Reimagining train-to-ground communications

A converged train-to-ground network solution for metro-urban railways

Application note

NOKIA

Abstract

As urban populations continue to grow, metro-urban railways must also grow to meet the demand. Operators face the challenge of modernizing their infrastructure with smart digital innovations and technologies. This application note explains how the Nokia Train-to-Ground solution is a key communication component for digital rail operations.

Contents

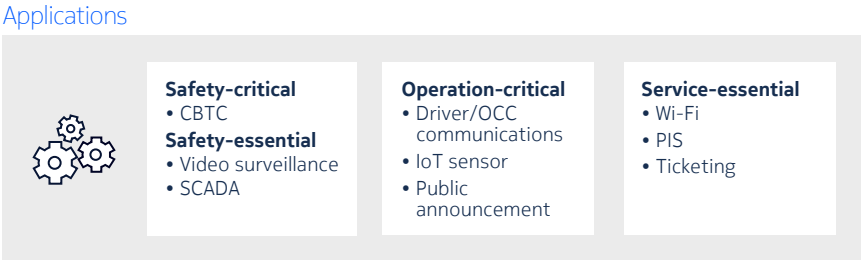
Metro-urban railways must digitalize to meet demand

According to the latest United Nations data, 68 percent of the global population will live in urban areas by 2050, up from 55 percent in 2018 and representing a net gain of 2.5 billion people.

As cities expand, demand for public transportation increases. To serve a growing ridership, it's necessary for metro-urban railway operators to increase transport capacity and improve service reliability while maintaining passenger safety.

To meet these challenges, many operators are embracing the digital rail paradigm by adopting digital applications across their infrastructure. These range from safety-critical communications-based train control (CBTC) to operation-critical Internet of Things (IoT) sensors to service essential passenger information and Wi-Fi™ (see Figure 1).

Figure 1. Metro-urban railway operators adopting digital applications



Digital rail requires a reliable, efficient and secure communications network infrastructure to connect all application subsystems and components across the railway system. Many of these applications are delay sensitive or bandwidth intensive (see Table 1), placing immense strain on the network infrastructure in general and on the train-to-ground network in particular.

Table 1. Typical on-board applications and associated QoS requirements

	Latency tolerance	Bandwidth	Reliability	Criticality
CBTC	Low	Low	High	High
Video surveillance	Medium	High	Medium	High
Driver/OCC communications	Low	Low	Medium	Medium
IoT/predictive maintenance	High	Low	Low	Medium
Passenger Wi-Fi	High	High	Low	Low

The train-to-ground network is an extensive communications network covering from train to ground (track) and beyond, all the way to the operations control center (OCC). The network carries all on-board application data and faces daunting challenges due to limited bandwidth at its wireless link as well as inherent radio link vulnerabilities. As a result, a lot of attention has been focused on the need for a network overhaul[1].

1 For a broader discussion of the rationale for rethinking the train-to-ground network, read the white paper Nokia train to ground..

Rethinking the train-to-ground network

Traditionally, when railway operators adopt a new on-board application, they deploy a new, purpose-built train-to-ground network. For example, CBTC and closed circuit television (CCTV) would use two separate Wi-Fi networks while voice communications would rely on a land mobile radio (LMR) network. Consequently, operators would need to operate multiple, disjoint train-to-ground networks to support these applications.

The radio technologies used are diverse and often proprietary. Some are even approaching end of life. Moreover, they are not interoperable.

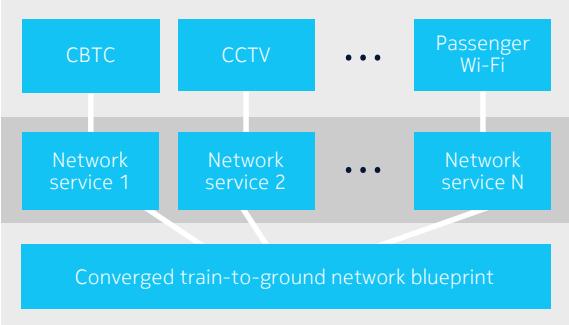
This paradigm incurs high operations costs and intensive maintenance efforts. It also hampers digital innovation because the networks have no evolutionary path to embrace future applications.

Therefore, operators should rethink their train-to-ground networks so these can support digital applications today and emerging ones tomorrow. To accelerate adoption of the digital rail paradigm, it is necessary to embrace a new train-to-ground network architecture that meets the following network requirements.

Service convergence over one network

With a plethora of applications, the old paradigm of an application-specific, purpose-built communications network is no longer feasible. Instead, a new, converged network architecture (see Figure 2) can support service convergence over one common network.

Figure 2. A converged train-to-ground network blueprint



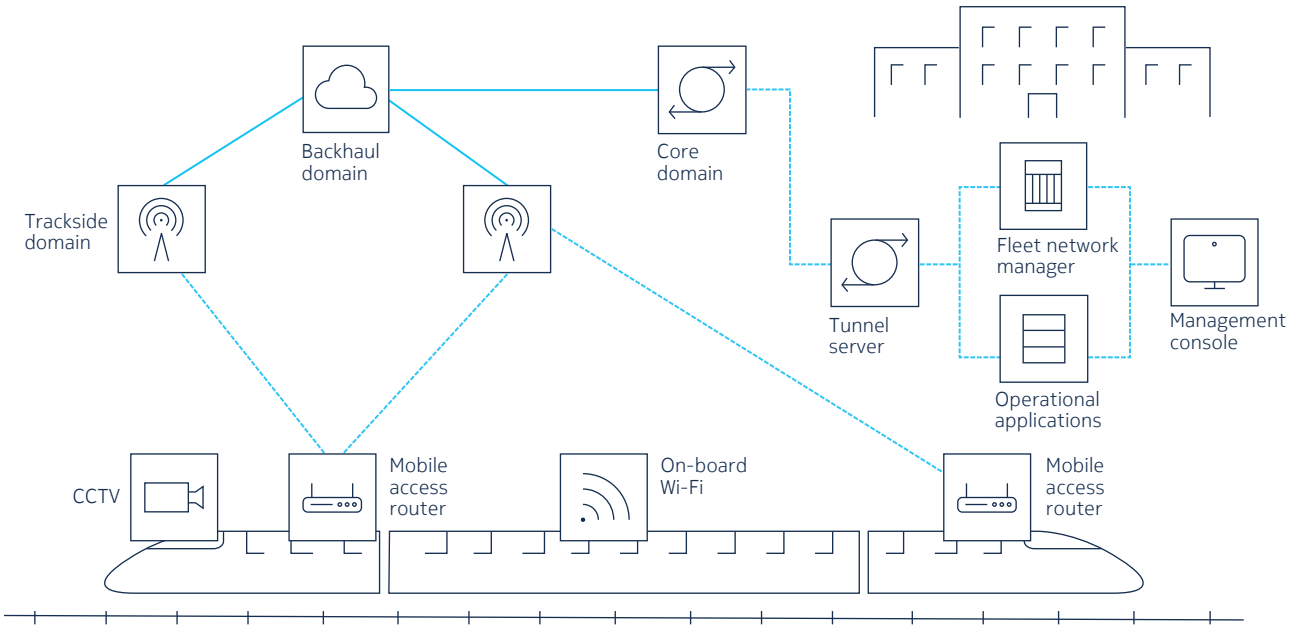
With this service-centric approach, the new train-to-ground network can offer tailored, segregated network service on an on-board mobile access router (MAR) for different rail applications, according to each application's unique quality of service (QoS) requirements.

Utmost resiliency

A communications network outage that affects safety-critical applications can disrupt or even stop train services, causing significant passenger delay and dissatisfaction as well as incurring economic loss and tarnishing a city's reputation. Therefore, operators should strive to design and deploy the train-to-ground network with utmost network resiliency.

However, the network comprises multiple domains with its network communication paths straddling the domains (see Figure 3). As a result, attaining utmost resiliency requires extensive redundancy protection along the whole path.

Figure 3. Data traversing multiple domains of the train-to-ground network



Reliable data delivery

Because of the train-to-ground network's restricted bandwidth when compared to a fiber network, it is more difficult to constantly deliver data with high QoS. Moreover, the network will need to adapt to radio link performance that is occasionally unreliable due to fading or interference. As a result, a smart, self-adapting QoS algorithm is necessary to deliver data in an assured manner.

Rigorous security

Digital transformation ushers in wide use of information and communications technology (ICT) in rail operations, expanding the attack surface and engendering new vulnerabilities. Consequently, cyber security has become a top concern.

Operators need to protect the rail infrastructure in general, and the train-to-ground network in particular, from malicious attacks. (To learn more, visit the Cyber security for railways web page.)

Scalable, real-time network management

With many trains on the move, operators need to manage and monitor many train-to-ground communication sessions simultaneously. A scalable network management system is essential to provide a complete view of the whole fleet at all times.

Evolving for future needs

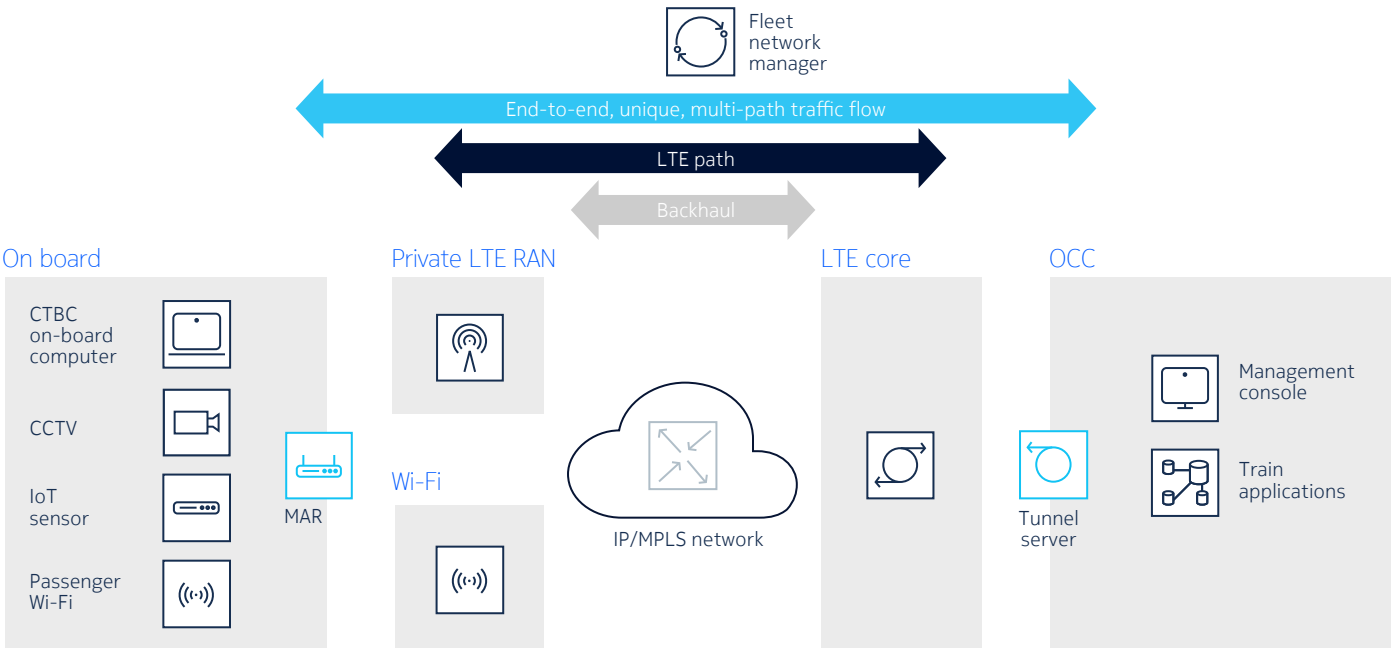
Like big data and artificial intelligence/machine learning, ICT is advancing at an unprecedented pace. Rail operators can harness ICT capabilities as they continue their digital transformation journey.

New rail applications may become even more bandwidth intensive or may require ultra-reliable low latency machine-to-machine communications. Therefore, it is important that the train-to-ground architecture can continue to evolve to acquire new capabilities for future needs.

The Nokia Train-to-Ground solution

In response to the train-to-ground architecture challenge, we offer a converged train-to-ground network solution. Based on a service-centric architecture, the Nokia Train-to-Ground solution is architected to provide multiservice capability for a plethora of applications. Resilient, reliable and secure broadband communications connect on-board equipment with the OCC (see Figure 4).

Figure 4. The Train-to-Ground solution architecture blueprint



The solution blueprint contains three architectural layers:

- Service layer
- Wireless access layer with LTE
- Backhaul transport layer

Service layer

The top, service, layer provides end-to-end routing services for unique, multi-path traffic flows provisioned between the MAR and the tunnel server.

The MAR provides segregated, tailored network services for all traffic from on-board applications and equipment. Identified by a unique IP subnet and protocol type, such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), on-board traffic can be prioritized according to the type of service assigned, ensuring that the most critical services have the highest priority.

The data is then encapsulated over an IP tunnel and transmitted over one or more radio links (LTE/Wi-Fi) managed by Nokia multi-path connectivity software.

After reaching the tunnel server, the IP tunnel is terminated and traffic is routed to application servers in the OCC, data centers and other parts of the rail infrastructure.

Wireless access layer with LTE

The middle layer of the Train-to-Ground solution architecture is an LTE path from train to trackside to the core system in the OCC. This path is provided by a private LTE system comprising the RAN and the LTE core.

The RAN is a set of LTE base stations called eNodeBs (eNBs) deployed throughout the rail system. The eNBs connect LTE user equipment (the MAR or other LTE user equipment) to the core.

If deploying a private LTE system is not feasible, another valid option is to use a Wi-Fi network or a commercial LTE service. These can also serve as the backup system to the private LTE system.

Backhaul transport layer

The bottom, transport, layer is a private IP/MPLS backbone network. The backbone network provides LTE backhaul service, connecting all the eNBs to the LTE core.

Capitalizing on the superior capabilities of IP/MPLS, including flexible Layer 2 and Layer 3 network services, deterministic QoS, multi-fault resiliency and strong security, the backbone network also links up other trackside devices and in-station equipment without degradation of train-to-ground backhaul performance.

The rest of this paper introduces the Nokia Train-to-Ground solution capabilities and how they can meet the requirements discussed in the preceding section.

Solution capabilities

The Nokia Train-to-Ground solution provides numerous capabilities, as outlined in the following sections.

Multiservice

At the core of the train-to-ground multiservice capability, which delivers service convergence, is the MAR and its multi-network aggregation manager (MNAM).

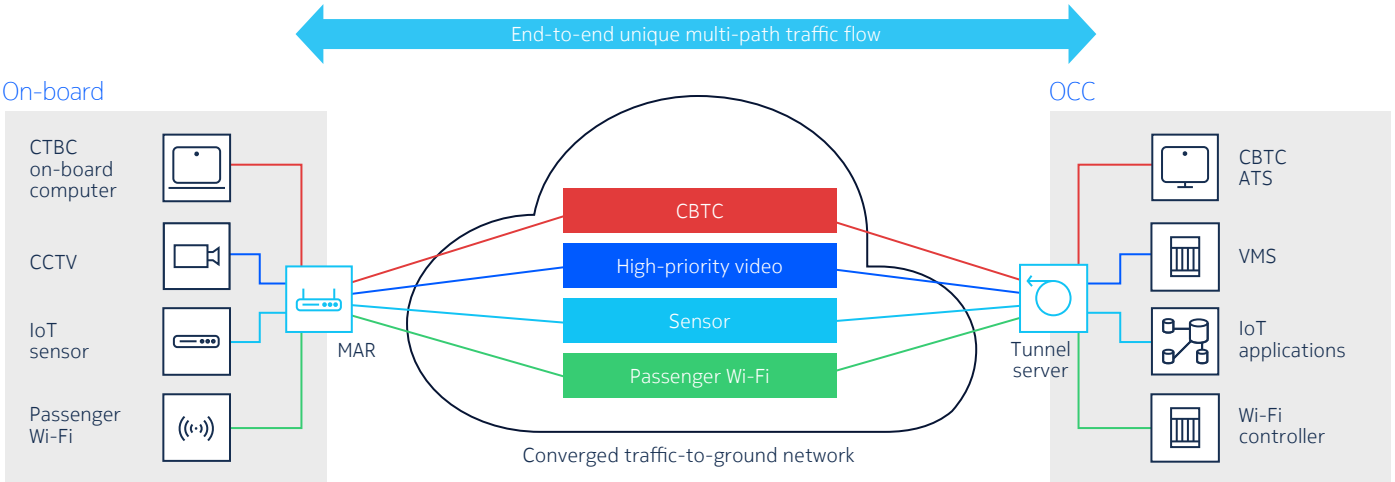
The MAR is the gateway for all on-aboard applications and provides flexible network services that segregate data with the use of virtual LANs (VLANs).

VLAN traffic is then prioritized, encapsulated in an IP tunnel, and transmitted over a set of aggregated wireless links. The IP tunnel is terminated at the tunnel server, which routes traffic to corresponding application servers.

The MNAM is an intelligent data-forwarding agent that receives data from IP and Ethernet layers and sends them out over aggregated multi-network/multipath wireless links with reliable, optimal delivery.

Data can be confined in its own VLAN service and unique traffic flow throughout the path, segregated from all other applications. This service-centric approach virtually segments end-to-end train-to-ground communications into different virtual domains, starting from the radio link (see Figure 5).

Figure 5. A multiservice train-to-ground network solution



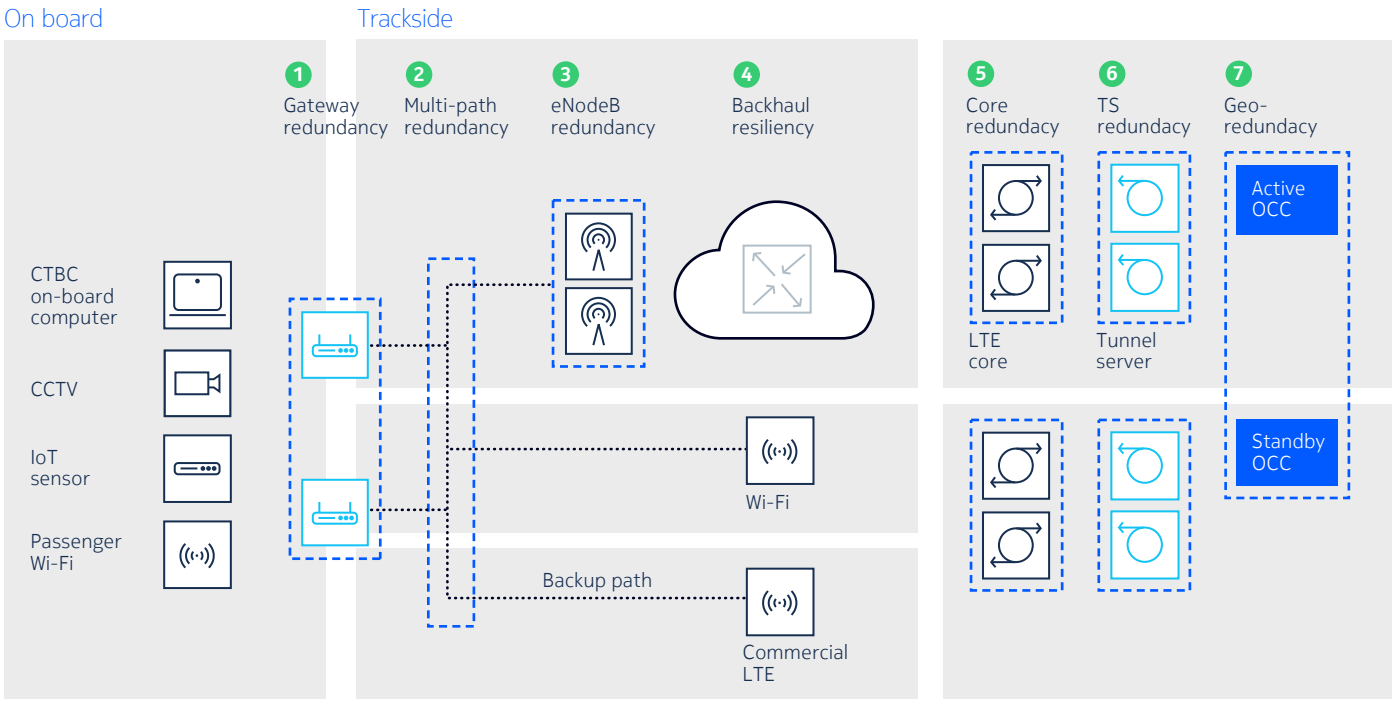
Multi-fault resiliency

Utmost resiliency for highly reliable train service is crucial for network operators because the train-to-ground network carries safety-critical and operation-critical data. If a link or a component in the path fails, communications would fail and train services would be affected. Therefore, the train-to-ground network needs to have a full set of robust redundancy protection mechanisms deployed along the communication path to withstand multi-fault failure scenarios.

The communication path begins at the MAR, continues through the RAN, then the backhaul network, and finally terminates at the tunnel server. As shown in Figure 6, the key elements in the end-to-end protection are:

1. MAR redundancy pair
2. Multi-network/multi-path radio link aggregation
3. eNB redundancy pair
4. Resilient IP/MPLS backhaul
5. LTE core redundancy pair
6. Tunnel server (TS) redundancy pair
7. OCC geo-redundancy

Figure 6. End-to-end multi-fault resiliency

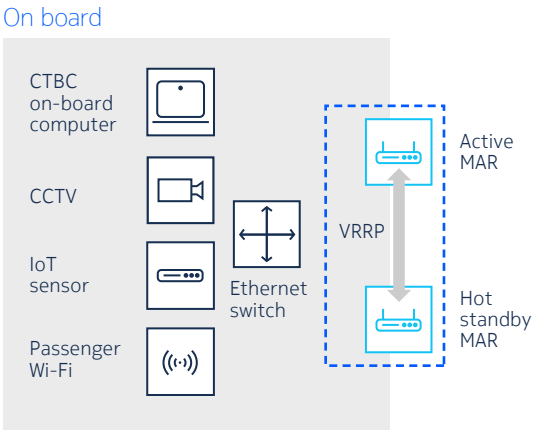


1. MAR redundancy protection

The MAR is the on-board IP gateway connecting to all on-board equipment. Deploying a redundant MAR pair (see Figure 7) is vital for high-availability IP access.

The standby MAR assumes the role of active router and starts serving as the active IP gateway when it detects that the active MAR fails.

Figure 7. Deploying MARs in a redundant router pair



The MAR redundancy pair has one active router and one standby router. They communicate using the Virtual Router Redundancy Protocol (VRRP) for redundancy switching of connected on-board equipment.

The standby MAR assumes the role of active router and starts serving as the active IP gateway when it detects that the active MAR fails.

2. Multi-path radio link aggregation

The radio link is inherently more susceptible to interference and performance degradation. Therefore, a multi-network/multi-path approach is crucial for the redundancy train-to-ground network to reliably carry on-board data, particularly safety-critical data such as from CBTC.

With multiple active radios, the active MAR simultaneously connects to multiple LTE and Wi-Fi networks. It aggregates all the radio links and can spread data across all of them. In addition to the active MAR radio links, the MNAM also aggregates the radio links of the hot standby MAR.

In this way, the two MARs form an active-active radio redundant pair, significantly increasing the number of radio links available for transmission. If one radio link fails, the MNAM dynamically adapts to minimize the service impact.

This multi-network/multi-path approach provides higher bandwidth capacity, better bandwidth utilization and stronger resiliency, improving on-board application performance.

3. eNB redundancy protection

As shown in Figure 8, there are two eNB redundancy options:

- Colocated option: The two redundant eNBs are located in the same place along the track, providing nodal redundancy protection.
- Interleaving option: The two eNBs are deployed in an alternate, interleaving manner along the track. This option provides geo-redundancy protection in addition to nodal redundancy protection. However, this option requires more installation effort because the number of installation sites along the track and power distribution points is now doubled.

Figure 8a. Colocated eNB redundancy

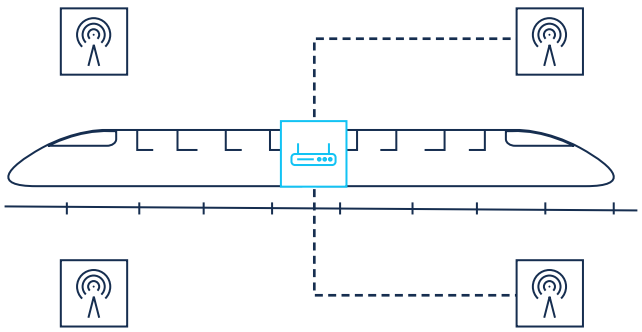
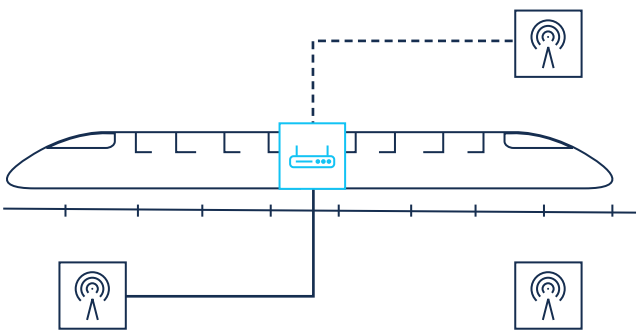


Figure 8b. Interleavng eNB redundancy



4. Resilient IP/MPLS backhaul

The backhaul network connecting all eNBs with the LTE core also serves as the communication foundation of the railway infrastructure because it links all trackside and in-station equipment to equipment and servers in the OCC and data centers.

While IP/MPLS has many resiliency capabilities, including nonstop routing, fast reroute and secondary label-switched path protection, it is crucial that the backhaul network have rich and diverse connectivity so that IP/MPLS can still reroute data — particularly surveillance video — around multiple failure points[2]. This capability is key to retain situational awareness when major disasters occur.

5. and 6. Server redundancy protection

The LTE core and the tunnel server are the gateway servers terminating all LTE paths and the corresponding unique, multi-path traffic flow from the MAR. Any server failure renders the train-to-ground communications from all trains out of service, disrupting all on-board applications and bringing train services to a complete halt.

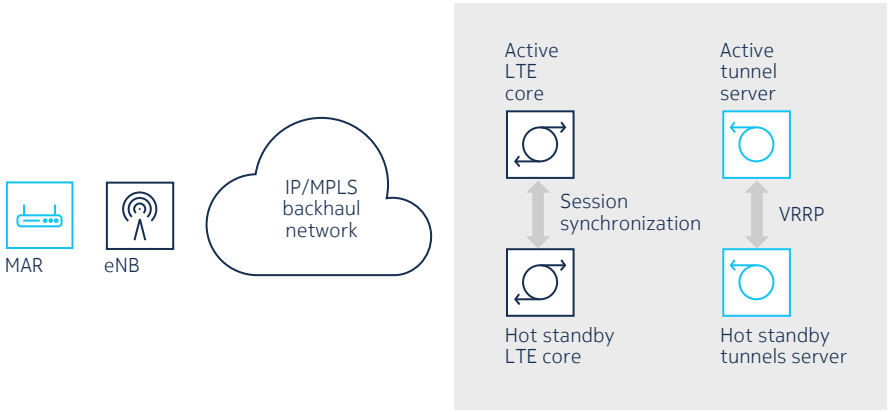
Consequently, it is necessary to support the LTE core and the tunnel server in duplex mode, with an active core and a standby core for each of them.

In typical duplex mode implementations, all communication sessions need to be reestablished during protection switching. This suspends all on-board communications until new sessions can be established, incurring operations risk during the reestablishing window.

When a large number of MARs all try to reestablish their sessions, this causes a control traffic storm. Such an event could exhaust CPU cycles and memory in the backup server as well as taking tens of minutes to restore all sessions.

With hot redundancy protection technology (see Figure 9), when the active LTE core or the active tunnel server — or both — fail, the MAR immediately starts forwarding traffic to the standby server(s) without disrupting on-board applications.

Figure 9. LTE core and tunnel server in redundancy pairs



2 For more discussion on this topic, read the application note Converged IP/MPLS networks for urban railways.

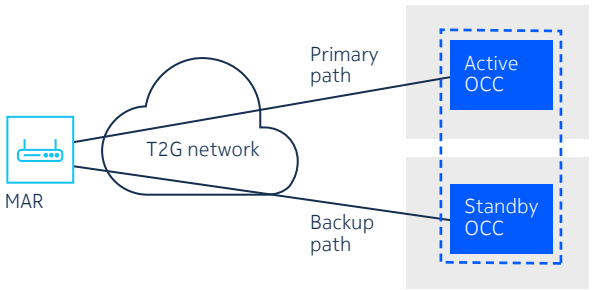
7. Geo-redundant protection of the OCC

The OCC is the nexus of rail operations where operators monitor, control and analyze the rail system operating conditions as well as respond to incidents. Therefore, it is critical that the OCC never goes out of service.

With extreme weather events such as severe flooding and storms becoming more intense and more frequent, it is crucial to have a standby OCC equipped with an identical network and application environment at a different location.

When the active OCC becomes nonoperational, all MARs send data to the LTE core and tunnel server in the standby OCC so that train services can continue (see Figure 10).

Figure 10. A geo-redundant OCC pair



Smart, application-aware QoS

The MAR does not just simply route on-board data to the multi-path radio links. It has a unique, smart and application-aware QoS scheduler for reliable, optimal, priority-based data delivery.

By examining the VLAN header, protocol number, Differentiated Services Code Point (DSCP) and UDP/TCP ports, the MAR classifies IP flows of all on-board applications into a priority class. The MAR then schedules data transmission according to the classified priority.

To attain reliable, optimal delivery for critical applications such as CBTC, the MAR can replicate the CBTC data over all radio links.

The far-end tunnel server forwards the first copy of CBTC data received to the application server for lowest delay. If packet loss or corruption occurs during transmission over the lowest-delay radio link, the tunnel server uses the uncorrupted copy received from other radio links to ensure that CBTC stays up and running.

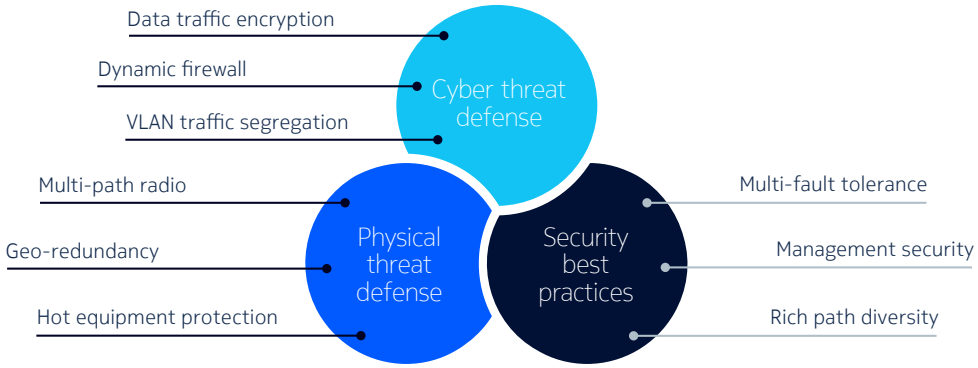
Strong network defense[3]

As railway infrastructure becomes connected and its operations depend heavily on ICT, the attack surface expands significantly. The attacks range from cyber attacks trying to eavesdrop, interrupt and infiltrate, to physical attacks that sabotage communications facilities and sever cables.

3 For more information about network security, read the white paper Cybersecurity for railways.

Secure by design, the Nokia Train-to-Ground solution is an integral part of a defense-in-depth framework to protect from cyber and physical threats (see Figure 11). The MAR offers a wide range of security capabilities.

Figure 11. Comprehensive network security with the Nokia Train-to-Ground solution



With segregated VLAN routing services, all application data is confined to its own service domain, thwarting attackers from moving laterally from one application domain to another. For example, a compromised on-board camera cannot be used as a springboard to go on to the CBTC domain.

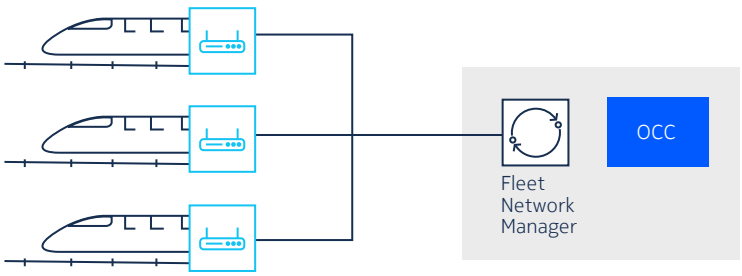
In addition, with standards-based encryption featuring secure socket layer (SSL) and IP security (IPSec), plus dynamic firewall filtering and probe packet insertion, the MAR protects the traffic from eavesdropping and man-in-the-middle attacks.

Coupled with the redundant protection schemes discussed earlier in this section plus security best practices, the converged train-to-ground network effectively deters cyber and physical attacks, enabling the rail system to operate without compromise.

Fleet Network Manager

The Nokia Fleet Network Manger (FNM) maximizes operations synergy by managing end-to-end train-to-ground communications remotely (see Figure 12).

Figure 12. FNM managing fleet communications



In addition to configuration plus event and alarm management, the FNM manages all train-to-ground communications on a fleet level from the OCC by collecting real-time data usage, operating statistics and performance information. The FNM also supports geo-fencing.

The FNM provides a complete overview of communication service performance of the entire fleet or any specific set of trains.

Evolving towards the future

The converged Nokia Train-to-Ground solution is a platform for continued future technology adoption. LTE is an open-standard, 3GPP-based wireless technology deployed globally with a vast and diverse ecosystem to enrich its use cases.

As urban-metro railway operators embrace new applications to attain more oversight, such as trackside monitoring, the LTE network can evolve to support standards-based Narrowband IoT (NB-IoT and LTE for Machines (LTE-M) technologies to connect trackside sensors.

Operators can also harness mission-critical push-to-talk (MC-PTT) and push-to-video (MC-PTV) capabilities to migrate legacy LMR-based applications over the train-to-ground network.

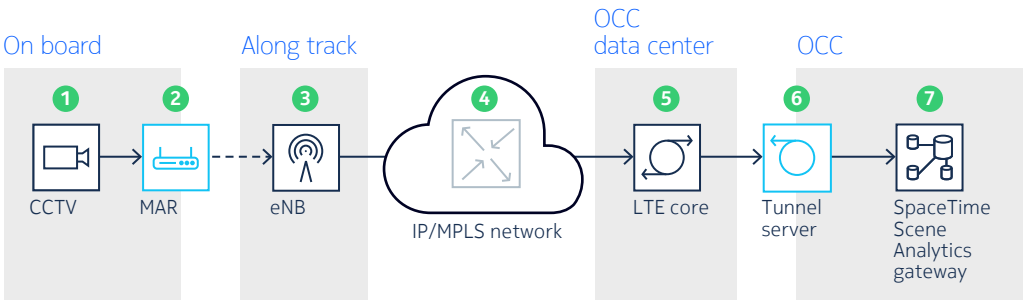
As operators look ahead to new applications that require ultra-low latency or are bandwidth intensive, the LTE system can gracefully evolve to support 5G radio as needed.

The IP/MPLS backhaul network can also evolve to unleash segment routing capability to facilitate seamless network-cloud networking in the future.

Putting everything together

Figure 13 shows the end-to-end journey of on-board CCTV video data that is to be analyzed by an intelligent Nokia SpaceTime Scene Analytics gateway.

Figure 13. The train-to-ground journey of video data: An end-to-end view



The data is processed and “touched” by many network elements, as outlined in the following steps.

1. The CCTV camera sends IP video data to the MAR.
2. The MAR classifies the application data and harnesses its MNAM capability to transmit optimally over wireless links.
3. The eNB, upon receiving the wireless data, sends it to the backhaul IP/MPLS router over an Ethernet interface.
4. The router transports the wireless data to the LTE core equipment.
5. The LTE core equipment processes the wireless data and forwards it to the tunnel server.
6. The tunnel server terminates the VPN tunnel and routes the data to the destined SpaceTime Scene Analytics gateway.
7. The Scene Analytics gateway analyzes video data in real time to detect anomalies.

Any deficiency in the path affects on-board application performance. Therefore, a well-designed, end-to-end train-to-ground network architecture is essential to consistently deliver data with assurance.

Summary

Metro-urban railway operators are at a critical juncture. Urban populations will continue to grow at a rapid pace in the foreseeable future. This growth poses great challenges to operators to provide reliable, sustainable and safe urban transport.

To meet these challenges, operators need a modernized infrastructure with smart digital innovations and technologies. The converged Nokia Train-to-Ground solution is a key communication component for digital rail operations.

Nokia has served railway operators for more than 30 years. We are a leader in the Global System for Mobile Communications – Railway (GSM-R) standard and have been actively involved in the development of the Future Railway Mobile Communication System (FRMCS) standard.

Nokia also provides leading mission-critical communications solutions in 5G, LTE, GSM-R, IP/MPLS, packet optical and microwave transport. Complemented by a full suite of professional services, including integration, audit, design and engineering practices for wireless and wireline networks, Nokia has the unique capability and flexibility to help operators lay the tracks for a digital rail future.

Learn more

To learn more about Nokia solutions for railways, visit the following Nokia web pages:

- Mission-critical transmission networks for railways
- Railways

Abbreviations

ATS	automatic train system
CBTC	communications-based train control
CCTV	closed circuit television
CPU	central processing unit
eNB	eNodeB
FNM	Nokia Fleet Network Manager
ICT	information and communications technology
IoT	Internet of Things
IP	Internet Protocol
LAN	local area network
LMR	land mobile radio
LTE	long term evolution
MAR	mobile access router
MNAM	multi-network aggregation manager

MPLS	multiprotocol label switching
OCC	operations control center
PIS	passenger information system
QoS	quality of service
RAN	radio access network
SCADA	supervisory control and data acquisition
TCP	Transmission Control Protocol
TS	tunnel server
UDP	User Datagram Protocol
VLAN	virtual LAN
VMS	virtual management system
VRRP	Virtual Router Redundancy Protocol

About Nokia

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

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners 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: (February) CID210507