Is your backbone network ready for FRMCS?

White paper

Future Railway Mobile Communication System (FRMCS) is the anticipated wireless communications system for digital rail to succeed GSM-R. In FRMCS, the transport network is foundational as it links the RAN and core domains together. While many railway operators have migrated their backbone communications networks from SDH/SONET to IP/MPLS to support numerous rail applications, these networks fall short on multiple fronts for FRMCS transport. This paper identifies the gaps and articulates how the backbone network can evolve to meet new requirements.

Contents

The advent of FRMCS

The future of digital railways hinges on fully harnessing advanced communications to increase safety, reduce costs, improve the journey experience and achieve climate neutrality. Led by the European Railway Agency (ERA) and UIC, Future Railway Mobile Communication System (FRMCS) is the emerging global standard for railway mobile communications. With a vast portfolio of use cases, it aims to improve operations with digital capabilities. Based on their unique operational requirements and priorities, rail operators can consider different possible FRMCS deployment scenarios to accommodate different categories of use cases:

- Scenario 1: This scenario focuses on the category of critical communications use cases essential for train movements and safety or legally obligatory functions, such as emergency voice communications, shunting, presence, trackside maintenance, automatic train operation (ATO), automatic train control (ATC) and automatic train protection (ATP). This category is mission critical as railway operators strive to improve infrastructure capacity and enhance safety. It is also time critical as GSM-R is being gracefully phased out.
- Scenario 2: In addition to the use cases from scenario 1, this scenario includes the category of performance communications use cases to improve the reliability, safety and performance of the railway operation and services, such as remote condition monitoring, telemetry data transmission, pantograph and train-front CCTV.
- Scenario 3: Building upon the previous scenarios, this scenario incorporates the category of business communications use cases to enhance the journey experience, such as the passenger information display system (PIDS) and on-train passenger Wi-Fi and infotainment.

The deployment scenario chosen by a railway operator will depend on factors like available spectrum, budget, operational priorities and the desired level of digitalization. A phased approach, starting with safety-critical applications and gradually expanding to other scenarios, may be a practical strategy for many operators.

FRMCS network architecture

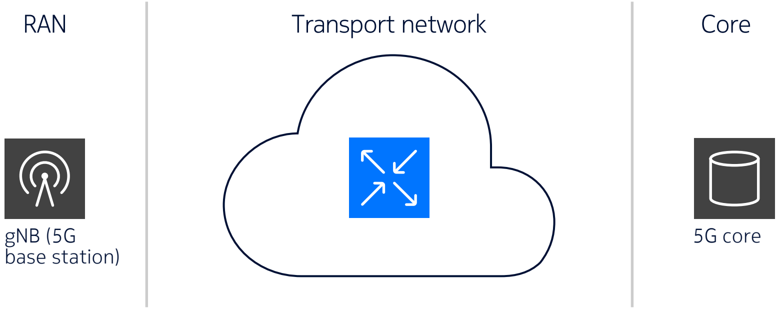
FRMCS is architected to achieve maximum flexibility by separating the railway functions from the network and radio bearer. In other words, FRMCS can use standard mobile radio technologies such as LTE, 5G or even satellite communications. However, for interoperability and economy of scale, it is also important to harmonize radio technologies across countries. Notably, the perspectives from ERA and UIC show a clear preference for 5G, a choice supported by major European railway operators.

5G is a global radio standard defined by 3GPP. A high-level 5G network architecture comprises three domains (Figure 1):

1. The radio access network (RAN) comprising base stations connecting to wireless users and devices
2. The 5G core receiving wireless data from the RAN and forwarding to applications in data centers or on-premises cloud infrastructure
3. The transport network connecting the RAN and the core.

While 5G is a wireless technology, it requires the transport network to backhaul data from the RAN to the core. Hence the transport network is considered to be the foundation of 5G. The rest of this paper will focus on 5G transport: the backbone network.

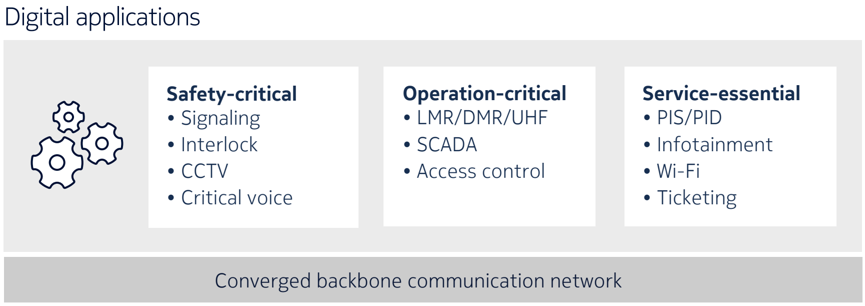
Figure 1. A high-level 5G architecture



Is your backbone network ready for 5G transport?

Deploying a dedicated 5G transport network is not feasible for many operators. A sound strategy would be to utilize a renewed railway backbone communications network (abbreviated as backbone network hereafter). Railway operators have been modernizing their backbone networks to reliably support many critical and essential rail applications (Figure 2).

Figure 2. Common digital applications used by railway operators today

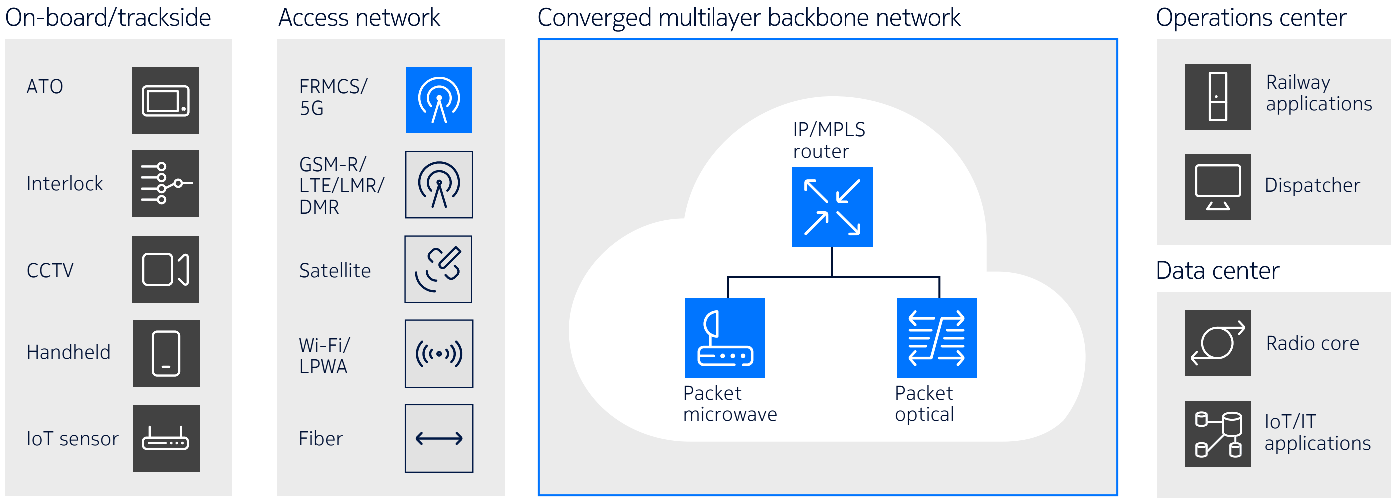


The backbone network is a multilayer secure network, comprising IP/MPLS for multiservice operating over fiber, packet optical and microwave packet for transport. The backbone is built with these four mission-critical network essentials: strong resiliency, multiservice capabilities, deterministic quality of service (QoS) and robust cyber security:

- **Multiservice capability**: The backbone network needs to support a mix of new IP-based applications such as FRMCS, signaling, interlocking and CCTV, as well as potentially TDM-based applications like GSM-R, the old SCADA system and emergency voice.
- **Strong resiliency**: Network outages can have grave safety consequences. The backbone network can leverage the full set of IP/MPLS multilayer/multifault redundancy protection for high network availability.
- **Deterministic QoS**: The backbone needs strong and flexible QoS capabilities to constantly meet the network performance requirements for each application, including applications that have stringent delay and jitter requirements, such as legacy TDM for GSM-R or ERTMS.

To extend connections throughout the expansive railway infrastructure, the backbone links with various access domains from cable wire and optical fiber to different generations of wireless technology. In the new FRMCS era, the backbone will connect to the 5G domain (Figure 3). To do that, the backbone needs to meet the new 5G transport challenges explained below.

Figure 3. The converged IP/MPLS backbone for 5G transport blueprint



5G transport challenge

High network flexibility

The introduction of 5G would most probably require more next-generation Node B (gNB) deployments across the rail infrastructure than the number of GSM-R sites. Furthermore, the continued digitalization of rail operations will increase the number intelligent rail assets and devices connected to the transport network. To support this growth, the transport network needs to scale up in its capacity to provide more network services. The transport network also needs to expand in network size and control plane to accommodate more routers and enhanced traffic engineering and load balancing capabilities to steer data flow in the network with finer granularity.

Time synchronization

Railway operators are no strangers to synchronization. They have been distributing frequency synchronization with line timing technology using SDH/SONET links and synchronous Ethernet to GSM-R and LMR base stations. However, 5G requires time-of-day synchronization for TDD base stations and advanced cellular capabilities such as Coordinated Multipoint (CoMP) transmission and reception.

However, line timing technology cannot be evolved to support accurate time synchronization. New timing over packet technology such as IEEE 1588 would be required to meet the need.

OT cloud networking

With a cloud-native architecture, the 5G core can fully harness the power of cloud computing to maximize its flexibilities and capabilities. The 5G core can be hosted in central on-premises data centers or at the regional compute facilities so that large railway networks can be closer to the 5G user equipment and wayside equipment to boost the performance of applications. This set of dedicated on-prem servers is referred to as operational technology (OT) cloud. In addition to hosting 5G core software, it can also host other critical applications such as TMS, CAD and SCADA. Moreover, as key rail applications, including interlocking and signaling, continue to evolve to benefit from the latest IT technologies, the OT cloud can enhance application performance and agility, enabling railway operators to adapt to a changing operational environment without compromising critical applications availability and performance.

Robust transport network security

Railway systems are high-value targets for malicious actors in the cyber space. As rail operations become increasingly digitalized, the attack surface of rail infrastructure and operations expand significantly. An impregnable cyber defense requires a zero-trust approach and a multilayer defense-in-depth framework across the infrastructure, network and application layers.

As FRMCS emerges as a central pillar of the digital rail infrastructure, ensuring the confidentiality, integrity and availability of FRMCS data when traversing the transport network becomes paramount. Moreover, the FRMCS system itself also needs robust security defense from cyber threats too. The transport network serves as a powerful first line of defense safeguarding the FRMCS system and data, as well as the rest of the rail infrastructure.

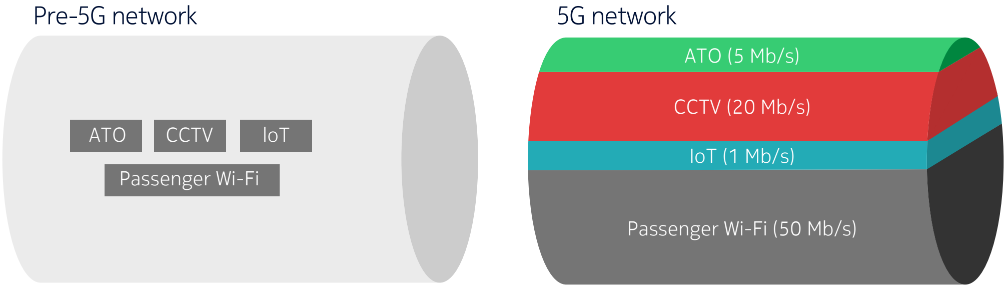
With the looming advent of quantum computers, many current network security measures will become vulnerable. To defend against the quantum threat, the transport network security posture needs to be strengthened with quantum-safe encryption.

Dynamic 5G transport slicing

The adoption of FRMCS represents a significant investment that brings immense benefits to rail operations. However, due to the immense challenge of implementing FRMCS while gracefully phasing out GSM-R without operations interruption and safety degradation, a practical deployment is likely to follow a phased approach, as outlined in the beginning of this paper.

5G supports a key capability called network slicing, which is ideally suited for this phased approach. Network slicing enables a shared wireless network to offer multiple services while consistently meeting stringent QoS requirements such as bandwidth and deterministic delay for each rail application. A 5G network slice is a virtual network partition that contains dedicated resources to support a specified set of services, applications or users with different QoS or security levels (Figure 4). For example, ATO requires stringent latency for train control, while CCTV is very tolerant of delay. Operators can provision a slice for each application with dedicated network resources. With this service-centric paradigm, 5G enables operators to harness the full power of digital applications not just on board; it can also wirelessly connect to devices along tracks, in rail stations and the switchyard, at speed and scale.

Figure 4. 5G brings in network slicing dedicated to different applications



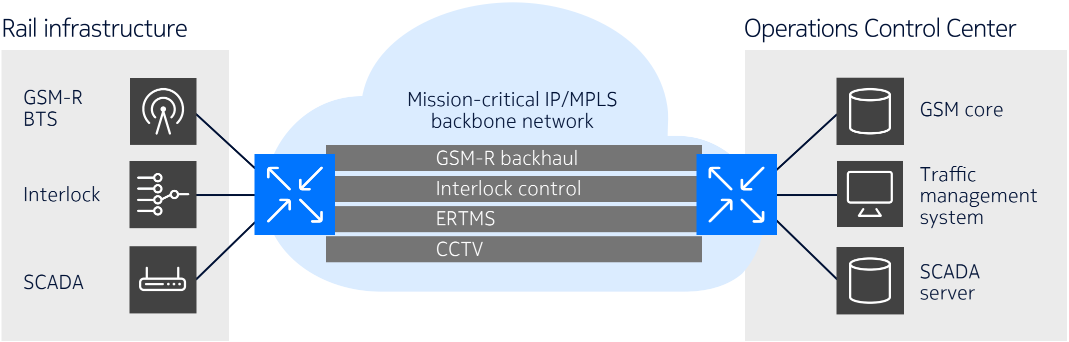
Creating a 5G slice requires orchestrating the provisioning of a slice in each of these three domains (RAN, core and transport) and seamlessly interconnecting them. The transport network manager needs to take on the role of transport slice controller as part of the end-to-end orchestration with the RAN and core domains.

Evolve the backbone for FRMCS

Harnessing the full power of segment routing in IP/MPLS transport backbone

Many rail operators have deployed IP/MPLS transport backbone networks as a multiservice communications platform supporting numerous rail applications (Figure 5). They utilize IP/MPLS network capabilities including advanced Layer 2 and Layer 3 services, deterministic QoS and traffic engineering as the foundation to their digitalization efforts.

Figure 5. IP/MPLS transport backbone today

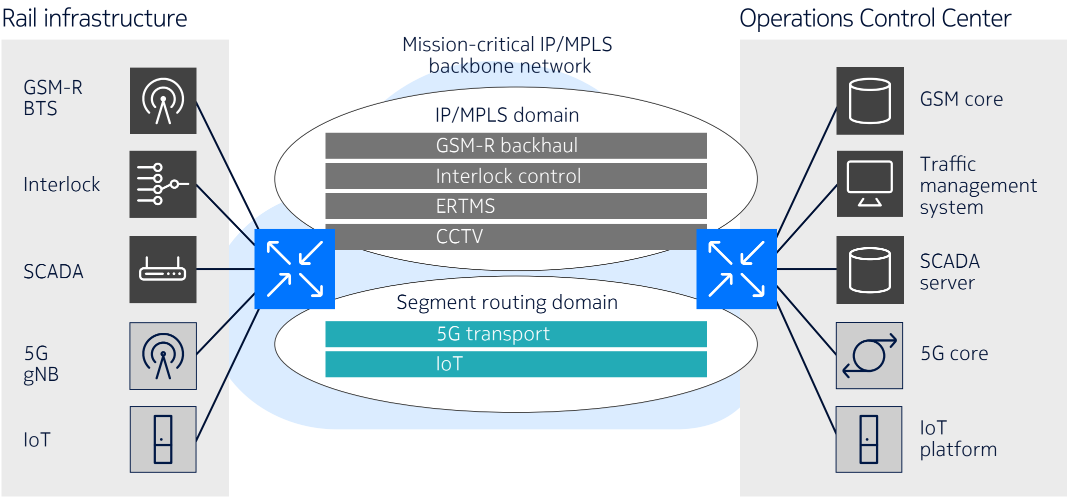


As they embrace 5G and more digital applications including IoT, they will continue to expand the network. One sound network strategy is to extend their IP/MPLS network with Segment Routing for further service scalabilities and network capabilities as they deploy FRMCS and other digital innovations (Figure 6).

Segment Routing is another approach to distribute labels to routers in IP/MPLS networks. It uses existing routing protocols (OSPF or IS-IS) already running in the network by adding segment routing extensions to distribute labels, also known as segment IDs (SIDs). By simplifying label management and distribution, this approach helps the network to scale massively for future growth. IP/MPLS network operators can seamlessly adopt segment routing, without impacting hardware requirements, routing design and existing network services, while providing simplification of path establishment, network scaling and better control of data traffic.

Additionally, combined with a Path Computation Engine function in the transport network manager, the IP/MPLS transport network now has enhanced capabilities for network path computation and traffic engineering. It enables more effective load sharing with high data flow granularity by allowing fine-grained control over packet forwarding paths. It also supports end-to-end traffic engineering for paths spanning multiple routing areas, a common design practice in large-scale networks.

Figure 6. IP/MPLS transport backbone with segment routing



Harnessing IEEE 1588v2 to distribute time synchronization for 5G RAN

The straightforward solution for time synchronization is to deploy a GNSS receiver throughout the rail infrastructure. However, this is not always feasible. Additionally, since precise time synchronization is fundamental to the 5G system, it is important to have an alternate source of timing. With the advent of IEEE 1588v2 technology, the backbone network can distribute both time and frequency synchronization everywhere.

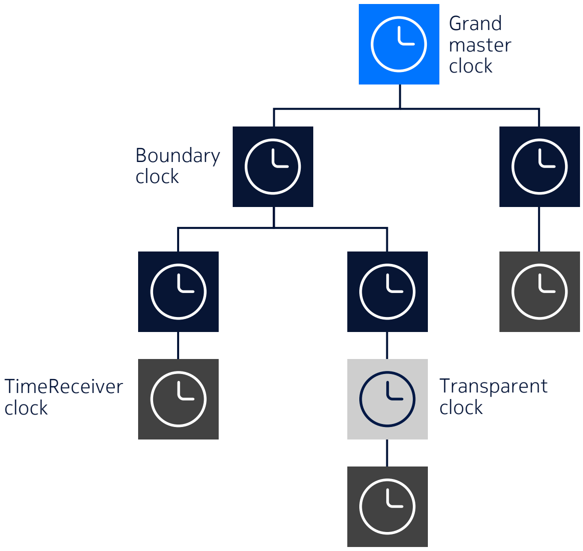
IEEE 1588v2 was originally designed for critical industrial automation. An IEEE 1588v2 synchronization topology is hierarchical topology consisting of different clock types (Figure 7):

1. Grand master clock (GMC) – The GMC connects with a primary time clock reference (PTCR), typically GNSS or atomic clock. It acts as the timeTransmitter[1], transmitting Sync messages with timestamp info to downstream clocks in the clock hierarchy.
2. Boundary clock (BC) – A BC acts as a timeReceiver[2] to the upstream BC, recovering time from received Sync messages. It then uses this timing to act as a timeTransmitter, sending its own Sync messages to BCs or timeReceiver clocks downstream. In this way, the BC bridges timing info between upstream and downstream clocks, allowing precise timing propagation through the network.
3. Transparent clock (TC) – a TC transparently forwards all received messages downstream without modifying the contents. However, to account for delays it introduces, a TC uses specialized hardware to precisely measure the residence time of PTP messages and update the timestamps accordingly to compensate for the delay it incurs. Unlike a BC, it does not recover time information nor actively participate in the timeTransmitter-timeReceiver hierarchy.
4. TimeReceiver clock – A timeReceiver clock receives PTP messages from the associated timeTransmitter clock. It uses the timing information in these messages to recover and synchronize its local time for local applications. gNBs have a timeReceiver clock to recover the time.

[1] TimeTransmitter has replaced the term master as per IEEE 1588g, 2022

[2] TimeReceiver has replaced the term slave as per IEEE 1588g, 2022

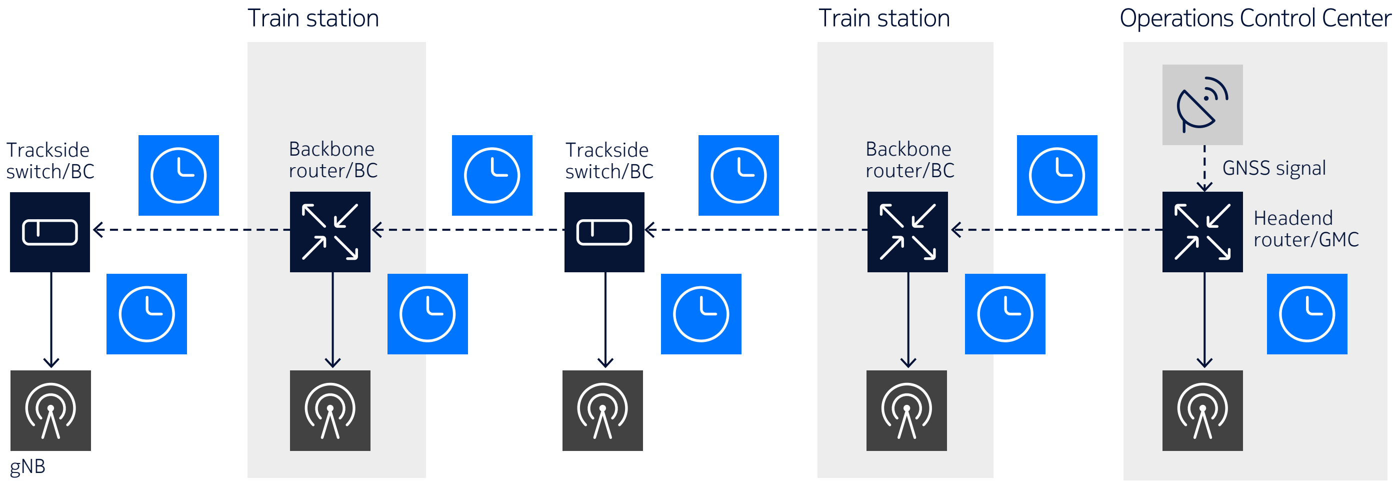
Figure 7. A hierarchical IEEE 1588v2 synchronization network topology



Railways have been distributing frequency synchronization in their legacy TDM-based backbone for a long time. A major application that needs frequency synchronization is GSM-R base stations along the track. GSM-R base stations need a frequency reference to drive RF carriers. Traditionally, frequency synchronization is distributed using synchronous physical links such as T1/E1, DS3 and OC-3/STM-1. With an IP/MPLS-based backbone network, synchronous Ethernet has become the prevalent means to distribute frequency synchronization.

With FRMCS/5G, time synchronization is needed. Rail operators need to resort to IEEE 1588v2. Backbone routers now need to support advanced 1588v2 capabilities such as GMC and BC to distribute accurate timing information required by 5G base stations. In addition, as 5G base stations (gNB in 5G terminology) would be deployed along the tracks, track switches would also need to support BC capability (Figure 8).

Figure 8. Railway 1588v2 blueprint for time and frequency synchronization

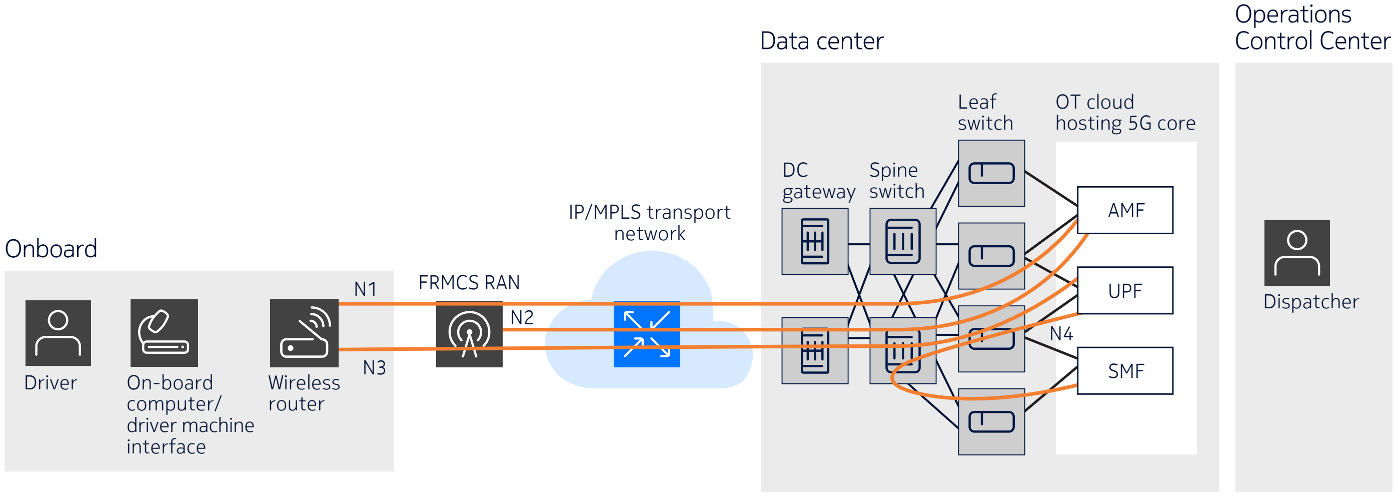


OT cloud networking for cloud-native 5G core and more[3]

Rail OT applications are increasingly developed and deployed in a cloud environment. Pioneering this trend is critical communication software such as 5G core. Due to its criticality, it is typically deployed in a set of compute resources dedicated to OT applications (generally termed OT cloud), inside the railway operator's data center. Therefore, the FRMCS backbone needs to support this new OT cloud networking use case.

Using an IP/MPLS data center gateway, the IP/MPLS FRMCS transport network can internetwork seamlessly with the data center fabric (Figure 9). Harnessing Ethernet virtual private network (EVPN) service, the backbone can interwork with the data center fabric at the Ethernet, IP, BGP and service layers, enabling network agility to support dynamic OT cloud networking connecting the RAN to the core domains.

Figure 9. E2E OT cloud networking for 5G communications

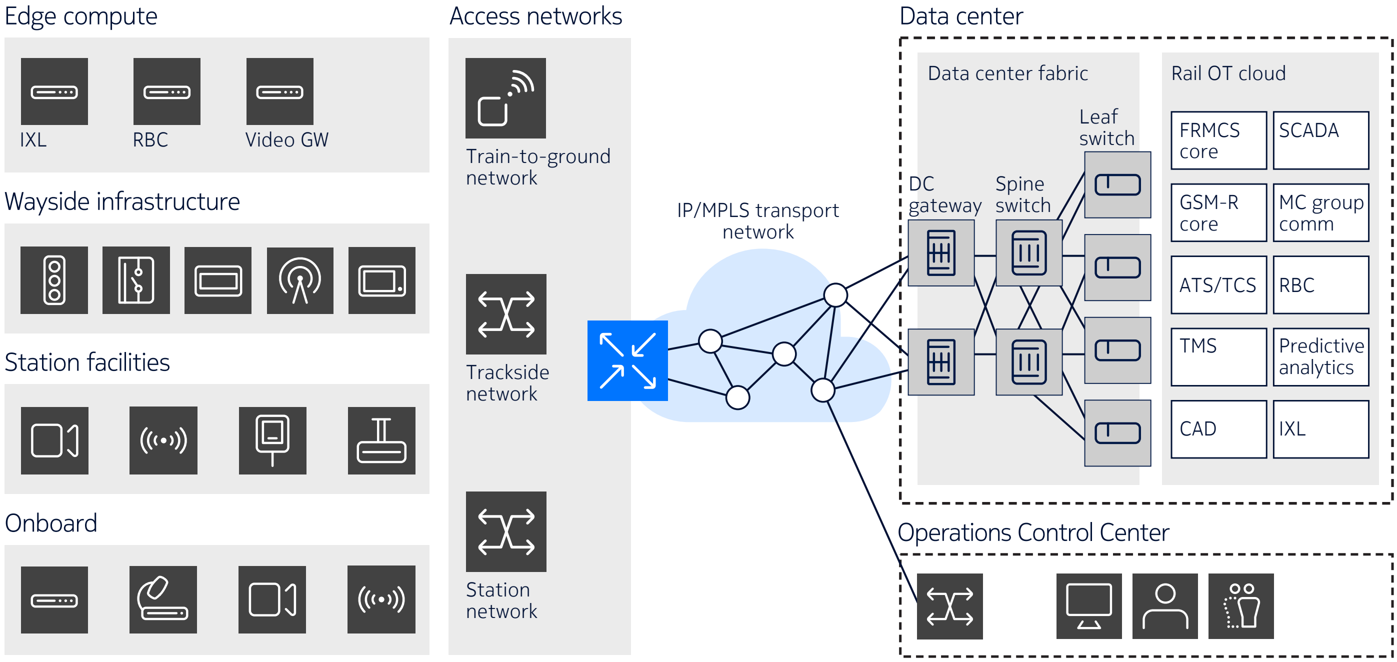


AMF: access and management mobility function
SMF: session management function
UPF: user plane function

With more OT applications including interlocking, signaling, SCADA and CAD running in a cloud environment, OT cloud networking is expanding its pivotal role of providing end-to-end communications between wayside equipment and applications inside the data center to support a wide range of applications ranging from ATO to interlocking and video analytics to ERTMS (Figure 10).

[3] Read OT cloud networking paper: https://onestore.nokia.com/asset/213221

Figure 10. E2E OT cloud networking for a wide range of digital rail applications



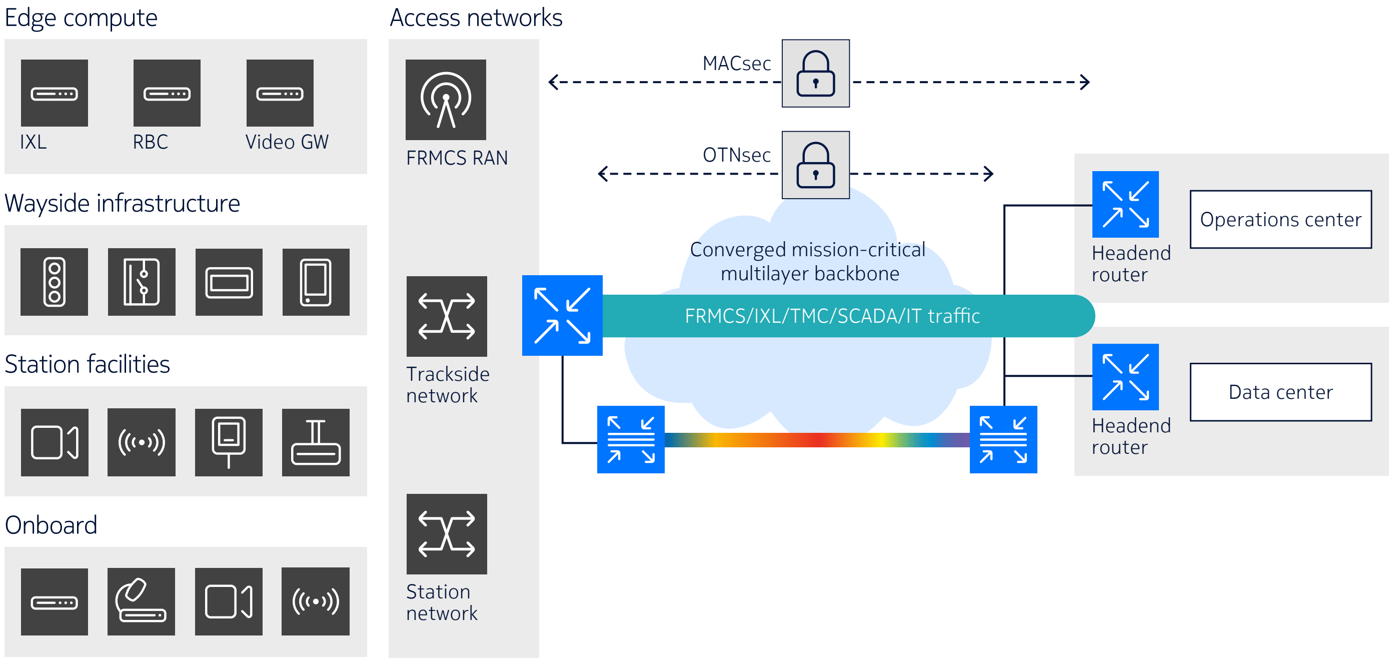
Quantum-safe network security

The wide adoption of digital technologies and rail applications significantly expands the cyberattack surface of the rail infrastructure. Furthermore, bad actors have access to more extensive resources and their attack methods are evolving to become more sophisticated. The backbone network, as the first line of cyber defense for FRMCS and railway infrastructure, needs to improve its security posture to continue effectively safeguarding the rail infrastructure. The first and foremost requirement on the backbone network is to adopt a zero-trust approach, which makes intrusion from complex to impossible, and in case it happens, it would constrain the impact of an attack to the minimum. Hitherto, encryption has been an effective means to defend against attacks including eavesdropping, man-in-the-middle (MITM) and denial of service (DoS). However, the rapid advancement of quantum computing and quantum algorithm is poised to upend the cybersecurity landscape. A bad actor running Shor's algorithm on a quantum computer can break the protection of asymmetric key encryption such as Diffie-Hellman, making the rail system vulnerable to eavesdropping. Once the data were captured and analyzed, more sophisticated attacks such as MITM and DoS attacks can be launched to disrupt railway operations and jeopardize safety.

While post quantum cryptography is still in the standardization process, rail operators can act today to protect their infrastructure. A multilayer defense-in-depth approach employing Layer 1 OTNsec and Layer 2 MACsec with symmetric encryption AES-256 can offer quantum-safe protection to thwart quantum attacks today (Figure 11)[4].

[4] Please read this paper: https://onestore.nokia.com/asset/213898

Figure 11. Multilayer defense-in-depth encryption in the transport backbone



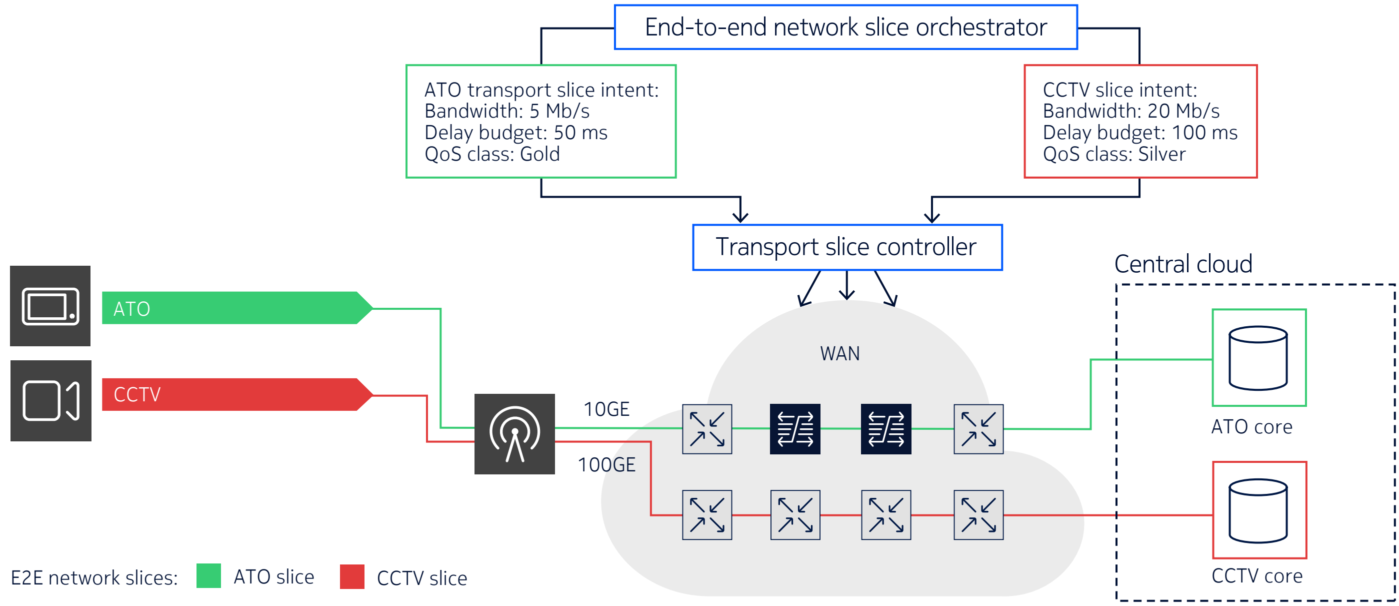
Harnessing network automation for 5G transport slicing

Transport slicing is the foundation of the end-to-end 5G slice. The transport network manager needs to take on the role of transport slice controller as part of the end-to-end orchestration. Utilizing network automation and open northbound API, the backbone becomes programmable. Through the API the orchestrator can provision a transport slice in the backbone. The orchestrator provides the backbone manager the service requirements (also known as service intent) including RAN and core endpoint locations, as well as transport QoS requirements to support different FRMCS applications such as delay-sensitive ATO and bandwidth-intensive CCTV. The backbone manager uses its intent-based network automation capability to build a dedicated transport slice, which is essentially a backbone VPN, to connect the endpoints with the right QoS settings. Since this process requires neither manual configuration nor intervention, it significantly accelerates the provisioning speed and eliminates human errors.

For example, a rail operator is to create two slices: one for ATO, which only needs moderate bandwidth but is sensitive to delay, and another one for CCTV, which is bandwidth intensive with no delay constraints. The service intent for the ATO transport slice is to minimize the number of router hops for higher availability while meeting the delay budget, while for CCTV, it is to optimize for bandwidth.

Based on this intent information, the network manager will allocate the necessary network resources to build two separate slices (green and red) in the backbone (Figure 12). For the ATO transport slice, as the intent is to minimize delay, the WAN manager will find a path with the fewest number of routers. In this case, the path selected is a 10GE link going through the DWDM optical core before reaching the far-end router. Regarding the CCTV slice, it will find a path with 100GE, which is rich in bandwidth. Both paths can fully meet the service intents.

Figure 12. Intent-based automated transport slice provisioning

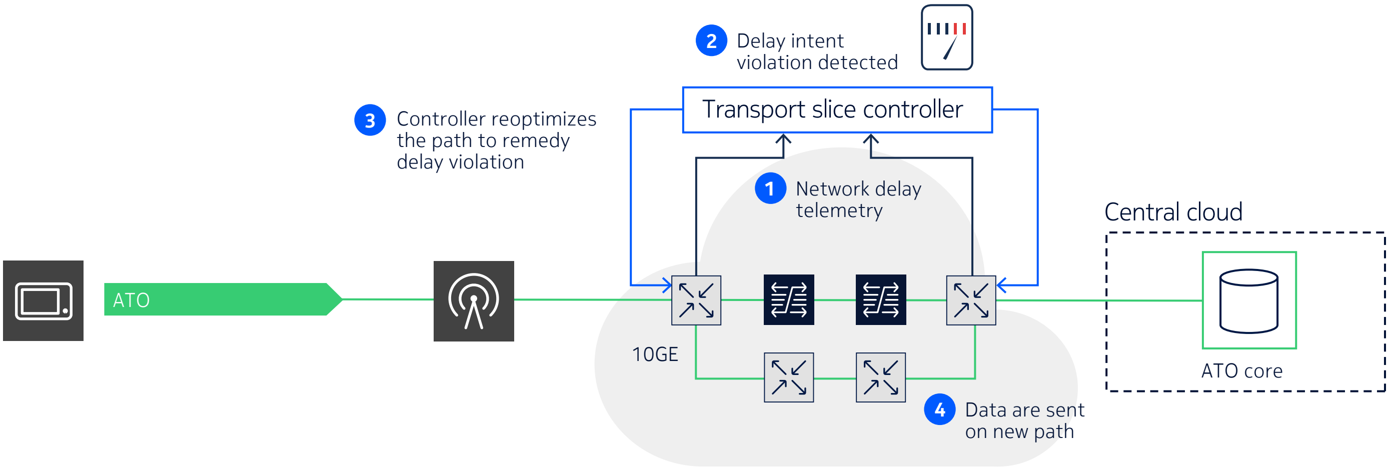


As the backbone network is dynamic and the amount of data carried in the network constantly changes to impact network performance, the transport slice needs to be responsive to consistently meet the intents. The backbone manager performs the following:

1. Continually collects telemetry data for network statistics and OAM measurement such as delay
2. Proactively monitors the delay performance
3. Reoptimizes the path if the performance falls short of the intent
4. Reroutes the data to the new path with bigger bandwidth (Figure 13).

This closed-loop mechanism of service assurance and optimization is critical to ensure constant high application performance, particularly for delay-sensitive applications such as ATO.

Figure 13. Automated assurance and optimization for transport slice


2 Delay intent violation detected
3 Controller reoptimizes the path to remedy delay violation
Transport slice controller
1 Network delay telemetry
Central cloud
ATO
10GE
ATO core
4 Data are sent on new path

Conclusion

Railway operators are embracing a broadband T2G future with FRMCS/5G to wirelessly connect rolling stocks, railway crew, wayside equipment, applications and services everywhere. The converged IP/MPLS backbone network is the foundation of 5G deployment. It needs to evolve to acquire new capabilities including network automation, multilayer management, time synchronization distribution, OT cloud networking and quantum safe networking for high performance and secure FRMCS transport.

Nokia offers a broad product portfolio that spans IP/MPLS, data center fabric, packet optical, microwave, FRMCS/5G, GSM-R, LTE, security, IoT and analytics. Complemented by a full suite of professional services (network audit, design and engineering practices), Nokia has the unique capability and flexibility to help railway operators implement their network transformation to thrive in the digital future.

To learn more about Nokia solutions for railways and the Nokia IP/MPLS portfolio, visit our Railways Backbone Solution webpage.

Abbreviations

AMF	access and mobility management function
ATO	automatic train operation
BC	boundary clock
BGP	Border Gateway Protocol
CCTV	closed circuit television
CoMP	Coordinated Multipoint
DMI	driver machine interface
DMR	digital mobile radio
DoS	denial of service
DWDM	Dense Wavelength Division Multiplexing
E2E	end-to-end
ERA	European Railway Agency
ERTMS	European Railway Traffic Management System
FRMCS	Future Railway Mobile Communication System
GMC	grand master clock
gNB	next-generation Node B
GNSS	global navigation satellite system
GPS	global positioning system
GSM-R	Global System for Mobile Communications – Railway
IoT	Internet of Things
IS-IS	Intermediate System-to-Intermediate System

LMR	land mobile radio
LPWA	low power wide area
LTE	Long Term Evolution
MACsec	Media Access Control security
MITM	man-in-the-middle
MPLS	Multiprotocol Label Switching
OAM	operations, administration and maintenance
OSPF	Open Shortest Path First
OTNsec	OTN security
PIS	passenger information system
PID	passenger information display
PTCR	primary time clock reference
QoS	quality of service
RBC	radio block center
RF	radio frequency
SCADA	Supervisory Control and Data Acquisition
SDN	software-defined networking
SMF	session management function
TC	transparent clock
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
UHF	ultra-high frequency
UIC	International Union of Railways (Union Internationale des Chemins de fer)
UPF	user plane function
VPN	virtual private network

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (July) CID210545