ETSI TR 103 459 V1.1.1 (2019-01)

Rail Telecommunications (RT);
Future Rail Mobile Communication System (FRMCS);
Study on system architecture

Reference
DTR/RT-0011

Keywords
architecture, railways

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Railway Telecommunications (RT).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Since the first studies on the successor to GSM-R have been launched by UIC in 2012, the railway community has been considering how to meet railway requirements with a future proof and flexible radio communication system.

The rail needs are defined in the User Requirements Specification (URS) delivered by the UIC Project Future Rail Mobile Communications System (FRMCS) [i.1]. Those requirements are the basis for the development of the GSM-R successor, in the form of individual and technology independent applications.

The present document is a study on system architecture which describes a potential high-level functional architecture, investigating how the rail requirements can be met. The need for interworking with the legacy GSM-R system during the transition period to its successor is also considered. The document presents a high level grouping of FRMCS features for each major system function. In addition, it investigates different technical options and solutions to address those requirements.

A comparison of technical solutions (including 4G versus 5G) in the context of typical rail applications is presented. While no conclusion can be drawn, it is understood that several building blocks defined in 3GPP can be used to address most of the requirements. However, it is acknowledged that a gap analysis should be undertaken to identify which rail features require a potential standardization effort in ETSI. In addition, a mapping of applications to system functions, and a mapping of system functions to subsystems and network elements would be needed to refine the FRMCS architecture.

Introduction

GSM-R has been a great success not only in Europe where more than 100 000 Km of railway tracks are daily operated through GSM-R but also worldwide, and this number will double within the next years due to the on-going installations of this technology all over the world.

As the needs of the railways are constantly evolving, and that the telecom standards evolution remains dependent of the telecom industry evolution cycles, with an end of support for GSM-R planned by 2030 onwards, UIC launched in 2012 the first studies for a successor to GSM-R, pertinently named Future Rail Mobile Communications System (FRMCS). The UIC Project then concretely delivered the new User Requirements Specifications (URS) [i.1] focusing mainly on rail communication needs as a basis for the development of the GSM-R successor.

The present document is a study on system architecture, investigating how the requirements from the URS can be met; keeping in mind that interworking with the legacy GSM-R system is necessary during the transition period from GSM-R to its successor.

1 Scope

The present document:

1) Provides a reference model of FRMCS system architecture from a functional point of view.

2) Provides a high-level description of the functions that address FRMCS requirements (as specified by FRMCS URS and Use Cases).

3) Defines internal and external boundaries of the FRMCS system (e.g. transport versus applications, external systems, external networks, etc.).

4) Defines further potential steps.

The present document describes a potential high-level functional architecture, as well as a high level grouping of FRMCS system functions and mapping towards requirements.

In addition, the present document investigates different technical possibilities, e.g. 3GPP building blocks, to address the requirements of the FRMCS system. Some of the currently developed techniques, e.g. Service Based Architecture (SBA) or Software Defined Networks (SDN), have not been considered in the present document and might be included in a future release.

Finally, the present document identifies the next steps to ensure the complete definition of the FRMCS system.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] UIC FRMCS URS v3.0: "User Requirements Specification".

[i.2] Recommendation ITU-T I.112: "Vocabulary of terms for ISDNs".

[i.3] ETSI TS 124 010: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface layer 3; Supplementary services specification; General aspects (3GPP TS 24.010)".

[i.4] 3GPP TR 22.889: "Study on Future Railway Mobile Communication System".

[i.5] IEC 61375-1:2012: "Electronic railway equipment - Train communication network (TCN) - Part 1: General architecture".

[i.6] ETSI TS 136 300: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300)".

[i.7] ETSI TS 123 501: "5G; System Architecture for the 5G System (3GPP TS 23.501)".

[i.8] NGMN Alliance 5G White Paper v1.0.

[i.9] ETSI TS 123 401: "LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401)".

[i.10] IETF RFC 7866: "Session Recording Protocol".

[i.11] ETSI TS 103 389: "Railway Telecommunications (RT); Global System for Mobile communications (GSM); Usage of Session Initiation Protocol (SIP) on the Network Switching Subsystem (NSS) to Fixed Terminal Subsystem (FTS) interface for GSM Operation on Railways".

[i.12] ETSI TS 133 180: "LTE; Security of the mission critical service (3GPP TS 33.180)".

[i.13] ETSI TS 122 278: "LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278)".

[i.14] 3GPP TR 28.801: "Telecommunication management; Study on management and orchestration of network slicing for next generation network".

[i.15] ETSI TS 122 261: "5G; Service requirements for next generation new services and markets (3GPP TS 22.261)".

[i.16] ETSI TS 138 211: "5G; NR; Physical channels and modulation (3GPP TS 38.211)".

[i.17] P. Marsch et. al (editors): "5G System Design - Architectural and Functional Considerations and Long Term Research", Wiley, May 2018.

[i.18] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

FRMCS client: client enabling the use of the FRMCS communication services and railway services for the railway applications including railway services

FRMCS communication services: services enabling the exchange of information (control plane) between FRMCS Users and/or external systems to manage communication between two or multiple FRMCS Users by using the capabilities of the FRMCS transport system

FRMCS gateway: gateway coordinating and managing FRMCS Users access to the FRMCS Transport Services offered by the FRMCS System

NOTE: The FRMCS Gateway may support the FRMCS Proxy and the Legacy Conversion functions.

FRMCS proxy: function interacting with the FRMCS communication services and acting in the place of railway applications for user plane purposes

FRMCS supporting and enabling services: services providing functions to enable communication services for FRMCS users based on the 3GPP defined mission critical services and other enabling functions such as location and recording

FRMCS system: telecommunication system conforming to FRMCS specifications, consisting of FRMCS transport system and FRMCS communication services

FRMCS transport system: system encompassing the amount of terrestrial and/or non-terrestrial radio access sub-systems consisting of 3GPP access and/or non-3GPP access, wireline access, the core sub-system having multi-access capabilities and the User Equipment

FRMCS user: human or machine making use of FRMCS communication services

FRMCS user identity: unique identity associated with a single or multiple FRMCS user and can be complemented by alternative addressing schemes

legacy conversion: function that provides conversion towards legacy interfaces (e.g. V.24 serial interface)

NOTE: The Legacy Conversion provides encapsulation/de-capsulation for control and user plane data as well as the necessary conversion of the physical interfaces between legacy GSM-R UE and FRMCS. The Legacy Conversion is based on FRMCS Proxy functions to use the FRMCS Communication Services.

non-MCX enabled: subset of the FRMCS System that provides simple connectivity by using the FRMCS Transport System and does not interact with the FRMCS communication services and railway services

on-board transport system: system providing on-train only transport services and enables the interaction with the FRMCS Gateway and the FRMCS communication services where applicable

proxy: person or entity acting or being used in the place of someone or something else

railway applications: applications that provides critical, performance and business related railway functionality using communication services offered by the FRMCS System

railway services: railway specific services, using enabler services including 3GPP building blocks necessary for railway applications

reference point: conceptual point at the conjunction of two non-overlapping functional groups

NOTE: See Recommendation ITU-T I.112 [i.2].

train communication network: sub-system of on-board transport system that aggregates various train backbones

user equipment: equipment that allows a user access to transport services via 3GPP and/or non-3GPP accesses

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
4G	Fourth Generation Mobile Networks
5G	Fifth Generation Mobile Networks
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
APN	Access Point Name
ARP	Allocation and Retention Priority
AS	Access Stratum
ASCI	Advanced Speech Call items
ATO	Automatic Train Operation
AUSF	Authentication Server Function
BGCF	Breakout Gateway Control Function
BICN	Bearer Independent Core Network
CN	Core Network
COTS	Commercial off-the-shelf
CUPS	Control and User Plane Separation
DCN	Dedicated Core Network
DCN-ID	Dedicated Core Network Identity
DECOR	Dedicated Core Networks
DN	Data Network
DRB	Data Radio Bearer
EAP	Extensible Authentication Protocol

eDECOR	enhancements of Dedicated Core Networks
EIRENE	European Integrated Railway Radio Enhanced NEtwork
eNB	evolved NodeB
EPS	Enhanced Packet System
ETCS	European Train Control System
E-UTRAN	Enhanced UMTS Terrestrial Radio Access Network
EVC	European Vital Computer
FA	Functional Addressing
FEEI	Fachverband der Elektro- und Elektronikindustrie Bereich Technik
FFS	for further study
FQDN	Fully Qualified Domain Name
FRMCS	Future Rail Mobile Communications System
FRMCS	Future Railway Mobiel Communication System
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GSM-R	Global System for Mobile communication for Railways applications
GUMMEI	Globally Unique MME Identifier
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber server
IEEE	Institute of Electrical and Electronics Engineers
IMS	Internet Multimedia Subsystem
IN	Intelligent Network
IoT	Internet of Things
IP	Internet Protocol
KASME	Key transferred from the HSS to the Access Security Management Entity
KMS	Key Management Server
LAA	Licensed-Assisted Access
LDA	Location Dependent Addressing
LTE	Long Term Evolution
LTE-U	Long Term Evolution-Unlicensed
LWA	LTE-WLAN Aggregation
MAC	Media Access Control
MC	Mission Critical
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCVideo	Mission Critical Video
MCX	Mission Critical services
MGCF	Media Gateway Control Function
MGW	Media GateWay
MME	Mobile Management Entity
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MORANE	MObile radio for RAilway Networks in Europe
NAS	Non-Access Stratum
NEF	Network Exposure Function
NGMN	Next Generation Mobile Network
NR	New Radio
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
OTT	Over The Top
PCF	Policy Control Function
PCRF	Policy and Charging Rule Function
PDCP	Packet Data Convergence Protocol
PDU	Packet Data Unit
PLMN	Public Land Mobile Network
PLMN-ID	Public Land Mobile Network Identification
PSTN	Public Switch Telephone Network
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Nework
RAT	Radio Access Technology

RBC	Radio Block Centre
REC	Railway Emergency Call
RLC	Radio Link Control
RRC	Radio Resource Control
S/P-GW	Serving Packet GateWay
SBA	Service Based Architecture
SBC	Session Border Controller
SDAP	Service Data Adaptation Protocol
SDF	Service Data Flow
SDN	Software Defined Networks
SGSN	Serving GPRS Support Node
SIEM	Security Information and Event Management
SIL	Safety Integrity Level
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMF	Session Management Function
SS7	Signalling System No 7
SST	Slice/Service Type
TAU	Tracking Area Update
TC	Technical Committe
TCN	Train Communication Network
TCP	Transmission Control Protocol
UDM	Unified Data Management
UE	User Equipment
UIC	Union Internationale des Chemins de Fer
UPF	User Plane Function
URS	User Requirements Specification
USDM	User & Service Data Management
UTRAN	UMTS Terrestrial Radio Access Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

4 High level approach description

4.1 Introduction

The FRMCS functional architecture objective is a clear separation between FRMCS Communication Services and FRMCS Transport System to enable bearer flexibility/multi-access support. The FRMCS Transport System is embedded within the FRMCS Communication Services, which provide a generic interface for Railway Applications to support the communication between FRMCS Users. Railway Services address specific railway operational requirements, which are not covered by FRMCS Communication Services.

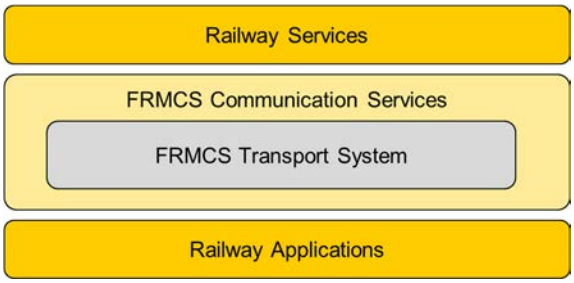

Figure 1: High Level functional layers

The FRMCS architecture can be vertically split into Railway Applications using FRMCS Communication Services and other, which are Non-MCX enabled.

Railway Applications, which use functions from the FRMCS Communication Services (see Figure 1) start with registration, authorization and request communication services from the FRMCS System. These Railway Applications are supported by the FRMCS Communication Services and utilize related functionality, including addressing (functional aliases), access and admission control, location, prioritization management and application interworking.

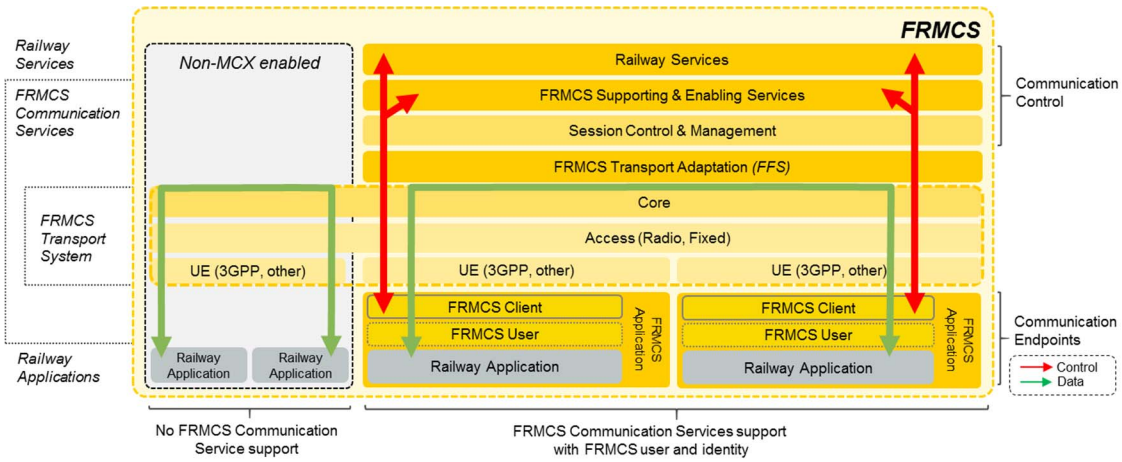

Figure 2: Reference model of the FRMCS System

The FRMCS Transport System consists of the core and the access services encompassing various access system which provide connectivity to the User Equipment (UE). FRMCS Communication Services obtain from FRMCS Transport System the required communication priority, latency and reliability. Non-MCX enabled applications rely on FRMCS Transport services and have no interaction with FRMCS Communication Services.

NOTE 1: A commercial off-the-shelf camera, which requires only bearer connectivity, obtains FRMCS Transport Services and communicate with its destination application or user.

NOTE 2: Train Control Applications can be MCX enabled or Non-MCX enabled (refer to clause 6.1).

4.2 FRMCS functional architecture

This clause focuses on the applications and functionality that only obtain FRMCS Communication Services. In other words, the Railway Applications that use FRMCS Communication Services are associated with a FRMCS Users and identities.

The FRMCS System consists of different functional layers to support Railway Applications as well as supporting the interworking with external systems, including legacy systems or supporting sub-systems.

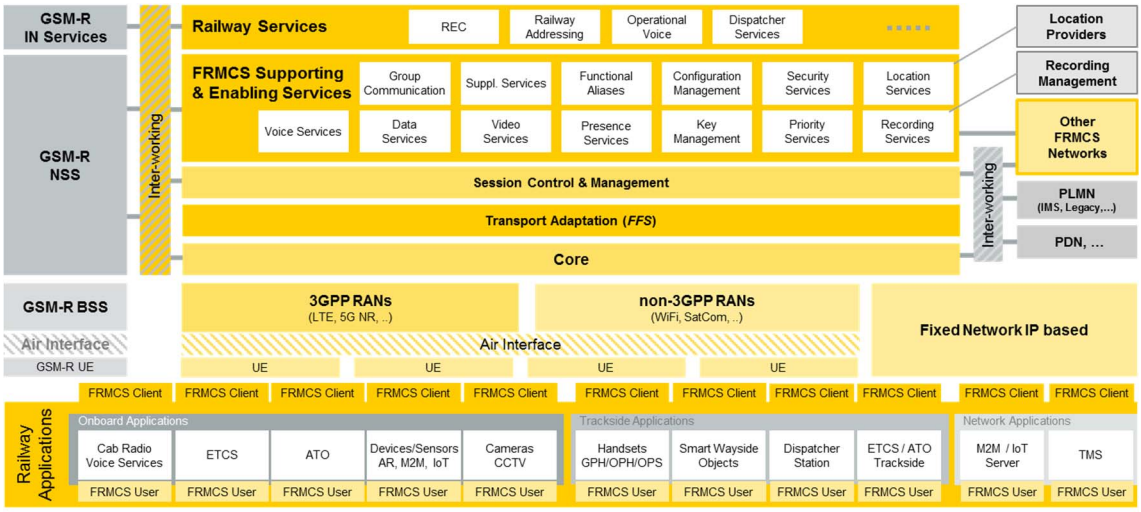

Figure 3: FRMCS functional architecture

The core and the access services including the relevant UEs form the FRMCS Transport Service. The core is based on 3GPP functions and provides the ability to integrate the access service consisting of various access system (3GPP or non-3GPP) as well as fixed broadband access systems.

FRMCS Communication Services obtain FRMCS Transport Services, which provide transport adaptation. In addition, the transport adaptation functionality may provide transparent and flexible communication services with different transport bearers provided by one or more access networks (alternative, redundant or aggregated bearer usage). The main purpose of the FRMCS transport adaptation functionality is to manage and combine one or more transport bearer services for an application communication session and make the underlying transport layer details, network changes or handovers completely transparent to the Railway Applications layer.

NOTE 1: The transport adaption functionality is FFS.

Session control & management layer is part of the FRMCS Communication Services layer and is aligned with 3GPP, e.g. IMS. It manages the application session control, orchestrate communication requests and invoke services necessary for user and service data management functions as well as e.g. policy management and control.

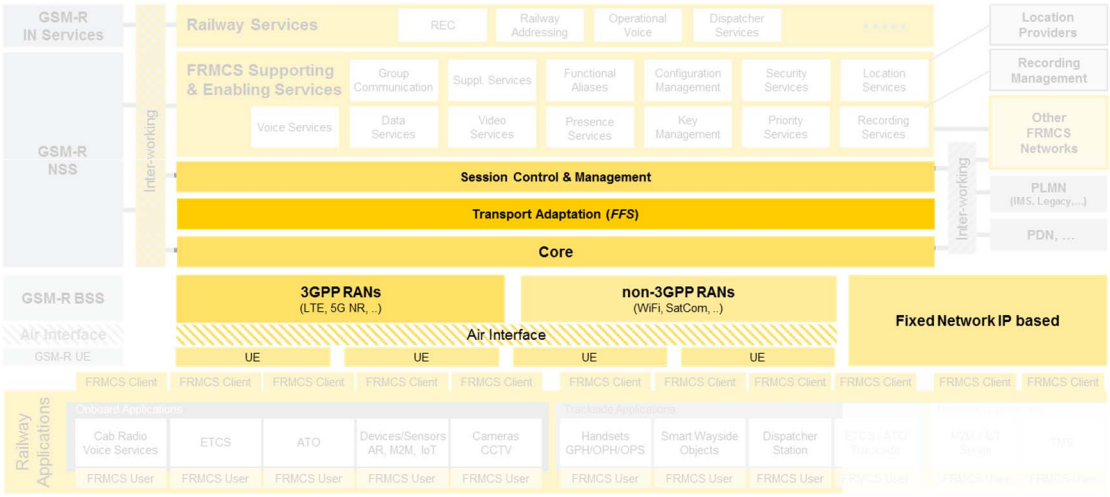

Figure 4: Service control & management, core and transport (access network) layers

The FRMCS Communication Services also support services that are based on the 3GPP Mission Critical Services and other supportive functionality as such as location management, recording or interworking with other external systems. The 3GPP MCX framework provides point-to-point and group communication for voice, data and video. In consequence, the MCX framework is the heart of the FRMCS Communication Services to manage Railway Applications. The 3GPP MCX framework functions support FRMCS User registration and flexible addressing including i.e. functional aliases, location management and communication logging.

In addition, the 3GPP MCX framework requires extension for supplementary services (ETSI TS 124 010 [i.3]) and the capability for recording voice and data sessions, which might be defined by upcoming 3GPP releases or need to be captured in ETSI TC RT specifications. FRMCS recording functionality requires further analysis to assess the implications of end-to-end encryption requirements as outlined in the discussion clause 6.6.

NOTE 2: Further requirements to the 3GPP MCX framework to support Railway Applications and Use Cases in 3GPP TR 22.889 [i.4] are FFS.

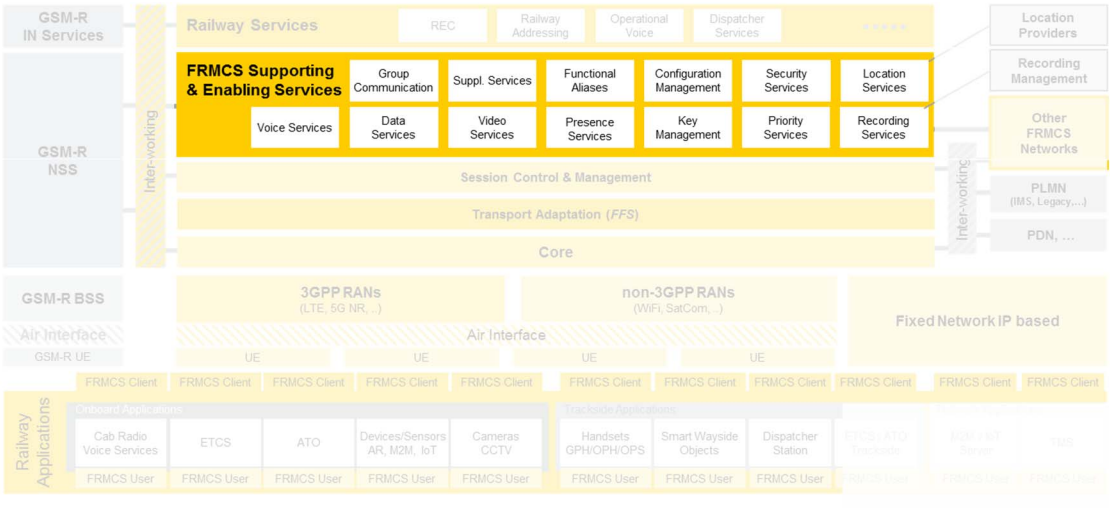

Figure 5: FRMCS Service layer covering the MCX framework

The Railway Services in Figure 6 describes specific service logic and control functions beyond the functionality offered by the 3GPP MCX framework. For example, the railway emergency call interacts with various 3GPP MCX functions, including group communication, functional alias, user positioning to affiliate to a group communication.

The Railway Applications can reside within the train (on-board) or along the tracks (trackside) or deployed centrally as network Railway Applications. Railway Applications (MCX enabled) are associated with FRMCS Users and identities and use services offered by the FRMCS Communication Services. A Railway Application can request a communication session or become part of a point-to-point or group communication session with other Railway Applications.

NOTE 3: The communication requirements between the ETCS application on-board (EVC) and the associated trackside application (RBC) can be based on an on-board Railway Application exchanging information with the relevant Railway Application trackside. The on-board Railway Application would obtain FRMCS Communication Services.

NOTE 4: The interworking between Railway Applications and non-MCX enabled Railway Applications is FFS.

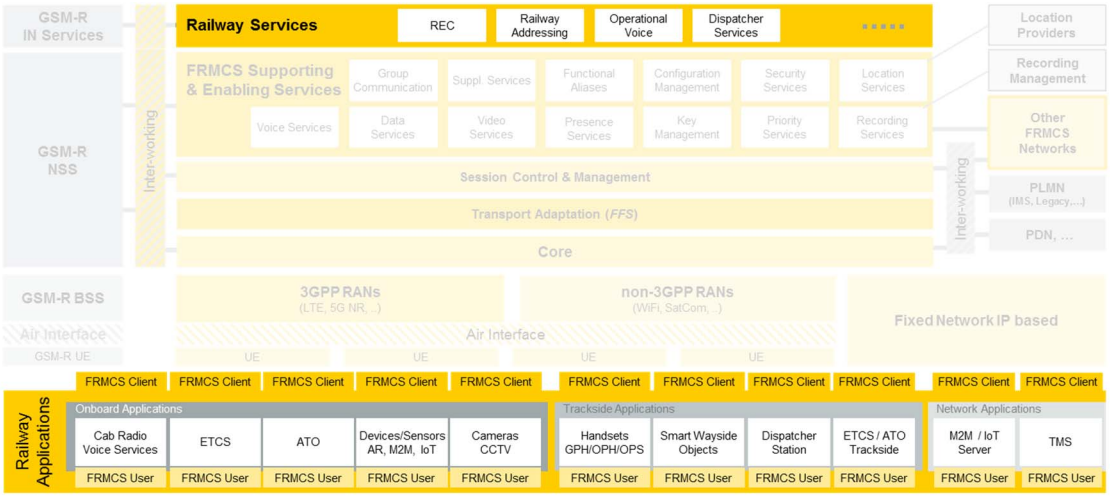

Figure 6: Railway Services and Railway Applications

NOTE 5: Railway Addressing can also cover Location Dependent Addressing or Follow Me functionalities.

Finally, the FRMCS System foresees also functionality to support the interworking with GSM-R systems. In detail, the interworking supports the bearer connectivity including transcoding or media mixing for voice and encryption/decryption as well as call control interactions and services interworking for supplementary services, EIRENE services (e.g. functional addressing alignment with FRMCS functional alias).

In addition, the FRMCS System enables the interconnection and usage of communication services between FRMCS based networks for roaming users. In addition, it also supports communication services with other external systems, including public mobile and fixed line operators networks, as well as using railway supporting functions including railway specific location information providers (e.g. train describer databases).

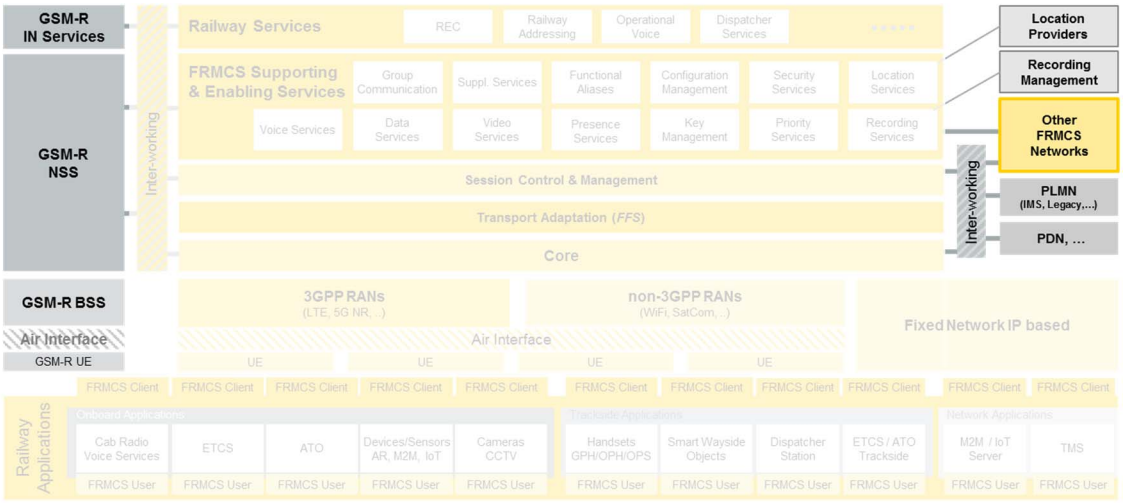

Figure 7: External systems

4.3 Functional Example

The following example should help to clarify the functional scope and purpose of the different layers in the FRMCS reference architecture. The Railway Emergency Calls (REC) represents a complex service that leverages a number of support functions as well as involving different Railway Applications and the associated FRMCS Users into a communication session.

The REC call is in the example below initiated by the train driver registered as FRMCS User with the train driver FRMCS User Identity. The service invocation is validated by the MCX framework and passed on to the Railway Service for REC. The REC service is invoking different functions from the FRMCS Service layer to create a group communication session with other FRMCS Users in the area.

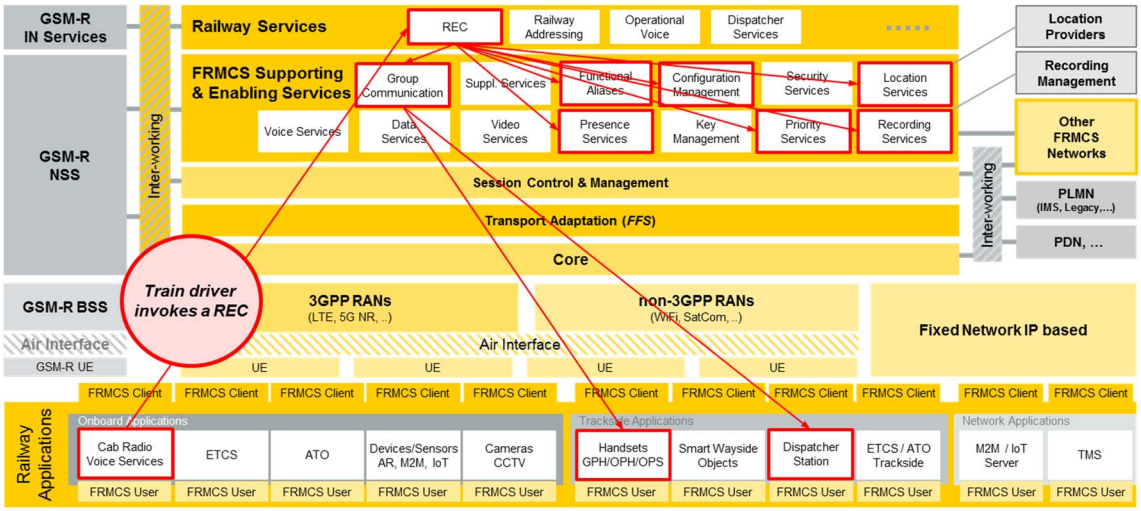

Figure 8: Railway Emergency Call Functional Example

4.4 On-board architecture

The on-board reference architecture represents the on-train FRMCS subsystem and covers the following functional components:

- On-train Railway Applications supporting voice, data and video services and requiring FRMCS Transport Services, and possibly natively including an FRMCS Client or utilizing a separate FRMCS Client to also use FRMCS Communication Services beyond the FRMCS Transport Services.
- On-train FRMCS Gateway (or multiple gateways, see below) to coordinate the FRMCS Transport and Communication Services between Railway Applications on-board, and between Railway Applications on-board and trackside.
- On-train User Equipment (UE) (or multiple UEs, see below) which supports the FRMCS Transport services for one or more radio access networks.

It is expected that multiple FRMCS Users and/or Railway Applications share the same on-board to trackside transport capabilities. The FRMCS Gateway provides the physical adaptation and encompasses the means to manage the on-board and train to ground communication and transport service needs.

For improving availability, the on-board network could support more than one FRMCS Gateway. The number of FRMCS gateways depends on the integration requirements on the train.

The FRMCS Gateway handles the FRMCS Transport Services and provides access to the one or more on-train Railway Applications through the IP-based on-board communication network. The on-board communication network should be compatible to the train communication network (TCN) as defined in IEC 61375-1 [i.5] and is not in the scope of the FRMCS functional architecture.

The on-board reference architecture is depicted in Figure 9.

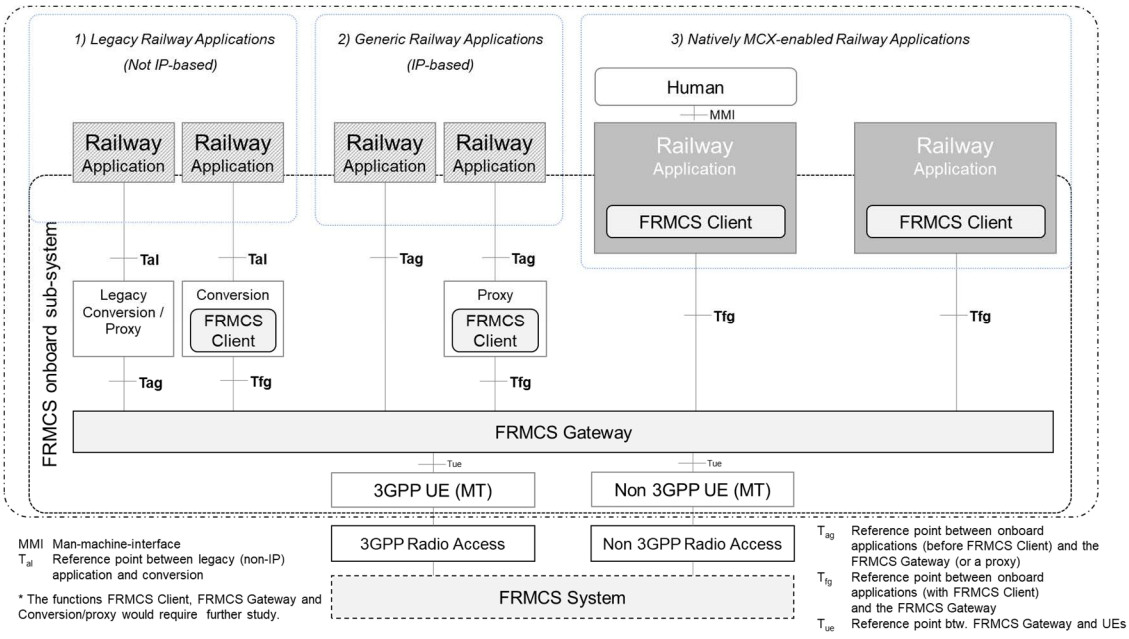

Figure 9: On-board reference architecture

The Railway Applications are here categorized into the following groups (shown from left to right in Figure 9):

1) Legacy Railway Applications, which rely on non-IP interfaces and protocols, for example a V.24 serial interface. These require a Legacy Conversion to IP and Proxy functionality to use FRMCS Transport Services. As shown in Figure 9, Legacy Railway Applications may or may not involve an FRMCS Client, if these should explicitly use, e.g. Functional Aliasing or other FRMCS Communication Services beyond FRMCS Transport Services.

2) Generic Railway Applications supporting IP transport services and connectivity (e.g. IP based IoT sensors or COTS IP cameras). Similar to the Legacy Railway Applications, these may or may not make use of an FRMCS Client if FRMCS Communication Services beyond FRMCS Transport Services are to be used.

3) Railway Applications which are natively MCX-enabled and which already inherently include an FRMCS Client.

5 Mapping of FRMCS System Functions

Table 1 provides an example of high level mapping and grouping of the features (authentication, addressing, access control, etc.) required by FRMCS applications onto System Functions (Radio, Core, Session control, MCX, Railway Applications, UE, etc.).

Table 1: Example of high level mapping and grouping of features

System Function	related features
MC Client	MCX functions, authentication/authorization, Application interface
UE (terminal)	Arbitration, authentication, location, Pro-Se, inter RAT service continuity
Radio	Priority handling, arbitration, location, resource management, ciphering
Core	Authentication, authorization, data transport, bearer handling, QoS, encryption
Session Control	Session control, addressing, routing, QoS, security
MC Common	Addressing, functional alias, presence, config, priority, arbitration
MC Voice (MCPTT)	P2P voice, voice group communication, assured voice communication
MC Data	P2P data, data broadcast
MC Video	P2P video, group video
User & Service Data Management (USDM)	Access to the data, authentication, authorization, service profile, configuration storage
Recording	Session recording, (voice, data, etc.)
Location	Location information interface, location collection/query
Interworking	Bearer interworking, service interworking
Multi-Bearer control & management	Selection, aggregation and management of different bearers and radio networks
Network Management	Manage user & service data, billing request, network configuration, network management, recording control & management

6 Discussions

6.1 FRMCS/MCX support for Railway Applications

6.1.1 General considerations

The FRMCS System is relying on the MCX functionality to provide voice services including point-to-point and group communication to railway users. For data centric Railway Applications the question can be raised, if applications should utilize the MCData functions and features or if such applications simply require a plain data pipe, which is provided by the core and transport layers of the FRMCS architecture.

It seems undisputable, that data centric applications, which require group communication would benefit significantly from the MCX framework functions to exchange data between all members of a group based on centralized configuration and dynamic group associations. Examples range from railway emergency alert and shunting data communication to trackside warning system, etc. Furthermore, the discussion around using the MCX framework for data communication seems comparable to the discussion how voice point-to-point calls are managed. TC RT agreed that point-to-point voice calls should be handled by the MCPTT framework and handled as private calls. For coherency reasons the same might apply for data communication service handling.

The discussion could even be extended, which would lead to the question where the boundaries of the FRMCS System are and what attributes are required to make a Railway Application an FRMCS application.

6.1.2 Arguments for loose coupling of data centric Railway Applications

Railway Applications like ETCS or ATO do not necessarily rely on a FRMCS User (and FRMCS equipment e.g. EVC) on-board as well as the associated FRMCS User trackside, because these applications can use a plain point-to-point data connection without the MCX framework leveraging only the FRMCS core and transport functions. Especially already deployed on-board applications which will likely not be changed cannot be adapted to use the FRMCS service layer functions. ETCS or ATO can rely on a FRMCS User, if there are requirements for Functional Addressing (FA) or location based addressing (LDA), but operators should be able to use them without the MCX framework. In FRMCS Functional Aliasing will only be available within the MCX framework.

The whole FRMCS has two parts that are MCX enabled and non-MCX enabled. There are use cases which do not require the MCX framework e.g. ETCS/ATO, critical video (without role management). The whole FRMCS System will be still aware of all the data and voice communications (independently in which sub-network it is) and can ensure the prioritization via QoS classes within the core and radio subsystems.

6.1.3 Arguments for integration of data centric Railway Applications

From a single data application perspective (e.g. ETCS) the benefits and additional value to integrate MCX functionality might look limited and cause a more complex solution, because each application could rely on a data pipe with a defined QoS profiled provided by the system, in more detail by the core and transport subsystems.

From a system perspective, the FRMCS system should be aware of all applications using the system to allow control and management of functions and enable the admission and prioritization not only on the bearer level but also at the application level. As example, the QoS use cases in 3GPP TR 22.889 [i.4] include a requirement for arbitration of application and the feedback capability to inform applications, which are pre-empted by the system. In conclusion, a pure QoS based approach on the transport layer does not support the admission and pre-emption requirements for FRMCS.

Furthermore with the support of MCX capabilities the applications receive an identity in the system, which is used to give the applications access to the system, make the application entities addressable by other applications, an support the interaction and if necessary pre-emption of applications in case of resource shortage or outage and failure scenarios. A core and radio based approach would still be able to manage the data transmission in line with the configured priorities, but the applications would not explicitly become aware of QoS profile changes introduced by the system due to resource limitations.

An additional argument might not be so obvious. One key characteristic of the FRMCS System is the flexibility and independence of applications from the underlying transport layer. In other words the application should not manage the requests for a specific radio bearer or a radio QoS profile, rather generically request communication services from the FRMCS System. The FRMCS System would in response and based on the available resource and radio technologies assign one or more physical bearers to the application session. Even during intra-RAT, inter-RAT or network handovers, the FRMCS System would manage the physical radio bearer and switch to another bearer without radio related application interactions. Railway Applications using plain IP services offered by the core and radio subsystem will not be able to leverage generic FRMCS Communication Services and need to manage and control the radio bearers on their own. Applications with MCX support could inform the FRMCS System which communication services are required, which enables the FRMCS System to select the right radio bearers and make it available to the applications. Without the MCX interaction these application based requests for communication services are difficult to support.

Finally applications, which are already deployed and are complex to be adapted (e.g. legacy Railway Applications) or applications which have a limited functional scope (e.g. IP cameras, IoT sensors, etc.), could be supported with the introduction of a FRMCS Proxy function. The proxy would support the necessary MCX functions to give the application an identity, manage the communication requests and act as representative for the application.

6.1.4 Assessment

Non-MCX enabled Applications	MCX enabled Applications
FRMCS awareness or visibility	
FRMCS Communication Services have no visibility of the application, with the exception of the IP address assigned to this application.	Every application authenticates with the FRMCS System (MCX framework) and receives a FRMCS User Identity linked to a MCX functional alias. The identity is associated with an application profile that relates to permissions and authorization for using features or communicating with other FRMCS identities.

Non-MCX enabled Applications	MCX enabled Applications
Addressability	
Applications have to manage their addressability independently and based on IP addresses or FQDNs.	The FRMCS User Identity (MCX functional alias) is used to find the communication end point and will be translated by the FRMCS System to a FQDN or IP address which adds another level of abstraction offering further flexibility and options to overcome IP address complexity.
Prioritization and pre-emption	
Pre-emption applies to the communication flow, where low prioritized packets might be dropped in case of pre-emption. If dynamic and application driven QoS request and changes are required, the application could interact with the 3GPP QoS framework, in detail interface with the PCRF/PCF function.	The application profile within the MCX framework supports the prioritization and pre-emption on the application level, similar to GSM-R where a call is pre-empted rather than single media packets are dropped. The application profile does also determine the QoS selection for the radio bearer offered to the application and can adapt the QoS dynamically on the application level as well as the applications receive feedback in case application pre-emption is required or other changes to the available QoS profile would occur. Furthermore, the QoS per radio bearer is no explicitly done by the application but the FRMCS translates the generic application communication requirement request to a QoS request for the available and selected radio bearer.
Application admission control	
Directly linked with the 3GPP admission control	The MCX framework is able to grant admission or reject the application due to missing permissions or limited resource availability that is already consumed by prioritized applications.
Communication authorization/permission	
Once the application has an IP address assigned it can send data to other users or applications without any centralized control. Only the usage of firewalls and address assignments could be used to control the communication between applications.	For MCX enabled applications, each communication requested to another FRMCS User Identity is processed by the FRMCS System (MCX framework) and only if the application has the authorizations or sufficient permissions the communication is granted. This functionality would be comparable to the access matrix in GSM-R now also available to data applications.
Communication services requests	
The application has one or more IP addresses and would need to manage and control the radio bearers as well as supporting multi-path or redundant communication to combine or aggregate bearer communication.	MCX enabled applications request communication services through the control messaging with the FRMCS System (MCX framework) and the FRMCS System makes a single data connection available, which might be based on a multi-path or redundant connection using one or more physical radio bearers. Using the MCX control messaging decouples the applications from the radio technology and enables a flexible interaction with the communication services.
Simple application/Legacy application support	
Adding MCX functionality to simple applications like IP cameras or IoT sensors introduces higher costs and limits the selection of commercially available products. In addition, the cost and complexity to upgrade all legacy Railway Application with MCX functionality is likely unbearable and not acceptable for railway undertakings.	To maintain a consistent and coherent system approach it is advisable to support FRMCS System (MCX framework) capabilities for all users of the FRMCS System. The preferred approach is the integration of MCX functions within the application, but for simple and legacy applications an alternative could be foreseen. Proxy FRMCS functions which support the required MCX features could act for the applications and request or interact with the FRMCS System (MCX framework).
Communication security	
To support secure data transmission each application would need to have additional functionality to support communication ciphering.	The MCX framework supports secure transmission and a MCX enabled application just inherits the benefits without the need to implement communication security protocols or features. In addition a common secure communication function also improves the interoperability between on-board and trackside.
Application Impact	
Application can rely on a IP only connection. For ETCS the existing ETCS over GPRS specification can be used. Only minor changes are foreseen to ETCS/Euroradio stack to enable a smooth migration the need for MCX support.	Application need to be enhanced to support FRMCS functionality and manage FRMCS identities.

6.2 FRMCS/4G support for Railway Applications

6.2.1 Use cases

The assessment of the appropriate 3GPP core technology should be based on evaluating the needs of the Use Cases in Table 2.

Table 2: Use cases (4G support)

Use Case	
Allocation and isolation of FRMCS communication resources (was End-to-End Network Slicing for FRMCS)	Precursor techniques are available in 4G, such as APN-based slice selection, PLMN-ID based slice selection, DECOR and eDECOR.
FRMCS Bearer Flexibility	LTE EPS provides mobility mechanisms to support frequent handovers within and across 3GPP legacy systems or E-UTRAN and non 3GPP access systems in order to avoid service degradation (ETSI TS 122 278 [i.13]). Furthermore, there are LTE-U, LAA, LWA and MulteFire which provide further options to augment standard LTE carriers with the unlicensed bands of WiFi networks. Satellite access can be connected via fixed IP connection.
QoS in a Railway Environment	See clause 6.2.2.
FRMCS System Security Framework	LTE Authentication: EPS AKA (Authentication and Key Agreement) procedure is used in LTE networks for mutual authentication between users and networks. NAS Security: it is designed to securely deliver signalling messages between UEs and MMEs over radio links, performs integrity check (i.e. integrity protection/verification) and ciphering of NAS signalling messages. Different keys are used for integrity check and for ciphering. While integrity check is a mandatory function, ciphering is an optional function. NAS security keys, such as integrity key (KNASint) and ciphering key (KNASenc), are derived by UEs and MMEs from KASME. AS Security: it is purposed to ensure secure delivery of data between a UE and an eNB over radio links. It conducts both integrity check and ciphering of RRC signalling messages in control plane, and only ciphering of IP packets in user plane. Different keys are used for integrity check/ciphering of RRC signalling messages and ciphering of IP packets. Integrity check is mandatory, but ciphering is optional.
Roaming	Basic 4G roaming supported. MCX users who roam onto a visiting network would roam onto the visiting MCX server. The visiting network server would query the home network MCX server Functional Alias info via the MCPTT-1 interface.
Service awareness	See 4G QoS clause 6.2.2.
Availability - increasing measures	LTE supports fall-back to other RATs.
FRMCS Equipment capabilities for multiple FRMCS Users	LTE can allocate one IPv4 or IPv6 address for the PDU sessions within an APN.

6.2.2 QoS Management in LTE

Given the large diversity of communication requirements of the envisioned FRMCS applications, for instance ranging from a few kbps to multiple Mbps, and from latency requirements on the order of seconds to those on the order of 10 ms (3GPP TR 22.889 [i.4]), it is essential that the FRMCS System is able to differentiate data packets related to different applications, in order to handle and prioritize these correctly according to their requirements. In this clause, the Quality of Service (QoS) management architectures and mechanisms in LTE releases is shortly elaborated.

In the LTE QoS architecture (ETSI TS 136 300 [i.6]), the finest granularity of differentiating mobile data is on the level of radio bearers, which are characterized by a QoS class identifier reflecting aspects such as priority, acceptable delay and packet loss rate, and which can be of type guaranteed bit rate or non-guaranteed bit rate. Within one bearer, all data packets are treated within the same way, which would mean in an FRMCS context that multiple bearers would have to be set up for one terminal in order to be able to treat packets related to different FRMCS applications such as voice, ETCS/ATO and critical video differently, which would be rather inefficient Also, the LTE architecture always implies a one-to-one mapping of radio bearers to EPS bearers, which essentially means that the granularity of service differentiation in the core network is by definition the same as in the RAN.

6.3 FRMCS/5G support for Railway Applications

6.3.1 Use cases

The assessment of the appropriate 3GPP core technology should be based on evaluating the needs of the Use Cases in Table 3.

Table 3: Use cases (5G support)

Use Case	
Allocation and isolation of FRMCS communication ressources (was End-to-End Network Slicing for FRMCS)	Network Slicing requires a 5G core technology. Refer to 3GPP TR 28.801 [i.14] for more details.
FRMCS Bearer Flexibility	5G expands the use of heterogeneous network allowing a common core to control both 3GPP and non-3GPP access See ETSI TS 122 261 [i.15]. It will support a harmonised QoS and policy framework that applies to multiple accesses.
QoS in a Railway Environment	See clause 6.3.1.
FRMCS System Security Framework	Primary authentication: Network and device mutual authentication in 5G is based on primary authentication. This is similar to 4G but there are a few differences. The authentication mechanism has in-built home control allowing the home operator to know whether the device is authenticated in a given network and to take final call of authentication. In railway this would be particularly useful for trains roaming onto another railway network. Primary authentication is radio access technology independent, thus it can run over non-3GPP technology such as IEEE 802.11 [i.18] WLANs. This would allow authentication to be consistent across the various flexible bearers. Secondary authentication: in 5G it is meant for authentication with data networks outside the mobile operator domain. For this purpose, different EAP based authentication methods and associated credentials can be used. A similar service was possible in 4G as well, but now it is integrated in the 5G architecture. Inter-operator security: Several security issues exist in the inter-operator interface arising from SS7 or Diameter in the earlier generations of mobile communication systems. To counter these issues, 5G Phase 1 provides inter-railway security from the very beginning. Privacy: Subscriber identity related issues have been known since 4G and earlier generations of mobile systems. In 5G a privacy solution is developed that protects the user's subscription permanent identifier against active attacks. A home network public key is used to provide subscriber identity privacy. Service Based Architecture (SBA): The 5G core network is based on a service based architecture, which did not exist in 4G and earlier generations. Thus 5G also provides adequate security for SBA.

Use Case	
Roaming	5G has an advantage on 4G of maintaining a network slice when roaming onto an external 5G network using Network Slicing Federation. In ETSI TS 123 501 [i.7], the Slice/Service Type (SST) is used to refer to an expected network slice behaviour in terms of features and services. Standardized SST assigned by the 3GPP are used in order to identify slices uniquely around the world. Railway Industry could add its own universally recognized Network/Slice service types to fulfil FRMCS requirements. MCX users who roam onto a visiting network would roam onto the visiting MCX server. The visiting network server would query the home network MCX server Functional Alias info via the MCPTT-1 interface.
Maintainability	FRMCS on-board gateway will contain SIM cards to support multiple frequency bands For partition within a frequency band 5G New Radio has introduced the feature Carrier Bandwidth Parts. According to ETSI TS 138 211 [i.16], clause 4.4.5, A carrier bandwidth part is a contiguous set of physical resource blocks, selected from a contiguous subset of the common resource blocks for a given numerology(u) on a given carrier.
Service awareness	See clauses 6.3.2 and 6.3.3.
Availability - increasing measures	5G RAN supports Multi-RAT Dual connectivity where one UE can maintain 2 parallel connections over 2 separate RATs.
FRMCS Equipment capabilities for multiple FRMCS Users	The UE would manage a separate IP address for each FRMCS user managed by the UE. 5G includes an UE IP address management which allows allocation and release of the UE IP address as well as renewal of the allocated IP address, where applicable. The UE would request a PDU session for each FRMCS User managed. The UE sets the requested PDU Session Type during the PDU Session Establishment procedure based on its IP stack capabilities as follows: UE supporting IPv6 and IPv4 should set the requested PDU Session Type according to UE configuration or received policy (i.e. IPv4, IPv6 or IPv4v6).

6.3.2 QoS Management in 5G/NR

The QoS management architecture in 5G has from the beginning been designed to allow for a much more fine-granular treatment of different data packets, and also a more flexible and independent QoS handling in core network and RAN.

This is enabled through the introduction of so-called QoS flows (ETSI TS 123 501 [i.7]), which are described through QoS profiles which for instance contain the information whether the flow is of type guaranteed bit rate or non-guaranteed bit rate, and an allocation and retention priority (ARP), and which are defined and managed by the Session Management Function (SMF) in the 5G core network. A single PDU session can relate to multiple QoS flows, so that even within a PDU session data packets can be treated in a differentiated way.

In the downlink, the User Plane Function (UPF) in the core network then uses service data flow (SDF) classification rules provided by the SMF to map individual data packets to the defined QoS flows, and the new Service Data Adaptation Protocol (SDAP) in the RAN then maps these to data radio bearers (DRBs). In the uplink, the terminal evaluates individual data packets against QoS rules provided by the SMF, and assigns these accordingly to QoS flows and subsequently to data radio bearers. Alternatively, so-called reflective QoS handling can be applied, where the terminal uses the classification of downlink packets to derive that of uplink packets.

5G Policy framework has an Application detection mechanism in the core so watch service flow can be assigned its own prioritization, pre-emption and arbitration rules and can be gated for only authorized traffic.

5G policy framework only communicates its policy decision to end-points via Applications Functions. In the case of FRMCS this would be an MCX server. Therefore, each FRMCS user requiring a notification of pre-emption would need to be registered on the MCX server. However autonomous FRMCS applications would have a deterministic high priority arbitration rule applied to them similar to the Ultra-Reliable-Low-latency devices introduced in 5G. These devices would always have prioritized access to resources and could never be pre-empted. As such there would be no need for them to use the MCX framework.

6.3.3 Comparison and Suitability of QoS Management Options for Rail Operations

The different QoS management architectures in LTE and 5G/NR are illustrated in Figure 10, and their key properties are summarized in Table 4.

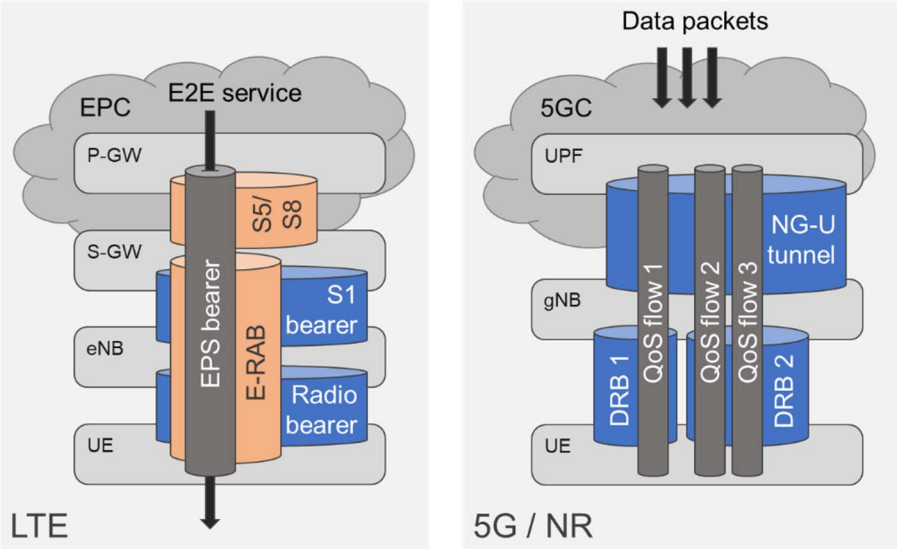

Figure 10: Comparison of QoS management architectures in LTE and 5G/NR

NOTE: Figure 10 is derived from [i.17].

Table 4: 4G/5G key properties

	LTE	5G/NR
Granularity of QoS differentiation	Radio bearers/EPS bearers	Individual data packets within a PDU session
QoS management in core network and RAN	Coupled	Independent, i.e. core network maps packets to QoS flows, and RAN independently maps QoS flows to radio bearers

While both the LTE and 5G QoS architectures would in principle support FRMCS application needs, it is expected that the 5G approach is significantly more efficient, as a single terminal could be served with one radio bearer, while still allowing for the differentiation of packets relating to different FRMCS applications. In addition, the 5G approach also allows differentiating packets within one PDU session. This is for instance beneficial for any applications based on protocols (like TCP) that require an initial session setup, as packets related to this setup could be prioritized for faster session establishment, while subsequent packets, e.g. conveying video data, could be treated at normal priority.

6.4 Communication system resource sharing

6.4.1 Network Sharing

Network Sharing refers to the usage of the same physical communications infrastructure by multiple tenants. As an example, multiple network operators may operate independent core networks, but share the same radio access.

In the case of network sharing, all tenants share the same resources and functionality equally, therefore, it is not possible to differentiate or customize the shared resources and functionalities to the needs of individual tenants. Consequently, any kind of prioritized transport with predictable QoS and bit rate is impossible. In such setup, it is also not possible that single tenants have the full authority and control over the network shared among multiple tenants, as required by national safety authorities in many countries.

6.4.2 Network Slicing

Network Slicing builds upon network sharing and refers to the creation and operation of multiple virtual E2E networks, tailored to specific use cases or business models (for instance related to different vertical industries), on a common physical communications infrastructure. A network slice can span all domains of the network, from the radio access via the backhaul transport network to the core functionality, and encompasses specific control and user plane handling needed for each slice.

NOTE: Figure 9 in [i.8] gives an illustration of the concept of network slicing.

It should be stressed that Network Slicing also builds on top of a given QoS management architecture, as detailed in clause 6.2. While the QoS management allows network functions such as MAC schedulers to apply different priorities to different data packets, Network Slicing goes a substantial step further in that completely different network functions and configurations thereof could be applied to data packets belonging to different slices. Further, Network Slicing also allows to have - within few constraints - slice-specific locations of functions (e.g. in one slice, functions beyond a certain protocol stack layer may be virtualized and run in the Cloud, while in another these are run on an Edge Cloud for reduced E2E latency). Finally, each slice may have a largely individual management and orchestration setup and corresponding responsibility split between the involved players. For instance, one slice could be completely managed by a MNO, while for another slice a large part of the network functionality is handled by the tenant (e.g. a railway infrastructure manager) itself.

Ultimately, these properties lead to a fundamental difference between Network Sharing and Network Slicing, as shown in Table 5. While for the former hardly any differentiation of the traffic of different tenants is possible, Network Slicing enables the configuration and operation of virtually independent E2E logical networks which are highly customizable and controllable, as if they were based on physically separated networks.

Table 5: Differences between Network Sharing and Network Slicing

	Network Sharing	Network Slicing
Network functions	Same for all tenants sharing the network	Can be slice-specific (except functions that strictly apply to all slices, such as overall admission control)
Location of network function instantiation	Same for all tenants sharing the network	Can be slice-specific (except functions that apply equally to all slices, e.g. related to common control signals)
Network management and orchestration	Same for all tenants sharing the network	Can be slice-specific (again except for functions that apply equally to all slices)
Authority/control of a tenant over its usage of the network	Not possible	May be provided, e.g. through tenant-owned management and orchestration and pre-emption of the tenant's slice over others

Network Slicing may be highly attractive for future rail operations, as it would for instance enable that mobile network operators provide rail communication services and commercial mobile broadband connectivity using a common physical network infrastructure. Rail operations would then be run in a separate slice in the network, with various protection mechanisms in place to ensure that related strict latency, reliability, availability and security requirements can be met. In some countries, such Network Slicing may be the only economically viable solution for future rail operation, for instance due to scarce dedicated rail spectrum.

A specific Network Slicing option for instance captured in Use Case 12.19.2 in version 16.1.0 of 3GPP TR 22.889 [i.4] foresees that rail operations could be based both on rail-dedicated spectrum and a related communication network, and a network slice offered by a public mobile network operator and using licensed spectrum. Another possible scenario is that multiple railway undertakings base their operations (partially) on a common communications system, utilizing an individual slice per railway undertaking (3GPP TR 22.889 [i.4]). Network slicing will then provide then the required privacy and predictable QoS to each individual railway undertaking. The aforementioned possibility to have slice-specific network functions including their locations would also allow to separate FRMCS application categories (critical, performance, business), if a network is owned and operated by a single infrastructure manager.

For instance, for latency-critical FRMCS applications (see 3GPP TR 22.889 [i.4]), the core network user plane functions may be moved to the edge, while for others these could resides in a centralized location.

Consequently, there are at least the following four different use cases for network slicing:

1) MNO with rail-dedicated and commercial-dedicated network slices.

2) Railway-owned network with rail-dedicated spectrum together with commercial spectrum offered by a MNO.

3) One network slice per railway undertaking (multi-tenancy) in a railway-owned network.

4) One network slice per application or group of applications in a railway-owned network.

Network Slicing is to a large extent a matter of implementation, though 3GPP has standardized various means to support Network Slicing, as will be elaborated in the sequel.

It is important to stress that E2E Network Slicing as per the NGMN definition [i.8], and in a form that meets the needs of Use Case 12.19.2 in version 16.1.0 of 3GPP TR 22.889 [i.4], is only possible from 3GPP NR Rel-16 onwards.

6.4.3 Precursors of Network Sharing and Slicing in Release 13/14

LTE Release 13 introduced the option to use "slice"-specific S/P-GWs or MME entities based on APN or PLMN identity, while the remainder of the core network functionality and the radio access are shared among multiple "slices" (though the term "slice" was not yet commonly used at that time). Further, the 3GPP Dedicated Core Network (DCN) or DECOR feature was introduced, where dedicated core network nodes form a DCN serving subscribers or devices with a certain "usage type" (e.g. machine-to-machine or enterprise). In Release 14 eDECOR feature, the DCN selection mechanism was extended to be assisted by the device, which can send its usage type to the RAN (see ETSI TS 123 401 [i.9]). Some details on the mentioned solutions are provided below.

APN-based slice selection allows to select a specific S/P-GW per APN, though with the downside that a terminal that needs to be involved in multiple slices would need to have multiple IP addresses assigned.

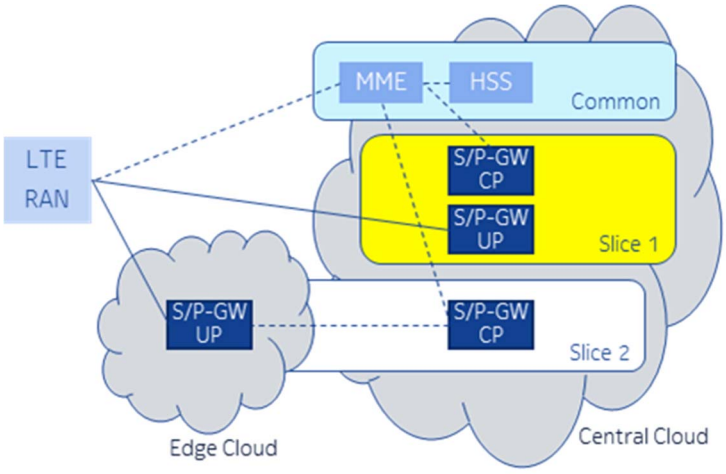

Figure 11: APN-based Slice Selection

PLMN-ID-based slice selection (like MOCN) allows to select MME, S/P-GW per slice, but with the drawback that a separate PLMN has to be created and managed for each slice.

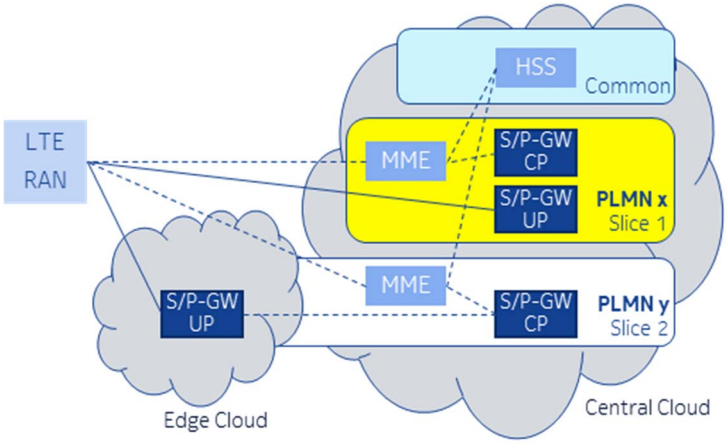

Figure 12: PLMN-ID-based slice selection

DECOR (3GPP Release 13) allows a "master" core slice to "assign" users to a dedicated core slice This feature works with earlier UE releases (no impacts to UE), and the new optional subscription information "UE Usage Type" is stored in the HSS. The principle is that during the initial Attach procedure it is checked if the MME/SGSN belongs to the right DCN (DCN identified by the UE Usage Type), by interrogating the HSS. Then if necessary redirect the UE to an MME belonging to the right DCN. After that, the UE is maintained in its DCN during mobility thanks to the GUMMEI for MME selection by the RAN. A drawback is that a separate core network should be built for each DCN-ID (slice).

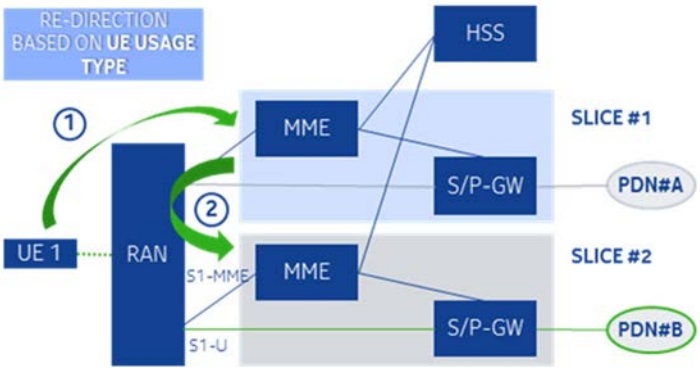

Figure 13: DECOR

eDECOR (3GPP Release 14) allows a UE to provide a DCN-ID to RAN allowing MME selection during initial registration. Unlike DECOR, eDECOR requires UE modifications (only UE from Release 14 support). During the Attach/TAU procedure, the Core Network provides the UE with a DCN-ID, which is valid in the PLMN only. The UE stores the DCN-ID for that PLMN. At each further Attach/TAU, the UE sends the DCN-ID at AS level. The RAN uses the DCN-ID to route the NAS signalling to the appropriate DCN. With that, a redirection may occur only when the UE attaches for the very first time to a PLMN: after the DCN-ID has been provided to the UE, there will be no rerouting procedure by the CN. The solution is only usable in HPLMN, again has the drawback that a separate core network is built for each DCN-ID.

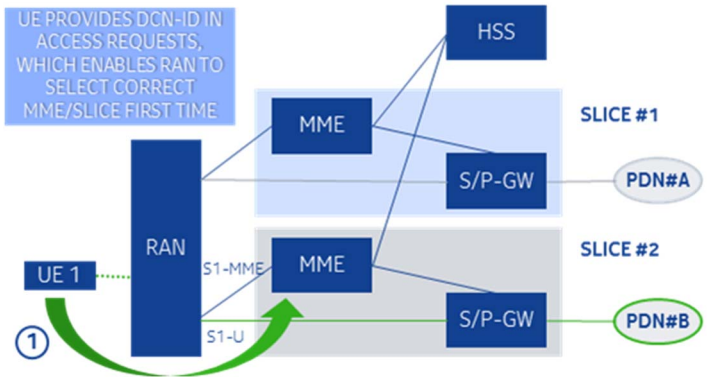

Figure 14: eDECOR

All mentioned LTE Release 13/14 options can be seen forms of network sharing (of the RAN and large parts of the CN), with "slice"-specific MMEs and/or S/P GWs.

6.4.4 E2E Network Slicing as enabled through NR Release 15

6.4.4.1 General considerations

NR Release 15 is the first release supporting E2E Network Slicing, including also slicing of the CN with all the flexibilities stated in clause 6.4.2, and in particular also slicing of the RAN. To ensure native Network Slicing support, various related requirements are included in 3GPP TR 22.889 [i.4], e.g. related to:

- Provisioning: create/modify/delete network slices, provision network functions to be used in network slices, define network services and capabilities supported by a network slice.
- Managing association to slices: configure association of devices and services to network slices, move/remove user between/from slices.
- Interoperating: support roaming and non-roaming using the same home slice, support devices simultaneously connected to multiple slices.
- Supporting performance and isolation: support dynamic slice elasticity, ensure performance isolation during normal and elastic slice operation and during slice creation or deletion, enable operators to differentiate performance and functionalities between slices.

6.4.4.2 RAN slicing

E2E Network Slicing support from NR Release 15 onwards inherently offers a plethora of options to do RAN slicing, i.e. to integrate or separate different slices in the RAN, as depicted in Figure 15, depending on spectrum availability, homologation requirements and business considerations. For instance, if homologation requires a stricter physical separation of slices, these could utilize different sub-parts of the spectrum (but otherwise share the same radio equipment and baseband processing). If a tighter level of integration is possible, physical layer and MAC functionality could be shared across slices (for instance with a MAC scheduler ensuring that requirements of critical slices are met by instantaneous prioritization over other slices), while the RRC, SDAP, PDCP and RLC functionality could be highly slice-specific.

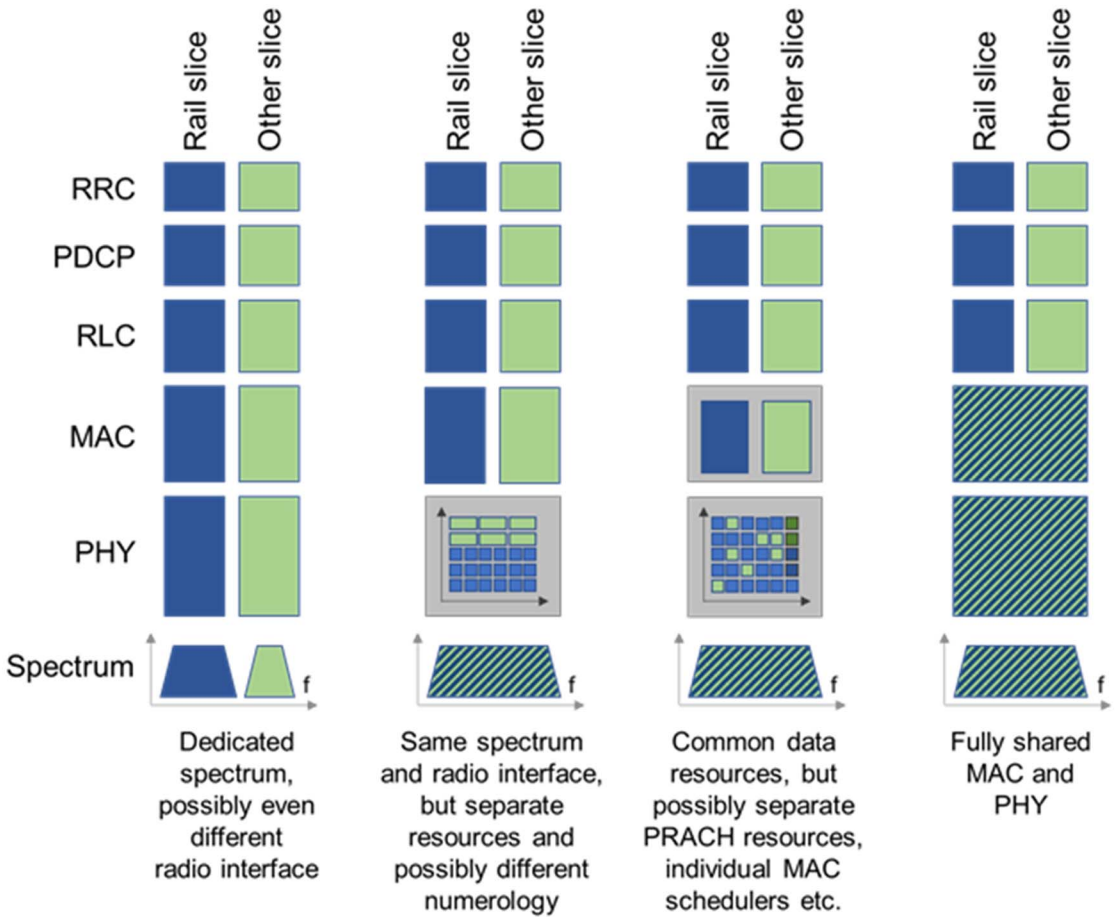

Figure 15: Options of slice integration/separation in the RAN

NOTE: Figure 15 is derived from [i.17].

6.4.4.3 CN slicing

The concepts of CN slicing architecture were introduced to components and functionalities later appeared in ETSI TS 123 501 [i.7]. The architecture is based on the concept of Control and User Plane Separation (CUPS), context-aware user plane anchoring, and distributed network functions with common slicing control functions. This enables flexible network deployment and operation, by distributed or centralized deployment and the independent scaling between control plane and user plane functions - while not affecting the functionality of the existing nodes subject to this split.

With the introduction of the Service Based Architecture concepts in the 5G core to enable CN slicing, the CUPS concepts were evolved and new network functions as shown in the following diagram were defined.

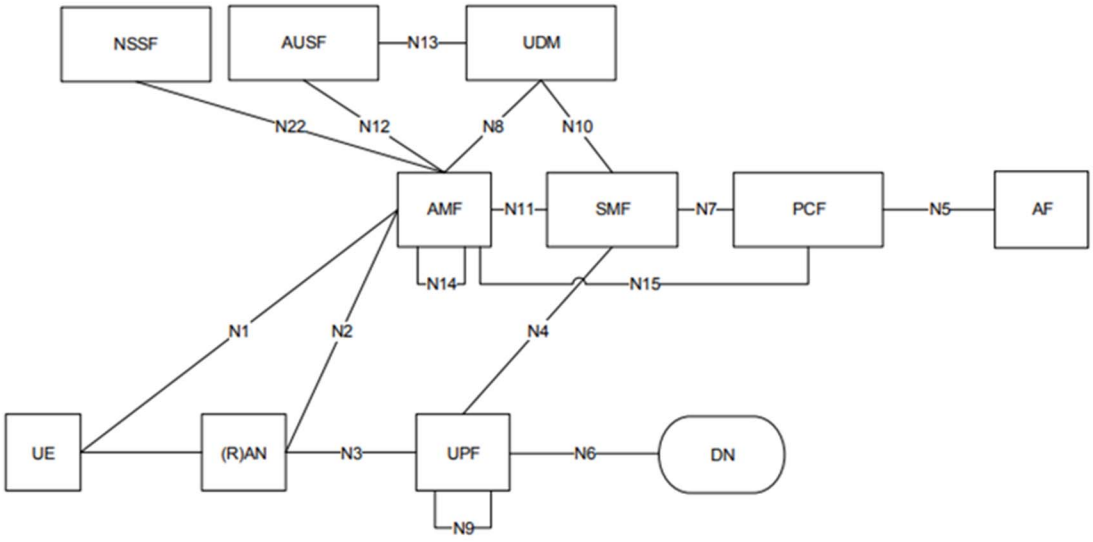

Figure 16: 3GPP 5G Reference Non-roaming Architecture

These functions include: **AUSF** Authentication Server Function, **AMF** Core Access and Mobility Management Function, **DN** Data network, **NEF** Network Exposure Function, **NRF** Network Repository Function, **NSSF** Network Slice Selection Function, **PCF** Policy Control function, **SMF** Session Management Function and **UDM** Unified Data Management.

The combination of the RAN slicing capabilities with the new CN slicing functions provides the basis for E2E Network Slicing in the 5G system.

6.4.5 Comparison and Suitability of Network Sharing and Slicing Options for Rail Operations

The aforementioned precursors of Network Sharing and Slicing and the E2E Network Slicing support in NR Release 15 are compared in Table 6.

Table 6: Slicing solutions

	APN-/PLMN-based MME and S/P-GW selection	DECOR	eDECOR	NR Rel. -15
RAN	RAN is shared among the slices, but not slice-aware, hence no differentiation of slice treatment is possible. Radio bearers-QCI (Service Type) QCI # increased to xx			Yes, RAN slicing explicitly supported, possibly with different choice/configuration/of network functions and of their locations per slice
UE access to multiple slices at same time	Yes, but with different IP addresses or need for multiple PLMNs	No, but UE can use multiple APNs/GWs within same DCN-ID		Yes
Core Network	S/P-GW selected based on APN/PLMN, otherwise a shared CN	DCN consists of logical/physical MMEs, S4/Gn-SGSNs, SGWs, PGWs and even PCRFs		Yes, possible with different choice/configuration/network functions and of their locations per slice
Slice selection	Based on APN/PLMN	UE Usage Type parameter from HSS	DCN-ID sent by UE during Attach/TAU	Based on NSSAI

Starting in 3GPP Release 15 the New Radio (5G NR) enables E2E Network Slicing including RAN slicing, which is identified in the Use Case 12.19.2 in 3GPP TR 22.889 [i.4].

6.5 SIP core vs. IMS functions

From a MC framework perspective the SIP core contains a number of sub-entities responsible for registration, service selection and routing in the signalling control plane.

The SIP core should be either:

- 3GPP IMS; or
- SIP core, which internally need not comply with the 3GPP IMS architecture, but with those Reference Points of 3GPP IMS which are required to provide the MCPTT service.

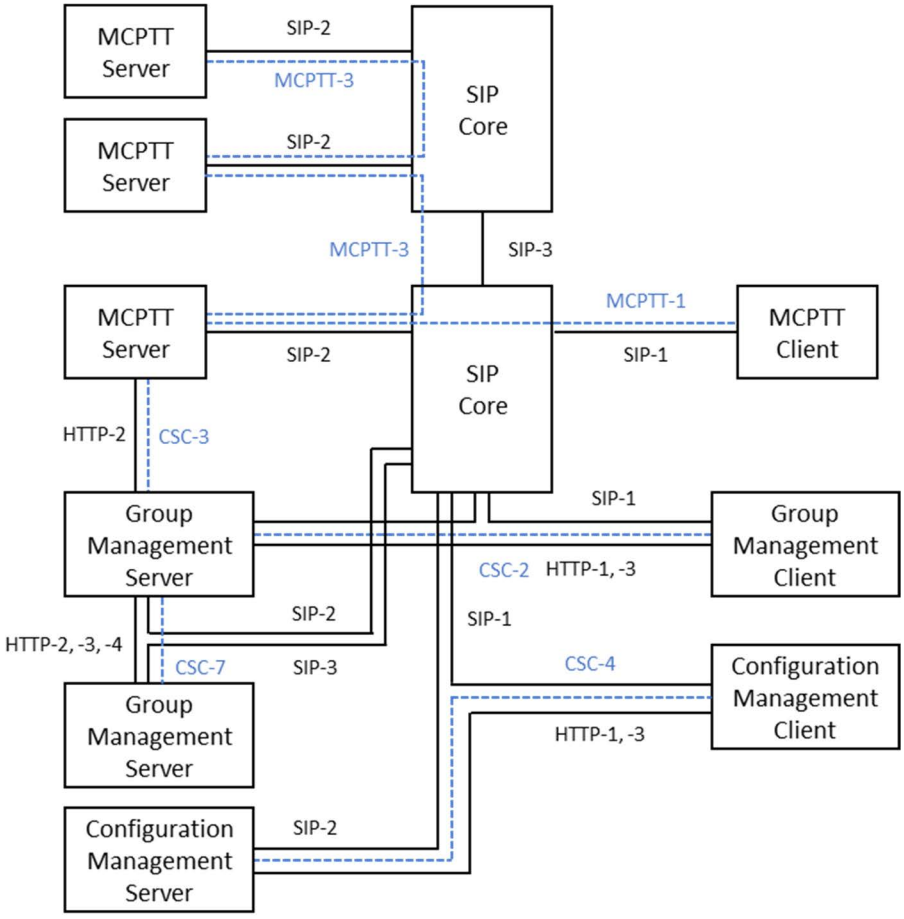

Figure 17: 3GPP MCPTT interfaces

The data related to the functions of the SIP core, e.g. for data for application service selection, the identity of the serving registrar or authentication related information may be provided by the PLMN operator responsible for the bearer plane. In this case, the SIP database that is the source of the data may be part of the HSS. Alternatively, this data may be provided by the MCPTT service provider. In this case, the source of the data may be the MCPTT service provider's SIP database.

Even if not mandatory for MCX the use of IMS functions is beneficial to FRMCS and could be used to orchestrate and manage service logic invocations, support policy control and enable the interworking and interconnect with external networks, including GSM-R, PLMN, other FRMCS networks, etc.

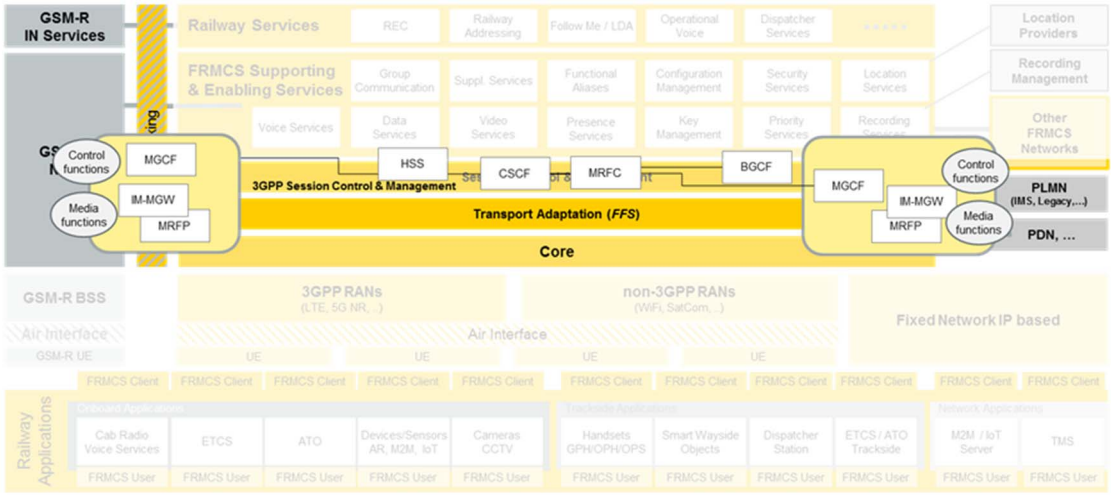

Figure 18: 3GPP MCPTT interfaces

Interworking and interconnect for 3GPP BICN based GSM-R networks would be based on the MGCF and MGW functionality defined in IMS. The service interworking for supplementary services, ASCI services or IN based MORANE services would require interworking functionality between the MCX subsystem and the relevant subsystems within the GSM-R networks.

For the interworking of IN based services, one key aspect is the interworking of MCX Functional Aliases with GSM-R Functional Numbers. The main related functionalities are a mapping of MCX Functional Aliases and GSM- R Functional Numbers, and a function that ensures consistency of that data in the FRMCS and the GSM-R network. To provide both of the above functions, one solution is a single application server serving both the FRMCS and the GSM-R network.

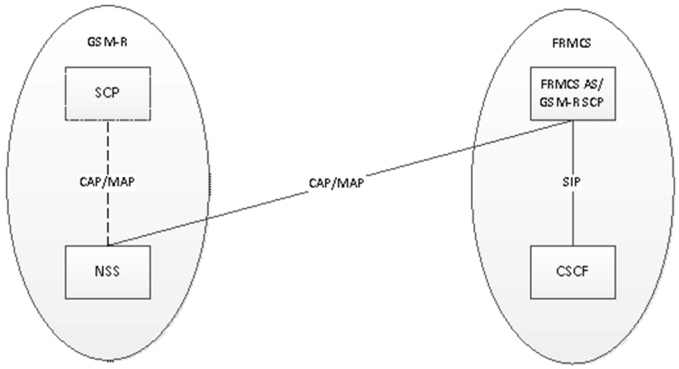

Figure 19: FRMCS and GSM-R Railway Services interworking

The MGCF and MGW functions are also used for the interconnection with PLMNs and PSTN networks. For the interconnection to other IMS based networks or FRMCS networks the BGCF and/or SBC functions would be needed.

A SIP core without these IMS functions would imply the interworking for bearers and plain telephony services has to be defined and implemented in the MCX domain.

Introducing IMS Core instead of SIP Core gives as mentioned in previous paragraphs the opportunity to shortcut MCX domain and therefore to be open to external networks and systems being capable to manage similar services (OTT solutions). Such opportunity can be seen positively (flexibility, open to any kind of network through IMS routing and services facilities, etc.) but also negatively (security backdoor to access pure Railway Application domain).

6.6 Communication Recording

6.6.1 Overview of recording options

Communication recording can be categorized and applies as follows to:

- Type of media:
  - Voice.
  - Data.
  - Video.
- Type of communication:
  - Group communication (point-to-multipoint).
  - Private communication (point-to-point).
- Mode of communication:
  - On-network.
  - Off-network.
- Recording information:
  - Metadata/signalling.
  - Media.

In addition, communication recording needs to consider and be able to handle encrypted communication (when end-to-end security measures are applied) and "normal" non-encrypted communication.

The following basic recording options can be implemented within FRMCS:

- UE based recording.
- Centralized recording.

6.6.2 Description of recording options

6.6.2.1 UE based recording

The UE based recording is implemented on the principle, that the UE records and stores metadata and media information. The UE then uploads such recorded and stored information to a central recording database either after the communication has finished or at periodic intervals. In any case, the UE requires connectivity to the central recording database only for upload and not for recording itself.

A key advantage for the UE based recording is the ability to support the capturing of direct off-net communication, where no centralized function is able to record any data.

However, several challenges become apparent if the bearer and control communication recording is located on the UE side:

- The device has to ensure that all communication activity which requires recording also activates the recording functionality without the interaction of the user or the ability to block or disabling the recording.
- The recorded communication data as well as the relevant metadata needs to be stored on the device and transferred back to a central recording management system for further processing.
- The integrity and completeness of the recording activity, the recording storage and the upload back to the central recording database has to be ensured.

- The interface between the recording service on the UE and the central recording database for upload of recorded information has to be standardized from scratch, as such principle is currently not used in any domain.

6.6.2.2 Centralized recording

The centralized recording is implemented on the principle that a central recording service is involved in any type of communication. Such a recording service can be seen as a special MCX user located at MCX server side, never initiating MCX call, but being inserted systematically in MCPTT, MCVideo and MCData (private and group communication).

A key advantage for the centralized recording is the storage of recorded metadata and media on a central recording database storage at the time the recording takes place.

However, several challenges become apparent if the bearer and control communication recording is centrally located:

- The central recording service needs to be involved in any type of communication as an MCX users, which is concerning media not immanent for private calls.
- The interface between the central recording service and the remainder of the FRMCS can be based on IETF RFC 7866 [i.10] as well as on ETSI TS 103 389 [i.11], but requires adaptations - and it is currently not included in 3GPP MCX stage 2 and stage 3 specifications (only in stage 1).

6.6.3 Security considerations

With end-to-end security, a recording device cannot be introduced in the bearer path to capture the communication exchange. Other options need to be considered.

In general, if end-to-end security is used, the data is encrypted using a key that is only known to the endpoints of the communication. However, recorded information should be decrypted latest during playback, earliest when stored on the central recording database. The decryption of recorded information during the storage, i.e. the central recording database stores only decrypted recording information, offers higher flexibility and does not require either availability of the keys in the KMS until the playback takes place nor storage of MCX keys on the central recording database. Nevertheless, the key should be known to the central recording service.

As option 1, the MCX framework includes a function that the keys used for media encryption for group communication is distributed to the MCX server to allow media mixing (which requires also decrypted media data). That method could be re-used for voice recording. From private calls there is no mixing required, therefore there is no option included to distribute the key to the MCX server. The key exchange for private calls is based on the MIKEY-SAKKE method. That method includes an option called forking which allows multiple devices to get the encryption key.

As option 2, the central recording service and database can be implemented as audit client with special access privileges as specified in clause 10.2 of version 15.2.0 of ETSI TS 133 180 [i.12]. Knowing the MCX key information, the central recording service and database can either de-crypt recorded information during playback or store recorded information already decrypted.

Other call related data is not end-to-end encrypted but only encrypted between client and MCX server. Therefore, this data is available for recording.

6.7 FRMCS Security

6.7.1 General Considerations

The FRMCS security should support the required features and functions to:

- Ensure all system users or entities are identified and authentication.
- Shield the system from unauthorized access.
- Defend the system from external threats and risks.

- Mitigate any implications from malicious attacks.
- Report any intrusion or malicious behaviour of users, terminals, system nodes and functions.

With the aim to protect and enable continuity of FRMCS Communication Services for FRMCS Users.

Each radio access systems within the FRMCS transport system and should provide identification, authentication and authorization functions to gain access to transport services. If supported each transport system should provide physical protection or defence schemes for any type of attack as well as providing integrity features, including but not limited to communication ciphering.

Human or machine users linked to a Railway Application requesting access to FRMCS Supporting and Enabling Services or the MCX framework require valid identification and authentication followed by the authorization to use configured or provisioned features and functions. The FRMCS services also support communication encryption for all services, including group voice and peer-to-peer voice based on MCPTT, video services using MCVideo and data exchanges based on MCData.

With the help of the MCX framework, a fully authenticated and authorized end-to-end encrypted communication session is supported.

The implementation of FRMCS functions and sub-systems in all layers of the FRMCS System should be fully redundant to avoid service impact if one function or node becomes unavailable.

Safety functions according to SIL1 to SIL4 is not supported by the FRMCS System and need to be implemented in the Railway Application layer to guarantee end-to-end integrity and functional correctness. The FRMCS System provides a secured communication session between the involved Railway Applications.

6.7.2 Security Structure Elements

The security function is needed for:

- The protection of data integrity, data confidentiality, information privacy.
- The non-repudiation of data transmission.

In the user-, control- and management plane for on- and off-network communication and is based on the following elements:

- Identification and authorization (e.g. at the beginning of a data transmission or for a system access control):
  - Identity management.
  - Role management.
  - Certification management.
  - Role management.
  - Protocol data management (e.g. time stamps or location stamps).
- Key and password management:
  - Generation, transmission, revocation and deletion of keys and passwords.
  - Certification management.
  - Encryption.
  - Data integrity check.
  - Context check (time, sequence of events, location, mobility, etc.).
- Authentication (e.g. at the beginning of a data transmission or for a system access control):
  - Encryption.

- Secured data transmission:
  - Encryption.
  - Data integrity check.
- Fraud protection:
  - Disabling a FRMCS System component from normal operation if is reported/recognized as stolen or lost (e.g. based on time, location, mobility, etc.).
  - Re-enabling a FRMCS System component to normal operation if is reported/recognized as recovered.
- Detection of IT-based threats and attacks:
  - Anomaly detection (time, sequence of events, location, mobility, etc.).
  - Correlation of events (time, sequence, location, mobility, etc.).
  - System's performance and functionality monitoring.
  - System's (e.g. data base) integrity check.
  - Log-file processing.
  - Communication matrix.
  - Honey-pot.
  - SIEM (Security information and event management).
- Reaction on IT-based threats and attacks:
  - Monitoring.
  - Reporting.
  - Short-term, midterm and long-term reactions.
- Forensic:
  - Monitoring.
  - Reporting.
  - Detection on IT-based threats and attacks (particularly SIEM and correlation of events).
  - Fraud protection.

7 Conclusions and Next Steps

The present document has investigated several technical possibilities to address the requirements defined in the FRMCS User Requirements Specification.

Several building blocks already defined in 3GPP can be used to address the requirements; however, some specific railway features might not be covered. It is recommended that a thorough gap analysis be performed to identify which one(s) would require a potential standardization effort outside of 3GPP. A specific focus could be placed on the external interfaces of the FRMCS system.

In addition, the compared merits of the different techniques presented in clause 6 of the present document should be further investigated to limit, if possible, the number of implementation options.

Finally, a complete mapping of applications to system functions, and a mapping of system functions to Subsystems and network elements could help in refining the FRMCS architecture.

Annex A:
Change History

Date	Version	Information about changes
July 2016	0.0.1	First publication of the TR after kick-off meeting held 26 February 2016 by ETSI On-line meeting
September 2016	0.0.2	Version 0.0.2 prepared by the Rapporteur with contribution from FEEI (Fachverband der Elektro- und Elektronikindustrie Bereich Technik) for the review dated 16 September 2016
October 2016	0.0.3	
July 2018	0.0.4	Structure of the TR adapted to the update of the Work Item
September 2018	0.0.5	Stable draft version of the TR
November 2018	0.0.6	Version presented for approval at TC RT #71
November 2018	0.0.7	Version presented for approval by Remote Consensus

History

Document history		
V1.1.1	January 2019	Publication