – supporting a secure and future-ready transition to architectures such as FRMCS. <<

Security in rail: protecting what matters most

Berg San

In modern railway operations, cybersecurity is essential, seamlessly integrated into daily operations while protecting safety and availability. Its role is to reduce risk, protect safety and availability, and enable reliable services without disrupting railway processes. Given increasing regulatory pressure – including NIS2 and upcoming requirements such as the Cyber Resilience Act – security is no longer optional. Explore how Frequentis and FRAFOS jointly ensure security is built in from the start.

Why is cybersecurity becoming so important in railway communications?

Railway operations are becoming increasingly connected, integrating voice, data, and video across multiple networks. While this enables greater efficiency and flexibility, it also expands the attack surface. At the same time, regulations such as NIS2 are raising the bar for critical infrastructure protection. In safety-critical environments, any disruption can have significant operational impact – making cybersecurity a fundamental requirement.

What does “secure by design” mean in practice?

At Frequentis, security is embedded across the entire lifecycle – from architecture to operation. This includes alignment with frameworks such as NIS2 and the Cyber Resilience Act. A standards-based approach ensures systems are resilient by design, supporting both operational security and compliance.

How do Frequentis solutions protect communication networks?

A key element is the Session Border Controller (SBC), based on technology from our partner FRAFOS. It secures communication by managing signalling and media traffic between network domains. The SBC can be deployed standalone or integrated into end-to-end solutions, ensuring secure interoperability across modern railway architectures.



Why are security monitoring and visibility critical for operational resilience?

Continuous monitoring is central. The IEC 63452 standard and the NIS2 regulation require monitoring platforms that detect anomalies and security events across Information Technology (IT) and Operational Technology (OT) environments, enabling early

» Like railway signalling, cybersecurity is rarely noticed, yet fundamental to every safe and reliable journey. <<

Berg San, Security Expert, Public Transport, Frequentis AG

detection and effective incident response without affecting safety-critical operations. FRAFOS SBC Monitoring at the edge and FTS Security Monitoring at the core deliver visibility, operational security insights, and continuous monitoring across critical railway and communication infrastructures. By integrating with SIEM (Security Information and Event Management) platforms, they support rapid threat detection and effective incident response.

How is system security maintained over time?

Cybersecurity does not end with deployment. Continuous patch management protects against evolving threats and supports compliance. Frequentis follows a controlled process including validation and deployment during planned maintenance windows, safeguarding both security and availability.

What is the overall benefit for railway operators?

By embedding security into every layer and combining Frequentis' rail expertise with FRAFOS cybersecurity capabilities, operators gain a strong partner on their journey towards secure communications. This enables full flexibility to address evolving requirements at every stage. As a recognised thought leader in rail security, Frequentis supports customers worldwide in building resilient, compliant, and future-proof communication systems. <<

Closing the information gap during disruptions

Kuno Skach

How quickly can your railway turn disruption data into passenger information?

RailDataFlow connects incident detection, operations and communications to close the information gap. When disruptions occur, fast and reliable information is critical. The RailDataFlow (RDF) research project, bringing together Control Center Apps, Mission Embedded, Frequentis, App Informatics and Raaberbahn, addresses this challenge by helping railways detect incidents earlier, eliminate information gaps and provide passengers with reliable information more quickly.

The process begins with AI-powered sensors on trains and at stations that identify incidents before they escalate. Alerts are fed into CCA OnSite, where sensor data, operational systems and staff reports are combined to create a shared operational picture. This enables field teams and control centres to coordinate more effectively and resolve incidents more quickly. CCA OnTrack then manages passenger communications. Everyone involved receives the same verified information, while dedicated communication channels connect control

centres, frontline staff and neighbouring railways to maintain a consistent operational picture across networks. The final step is direct passenger communication. Travellers can subscribe to their train and receive personalised disruption updates via their preferred messaging service or email. By connecting AI-powered detection, operational coordination and passenger communication, RailDataFlow closes the information gap and ensures reliable information reaches passengers when it matters most.



RailDataFlow turns incident data into timely, reliable passenger information.

AI-Powered Incident Management for resilient railways

Christian Stimakovits



Turning operational data into faster decisions

Every day, public transport operators manage vast amounts of operational data, from infrastructure and vehicle information to incident reports.

Artificial intelligence (AI) transforms this data into actionable insights, enabling faster decision-making, more reliable services, and greater operational resilience. Particularly during incidents, AI can significantly reduce the workload on operational teams. Within the Incident and Crisis Management (ICM) platform, an AI-powered incident form automatically generates a headline, incident description, and real-time

summary. This reduces administrative effort, improves situational awareness, and supports faster, more confident decision-making. As a future partner in Europe's Rail Joint Undertaking (ERJU), CNS-Solutions & Support GmbH (CNS) is contributing to next-generation concepts for intelligent incident management. Current developments include AI-enhanced ICM capabilities and an AI workflow engine prototype designed

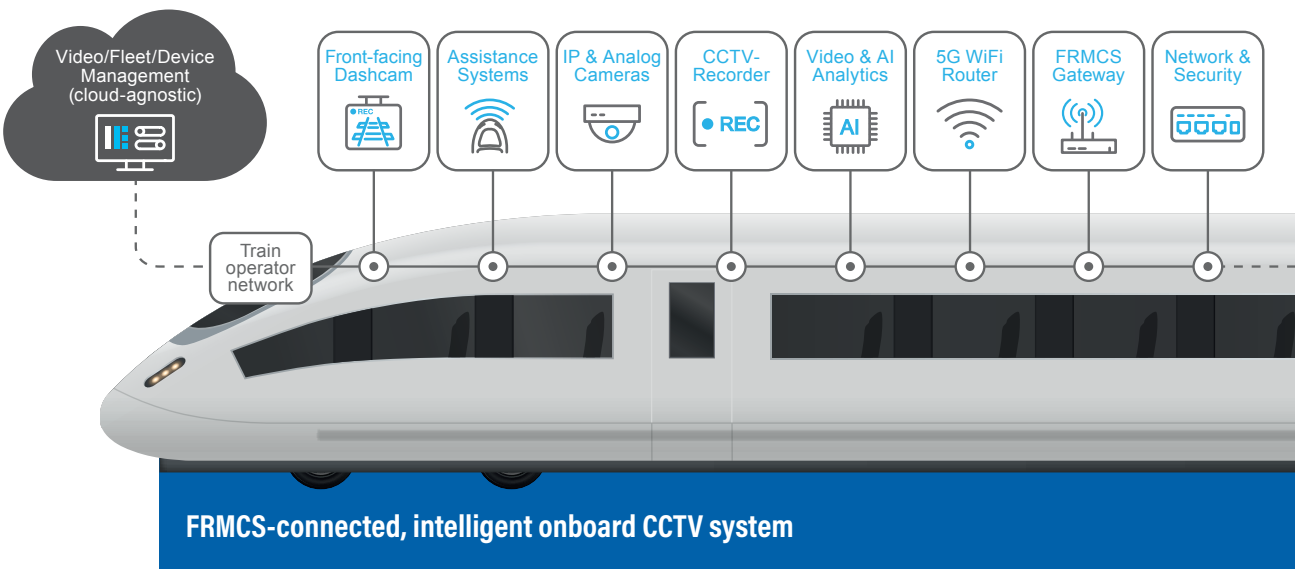
to automate operational processes. CNS is also evaluating AI-powered predictive incident prevention, using network and sensor data to identify emerging risks before they become disruptions. This will support optimised resource deployment, predictive maintenance, decision support, rail defect detection, weather impact forecasting, and early warning of potential incidents, helping operators keep services running smoothly.

FRMCS-ready CCTV system for safer, more secure journeys

Sylvia Oberauer

As the rail industry prepares for the transition from GSM-R to FRMCS, future railway applications require increasingly reliable data exchange between trains, infrastructure, and control centres.

Rail operators and GSM-R specialists therefore need FRMCS-ready onboard systems that integrate smoothly and securely into existing fleets while ensuring interoperability. This also applies to onboard systems such as intelligent video surveillance. Mission Embedded supports this transition through the implementation of the integrated Telecom On-Board Architecture (TOBA) and the development of a TOBA Box in collaboration with Frequentis. The TOBA Box consists of an FRMCS onboard gateway function and a radio function, both connected via the so-called OBrad interface. The integrated gateway function securely connects future railway applications to the FRMCS network and provides the basis for making onboard CCTV systems ready for FRMCS. Mission Embedded's intelligent on-



board CCTV system is designed for FRMCS readiness and combines, among others, rail-certified cameras, video recorders, secure communication and AI-based video analytics.

Beyond traditional surveillance, it enables intelligent functions such as available seat detection, passenger counting, and safety-critical event detection. Combined, these solutions

position Mission Embedded among the first providers of a future-proof, FRMCS-connected intelligent CCTV system for rail vehicles.

Trusted rail solutions spanning the globe

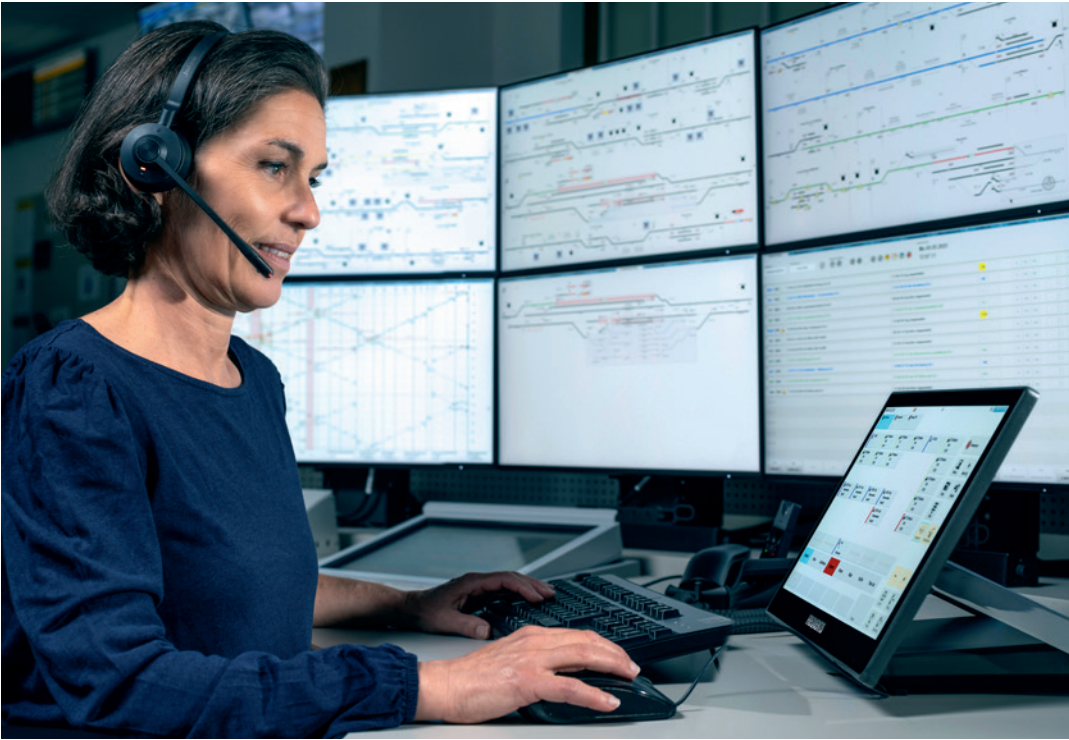
Gerald Sauprigl

With more than 10,000 dispatcher terminal positions delivered to customer control centres in over 25 countries, Frequentis solutions play a vital role in public transportation worldwide. The success story continues – discover recent projects ensuring safe, seamless public transport.



Queensland advances next-generation rail communications

Frequentis will deliver mission-critical data communication components for Stage 1 of Queensland's The Wave rail project. The Digital Radio System (DRS) package, in partnership with UGL Transport and Ericsson, supports Alstom's ETCS Level 2 implementation. The solution includes MCDATA services and trackside gateways, delivering a secure, scalable, and future-ready communications architecture that supports the evolution of digital rail operations.



Turning FRMCS vision into operational reality

As a partner in the Horizon Europe FP2-MORANE-2 research project, Frequentis is supporting the large-scale validation of FRMCS within the European Rail Traffic Management System (ERTMS) context – from laboratory testing to live field trials. In this landmark project, co-funded by Europe's Rail and the European Smart Networks and Services Joint Undertaking, Frequentis is helping to develop and test prototypes in European laboratories and under real track conditions, with a focus on interoperable control room solutions.

Many tracks, one destination

2

1

4

3

5

A

B

C

D

E

Solve the rail crossword and reveal the five-letter technology connecting this issue's stories.

Puzzle across

1. Who is your migration partner?

4. AI-powered incident management is advanced by Solutions & Support.

5. Security at the network edge starts with a Border Controller.

Puzzle down

2. Complete the name of the European validation project shaping future rail communications: FP2-.....

3. Intelligent onboard CCTV for FRMCS readiness comes from Embedded.

Solution

Transfer the letters from the highlighted boxes:

A

B

C

D

E

CROSSWORD SOLUTION: 1. FREQUENTIS 2. MORANE-2 3. MISSION 4. CNS 5. SESSION | RESULT: FRMCS

Imprint

Editor:

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com

Graphic Design:

cdc | brandcreation

Photos/Illustrations:

Frequentis AG image archive, CNS-Solutions & Support; Control Center Apps, Mission Embedded, FRAFOS, iStockphoto, Adobe Stock

The information contained in this publication is for general information purposes only. The technical specifications and requirements are correct at the time of publication. Frequentis accepts no liability for any error or omission. Typing and printing errors reserved.

The information in this publication may not be used without the express written permission of the copyright holder.