Future Railway Mobile Communication System

System Requirements Specification

Source: FRMCS AT Working Group
Date: 13 February 2023
Reference: FW-AT 7800
Version: 1.0.0
No of pages: 108

ISBN 978-2-7461-3119-4

Document history

Version	Date	Details
0.0.1	October 2019	Creation of the document
0.0.2	November 2019	Internal review in ATWG
0.0.3	December 2019	Internal review in ATWG
0.0.4	January 2020	Internal review in ATWG
0.0.5	February 2020	Internal review in ATWG
0.0.6	March 2020	Internal review in ATWG
0.0.7	April 2020	Internal review in ATWG
0.0.8	May 2020	Internal review in ATWG
0.0.9	June 2020	Internal review in ATWG
0.0.10	July 2020	Internal review in ATWG
0.0.11	August 2020	Internal review in ATWG
0.0.12	September 2020	Internal review in ATWG
0.0.13	October 2020	Internal review in ATWG
0.0.14	November 2020	Internal review in ATWG
0.0.15	December 2020	Internal review in ATWG
0.0.16	January 2021	Internal review in ATWG
0.1.0	7th July 2021	Version ready for internal review by ATWG
0.2.0	30th July 2021	Version ready for external review
0.2.1	5th Aug 2021	Version ready for external review (addition of one chapter)
0.2.2	1st Sep 2021	Official publication (incl. ISBN code)
0.3.0	26th Oct 2021	Version ready for internal review by ATWG
0.3.1	29th Oct 2021	Version ready for external review
0.3.2	29th Nov 2021	Correction made after external review comments
0.4.0	3rd Dec 2021	Version ready for external review including changes mainly to section 11, and minor changes to sections 6, 12 & 15
0.4.1	7th Dec 2021	Editorial changes (updated references to tables and figures), 15.5.3.1 updated
0.4.2	21 Jan 2022	Correction made after external review comments (sections 2, 3.2 and 6)
0.5.0	25 Jan 2022	Correction made online during workshop
0.5.1	4 April 2022	Correction made based on review during EECT Radio workshops 08/03/2022 & 25/03/2022 (agreed comments)
0.5.2	28 June 2022	Correction made after external review comments + a couple of open points in sections 11, 14 & Annex E + FRMCS FIS alignment on section 11 + Editorial changes (updated references to figures)
0.6.0	1 July 2022	Correction and consolidation made for external review
0.6.1	7 September 2022	Merge of TOBA SRS TOBA-7530 v.0.0.12 into FRMCS SRS (changes not reflected in 0.7.x series)
0.7.0	2 September 2022	Internal review in ATWG
0.7.1	6 September 2022	Internal review in ATWG
0.7.2	7 September 2022	Correction made after external review comments including applicability of requirements (M, O and I), EECT 20220713 agreed comments including H2H and H2N, EECT 20220713 comments for discussion, ETSI TC RT achievements.
0.8.0	29 September 2022	Correction made after external review comments including EECT 20220926 agreed comments, WP8.3 decisions on 21/09/2022, FRMCS SRS v0.6.1, changes made to TOBA SRS v0.1.0
0.9.0	12 October 2022	Correction made after external review comments including EECT 20221007 agreed comments, updated FRMCS Specifications map & removal of “void” clauses.
1.0.0	13 February 2023	Annex D added and official publication.

Table of contents

1 LIST OF ABBREVIATIONS 7

2 LIST OF DEFINITIONS 10

3 REFERENCES 14

3.1 APPLICABILITY 14
3.2 LIST OF REFERENCES 14

4 INTRODUCTION 16

4.1 BACKGROUND 16
4.2 PURPOSE OF THIS DOCUMENT 17
4.3 SCOPE 17
4.4 APPLICABILITY 18
4.5 DOCUMENT LIFE CYCLE 18

5 SYSTEM ARCHITECTURE DESIGN PRINCIPLES 19

5.1 SCOPE OF FRMCS SYSTEM AND SYSTEM ARCHITECTURE 19
5.2 PRINCIPLES FOR SYSTEM REQUIREMENTS 20

6 SYSTEM REFERENCE ARCHITECTURE AND REFERENCE POINTS 21

6.1 PREAMBLE 21
6.2 DESCRIPTION OF THE SYSTEM REFERENCE ARCHITECTURE 27
6.3 DECOMPOSITION INTO BUILDING BLOCKS 28
6.4 DESCRIPTION OF SYSTEM ARCHITECTURE REFERENCE POINTS 30
6.5 ADDRESSING 32

7 DESCRIPTION OF SUBSYSTEMS AND CONSTITUENTS 34

7.1 ON-BOARD FRMCS 34
7.2 ANTENNA FUNCTION 44

8 RADIO SPECTRUM 45

8.1 INTRODUCTION 45
8.2 OUT OF SCOPE 45
8.3 SPECTRUM PRINCIPLES 45
8.4 RMR FREQUENCY BANDS FOR EUROPE 45
8.5 PUBLIC MNO SPECTRUM IN EUROPE 46
8.6 FRMCS RADIO MODULE SUPPORT OF RADIO ACCESS TECHNOLOGIES AND FREQUENCY BANDS 46
8.7 FOR FURTHER STUDY 47

9 GSM-R INTERWORKING AND MIGRATION 48

10 INTERCONNECTION, ROAMING AND BORDER CROSSING 49

10.1 INTERCONNECTION 49
10.2 ROAMING 49
10.3 BORDER CROSSING 49

11 IDENTIFIERS 50

11.1 INTRODUCTION 50
11.2 SCOPE 51

11.3 IDENTITIES OF THE FRMCS TRANSPORT STRATUM 52
11.4 IDENTITIES OF THE FRMCS SERVICE STRATUM 52
11.5 USAGE AND DEPENDENCIES OF DIFFERENT FRMCS IDENTITIES 58
11.6 ROLE BASED IDENTIFICATION SCHEME 59
11.7 FOR FURTHER STUDY 64

12 BEARER FLEXIBILITY 65

12.1 INTRODUCTION 65
12.2 OUT OF SCOPE 65
12.3 GENERAL REQUIREMENTS 65
12.4 FRMCS MULTIPATH 65
12.5 FRMCS MULTI ACCESS 67
12.6 FRMCS INTRA-RAT 69
12.7 FOR FURTHER STUDY 69

13 NETWORK SLICING 70

14 QUALITY OF SERVICE AND PRIORITY 71

14.1 INTRODUCTION 71
14.2 OUT OF SCOPE 71
14.3 GENERIC REQUIREMENTS 71
14.4 QOS REQUIREMENTS 72
14.5 3GPP PARAMETERS 74
14.6 QOS SIGNALLING 77
14.7 FOR FURTHER STUDY 78

15 FRMCS CYBERSECURITY 79

15.1 INTRODUCTION 79
15.2 OUT OF SCOPE 79
15.3 FOR FURTHER STUDY 80
15.4 FRMCS SECURITY PRINCIPLES 81
15.5 FRMCS SECURITY REQUIREMENTS 82
15.6 MINIMUM FRMCS SECURITY LEVEL 84

16 POSITIONING AND LOCALISATION 86

16.1 INTRODUCTION 86
16.2 GENERAL PRINCIPLES AND SYSTEM REQUIREMENTS 86
16.3 POSITIONING AND LOCALISATION ARCHITECTURAL FRAMEWORK 86
16.4 ACCURACY 86
16.5 SECURITY 86
16.6 INTEGRITY 86
16.7 REFERENCE POINTS (COORDINATION SYSTEM) 86

17 NON-FUNCTIONAL SYSTEM REQUIREMENTS 87

17.1 INTRODUCTION 87
17.2 FRMCS SYSTEM MONITORING 87
17.3 ON-BOARD FRMCS 87

18 USER EQUIPMENT 89

18.1 MOBILE EQUIPMENT 89
18.2 CONTROLLER EQUIPMENT 89

19 SUBSCRIBER CONFIGURATION 90

20 SYSTEM CONFIGURATION 91

21 OFF-NETWORK COMMUNICATION 92

22 MISCELLANEOUS 93

ANNEX A. QOS REQUIREMENT VALUES OF FRS APPLICATIONS AND ITS CLUSTERING 94

ANNEX B. MAPPING BETWEEN APPLICATION REGIMES AND URS APPLICATIONS 95

ANNEX C. MAPPING OF FRS REQUIREMENTS TO SRS REQUIREMENTS 96

ANNEX D. INTEROPERABILITY REQUIREMENTS IN EU 108

1 List of abbreviations

3GPP	3rd Generation Partnership Project
5G	5th Generation of cellular telecommunications technologies standardised by 3GPP
5G-AKA	5G-Authentication and Key Management
5QI	5G Quality of Service Identifier
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AES-GCM	AES using Galois/Counter Mode
AMF	Access and Mobility Management Function
ARP	Allocation and Retention Priority
ATSSS	Access Traffic Steering, Switching and Splitting
ATO	Automatic Train Operation
ATP	Automatic Train Protection
CCS	Control Command and Signalling
CCS TSI	Control Command and Signalling Technical Specification for Interoperability
CCTV	Closed Circuit Television
CEPT	European Conference of Postal and Telecommunications
DNN	Data Network Name
DNS	Domain Name System
E2E	End to End service
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Management
ECC	Electronic Communications Committee
ECCSI	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption
ED	End Device
EN-DC	E-UTRA New Radio – Dual Connectivity
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EU	European Union
FA	Functional Addressing
FDD	Frequency Division Duplex
FFFIS	Form Fit Functional Interface Specification
FFS	For Further Study
FIS	Functional Interface Specification
FRMCS	Future Railway Mobile Communications System
FRS	Functional Requirements Specification
FS	FRMCS System
GDPR	General Data Protection Regulation
gNB	5G Base Station
GSM	Global System for Mobile Communications
GSM-R	Global System for Mobile Communications – Railway
GSM-R CS	GSM-R Circuit Switched
GSM-R PS	GSM-R Packet Switched
GUTI	Globally Unique Temporary ID
H2H	Host-to-Host
H2N	Host-to-Network
ID	IDentity
IETF	Internet Engineering Task Force
IM	Infrastructure Manager

IMPI	IMS Private User Identity
IMPU	IMS Public User Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPUPS	Inter-PLMN User Plane Security
ISDN	Integrated Services Digital Network
KMS	Key Management System
MC	Mission Critical
MCX	Mission Critical Services
MOTS	Modified Off The Shelf
NIA	Integrity Algorithm for 5G
NEA	Encryption Algorithm for 5G
NEF	Network Exposure Function
MNO	Mobile Network Operator
NA	Not Applicable
NR	New Radio
NR-DC	New Radio-Dual Connectivity
NTP	Network Time Protocol
OB	OnBoard
OB_{ANT}	On-board Antenna system reference point/interface
OB_{APP}	On-board Application reference point/interface
OB_{OM}	On-board Operation & Maintenance reference point/interface
OB_{RAD}	On-board Radio Module reference point/interface
OC	Organisational Code
OM	Operations & Maintenance
OTA	Over-The-Air
PA	Public Announcement
PCC	Policy and Charging Control
PCF	Policy Control Function
PDB	Packet Delay Budget
PDR	Packet Detection Rules
PER	Packet Error Rate
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMNO	Public Mobile Network Operator
QoS	Quality of Service
RAN	Radio Access Network
RBC	Radio Block Centre
RAT	Radio Access Technology
RF	Radio Frequency
RMR	Railway Mobile Radio
RRC	Radio Resource Control
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
RU	Railway Undertaking
SDN	Software-Defined Networking
SDP	Session Description Protocol
SEPP	Security Edge Protection Proxy
SIP	Session Initiation Protocol

SMF	Session Management Function
SRS	System Requirements Specification
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TBD	To Be Defined
TDD	Time Division Duplex
TOBA	Telecom On-Board Architecture
TR	Technical Report
TS	Technical Specification
TSI	Technical Specification for Interoperability
SBA	Service-Based Architecture
UE	User Equipment
UIC	Union Internationale des Chemins de Fer
UPF	User Plane Function
URS	User Requirements Specification

2 List of definitions

Terms	Definitions
Adapter	The Adapter is a Function that can manage connectivity to one or more radio modules using suitable industrial interfaces.
Administrative Domain	Domain managed by a single administrative authority (e.g., FRMCS Operator). The Administrative Domain is characterized by organizational/operator boundaries.
Application	Provides a solution for a specific communication need that is necessary for railway operations. In the context of this document, an application is interfacing with the FRMCS Access Point, to receive and transmit information to ground systems, (for example, ETCS, DSD, CCTV, passenger announcements, etc.).
Communication Services	Communication services enable two-way communication between two or more authorised service users (i.e., applications) from applications towards other applications/entities reachable through various networks.
Complementary Services	Ancillary services, e.g., providing and/or utilizing the location of the service user, supporting Communication Services and the Railway Application Stratum.
Control Plane	The control plane carries signalling traffic between the network entities.
Data Communication	Exchange of information in the form of data, including video (excluding voice communication), requiring corresponding QoS treatment.
Data Flow	Exchange of information in the form of data, including video and voice communication).
Data Network Name	According to 3GPP terminology ([TS 23.003]).
Distributed Architecture	In distributed architecture functions are present on different platforms and several of them can cooperate with one another over a communication network in order to achieve a specific common objective or goal.
Domain	According to 3GPP terminology ([TR 21.905]).
Driver	A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible, and safe manner.
Dual Connectivity	According to 3GPP terminology ([TS 37.340]).
FRMCS Application Identity	

Terms	Definitions
	The FRMCS Application Identity is an identity presented by the application to the MC client.
FRMCS Domain	A FRMCS Domain is an administrative domain which comprises a Service Domain and a Transport Domain under the control of an FRMCS Operator.
FRMCS Gateway Function	It is an on-board gateway responsible for the coordination and managing of access to the FRMCS transport services offered by the FRMCS system.
FRMCS Onboard System	According to [TOBA-FRS] terminology. Note1: FRMCS Onboard System and On-Board FRMCS terms can be used interchangeably.
On-Board FRMCS	According to [TOBA-FRS] terminology. Note2: FRMCS Onboard System and On-Board FRMCS terms can be used interchangeably.
FRMCS Operator	An FRMCS Operator is a railway Infrastructure Manager, or an operator delegated by a railway Infrastructure Manager who manages the Transport Domain and/or Service Domain for which FRMCS policies and FRMCS user subscriptions are applicable.
FRMCS Radio Module	Modem with one or more 3GPP or/and non-3GPP radio access technologies supported by the FRMCS system.
FRMCS Service Domain	Implementation of (parts of) the Service Stratum which belongs to and/or is operated by a unique organisation.
FRMCS Service User Identity	The FRMCS Service User Identity is an MC Service (User) Identity as defined in [TS 23.280].
FRMCS System	Telecommunication system conforming to FRMCS specifications, consisting of Transport Stratum and Service Stratum.
FRMCS Transport Domain	Implementation of (part of) the Transport Stratum which belongs to and/or is operated by a unique organisation.
FRMCS User	Human or machine making use of Communication Services and/or Complementary Services.
FRMCS User Identity	The FRMCS User Identity is a unique identity associated with a single or multiple (FRMCS) User and can be complemented by alternative addressing schemes. The FRMCS User Identity is an MC (User) Identity as defined in [TS 23.280].
Function	A function is an autonomous and identifiable functional entity. The On-Board FRMCS contains identified component(s). A Function can be physical and/or logical.

Terms	Definitions
Functional Identity	A description of the function performed by a called or calling party. The functional identity can include characters and numbers. This is used within the functional addressing scheme to identify an end user/system by function or identity rather than by a specific item of radio equipment or user subscription.
Integrated Architecture	Represents an architecture where functions (e.g., hardware components) are installed in a confined and predefined area without physical separation (e.g., directly attached with each other) within an intended area of use, e.g. On-Board a train.
Interchangeability	Interchangeability of Radio Modules is a maintenance capability that enables the addition or replacement of Radio Modules without impact on the train applications and the train-application interface, OBAPP
Interface	An interface represents identifiable implementation of a reference point. An interface exposes functionalities associated to Functions. An interface can be specified or unspecified in this specification.
Media	The exchange of information among Railway Applications endpoints passing through the FRMCS System.
Modularity	Decomposition of a system into subsystems with standardized interfaces.
Network Slice	According to 3GPP terminology ([TS 23.501]).
OB_{APP} Control Plane	Flow of information between applications and the On-Board FRMCS (e.g., through an API) pertaining to registration to the On-Board FRMCS and to request for services (communication-related or others) enabled by the On-Board FRMCS.
OB_{APP} User Plane	Flow of information to and from applications going through the On-Board FRMCS.
Policy and Charging Control	According to 3GPP terminology ([TS 23.503]).
Railway Application Stratum	Railway-specific functionalities using services offered by the FRMCS Service Stratum.
Radio Function	The Radio Function is currently FFS and a definition will be given when it is consolidated.
Radio Access Technology	According to 3GPP terminology ([TR 21.905]).
Reference Point	According to ITU-T terminology ([ITU-T-M.60]).
Reliability	

Terms	Definitions
	The probability that an item can perform a required function under stated conditions for a given time interval.
Scalability	Scalability refers to a system in which there is the possibility of extending it as the number of users and resources grows.
Security	According to 3GPP terminology ([TR 21.905]).
Service Continuity	According to 3GPP terminology ([TR 21.905]).
Service Stratum	Communication Services and Complementary Services.
Signalling	The exchange of information specifically concerned with the establishment and control of communications, and with management, in the FRMCS System.
SIP Core	According to 3GPP ([TS 23.280 clause 7.4.3.1.3.1]).
Subsystem	A Subsystem is a System included in higher order system.
System	A System is an autonomous functional entity. A System is composed of Function(s).
System Context	The System Context defines the part of the environment of a System, which is relevant for the definition of requirements for this System.
Transport Stratum	Set of access functions and corresponding core functions applicable for the FRMCS system.
User Equipment	According to 3GPP terminology ([TR 21.905]). In this context, the Mobile Termination (MT) corresponds to the FRMCS Radio Module that enables radio capabilities within the FRMCS Transport Stratum.
User Plane	The User Plane (sometimes called data plane or bearer plane) carries the user/application traffic.
Vendor Diversity	Possibility to use a Subsystem provided by one vendor with a Subsystem provided by another vendor.

3 References

3.1 Applicability

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

3.2 List of References

[FRMCS-URS]	FU-7100 v5.0.0 February 2020: “FRMCS User Requirements Specification”.
[FRMCS-FRS]	FU-7120: “FRMCS Functional Requirements Specification”.
[TOBA-FRS]	TOBA-7510: “FRMCS Telecom On-Board System – Functional Requirements Specification”.
[FIS]	FRMCS Functional Interface Specification
[FFFIS]	FRMCS FFFIS Form Fit Functional Interface Specification
[TR 21.905]	3GPP TR 21.905: “Vocabulary for 3GPP Specifications”.
[TS 22.261]	3GPP TS 22.261: “Technical Specification, Service requirements for the 5G system; Stage 1”.
[TS 22.280]	3GPP TS 22.280: “Mission Critical Services Common Requirements (MCCoRe); Stage 1”.
[TS 22.289]	3GPP TS 22.289: “Technical Specification, Mobile Communication System for Railways; Stage 1”.
[TR 22.889]	3GPP TR 22.889: “Technical Specification Group Services and System Aspects; Study on Future Railway Mobile Communication System; Stage 1”.
[TR 22.989]	3GPP TR 22.989: “Technical Specification Group Services and System Aspects; Study on Future Railway Mobile Communication System; Stage 1 (Release 18)”.
[TR 22.990]	3GPP TR 22.990: “Technical Specification Group Services and System Aspects; Study on Off-Network for Rail; Stage 1 (Release 18)”.
[TS 23.003]	3GPP TS 23.003; “Numbering, addressing and identification”
[TS 23.228]	3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”
[TS 23.280]	3GPP TS 23.280: “Common functional architecture to support mission critical communication”.
[TS 23.281]	3GPP TS 23.281: “Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2”
[TS 23.282]	3GPP TS 23.282: “Mission Critical Data – Architecture and flows”.
[TS 23.289]	3GPP TS 23.289: “Mission Critical Services over 5G System”.
[TS 23.379]	3GPP TS 23.379: “Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2”
[TS 23.501]	3GPP TS 23.501: “Technical Specification, System Architecture for the 5G System; Stage 2”.
[TS 23.502]	3GPP TS 23.502: “Procedures for the 5G System (Stage 2) v17.0.0, 03-2021”.
[TS 23.503]	3GPP TS 23.503: “Policy and charging control framework for the 5G System”.
[TS 24.282]	3GPP TS 24.282: “MCData Signalling Control – protocol specification”.
[TS 24.379]	3GPP TS 24.379: “Mission Critical Push To Talk (MCPTT) call control; Protocol specification”
[TS 26.179]	3GPP TS 26.179: “MCPTT: Codecs and media handling”.
[TS 33.180]	3GPP TS 33.180: “Technical Specification Group Services and System Aspects; Security of the Mission Critical (MC) service”.
[TS 33.203]	3GPP TS 33.203: ”3G security; Access security for IP-based services”.
[TS 33.501]	3GPP TS 33.501: “Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system”.
[TS 103 764]	ETSI TS 103 764: “Rail Telecommunications (RT); Future Rail Mobile Communication System (FRMCS); FRMCS System Architecture”.
[TS 103 765-1]	ETSI TS 103 765-1: “Future Rail Mobile Communication System (FRMCS); Building Blocks and Functions; Part 1: Transport Stratum”.
[TS 103 765-2]	ETSI TS 103 765-2: “Future Rail Mobile Communication System (FRMCS); Building Blocks and Functions; Part 2: Service Stratum”.
[TS 103 765-4]	ETSI TS 103 765-4: “Future Rail Mobile Communication System (FRMCS); Building Blocks and Functions; Part 4: FRMCS Trackside”.
[TS 103 792]	ETSI TS 103 792: “Rail Telecommunications (RT); Future Rail Mobile Communication System (FRMCS); GSM-R/FRMCS Interworking”.
[ECC decision (20)02]	ECC decision (20)02: “Harmonised use of the paired frequency bands 874.4-880.0 MHz and 919.4-925.0 MHz and of the unpaired frequency band 1900-1910 MHz for Railway Mobile Radio (RMR)”.

[EC Decision on 2021/1730]	COMMISSION IMPLEMENTING DECISION (EU) 2021/1730 of 28 September 2021: "Harmonised use of the paired frequency bands 874,4-880,0 MHz and 919,4-925,0 MHz and of the unpaired frequency band 1 900-1 910 MHz for Railway Mobile Radio".
[IR 65]	GSM Association IR.65: "IMS Roaming, Interconnection and Interworking Guidelines".
[i.1]	ISA 62443-1-2 D2E1: "Master glossary of terms and abbreviations".
[i.3]	https://csrc.nist.gov/glossary
[i.4]	"International Electrotechnical Vocabulary (IEV) - Part 903: Risk assessment,"
[i.5]	CENELEC TS 50701, IEC 60050-903: "Railway applications – Cybersecurity".
[i.7]	https://gdpr.eu/
[i.8]	ENISA, Security in 5G Specifications, Controls in 3GPP Security Specifications (5G SA).
[ITU-T-M.60]	ITU-T Recommendation M.60: "Maintenance terminology and definitions".
[TAF TSI]	Commission regulation Section 4.2.3 "Train preparation" and section 4.2.4 "Train running forecast" Technical document TAF/TSI: 'Annex D.2: Appendix F — TAF TSI Data and Message Model' listed in Appendix I.
[TAP TSI]	Commission regulation and its amendments Section 4.2.14: "Train preparation" and section 4.2.15 « train running information and forecast » Technical document B.30 annex III (see ERA-TD-105: TAF TSI - Annex D.2: Appendix F - TAF TSI Data and Message Model, Version 2.0.).
[SUBSET-037-3]	UNISIG SUBSET-037-3: "ERTMS/ETCS: EuroRadio FIS – FRMCS Communication Functional Module".
[RFC-8200]	IETF RFC 8200 July 2017: "Internet Protocol, Version 6 (IPv6) Specification".
[RFC-1034]	IETF RFC 1034 November 1987: "DOMAIN NAMES - CONCEPTS AND FACILITIES".
[RFC-1035]	IETF RFC 1035 November 1987: "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION".
[RFC-1123]	IETF RFC 1123 October 1989: "Requirements for Internet Hosts -- Application and Support".
[RFC-1995]	IETF RFC 1995 August 1996: "Incremental Zone Transfer in DNS".
[RFC-3261]	IETF RFC 3261 June 2022: "SIP: Session Initiation Protocol".
[RFC-3966]	IETF RFC 3966 December 2004: "The tel URI for Telephone Numbers".

4 Introduction

4.1 Background

4.1.1 The predicted obsolescence of GSM-R, combined with the long-term life expectancy of ETCS and the Railway business needs, have led to the European Railway community initiating work to identify a successor for GSM-R.

4.1.2 GSM-R is a MOTS technology based around manufacturers' commercial GSM offerings, enhanced to deliver specific "R" (railway) functionality. Due to the product modifications required to provide "R" functionality, and the need to utilise non-commercial radio spectrum, much of the equipment utilised for GSM-R comprises manufacturers' bespoke equipment and/or software variants.

4.1.3 The successor has to be future proof, learn from past experiences, lessons and comply with Railway requirements.

4.1.4 This document is one of the first steps in this process to identify a successor for GSM-R, where the railways' needs are identified and defined in a consistent and technology independent way as much as possible, the foundation for next steps on defining the FRMCS.

4.1.5 The FRMCS SRS is part of the FRMCS specifications as depicted in Figure 4-1.

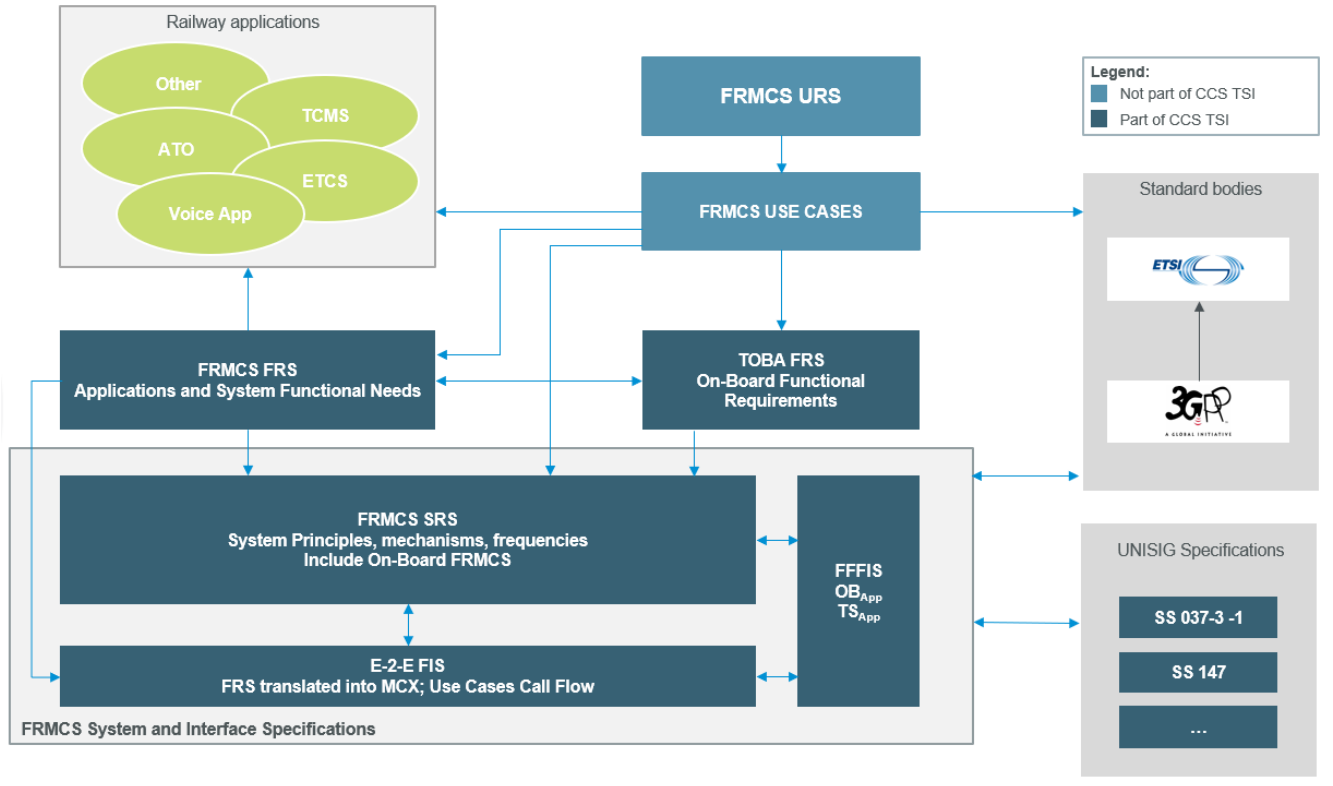


Figure 4-1: FRMCS specifications

4.2 Purpose of this document

4.2.1 The purpose of this document is to specify the system requirements satisfying the communication needs of the railway sector for the next generation communication system, as a successor of GSM-R. The new communication system is called FRMCS, the Future Railway Mobile Communication System.

4.2.2 The FRMCS System Requirements Specification (FRMCS SRS) shall enable Interoperability of rail communications within various administrative domains across geographical domains (i.e., Countries).

4.2.3 In addition, the FRMCS System Requirements Specification (FRMCS SRS) shall enable Telecom Interoperability to ensure interoperability of a variety of implementations in a multi-vendors ecosystem.

4.2.4 The necessary requirements of the On-Board FRMCS are detailed in chapter 7. (I)

4.3 Scope

4.3.1 The scope of the present FRMCS SRS is:

1. To define the system functions and mechanisms of an FRMCS System to enable the functional requirements of [FRMCS-FRS]. In addition, the FRMCS SRS provides necessary parameters and configurations of elementary functions and system blocks which are defined by ETSI Technical Specifications.

2. To define the FRMCS System Architecture Design principles (i.e., System characteristics).

3. To define the FRMCS System Reference Architecture (mobile and fixed), to define subsystems, components and the internal and external reference points or interfaces between them.

4. To refer all applicable standards and specifications upon which the FRMCS System is based.

5. To capture the non-functional System requirements (refer to section 17).

4.3.2 Requirements on radio spectrum will differ according to regions of the world. As an example, for the European Union, the CCS TSI will indicate the spectrum bands intended for interoperability as described in chapter RMR frequency bands for Europe.

Note: RMR encompasses GSM-R and its successor(s), including the Future Railway Mobile Communication System (FRMCS).

4.4 Applicability

4.4.1 The statements made in the present FRMCS SRS specification are assigned to the following categories:

- **Mandatory for the System (indicated by '(M)'** at the end of the clause). These requirements mean a condition set out in this specification that must be met without exception in order to deliver a system ensuring the fulfilment of essential functional and system needs, compliance to relevant standards and technical integration. The mandatory requirements are identified as sentences using the keyword "shall".

- **Optional for the system (indicated by '(O)'** at the end of the clause). These requirements may be used based on the implementers' choice. When an option is selected, the related requirement(s) of this specification becomes mandatory for the system. The optional requirements are identified as sentences using the keyword "should".

- **Information (indicated by '(I)'** at the end of the clause). These statements provide additional information to help the reader understanding a requirement.

Please note that NA is used to indicate that a particular item is not applicable and will therefore not need to be supported.

4.4.2 From chapter 5 onwards the category indication is included.

4.5 Document Life Cycle

4.5.1 This document is subject to the change management process established at UIC. (I)

Editor's note: The versioning and life cycle management process of this document is FFS.

5 System Architecture Design Principles

5.1 Scope of FRMCS System and System Architecture

5.1.1 The FRMCS System provides communication services applicable for operational purposes covering the following types of railways: (I)

1. High speed rail systems
2. Conventional rail systems

5.1.2 The FRMCS System should be applicable for operational purposes covering the following types of railways: (I)

1. Urban rail (including light rail)
2. Metro rail

5.1.3 To enable the functional requirements of [FRMCS-FRS], the FRMCS System defines the necessary technical building blocks and corresponding functionalities (refer to Annex C – Mapping of FRS to SRS requirements). (I)

5.1.4 To enable independence between Railway Applications and the necessary physical transmission, a Service Stratum is introduced as an abstraction layer, that acts as separation and adaptation layer between Railway Applications and Transport stratum. Therefore, in principle, the FRMCS Architecture consists of three major Strata, of which only two strictly belong to the FRMCS System, Service and Transport (refer to Figure 5-1): (I)

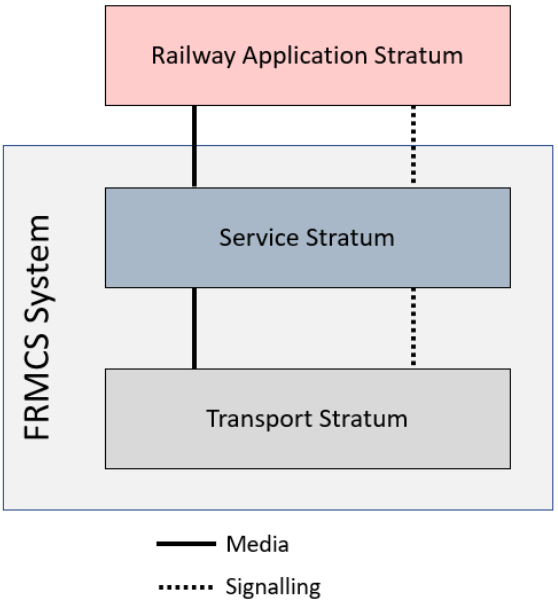


Figure 5-1 Railway Application, Service and Transport Strata

5.1.5 The FRMCS System shall provide interfaces to Railway Applications (e.g., ETCS), as depicted in Figure 5-1. (M)

5.2 Principles for System Requirements

5.2.1 The FRMCS System provides communication services with various patterns, precisely Voice, Video and Data, and combinations of these in a multimedia context. (I)

5.2.2 The FRMCS System provides complementary services such as (not exhaustive list): (I)

1. Location Information Services
2. Context aware services
3. Time synchronization services
4. Presence services

5.2.3 The FRMCS System supports QoS policies (priority, precedence) in order to discriminate between different types of railway applications as described in chapter Quality of Service and Priority. (I)

5.2.4 The FRMCS System provides communication services between many types of FRMCS Users, such as: (I)

1. Trains, including train drivers (via a FRMCS On-Board System, refer to 6.3.2) and onboard applications;
2. Trackside entities and applications (e.g., RBCs);
3. Railway personnel with FRMCS-capable handsets or communication devices;
4. Objects equipped with FRMCS communication capabilities (e.g., wireless sensors, drones).

5.2.5 The FRMCS System is able to support multiple Radio Access Technologies to facilitate evolution of technology. (I)

6 System Reference Architecture and Reference Points

Editor's Note: In the present version of the SRS, the Reference System Architecture focuses on describing the operation in on-network mode whereby communication entities rely on a telecommunication infrastructure for their communications. The off-network mode of operation (similar to what is known as "Direct Mode" in GSM-R) is FFS.

6.1 Preamble

6.1.1 Generalities

6.1.1.1 The FRMCS System provides communication services between many types of FRMCS Users, as described in section 5.2. (I)

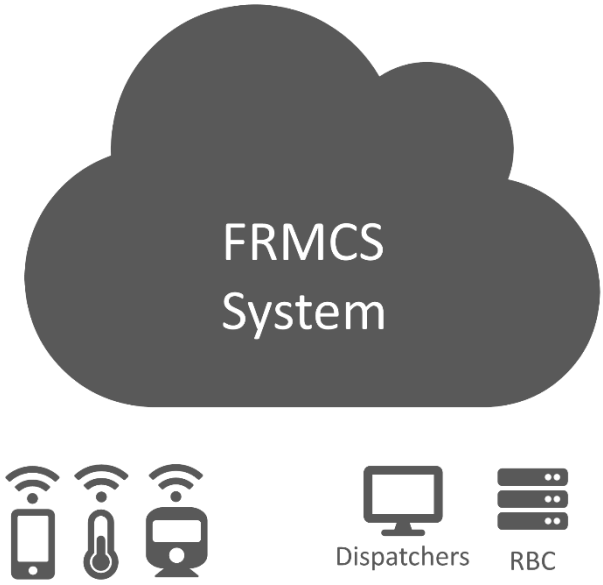


Figure 6-1 - FRMCS System and a subset of entities using communication services of the FRMCS System

6.1.1.2 A FRMCS Domain is an administrative domain which comprises a Service Domain and a Transport Domain under the control of an FRMCS Operator. (I)

6.1.1.3 The FRMCS System is constituted of one or multiple FRMCS Domains. FS_{NNI} is used to interconnect these FRMCS Domains (see Figure 6-2). The FRMCS On-Board System, specified in ([TOBA-FRS] and chapter 7), is a sub-system within the FRMCS System, installed onboard the trains and enabling communication services with the FRMCS Domains. (I)

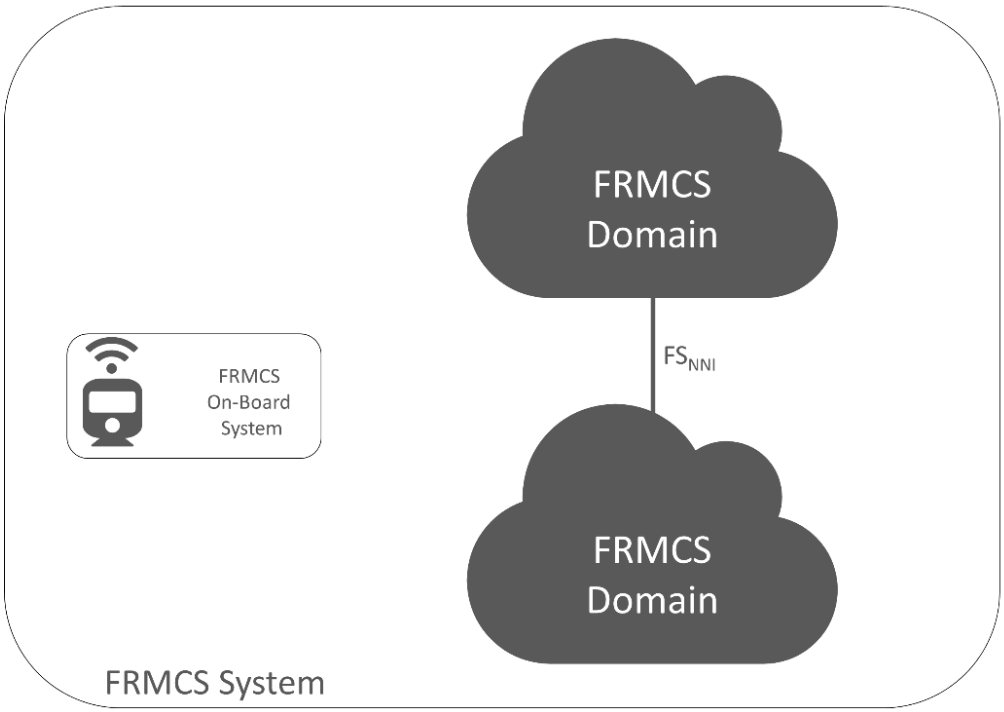


Figure 6-2 - FRMCS System and FRMCS Domains

6.1.1.4 The FRMCS System interworks with other systems such as GSM-R or systems that are neither GSM-R nor FRMCS. (I)

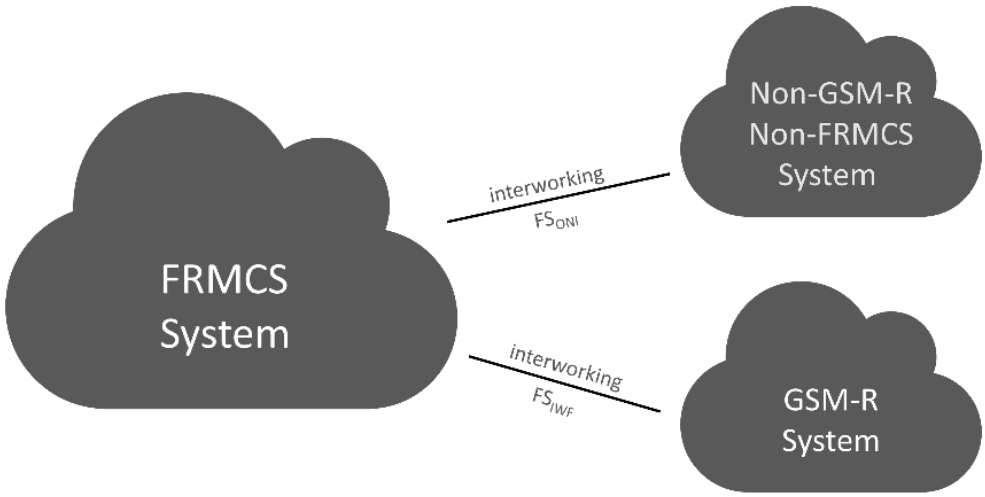


Figure 6-3 - Relation between the FRMCS System and external systems

6.1.1.5 The FRMCS System shall support interconnection between FRMCS Domains via the FS_{NNI} reference point (see 6.4.4.2). (M)

6.1.1.6 The FRMCS System shall support interworking with GSM-R systems via the FS_{IWF} reference point (see 6.4.4.1). (M)

6.1.1.7 The FRMCS System should support interworking with non-GSM-R / non-FRMCS systems via the FS_{ONI} reference point (see 6.4.4.3). (O)

6.1.1.8 FRMCS communication services shall rely: (M)

- on the transport services provided by access networks based primarily on 3GPP technology (with support of 3GPP and non-3GPP access) but supporting also non-3GPP transport networks,
- and on a service layer leveraging the functionalities of the 3GPP Mission-Critical framework (including a SIP Core).

6.1.1.9 An FRMCS Domain shall encompass the minimum necessary components: (M)

- In the Transport Domain:
  - A 5G Core Network,
  - An 5G Access Network supporting at least the RMR harmonized spectrum (see section 8),
- In the Service Domain:
  - A MCX infrastructure, including a SIP Core.

6.1.2 High-level architecture diagram of communicating entities within the FRMCS Domain

6.1.2.1 The following diagram provides a high-level perspective on the major functional blocks of the FRMCS Architecture. (I)

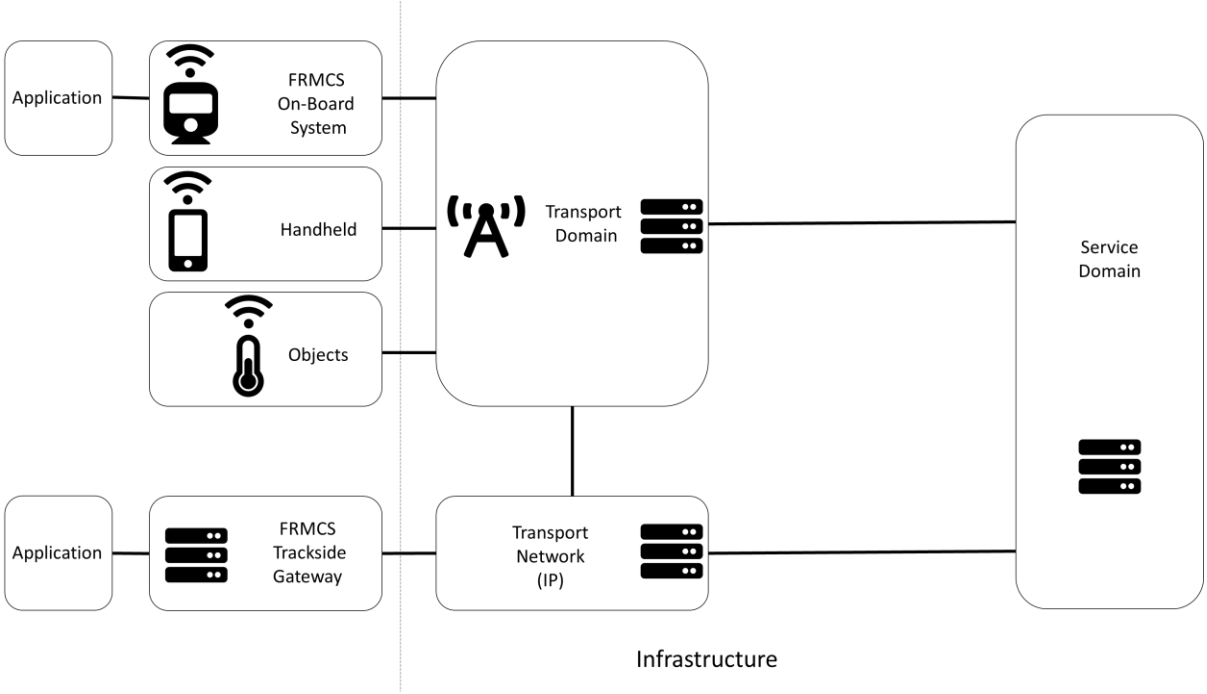


Figure 6-4 - high-level architecture diagram of communicating entities within the FRMCS system

Editor's Note: a proposal has been made to depict a realization of the architecture to provide as an example, possibly in an Appendix. TBD

6.1.2.2 The FRMCS On-Board System (see 6.3.2) provides communication services via capabilities of the Transport Domain to and from onboard applications / entities. (I)

6.1.2.3 The FRMCS Trackside Gateway (see 6.3.3) provides access to communication and supplementary services supported by the FRMCS System to and from trackside applications. (I)

6.1.2.4 The Transport Domain (see 6.3.6) comprises one or more FRMCS Transport Domains and zero or more Non-FRMCS Transport Domain. (I)

6.1.2.5 The FRMCS Service Domain (see 6.3.5) shall include a MCX infrastructure, including a SIP Core. (M)

6.1.3 Applications

Note: this section 6.1.3 is applicable to FRMCS On-Board System only, not to FRMCS capable handhelds and FRMCS-capable Objects.

6.1.3.1 General case

6.1.3.1.1 Applications using the FRMCS System shall use the OB_{APP} (for onboard applications) and TS_{APP} reference points (for trackside applications). (M)

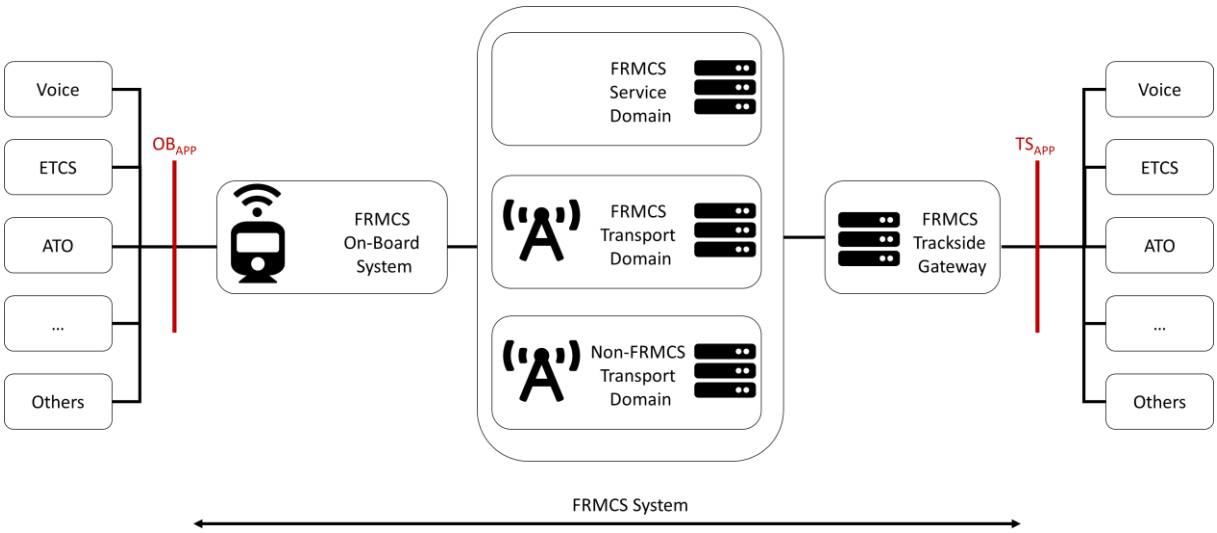


Figure 6-5 - FRMCS reference points used by application to access the FRMCS System

6.1.3.1.2 Applications using the FRMCS System can be categorized in various application regimes depending on the nature and extent of usage of the OB_{APP} and TS_{APP} reference points. (I)

Application regime	OB_{APP} / TS_{APP} coupling mode	FRMCS Service Stratum client in application?	FRMCS Service Stratum client in FRMCS On-Board System / in FRMCS Trackside Gateway?
Tight	Tight	Yes	No
Loose	Loose	No	Yes
Superloose	Loose (via agent)	No	Yes

Table 2 Application regimes (I)

Editor's Note: the applicability / feasibility of the Superloose application regime for a trackside application is FFS.

Editor's Note: Superloose application regime is defined as per the above table as the application being OBapp-unaware and interacting through an agent (out of FRMCS specs) implementing OBapp on behalf of the application. A supporting diagram is considered to be added in a future edition of the SRS.

Note: a communication via an agent is not valid for tight-coupling applications.

6.1.3.1.3 The "Coupling Mode" reflects whether an application environment encompasses a FRMCS Service Stratum client ("Tight Coupling Mode") or not ("Loose Coupling Mode"). (I)

Note: Applications using the Tight application regime have an application environment which spans across the Application Stratum / Service Stratum boundary.

6.1.3.1.4 For information on the mapping between application regimes and applications from the ([FRMCS-URS]), please refer to Annex B. (I)

Editor's Note: QoS chapter has done a broad categorization of mappings; consistency shall be somehow ensured

6.1.3.2 Applications leveraging a Coordinating Function

6.1.3.2.1 During the period of coexistence between GSM-R and FRMCS, railway applications that have to operate on either system depending on radio coverage, operational rules or for other reasons will make use of a “Coordinating Function” responsible for the interface with either the GSM-R CS, GSM-R PS or the FRMCS system. (I)

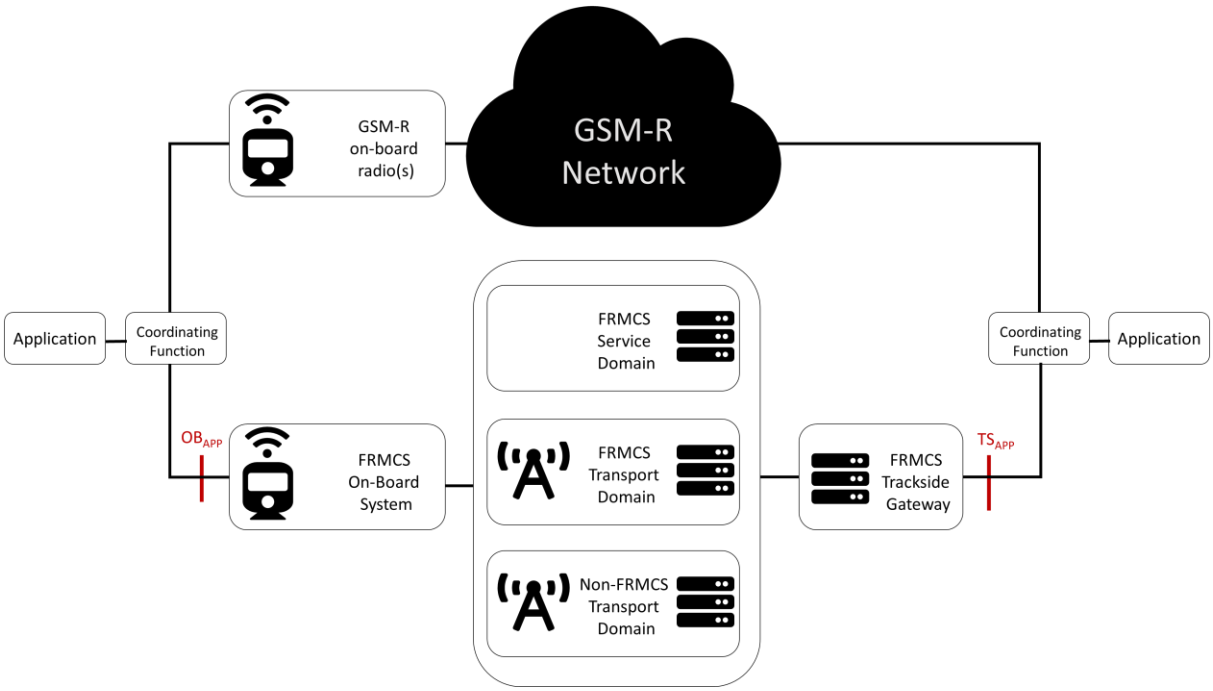


Figure 6-6 - the Coordinating Function in relation to the FRMCS System

6.1.3.2.2 For an application using a Coordinating Function to interface with the FRMCS System, the Coordinating Function uses the functionalities of the OB_{APP} reference point for an onboard application or the TS_{APP} reference point for a trackside application. (I)

Note: The Coordinating Function specification is out of the scope of the present SRS.

6.1.4 System Layers

6.1.4.1 The FRMCS Reference System Architecture is structured in two “layers” (also individually referred to as “Stratum”, plural “Strata”) called "Service Stratum" and "Transport Stratum". External to the FRMCS System, applications using the FRMCS System are grouped in a third "layer" named "Application Stratum". (I)

6.1.4.2 Application Stratum

Editor’s note: will be elaborated upon

6.1.4.3 Service Stratum

Editor’s note: will be elaborated upon

6.1.4.3.1 The Service Stratum shall enable interconnection between Service Domains (M).

6.1.4.4 Transport Stratum

Editor's note: will be elaborated upon. Amongst other things, the notion of Transport Domain and the possible presence of multiple Transport Domains (especially in case of FRMCS Multipath) would need to be described.

6.1.4.4.1 The Transport Stratum shall enable interconnection between Transport Domains (M).

6.2 Description of the System Reference Architecture

6.2.1 Intra-FRMCS-System Reference Architecture

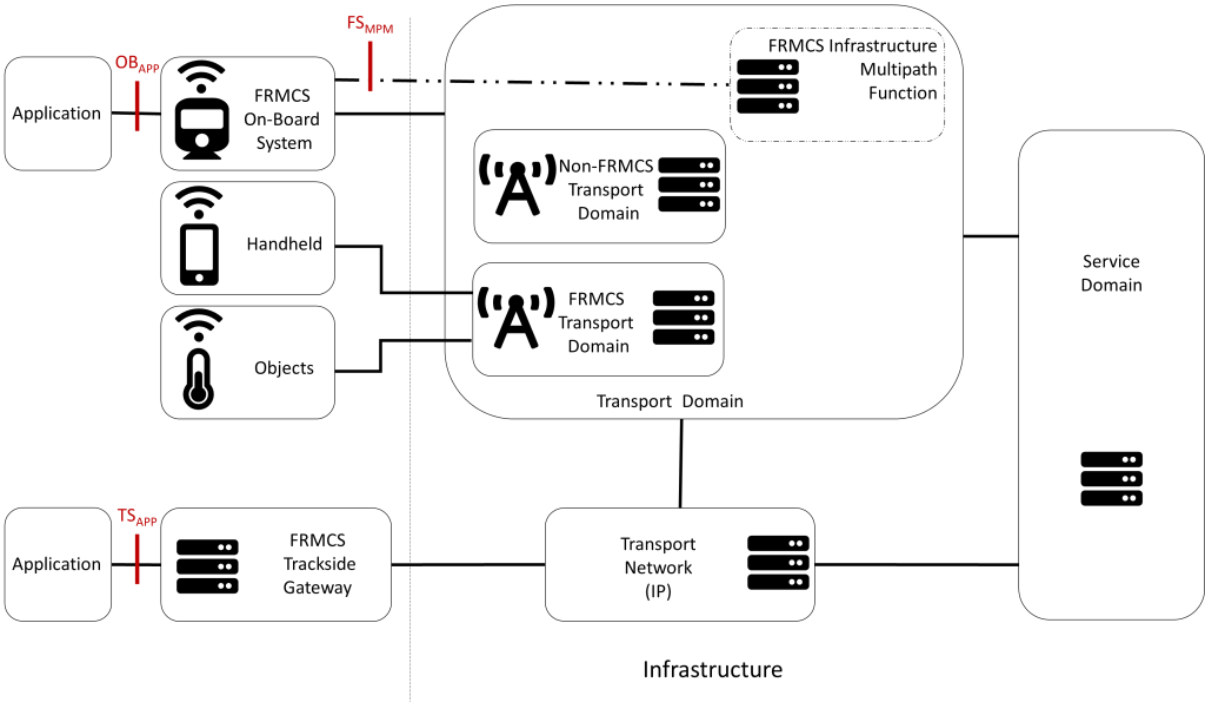


Figure 6-7 - System Reference Architecture

6.2.1.1 The building blocks of the System Reference Architecture are described in section 6.3. (I)

6.2.1.2 Reference points OB_{APP} (see 6.4.1.1), TS_{APP} (see 6.4.1.2), FS_{OMR} (see 6.4.3.1) and FS_{MPM} (see 6.4.2.1) are defined in subsequent sections. (I)

Editor's Note: need to reintroduce the FS_{OMR} in this section.

6.2.2 Inter-FRMCS Domain

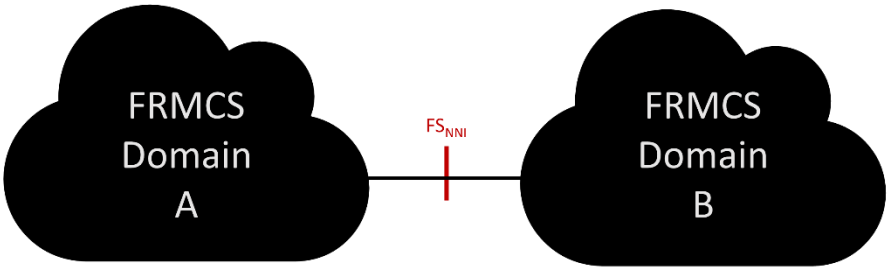


Figure 6-8 - FRMCS System: reference point between FRMCS Domains

6.2.2.1 The reference point FS_{NNI} is defined in a subsequent section (see 6.4.4.2). (I)

6.2.3 FRMCS System in relation to external systems

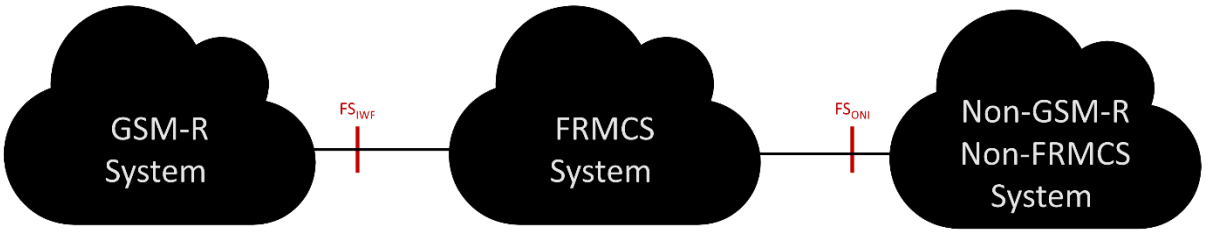


Figure 6-9 - FRMCS System: reference points towards external systems

6.2.3.1 Reference points FS_{IWF} (see 6.4.4.1) and FS_{ONI} (see 6.4.4.3) are defined in subsequent sections. (I)

6.3 Decomposition into building blocks

6.3.1 The major functional building blocks of the System Reference Architecture are described in the present section. (I)

Editor's Note: the specification of the "Handheld" building block is FFS.

6.3.2 FRMCS On-Board System

6.3.2.1 The FRMCS On-Board System provides wireless access to communication services supported by the FRMCS System to and from onboard applications. (I)

6.3.2.2 The responsibilities of the FRMCS On-Board System include:

- Providing communication services to and from authorized onboard applications. (I)
- Providing additional services to applications, e.g.
  - Status of the communication service
  - Positioning information (FFS)
  - Time Service information (FFS)
- Exposing functionalities of its Operation & Management Function to authorized external Operation & Management entities (I)
- Supporting FRMCS Multipath features through interaction with the FRMCS Infrastructure Multipath Function. (I)
- Controlling the User Equipment(s) interfacing with the Transport Domain. (I)

6.3.2.3 The FRMCS On-Board System conforms to the specifications in Chapter 7 of this document. (I)

6.3.3 FRMCS Trackside Gateway

6.3.3.1 The FRMCS Trackside Gateway enables communication services supported by the FRMCS System to and from authorised trackside applications. (I)

6.3.3.2 The FRMCS Trackside Gateway shall conform to ([TS 103 765-4]). (M)

6.3.4 FRMCS Infrastructure Multipath Function

6.3.4.1 The FRMCS Infrastructure Multipath Function is the infrastructure counterpart of the FRMCS On-Board Multipath Management Function within the FRMCS On-Board System. (I)

6.3.4.2 The responsibilities of the FRMCS Infrastructure Multipath Function include:

- negotiating and managing the use of multiple transport paths over multiple UEs with the FRMCS On-Board Multipath Function of the FRMCS On-Board System. (I)

6.3.4.3 The FRMCS Infrastructure Multipath Function shall conform to ([TS 103 765-1]). (M)

6.3.4.4 The concept of FRMCS Multipath is further discussed as part of the “bearer flexibility” concept in section 12. (I)

6.3.5 FRMCS Service Domain

6.3.5.1 A Service Domain shall enable access of users belonging to other Service Domains if they have been granted such right. (M)

6.3.5.2 A Service Domain shall enable communication between authorised users of other Service Domains if they have been granted such right. (M)

6.3.5.3 The FRMCS Service Domain functionalities shall be realized by a 3GPP MCX server infrastructure (including a SIP Core). (M)

6.3.5.4 The functionalities required for the FRMCS Service Domain shall conform to [TS 103 765-2]. (M)

6.3.6 Transport Domain

6.3.6.1 The Transport Domain comprises one or more FRMCS Transport Domain(s) and zero or more Non-FRMCS Transport Domain(s). (I)

6.3.6.2 A Domain within the Transport Domain consists of a Core Network managing one or more 3GPP and/or non-3GPP Access Networks. (I)

6.3.6.3 At least one of the Access Networks controlled by the core network of a FRMCS Domain shall support the RMR spectrum in accordance with [EC Decision 2021/1730]. (M)

6.3.6.4 An FRMCS Transport Domain shall include a 5G Core Network and one or more Access Networks under the control of the 5G Core Network. (M)

6.3.6.5 A Non-FRMCS Transport Domain is a Domain within the Transport Domain which does not satisfy the mandatory requirements of a FRMCS Transport Domain. (I)

6.3.6.6 The functionalities required for the FRMCS Transport Domain shall conform to [TS 103 765-1]. (M)

6.4 Description of System Architecture Reference Points

6.4.1 Application reference points

6.4.1.1 OB_{APP}

6.4.1.1.1 The OB_{APP} reference point is exposed by the FRMCS On-Board System and provides the means for onboard applications to make use of the communication services offered by the FRMCS On-Board System. (I)

6.4.1.1.2 The OB_{APP} reference point also provides the means for additional services to applications, e.g., (I)

- Status of the communication service
- Positioning information (FFS)

6.4.1.1.3 The use of the communication services exposed by the OB_{APP} reference point is conditional on the success of the authentication and authorisation steps (Local Binding) between an application and the FRMCS On-Board System. (I)

6.4.1.1.4 The OB_{APP} reference point shall conform to ([FFFIS]). (M)

6.4.1.1.5 The OB_{APP} interface shall enable data flow between on-board applications and On-Board FRMCS. (M)

6.4.1.1.6 The interface defined over OB_{APP} reference point shall enable data flow for voice communication. (M)

6.4.1.1.7 The interface defined over OB_{APP} reference point shall enable data flow for data communication. (M)

6.4.1.1.8 The interface defined over OB_{APP} reference point shall enable data flow for video communication. (M)

6.4.1.1.9 The interface defined over OB_{APP} reference point shall have the capability to enable integrity of data flow(s). (M)

6.4.1.1.10 The interface defined over OB_{APP} reference point shall have the capability to enable confidentiality of data flow(s). (M)

Editor's note: Integrity and Confidentiality are FFS in later release of this specification document.

6.4.1.1.11 The interface defined over OB_{APP} reference point shall be accessible via an API. (M)

6.4.1.2 TS_{APP}

6.4.1.2.1 The TS_{APP} reference point is exposed by the FRMCS Trackside Gateway and provides the means for trackside applications to make use of the communication services offered by the FRMCS Trackside Gateway. (I)

6.4.1.2.2 The use of the communication services exposed by the TS_{APP} reference point is conditional on the success of the authentication step (Local Binding) between an application and the FRMCS Trackside Gateway. (I)

6.4.1.2.3 The TS_{APP} reference point shall conform to ([FFFIS]). (M)

6.4.2 FRMCS Multipath reference points

6.4.2.1 FS_{MPM}

6.4.2.1.1 The FS_{MPM} reference point is defined between the FRMCS On-Board Multipath Function within the FRMCS On-Board System and the FRMCS Infrastructure Multipath Function. (I)

6.4.2.1.2 The FS_{MPM} reference point enables the negotiation and management of the use of multiple transport paths over multiple UEs between the FRMCS On-Board System and the infrastructure. (I)

6.4.2.1.3 The FS_{MPM} reference point shall conform to ([TS 103 765-1]). (M)

6.4.3 O&M reference points

6.4.3.1 FS_{OMR}

Editor's Note: the FS_{OMR} reference point is the system-level equivalent of the OB_{OM} reference point defined within the FRMCS On-Board System, and is FFS.

6.4.3.1.1 The FS_{OMR} reference point is exposed between the FRMCS On-Board Operation & Management Function within the FRMCS On-Board System and an Operation & Management entity within the infrastructure. (I)

6.4.4 FRMCS interworking and interconnection reference points

6.4.4.1 FS_{IWF}

6.4.4.1.1 The FS_{IWF} reference point is defined between a FRMCS System and an EIRENE system (GSM-R based system). (I)

6.4.4.1.2 The FS_{IWF} reference point enables the interworking between a FRMCS System and an EIRENE system. (I)

6.4.4.1.3 The FS_{IWF} reference point shall conform to [TS 103 792]. (M)

6.4.4.2 FS_{NNI}

6.4.4.2.1 The FS_{NNI} reference point is defined between two FRMCS Domains. (I)

6.4.4.2.2 The FS_{NNI} reference point enables the interconnection between two FRMCS Domains to support e.g., border-crossing. (I)

6.4.4.2.3 The FS_{NNI} reference point shall conform to ([TS 103 765-1]) for functionalities applicable to FRMCS Transport Domain. (M)

6.4.4.2.4 The FS_{NNI} reference point shall conform to ([TS 103 765-2]) for functionalities applicable to FRMCS Service Domain. (M)

6.4.4.3 FS_{ONI}

6.4.4.3.1 The FS_{ONI} reference point is defined between a FRMCS System and another non-GSM-R, non-FRMCS System. (I)

6.4.4.3.2 The FS_{ONI} reference point shall conform to ([TS 103 765-1]) for functionalities applicable to FRMCS Transport Domain. (M)

6.4.4.3.3 The FS_{ONI} reference point shall conform to ([TS 103 765-2]) for functionalities applicable to FRMCS Service Domain. (M)

6.5 Addressing

6.5.1 IP Versions

6.5.1.1 The FRMCS System shall support the IP version 6 protocol suite only as its key technology at internal reference points. (M)

Note: The IP version supported by the underlying networks may differ.

6.5.1.2 The FRMCS System shall support the IP version 6 ([RFC-8200]) protocol suite as its key technology at external reference points (e.g., OB_{APP} and TS_{APP}). (M)

Editor's note: The support of IPv4, in addition to IPv6 for backward compatibility will be investigated for next revision of the FRMCS SRS.

6.5.2 Addressing principles

6.5.2.1 The FRMCS System supports the addressing schemes Host-to-Host (H2H) and Host-to-Network (H2N). (I)

Editor's note: using application input to estimate target identities is FFS.

6.5.2.2 Host-to-Host (H2H) addressing scheme

6.5.2.2.1 An FRMCS "Host" represents a single application entity within the FRMCS System, as depicted in Figure 6-10. (I)

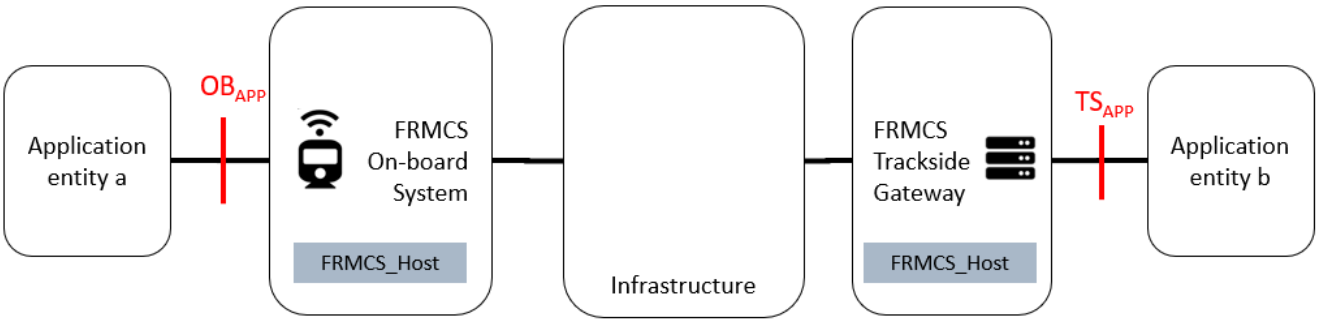


Figure 6-10: Host-to-Host (H2H) addressing principle (Loose-coupled example)

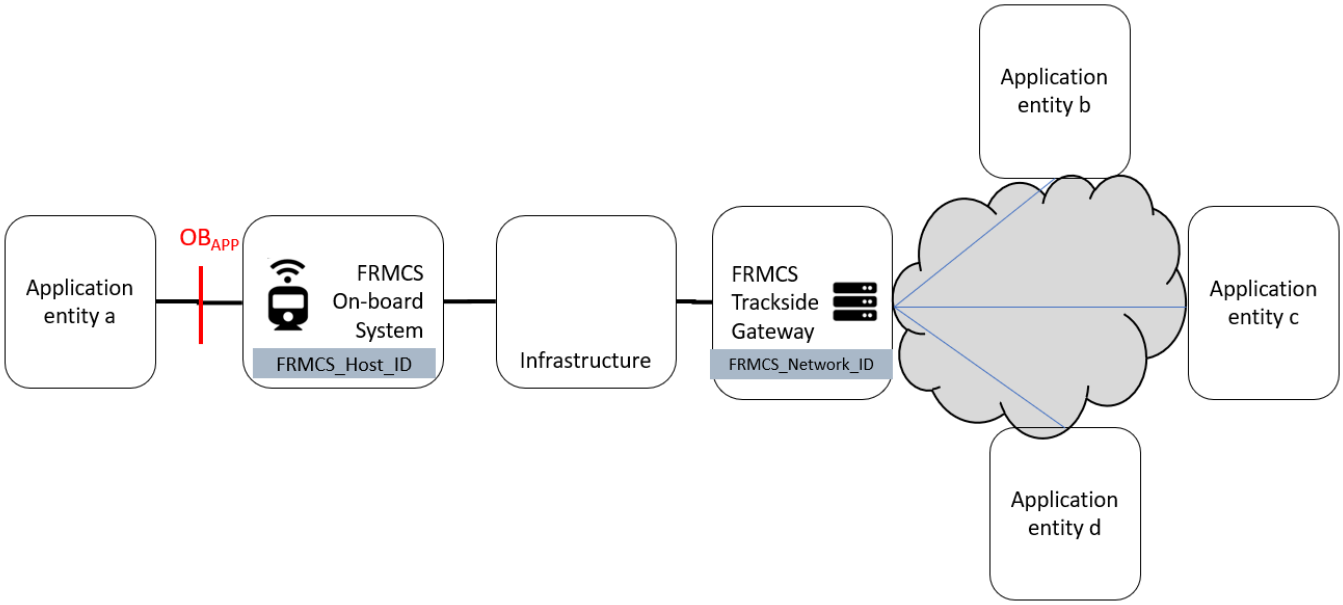
6.5.2.2.2 The FRMCS System shall support H2H approach for Loose-coupled and Tight-coupled Applications. (M)

6.5.2.2.3 Addressing within the FRMCS System of Automatic Train Protection (ATP) shall conform to H2H approach. (M)

6.5.2.2.4 Addressing within the FRMCS System of Automatic Train Operation (ATO) shall conform to H2H approach. (M)

6.5.2.3 Host-to-Network (H2N) addressing scheme

6.5.2.3.1 An FRMCS "Network" represents multiple application entities i.e., more than a single Application entity, within the FRMCS System, as depicted in Figure 6-11. (I)



Note 1: application entity represented by an FRMCS Host (e.g., a) is managing complementary application entities represented by an FRMCS Network (e.g., b, c and d).
Note 2: application entities (e.g., b, c, d) would refer to different functionalities (e.g., DNS, NTP, PKI, KMS in the context of ETCS)

Figure 6-11: Host-to-Network (H2N) addressing principle

6.5.2.3.2 The FRMCS System shall support H2N approach for Loose-coupled Applications. (M)

6.5.2.3.3 Addressing within the FRMCS System of complementary ATP applications (e.g., PKI, DNS, NTP, KMS) shall conform to H2N approach. (M)

7 Description of Subsystems and Constituents

Editor's note:
Needs to be developed further if deemed necessary:

7.1 On-board FRMCS

7.1.1 On-board scope

7.1.1.1 The On-Board FRMCS enables mobile communication services for entities/devices on board. (I)

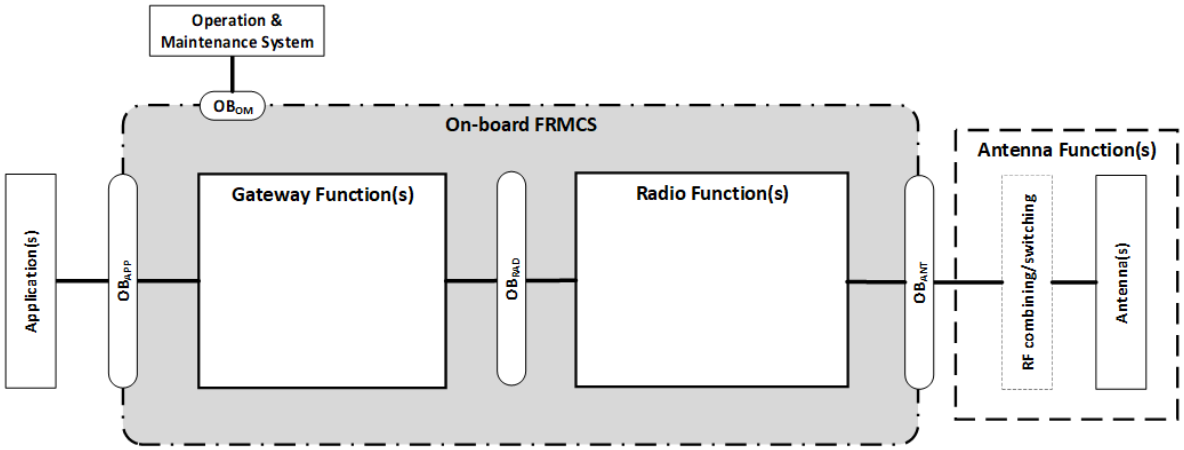


Figure 7-1: On-Board FRMCS architecture

7.1.1.2 On-Board FRMCS Boundaries

7.1.1.2.1 On-Board FRMCS boundaries are limited by external reference point(s). (I)
Note: Requirements for the corresponding OB_{APP} interface are specified in [FFFIS].

7.1.1.2.2 The reference point between On-Board FRMCS and FRMCS is OB_{ANT}. (I)

7.1.1.2.3 The reference point between the On-Board FRMCS and the Operation and Maintenance System(s) is OB_{OM}. (I)

7.1.1.2.4 The On-Board FRMCS encompasses FRMCS Transport Stratum and FRMCS Service Stratum as described in this document.
Note: QoS requirements are specified in chapter 14.

7.1.2 System Architecture Design Principles

7.1.2.1 Underlying principles

7.1.2.1.1 The architecture is derived from principles following a Top-down approach. (I)

7.1.2.1.2 The principles shall govern the architectural design and evolution of the On-Board FRMCS managed by this specification. (I)

7.1.2.1.3 Interoperability across and within FRMCS Domains shall be one of the underlying design principles of this document. (I)

7.1.2.2 Design Principles

7.1.2.2.1 The separation of Strata (as described in the present document) is a design principle of the On-Board FRMCS. (I)

Note: The TOBA architecture refers only to Service and Transport Strata, not to the Application Stratum.

7.1.2.2.2 Modularity is a design principle of the On-Board FRMCS. (I)

7.1.2.2.3 Scalability is a design principle of the On-Board FRMCS. (I)

7.1.2.2.4 Vendor diversity of Radio Modules is a design principle of the On-Board FRMCS. (I)

7.1.2.2.5 Interchangeability is a design principle of the On-Board FRMCS. (I)

7.1.2.2.6 Distributed Architecture is a design principle of the On-Board FRMCS. (I)

7.1.2.2.7 Untrusted environment for local communication is a design characteristic of the On-Board FRMCS. (I)

7.1.3 On-Board FRMCS Architecture overview

7.1.3.1 Introduction

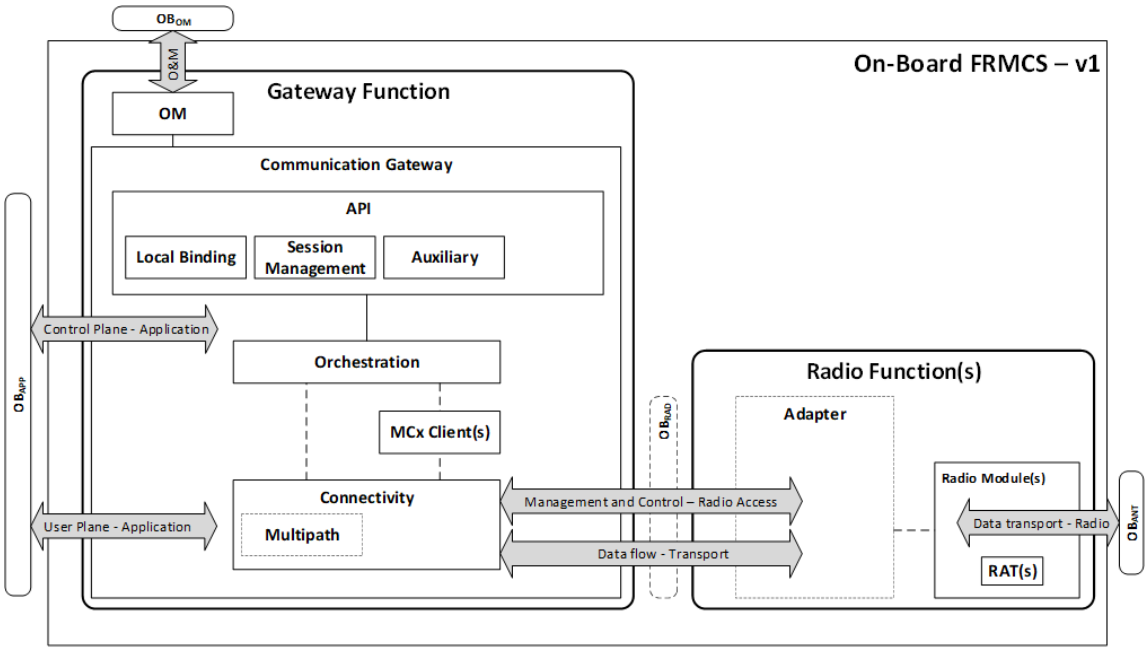


Figure 7-2: On-Board FRMCS architecture

7.1.3.1.1 The figure 7-2 represents the On-Board FRMCS Architecture which, together with its associated system requirements, describes the On-Board FRMCS v1. (I)

7.1.3.1.2 The schematic in Figure 7-2: is intended to support (at least) the following (I):

- Integrated classic architecture
- Integrated architecture providing interchangeability
- Distributed architecture

7.1.3.2 Architecture scope

7.1.3.2.1 The On-Board FRMCS includes the following functions (I):

- Gateway Function
- Radio Function

7.1.3.2.2 The Gateway Function includes the following functions (I):

- Communication Gateway
- OM

7.1.3.2.3 The Communication Gateway includes the following functions (I):

- API
- Orchestration
- MCX Client(s)
- Connectivity

7.1.3.2.4 The Radio Function includes the following functions (I):

- Adapter
- Radio Module(s)

7.1.4 Interfaces

7.1.4.1 External Interfaces

7.1.4.1.1 OB_{APP}

Note: Interface developed more in detail in section 6.4.2.1 of this document.

7.1.4.1.2 OB_{ANT}

7.1.4.1.2.1 Description

7.1.4.1.2.1.1 Interface OB_{ANT} is an implementation of the OB_{ANT} reference point. This interface enables communication over the air gap between On-Board FRMCS and Trackside. (I)

7.1.4.1.2.2 Interface Requirements

7.1.4.1.2.2.1 The On-Board FRMCS shall expose interfaces at the OB_{ANT} reference point. (M)

7.1.4.1.2.2.2 The On-Board FRMCS shall enable wireless Communication Services through external interfaces exposed at the OB_{ANT} reference point. (M)

7.1.4.1.2.2.3 OB_{ANT} should be implemented using suitable, current and widely adopted industry specifications. (I)

Editor's note: The system requirements of the OB_{ANT} interface will be specified in later version of this specification.

7.1.4.1.3 OB_{OM}

7.1.4.1.3.1 Description

7.1.4.1.3.1.1 Interface OB_{OM} is an implementation of the OB_{OM} reference point. (I)

7.1.4.1.3.1.2 Interface OB_{OM} enables on-board communication between Operation and Maintenance System and On-Board FRMCS. (I)

7.1.4.1.3.1.3 Interface OB_{OM} enables over the air gap communication between Operation and Maintenance System and On-Board FRMCS. (I)

Editor's note: OB_{OM} communication over the air gap is FFS (therefore not visualized in Figure 7-2:).

7.1.4.1.3.2 Interface Requirements

7.1.4.1.3.2.1 The On-Board FRMCS shall expose external interfaces at the OB_{OM} reference point. (M)

7.1.4.1.3.2.2 The On-Board FRMCS shall enable Operations and Maintenance by enabling the OB_{OM} interface over the air. (M)

7.1.4.2 Internal Interface between Gateway Function and Radio Function

7.1.4.2.1 OB_{RAD}

7.1.4.2.1.1 Description

7.1.4.2.1.1.1 Interface OB_{RAD} is an implementation of the OB_{RAD} reference point. (I)

7.1.4.2.1.1.2 Interface OB_{RAD} enables communication between Gateway Function and Radio Function(s). (I)

7.1.4.2.1.1.3 OB_{RAD} enables the objectives stated in clause 7.1.3.1.2. (I)

7.1.4.2.1.1.4 OB_{RAD} is used to control and manage radio modules within the Radio Function(s). (I)

7.1.4.2.1.2 Interface Requirements

7.1.4.2.1.2.1 OB_{RAD} shall enable Control Plane (Session) communication between Gateway Function and Radio Function(s). (M)

7.1.4.2.1.2.2 OB_{RAD} shall enable User Plane (Media) communication between Gateway Function and Radio Function(s). (M)

7.1.4.2.1.2.3 The OB_{RAD} Control Plane enables relocation of established communication session(s) between Radio Functions. (I)

7.1.4.2.1.2.4 OB_{RAD} Control Plane shall enable the selection and usage of Radio Function(s). (M)

7.1.4.2.1.2.5 OB_{RAD} Control Plane enables the selection and usage of the Radio Module(s) hosted by Radio Function(s). (I)

7.1.4.2.1.2.6 OB_{RAD} supports in-service replacement of Radio Function(s). (I)

7.1.4.2.1.2.7 OB_{RAD} is implemented using suitable, current and widely adopted industry specifications. (I)

Note 1: OB_{RAD} control plane is unrelated to OB_{APP} control plane.

Editor's note 1: OB_{RAD} User Plane requirements are FFS in later version of this specification.
Editor's note 2: Control Plane and User Plane terminology not aligned with Signalling and Media terminology. Alignment is FFS.

7.1.5 Gateway Function

7.1.5.1 Introduction

7.1.5.2 A Gateway Function encompasses Functions that enable the specification of (I):

- On-Board FRMCS system requirements related to communication service(s) enabled by FRMCS.
- System requirements related to the operation and maintenance of the On-Board FRMCS.

7.1.5.3 Communication Gateway

7.1.5.3.1 A Communication Gateway encompasses Functions related to communication service(s) for the On-Board FRMCS (I).

7.1.5.3.2 A Communication Gateway contains the following Functions with reference to Figure 7-2: (I):

- API
- Orchestration
- MCX Client(s)
- Connectivity

7.1.5.4 API

7.1.5.4.1 The API shall include the following functions (M):

- Local Binding
- Session Management
- Auxiliary

7.1.5.5 Local Binding

7.1.5.5.1 Introduction

7.1.5.5.1.1 The Local Binding function is a function of the API. (I)

7.1.5.5.1.2 The Local Binding Function enables authorized data flows and provides means to prevent unauthorized data flow(s). (I)

7.1.5.5.2 Requirements

7.1.5.5.2.1 For data flows associated to control plane of Application instances, Local Binding shall provide the following:

- Identification (M)

- Authentication (M)
- Integrity (M)
- Confidentiality (M)

7.1.5.5.2.2 Using Local Binding, the On-Board FRMCS should have the capability to identify itself to Applications. (O)

7.1.5.5.2.3 Using Local Binding, the On-Board FRMCS should have the capability to authenticate itself to Applications. (O)

7.1.5.5.2.4 For data flows associated to user plane of Application instances, Local Binding shall provide the following:

- Identification (M)
- Authentication (M)

7.1.5.5.2.5 For data flows associated to user plane of Application instances, Local Binding should enable the following:

- Integrity (O)
- Confidentiality (O)

Editor's note: Integrity and Confidentiality for the user plane are FFS.

7.1.5.5.2.6 With respect to Identification of Application instances Local Binding shall support an application registration process [FRMCS FFFIS]. (M)

7.1.5.5.2.7 The application registration process shall enable differentiation between the application coupling modes whether it is Loose or Tight as described in section 6.1.3.1. (M)

7.1.5.5.2.8 With respect to Identification of Application instances, Local Binding shall comply with Service Session parameters. (M)

Editor's note: This functionality is considered FFS.

Note: Technical details of Local Binding are further specified in the [FFFIS].

7.1.5.6 Session Management

7.1.5.6.1 Introduction

7.1.5.6.1.1 Session Management is a Function of the of API. (I)

7.1.5.6.1.2 Session Management enables or disables Communication Service Session(s). (I)

7.1.5.6.2 Requirements

7.1.5.6.2.1 Session Management shall enable communication service sessions between two single users. (M)

7.1.5.6.2.2 Session Management shall enable communication service sessions between one single user and multiple users. (M)

7.1.5.6.2.3 Session Management shall enable unicast communication. (M)

7.1.5.6.2.4 Session Management should enable multicast communication. (O)

7.1.5.6.2.5 Session Management shall include the capability to establish communication service sessions. (M)

7.1.5.6.2.6 Session Management shall include the capability to inform applications about the status of communication service sessions. (M)

Note: the boundaries of communication service are FFS.

7.1.5.6.2.7 Session Management shall include the capability to release communication service sessions. (M)

Editor's note: Potential additional service session functions are FFS.

7.1.5.6.2.8 Session Management shall include the capability to uniquely identify communication service sessions. (M)

7.1.5.6.2.9 Session Management shall only activate communication service sessions for Application instances identified and authorized by Local Binding. (M)

7.1.5.7 Auxiliary

7.1.5.7.1 Introduction

7.1.5.7.1.1 The Auxiliary Function is a function of the API. (I)

7.1.5.7.1.2 The Auxiliary Function manages status information pertaining to a data flow [FFFIS] (I).

7.1.5.7.2 Requirements

7.1.5.7.2.1 The Auxiliary Function shall have the capability to provide information to the application using push and/or pull mechanism. (M)

7.1.5.7.2.2 The Push mechanism shall allow immediate notification on unforeseen situations (e.g., loss of signal, etc.). (M)

7.1.5.7.2.3 The Auxiliary Function shall provide read-only information. (M)

7.1.5.7.2.4 The Auxiliary function shall provide FRMCS train-to-ground communication service availability status information (on/off). (M)

Editor's note: The Auxiliary Function will have further developments that are FFS in later version of this specification.

7.1.5.8 Orchestration

7.1.5.8.1 Introduction

7.1.5.8.1.1 The Orchestration Function is a function of the Communication Gateway. (I)

7.1.5.8.1.2 The Orchestration Function manages the routing of user plane data flow inside the communication gateway depending on the coupling mode (Loose or Tight [TOBA FRS]). (I)

7.1.5.8.2 Requirements

7.1.5.8.2.1 The Orchestration function shall have the capability to use information from Local Binding about the coupling mode (Loose or Tight [TOBA FRS]). (M)

7.1.5.8.2.2 The orchestration function shall have the capability to route user plane dataflows associated to locally bound Loose-Mode application instances to the appropriate MCx Client. (M)

Editor's note: Further development for the Orchestration Function is for FFS.

7.1.5.9 MCX Client(s)

7.1.5.9.1 Introduction

7.1.5.9.1.1 MCX for FRMCS framework is specified in [TS 103 765-2]. (I)

7.1.5.9.2 Requirements

7.1.5.9.2.1 The Communication Gateway shall host MCX Clients to enable Loose Coupled communication mode. (M)

7.1.5.9.2.2 MCX Clients hosted by On-Board FRMCS enable Loose Coupled communication mode [TOBA FRS]. (I)

7.1.5.9.2.3 The MCX Client manages communication service session(s) with the MCX server. (I)

7.1.5.10 Connectivity

7.1.5.10.1 Introduction

7.1.5.10.1.1 Connectivity is a function of the Communication Gateway. (I)

7.1.5.10.1.2 Connectivity concerns data flows in the OB_{APP} user plane. (I)

7.1.5.10.2 Requirements

7.1.5.10.2.1 Connectivity shall enable single path communication. (M)

7.1.5.10.2.2 Connectivity should contain the following function: FRMCS Multipath. (O)

Editor's note: additional functions of Connectivity are FFS.

7.1.5.10.2.3 Connectivity shall provide dataflow transport resources. (M)

7.1.5.10.2.4 Connectivity shall manage and control Radio Function(s) using OB_{RAD}. (M)

7.1.5.10.3 FRMCS Multipath

7.1.5.10.3.1 FRMCS Multipath is a function of Communication Gateway. (I)

7.1.5.10.3.2 FRMCS Multipath is a function that manages and controls concurrent user plane data flow distribution over OB_{RAD}. (I)

7.1.5.10.3.3 The multipath function confirms to the specifications in chapter 12.4 of this document. (I)

Editor's Note: support of Multi Access for On-Board FRMCS is FFS.

7.1.5.11 OM

7.1.5.11.1 Introduction

7.1.5.11.1.1 OM is a function of Gateway Function. (I)

7.1.5.11.1.2 OM is related to operation and maintenance of the On-Board FRMCS. (I)

7.1.5.11.2 Requirements

7.1.5.11.2.1 The OM shall use the OB_{OM} interface. (M)

7.1.5.11.2.2 OM shall enable Operation and Maintenance of On-Board FRMCS. (M)

7.1.5.11.2.3 The OM shall enable local configuration management of the On-Board FRMCS. (M)

7.1.5.11.2.4 The OM shall enable OTA configuration management of the On-Board FRMCS. (M)

7.1.5.11.2.5 The OM shall enable local fault management of the On-Board FRMCS. (M)

7.1.5.11.2.6 The OM shall enable OTA fault management of the On-Board FRMCS. (M)

7.1.5.11.2.7 The OM shall enable local software management to On-Board FRMCS. (M)

7.1.5.11.2.8 The OM shall enable OTA software management to On-Board FRMCS. (M)

7.1.5.11.2.9 Multiple concurrent OM Sessions should be possible. (O)

7.1.5.11.2.10 The OM shall enable distribution of authentication credentials related to OB_{APP}. (M)

7.1.5.11.2.11 The OM shall enable management of authentication credentials related to OB_{APP}. (M)

Note: The management and distribution scope are limited to the On-Board FRMCS.

Editor's note: The OM will be further specified in later version of this specification.

7.1.6 Radio Function

7.1.6.1 Introduction

7.1.6.1.1 The Radio Function is a function of the On-Board FRMCS. (I)

7.1.6.1.2 The Radio Function includes the following (I):

- Adapter
- Radio Module(s)

Editor's note: The presence of one or multiple Radio Modules associated to one Radio Function is FFS.

7.1.6.1.3 The Radio Function shall enable access for the Communication Gateway to the FRMCS Transport Stratum. (M)

7.1.6.1.4 The Radio Function enables transmission of control and user plane related data. (I)

7.1.6.1.5 The boundaries of the Radio Function are identified by reference points OB_{RAD} and OB_{ANT}. (I)

7.1.6.2 Adapter

7.1.6.2.1 The Adapter is a function of the Radio Function. (I)

7.1.6.2.2 The Adapter enables On-Board FRMCS integrated architectures. (I)

7.1.6.2.3 The Adapter enables On-Board FRMCS distributed architectures. (I)

7.1.6.2.4 The Adapter enables adaptation of generalized and standardized control and management commands to manufacturer specific radio module commands. (I)

7.1.6.2.5 The Adapter is meant to support interchangeability as defined in the definitions section. (I)

7.1.6.2.6 The Adapter encompasses hardware (e.g., connectors). (I)

7.1.6.2.7 The Adapter can encompass software. (I)

7.1.6.2.8 The Adapter shall interface to OB_{RAD}. (M)

7.1.6.2.9 The Adapter can manage connectivity to one or more radio modules. (I)

7.1.6.2.10 The Adapter shall interface to Radio Modules using suitable industrial interfaces (M)

7.1.6.3 Radio Module(s)

7.1.6.3.1 The Radio Module should be compatible with the Adapter. (O)

7.1.6.3.2 The FRMCS Radio Module has one external reference point, named OBANT. (I)

7.1.6.3.3 Radio Modules shall support frequency blocks allocated to RMR [ECC Decision (20) 02]. (M)

Note: Support for further radio frequency blocks is specified in chapter 8.

Editor's note 1: Radio Module MCX compatibly is FFS.
Editor's note 2: Migration aspects are not addressed in this version of the document, and they are FFS.
Editor's note 3: The Radio Module will be in more depth specified in later version of the specification.

7.2 Antenna Function

7.2.1 Introduction

7.2.1.1 The Antenna Function is outside the boundary of On-Board FRMCS. (I)

7.2.1.2 The Antenna Function can contain a RF combining and switching functions. (I)

7.2.1.3 On the antenna side single antennas can be used. (I)

7.2.1.4 On the antenna side MIMO antennas can be used. (I)

Editor's note: The Antenna Function will be in more depth specified in later version of the specification.

8 Radio Spectrum

8.1 Introduction

8.1.1 This section describes the requirements on the use of frequency bands applicable for FRMCS. (I)

8.2 Out of scope

8.2.1 No out of scope items identified. (I)

8.3 Spectrum principles

8.3.1 FRMCS shall support spectrum allocated for terrestrial use. (M)

8.3.2 FRMCS should support licensed as well as unlicensed frequency bands. (O)

Note: Spectrum licensing is a national matter.

8.3.3 FRMCS shall enable the use of a single frequency band as well as the simultaneous use (receive and transmit) of multiple frequency bands. (M)

8.4 RMR frequency bands for Europe

8.4.1 [EC Decision 2021/1730] identifies the radio spectrum (900 MHz,1900 MHz) for Railway Mobile Radio (RMR). (I)

Note: RMR encompasses GSM-R and FRMCS.

8.4.2 FRMCS shall support the use of 3GPP 5G NR technology for the paired frequency bands defined in [EC Decision 2021/1730] of: (M)

a. 874.4-880.0 MHz, uplink
b. 919.4-925.0 MHz, downlink

8.4.3 FRMCS shall support the use of 3GPP 5G NR technology for the unpaired frequency band defined in [EC Decision 2021/1730] of: (M)

a. 1900-1910 MHz

8.4.4 An FRMCS Operator shall implement the RMR 900 MHz frequency band (as identified in par. 8.4.2) or the RMR 1900 MHz frequency band (as identified in par. 8.4.3) or both frequency bands. (M)

8.4.5 FRMCS is able to flexibly use up to the maximum extent of spectrum available for rail in a given area. (I)

8.5 Public MNO Spectrum in Europe

8.5.1 FRMCS Radio Modules used for FRMCS communication purposes should support frequency bands allocated to public MNOs in Europe. (O)

8.5.2 FRMCS Radio Modules should support a subset of the frequency bands in use in Europe as listed in Table 3 applicable to ITU region 1. (I)

Frequency bands (MHz or GHz)	Band name	Uplink/Downlink (MHz)
TBD		TBD
...		

Table 3 Public Frequency bands for FRMCS Radio Modules (FFS) (I)

8.6 FRMCS Radio Module support of Radio Access Technologies and frequency bands

8.6.1 The train-borne equipment supports several types of FRMCS Radio Modules. (I)

8.6.2 FRMCS Radio Module types are for example (non-exhaustive list): (I)

a. Radio Modules which exclusively support RMR bands
b. Radio Modules which support RMR bands and a subset of other bands (e.g., PMNO and/or WLAN bands)
c. Radio modules which exclusively support a subset of PMNO bands
d. Radio modules which exclusively support WLAN (e.g., Wi-Fi) frequency bands

Note: FRMCS Radio Modules do (by definition) not necessarily support RMR frequency bands

8.6.3 An FRMCS Radio Module should support a single or multiple of the following frequency bands and corresponding RATs (O):

a. RMR frequency bands using 5G NR terrestrial
b. Public MNO frequency bands using 5G NR terrestrial
c. Public MNO frequency bands using 4G terrestrial
d. Non-3GPP terrestrial frequency bands using WLAN (e.g., Wi-Fi)

8.6.4 FRMCS Radio Modules should support the frequency bands (and corresponding RATs) in accordance with par. 8.6.3 which are used for FRMCS by different IMs at the trackside. (I)

8.6.5 The train-borne equipment (i.e., one or more FRMCS Radio Modules) shall support the RMR frequency bands as identifies in par. 8.4.2 and 8.4.3. (M)

8.6.6 The train-borne equipment (i.e., one or more FRMCS Radio Modules) should support a subset of the PMNO frequency bands as identified in Table 3. (I)

8.6.7 The train-borne equipment (i.e., one or more FRMCS Radio Modules) should support WLAN frequency bands. (I)

8.6.8 The train-borne equipment (i.e., one or more FRMCS Radio Modules) should support 5G NR non-terrestrial and/or legacy non-terrestrial frequency bands. (I)

8.7 For further study

8.7.1 Identification and designation of public MNOs bands (including associated RATs) used for FRMCS (Table 3). (I)

8.7.2 Definition of different FRMCS Radio Module types (including the supported frequency bands and associated RATs). (I)

8.7.3 Analysis and derivation of spectrum related requirements and associated RATs for the FRMCS and non-FRMCS Transport Domain. IMs will have to make country specific choices on which frequency bands and transport strata to support for FRMCS. IMs may at the infrastructure side for example only use RMR 900 frequency bands, only use RMR 1900 frequency bands, use PMNO frequency bands or a combination of all those options. (I)

8.7.4 Identification and designation of supported unlicensed spectrum (e.g., WLAN/Wi-Fi frequency bands). (I)

8.7.5 The specification of supported frequency bands and RATs for FRMCS handhelds. (I)

8.7.6 The support of 5G NR non-terrestrial and legacy non-terrestrial radio access including the Identification and designation of supported satellite spectrum. (I)

8.7.7 Coexistence of all selected bands (RMR and public MNO). (I)

8.7.8 The use of other (i.e., non-RMR) frequency bands outside Europe. (I)

9 GSM-R Interworking and Migration

Editor's note:
Interworking and Migration from GSM-R to FRMCS (including dispatcher systems) will not be addressed in version 1.0.0 of the FRMCS SRS but in a later version. This section will refer to ETSI TR 103 768 and TS 103 792. Specification of a coordinating function between GSM-R and FRMCS to support FRMCS On-Board Voice Application Function will be considered in this chapter.

10 Interconnection, roaming and border crossing

Editor's note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

10.1 Interconnection

Editor's note:
Address connectivity between (mobile) users within different administrative realms.

10.2 Roaming

Editor's note:
Address relocation of mobile users within administrative realms.

10.3 Border crossing

Editor's note:
Border crossing procedures are intended to be simplified compared to GSM-R.

11 Identifiers

11.1 Introduction

11.1.1 International standardisation of user identities is required to ensure interworking between FRMCS domains. Furthermore, standardised allocation labels to users of the corresponding strata are needed to facilitate schemes for identification, barring etc. (I)

11.1.2 This section addresses the following: (I)

- Types of identifiers
- Domain Name scheme
- Public identification scheme
- Group identification scheme
- Role based identification scheme

11.1.3 The details of the identities to be chosen for particular railways will depend upon the railway FRMCS Domain configuration, its interconnection with other railway FRMCS Domains and its interconnection with non-FRMCS Domains, e.g., PMNOs. (I)

11.1.4 Each FRMCS Operator needs appropriate communication-barring facilities to prevent unintended access to the FRMCS Domain by non-authorised users. (I)

11.1.5 There are several identities and addresses for all communication purposes of the FRMCS needed, e.g., for user authentication to be identified in the administrative domain and to be reachable for communication requests. (I)

11.1.6 An identity can be associated with a human user, a machine type application, or a service, i.e., an identity is the link to a service profile. The identity may be used for registration, authorisation and authentication purposes. (I)

11.1.7 To define the structure of an identity applicable for an FRMCS user, it needs to be distinguished whether it will only be used inside the FRMCS System (internal), or it will traverse the boundaries of the FRMCS System (external). (I)

11.2 Scope

The scope of this chapter is:

11.2.1 To describe the identities used in an FRMCS System for identification of users and services according to their committed stratum. (I)

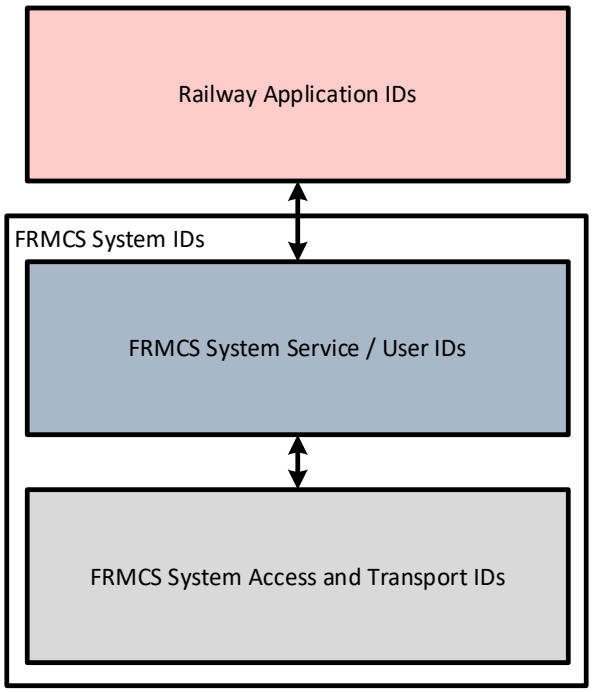


Figure 11-1: FRMCS identities [TR 103 459]

11.2.2 To define the structure of FRMCS System identities which are used to set up a communication link or communication links to registered and authenticated FRMCS users. (I)

11.2.3 To ensure that the Functional Addressing (FA) scheme as defined in the Functional Requirements Specification [FRMCS-FRS] is supported. (I)

The scope of this chapter is not (out of scope):

- To describe the interworking for identities and addresses for FRMCS ↔ GSMR and for FRMCS ↔ other networks. This is being described by ETSI in [TS 103 792]. (I)
- To define how applications are using identities and addresses and for which purpose. This is being described in the [FIS] and the [FFFIS]. (I)
- To define the format and scheme of an Application Identity. This is being described in the [FFFIS]. (I)

11.3 Identities of the FRMCS transport stratum

11.3.1 Data Network Name (DNN)

11.3.1.1 DNN is used for UPF/SMF configuration in the FRMCS transport stratum for the allocation of IP-address. (I)

11.3.1.2 The DNN shall have the format <frmcs.mncXXX.mccYYY.3gppnetwork.org>. (M)

11.3.1.3 A single DNN shall cover all IP flows established within an FRMCS Domain. (M)

11.3.1.4 It is not foreseen that FRMCS railway applications are able to influence the DNN selection. (I)

11.3.1.5 For FRMCS capable handhelds, DNN shall be configured at the MC Service UE (Service Stratum) in accordance with [TS 23.280] and [TS 23.289]. (M)

11.3.1.6 For future evolutions further DNN may be required. (I)

11.4 Identities of the FRMCS service stratum

11.4.1 Identification and addressing in the service stratum shall be based on MC IDs and on IMS / SIP Core IDs. (M)

11.4.2 Identities within the FRMCS System only

11.4.2.1 The following identities stay inside the FRMCS System boundaries: (I)

- MC ID
  Note: [TS 23.280] “The mission critical user identity is also known as the MC ID”.
- Public Service ID
- MC Service ID
  Note: [TS 23.280] “The MC service user identity is also known as the MC service ID”.
- Role based identities
- MC Group ID
- Private User ID (IMPI)
- Public User ID (IMPU)

11.4.2.2 The domain part of the FRMCS identities that stay inside the FRMCS System boundaries and are not used for interoperability shall follow an international or a private Domain Name System (DNS) space. (M)

11.4.3 Identities used with systems outside the FRMCS System

11.4.3.1 The following identities traverse the FRMCS System boundaries (excluding GSM-R interworking): (I)

- IMS IMPU

11.4.3.2 For interoperability purposes, the domain part of the IMS IMPU shall be composed in accordance with international public Domain Name System (DNS) space requirements. (M)

11.4.4 IMS / SIP Core identities

11.4.4.1 The source of IMS / SIP Core identities and their storage (e.g. ISIM, IMC (IMS Credentials), eSIM) are out of scope of this chapter. (I)

11.4.4.2 Private user identity for IMS / SIP Core

11.4.4.2.1 The FRMCS System shall make use of the Private User ID in accordance with [TS 23.003]. (M)

11.4.4.2.2 The Private User ID shall include at least MCC and MNC according to [ITU E.212]. (M)

11.4.4.2.3 In case that an IMSI is present, it shall be used as Private User ID. (M)

11.4.4.2.4 An IMSI shall be composed in accordance with [TS 23.003]. (M)

11.4.4.3 Public User Identity for IMS / SIP Core

11.4.4.3.1 A Public User ID (IMPU) is used in IMS / SIP Core for communication purposes. (I)

11.4.4.3.2 The FRMCS System shall make use for Public User ID in accordance with [TS 23.003]. (M)

11.4.4.3.3 For each Private User ID, at least two Public User IDs shall be present: one SIP URI and one Tel URI. (M)

11.4.4.3.4 A Public User ID shall consist of the following necessary, meaningful elements: (M)

- user identification
- domain part (e.g., <IM or RU>.<country>.<xxx>)
- user identification and domain part shall be separated by the delimiter <@>

11.4.4.3.5 For Public User IDs which traverse the FRMCS System boundaries the domain part shall be associated with public reachable domains. (M)

11.4.4.3.6 To support the use of MSISDN as a Public User ID, the network shall associate a Tel URI with an alphanumeric SIP URI using the mechanisms specified in [TS 23.228] and [TS 24.229] in accordance with [IR 65]. (M)

Alphanumeric SIP URIs

- Example: sip:voicemail@example.com

MSISDN represented as a SIP URI

- Example: sip:+447700900123@example.com;user=phone

MSISDN represented as a Tel URI

- Example: tel:+447700900123

11.4.4.4 Public Service ID

11.4.4.4.1 The Public Service Identity (ID) shall be in accordance with [TS 23.003]. (M)

11.4.4.4.2 A Public Service Identity identifies a service like MCPTT, MCDATA, MCVIDEO, or a specific resource created for a service on an application server. (I)

11.4.4.4.3 The Public Service Identity shall take the form of either a SIP URI (see [RFC-3261]) or a Tel URI (see [RFC-3966]). (M)

11.4.4.4.4 The domain part shall take the form: (M)

- ims.mnc<MNC>.mcc<MCC>.3gppnetworks.org

11.4.4.4.5 The following structure of Public Service Identities shall be used for all MC Services using the user part mcdata, mcptt and mcvideo: (M)

- sip:mcdata@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org for MCData Service
- sip:mcptt@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org for MCPTT Service
- sip:mcvideo@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org for MCVideo Service

Note: these are the Public Service Identities for Mission Critical Services. For other services, Public Service Identities can be added.

11.4.4.5 Private Service ID

11.4.4.5.1 A Private Service Identity (ID) is accordance with [TS 23.003] does not required further harmonization, since it is only used for registration, authorization and authentication of the FRMCS service. (I)

11.4.5 MC Identities

11.4.5.1 MC identification and addressing shall be in accordance with [TS 23.280]. (M)

11.4.5.2 MC ID

11.4.5.2.1 The MC ID shall be in accordance with [TS 23.280]. (M)

11.4.5.2.2 The following credentials shall be used for MC ID: (M)

- Unique identifier (e.g., URI-format: <identity>@<domain>)
- Secret (e.g., password, certificate, token)

11.4.5.3 MC Service ID

11.4.5.3.1 An MC Service ID shall always be used to identify a communication endpoint. (M)
Editor's note: to be changed according to section 6.5.2 on H2H and H2N.

11.4.5.3.2 One MC Service ID for each service (MCData, MCVideo, MCPTT) shall be associable with one MC ID. (M)

11.4.5.3.3 The format of the MC Service ID shall be in accordance with [TS 23.280]. (M)

11.4.5.3.4 The MC Service ID shall comply with the following format (M):

- sip:<User name>@<MC Service Domain>

Editor's note: Format of the variable "User_name" is for FFS.

11.4.5.3.5 A possible format of the MC Service ID is the role based identification scheme as described in chapter 11.6. (I)

11.4.5.4 MC Service Group ID

11.4.5.4.1 The MC Service Group ID is a globally unique identifier used by FRMCS System that represents a set of MC service users in accordance with [TS 23.280]. (I)

11.4.5.4.2 The Service Group ID for voice shall be an MC Service Group ID in accordance with [TS 23.379]. (M)

11.4.5.4.3 The Service Group ID for video shall be an MC Service Group ID in accordance with [TS 23.281]. (M)

11.4.5.4.4 The Service Group ID for data shall be an MC Service Group ID in accordance with [TS 23.282]. (M)

11.4.5.5 MC System ID

11.4.5.5.1 For the MC System ID, the following two formats shall be used, and both shall be implemented: (M)

- mcx.<company name>.<country top level domain>
  (e.g., mcx.dbnetz.de)
- mcx.mnc<MNC>.mcc<MCC>.3gppnetwork.org
  (e.g., mcx.mnc010.mcc262.3gppnetwork.org)

11.4.5.5.2 Format mcx.<company name>.<country top level domain> shall be used e.g., for human user interaction and follows the domain space tree as depicted in Figure 11-2: (M)

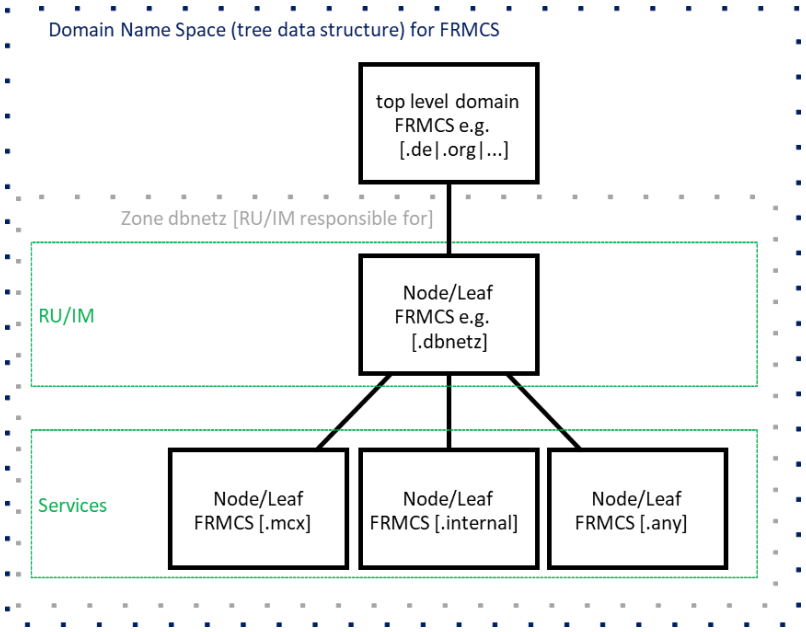


Figure 11-2: Domain Name Space for FRMCS (human-user interaction)

11.4.5.5.3 Format mcx.mnc<MNC>.mcc<MCC>.3gppnetwork.org shall be used e.g., for machine-to-machine communication and follows the domain space tree as depicted in Figure 11-3: (M)

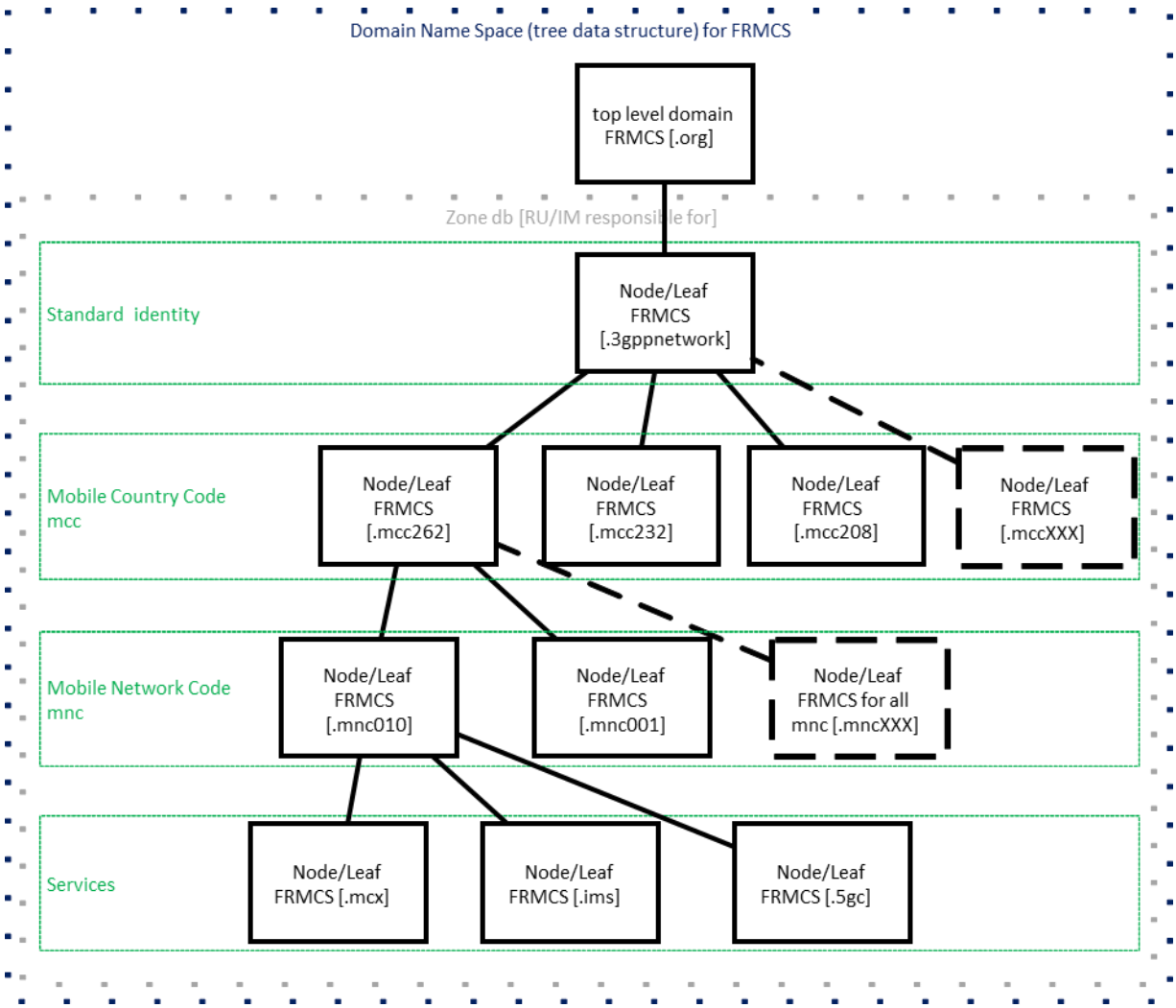


Figure 11-3: Domain Name Space for FRMCS (machine-type communication)

11.4.5.5.4 For FRMCS, the MC System ID corresponds to the MC Service Domain. (I)

11.5 Usage and dependencies of different FRMCS identities

11.5.1 Figure 11-4 shows the dependencies and location of the different identities using the stratum model of FRMCS. It shows in which stratum and on-board and trackside the different identities are located. The dashed lines are logical dependencies and solid lines are displaying physical (wireless/wireline) connections. (I)

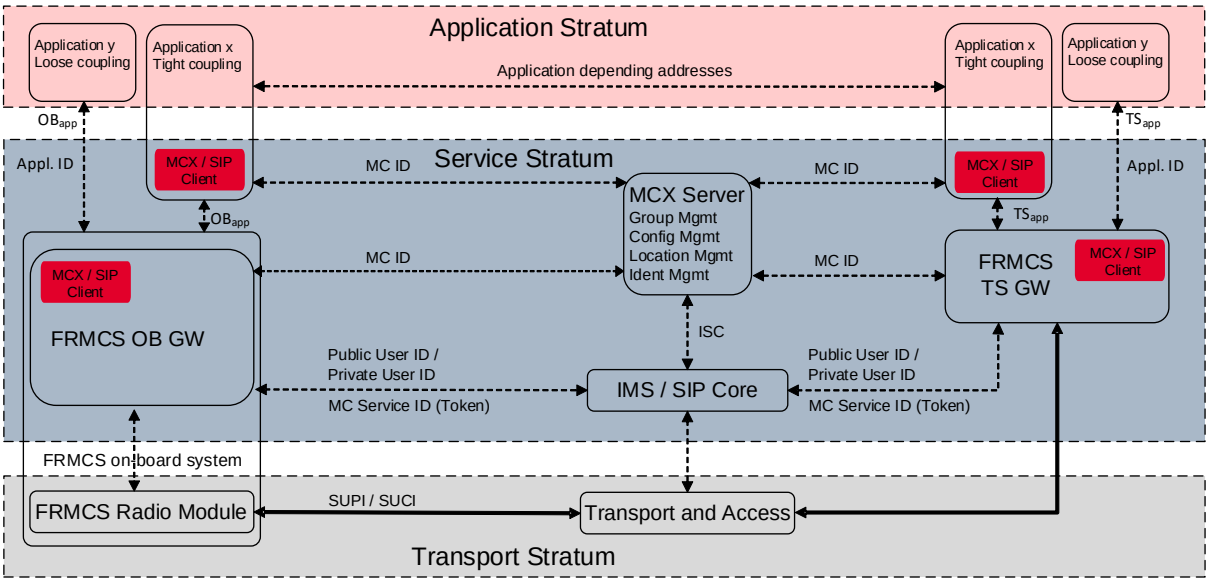


Figure 11-4: Identities and their location

11.6 Role based identification scheme

11.6.1 Identification scheme requirements

11.6.1.1 Within each FRMCS domain, each train number must be unique for the period of the journey. (I)

11.6.1.2 Every rail operational function shall be identified by a unique functional label conforming with “Table 4: Mapping of identities and labels”. (M)

11.6.1.3 The relationship between Functional Alias and their associated MC Service ID shall be available for the required period of time, e.g., for period of the journey (temporary binding or permanent binding, respectively). (M)

11.6.1.4 For associating a functional label with an MC Service ID / IMPU, Functional Alias in accordance with the requirements of [FRMCS FRS], [TS 22.280] and [TS 23.280] shall be used. (M)

11.6.1.5 The FRMCS system shall allow a FRMCS User to have no or any other number of Functional Aliases active. (M)

11.6.2 Identification scheme format

11.6.2.1 The Role based ID shall consist of some or all of the following labels: (I)

- *** (for national use or for future extensions)
- Identification label
- Location label
- Function label

11.6.2.2 Identification label, Location label and Function label shall be used in accordance with the [FRMCS FRS]. (M)

11.6.2.3 Identities shall have the format
***.Identification_label.Location_label.Function_label@Organizational_code (M)

11.6.2.4 Table 4 shows, which labels shall be used in which identities. (M)

		naming	Short dialling codes	Train function identity	Vehicle identity	Profile Addressing	Team identity	Controller identity	Equipment identity
Identification label									
	Train ID	*National format*		x					
	Vehicle Identifier	*Nat. / Internat. format*			x				
	Shunting 1	Shunt_1					x		
	Shunting 2	Shunt_2					x		
	Shunting 3	Shunt_3					x		
	Maintenance	Maintain					x		
	Railway Security	Secur					x		
	Equipment	Equip							x
Location label		*National format*				x	x	x	x
Function label									x
	Primary controller	Control_1	x					x	
	Secondary controller	Control_2	x					x	
	Power supply controller	Control_Power	x					x	
	Train driver Leading driver Driver	Driver_1		x	x	x	x		
	Driver 2	Driver_2		x	x				
	Driver 3	Driver_3		x	x				
	Driver 4	Driver_4		x	x				
	Driver 5 – reserved for Banking	Driver_5		x	x				
	Intercom	Intercom		x	x				
	Public address	Public		x	x				
	Chief conductor	Conduct_1		x	x				
	Second conductor	Conduct_2		x	x				
	Third conductor	Conduct_3		x	x				
	Fourth conductor	Conduct_4		x	x				
	Train crew 5 – 10	Crew_05 … Crew_10		x	x				
	Catering staff chief	Cater_01		x	x	x			
	Catering 2 -10	Cater_02 … Cater_10		x	x				
	Railway security services chief	Secur_01		x	x				
	Railway security 2 – 10	Secur_02 … Secur_10		x	x				
	Switchman	Switchman						x	
	Platform inspector	Platform_Insp						x	
	Railway undertaking dispatcher	RU_Dispatch						x	
	Technical inspector	Techn_Insp						x	
	Train preparation	Train_Prep						x	
	Emergency manager	Emerg_Manag						x	

	All	Whole_team				x			
	Train staff	Train_staff				x			
	Shunting team leader	Shunteam_01				x	x		
	Shunting team members	Shunteam_02 … Shunteam_30				x	x		
	Maintenance team leader	Mainteam_01				x	x		
	Maintenance team members	Mainteam_02 … Mainteam_10				x	x		
	Railway security team leader	Secteam_01				x	x		
	Railway security team members	Secteam_02 … Secteam_10				x	x		
	Vehicle Equipment ID	*National format*				x			
	Trackside Equipment ID	*National format*				x			
	Radio Block Centre (RBC)	in accordance with [SUBSET-037-3]							
	Onboard ETCS identity (Engine)	in accordance with [SUBSET-037-3]							
Organisation Code									
	Organisation Code	in accordance with [TAP TSI] / [TAF TSI]	x	x	x	x	x	x	x

Table 4: Mapping of identities and labels

11.6.2.5 It shall be possible to add new values for each label, e.g., Driver 6. (M)

11.6.3 Naming of labels

11.6.3.1 The naming of the labels shall be in accordance with “Table 4: Mapping of identities and labels”. In addition, the following naming for national / international formats shall apply: (M)

11.6.3.2 The train ID shall be allocated by each Railway. It shall be composed of a maximum of 41 alphanumeric characters. (M)

11.6.3.3 The Location Label shall be a

- Station ID
- Trackline ID
- Track section ID
- Area ID

The respective ID shall be allocated by each Railway. It shall be composed of a maximum of 41 alphanumeric characters. (M)

11.6.3.4 The ID for Vehicle / Trackside Equipment shall be allocated by each Railway. It shall be composed of a maximum of 41 alphanumeric characters. (M)

11.6.3.5 In Europe, the European Vehicle Number (EVN) as specified in “Structure and content of the European identification number (COMMISSION IMPLEMENTING DECISION [EU 2018/1614] of 25 October 2018 laying down specifications for the vehicle registers referred to in Article 47 of [Directive EU 2016/797] of the European Parliament and of the Council and amending and repealing Commission Decision [2007/756/EC]” shall be used as Vehicle Identifier. (M)

11.6.3.6 The naming of the Vehicle Identifier for countries outside the EU shall be defined by national or regional/international authorities. (M)

11.6.3.7 In Europe, the organisational code (OC) shall be in accordance with [TAF TSI] / [TAP TSI]. For the domain name of identities, the domain associated with the OC shall be used. (M)

11.6.3.8 For FA where the destination domain name / OC is not known, the FA can be created without OC. The FRMCS System where the connection is originated shall insert the applicable domain. (M)

11.7 For Further Study

11.7.1 The identification scheme in the transport stratum (SUPI / SUCI). (I)

11.7.2 The use of the organizational code is FFS under the light of global applicability (e.g., organizational code outside EU). (I)

11.7.3 CCS data application addressing associated with UNISIG (e.g., ETCS). (I)

11.7.4 The possibilities to address a train crossing national borders with a unique train number. (I)

11.7.5 The Slice ID in the transport stratum. (I)

11.7.6 The possible usage of a Generic Public Subscription Identifier (GPSI) (I)

11.7.7 Temporary identifiers to ease usage and improve security (I)

11.7.8 Format of a MC service Group ID. (I)

11.7.9 A dedicated section to Application Identifiers (to cover e.g., static ID, remote address as described in [FFFIS]). (I)

12 Bearer flexibility

12.1 Introduction

12.1.1 The lifecycle of railway applications is in general longer than the lifecycle of access/transport systems. It is intended that future transport technologies will be introduced as FRMCS evolves with no impact on railway applications. (I)

12.1.2 The FRMCS principle on separation between application and transport strata motivates the use of a variety of transport/access systems (both in the mobile and fixed domain). (I)

12.1.3 Bearer flexibility enables the use of the transport/access networks which are available within the administrative domains of an FRMCS Operator and/or a PMNO. (I)

12.2 Out of scope

12.2.1 No out of scope item is identified. (I)

12.3 General requirements

12.3.1 FRMCS Bearer flexibility encompasses two capabilities: FRMCS Multi Access and FRMCS Multipath. (I)

12.3.2 FRMCS Multipath (see section 12.4) enables the (sequential or simultaneous) use of multiple UEs on the same or different transport domains. (I)

12.3.3 FRMCS Multi Access (see section 12.5) enables the (sequential or simultaneous) use of multiple radio access technologies on a single UE and a single (FRMCS) Transport Domain. (I)

12.3.4 FRMCS Multipath can be applied over an FRMCS Transport Domain that encompasses FRMCS Multi Access. (I)

12.3.5 FRMCS Multi Access shall be defined for a single UE. (M)

12.3.6 FRMCS Multipath shall encompass multiple UEs and is applicable to both mobile radio modules (e.g., at OnBoard System) and wireline accesses (e.g., at Trackside). (M)

12.3.7 FRMCS Intra-RAT capability (see section 12.6) enables at a time the selection of either 5G NR terrestrial access making use of RMR spectrum or 5G NR terrestrial access making use of spectrum allocated to PMNO (i.e., RAN Sharing with a public MNO), in a single UE. (I)

12.4 FRMCS Multipath

12.4.1 FRMCS Multipath is the capability that enables data connectivity using multiple transport paths over separate UEs. (I)

12.4.2 A transport path provides data connectivity between two reference points, through a single transport domain (using a single UE). (I)

12.4.3 FRMCS Multipath shall make use of transport paths over one or multiple of the following Transport Domains: (M)

1. FRMCS Transport Domain
2. Non-FRMCS Transport Domains

12.4.4 Examples of Non-FRMCS Transport Domains are (I) :

a. Public MNOs

b. Non-terrestrial radio access

c. WLAN/Wi-Fi

d. 4G EPS (operated by an FRMCS Operator)

12.4.5 The FRMCS Multipath is handled by FRMCS Multipath function as illustrated in Figure 14. (I)

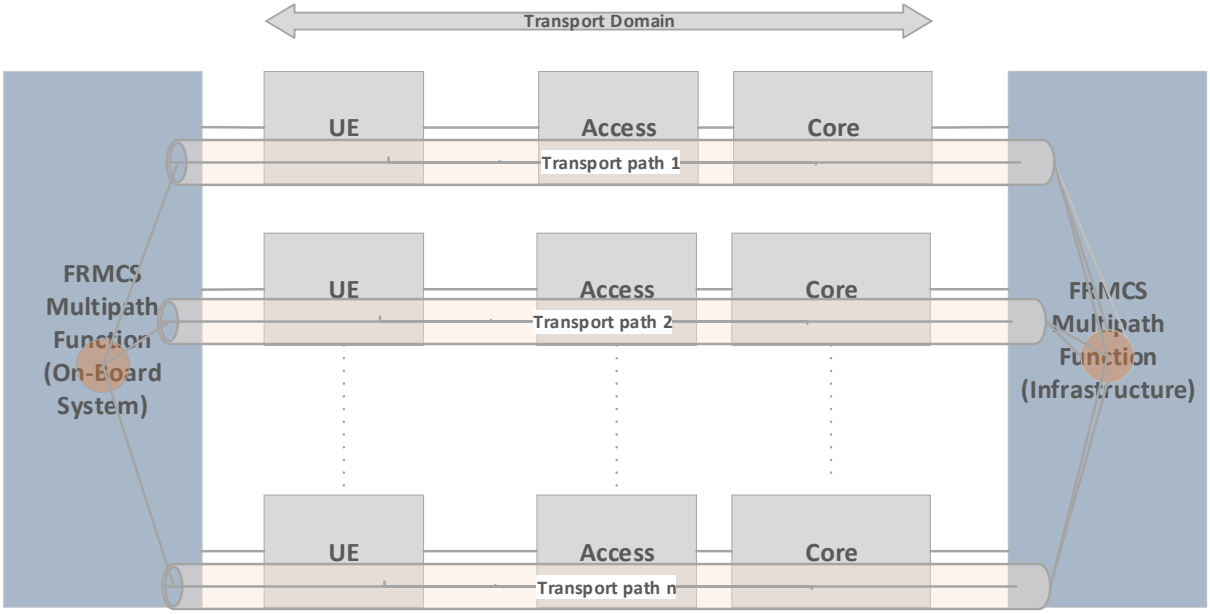


Figure 14 Principle of FRMCS Multipath operation

12.4.6 The decision on which Transport Domains to be used for a communication session shall be transparent to the Application Stratum. (M)

12.4.7 FRMCS Multipath shall support selection of the appropriate Transport Domain (including the corresponding UE). (M)

12.4.8 FRMCS Multipath shall support transition between UEs and the corresponding Transport Domains. (M)

12.4.9 FRMCS Multipath should support aggregation of transport paths across multiple Transport Domains (and the corresponding UEs). (O)

12.4.10 For FRMCS Multipath a rule set is applicable which governs the selection of one or more transport paths based on certain criteria. (I)

12.4.11 The rule set criteria include: (I)

- The quality of a transport domain (e.g., the instantaneous quality of a transport path in terms of data rate, latency and packet error rate).
- The attributes of the communication session (e.g., QoS and priority requirements of the communication session or data sensitivity of the communication session).

12.4.12 The rule set is applicable to the FRMCS On-Board System and infrastructure. (I)

12.4.13 The FRMCS Multipath function at network infrastructure side shall be able to configure the rule set. (M)

12.4.14 The FRMCS Multipath capability of the FRMCS On-Board System shall be notified to the FRMCS Multipath function at network infrastructure side. (M)

12.4.15 FRMCS Multipath should be supported by the infrastructure (network side). (O)

12.4.16 To enable FRMCS Multipath, the FRMCS On-Board System should support multiple UEs. (O)

12.4.17 FRMCS Multipath should be supported by the FRMCS On-Board System. (O)

12.4.18 FRMCS Multipath shall be based on an (evolved) standard (e.g., IETF). (M)

12.5 FRMCS Multi Access

12.5.1 FRMCS Multi Access is the capability of a single UE to use, simultaneously or sequentially, multiple access technologies within the FRMCS transport domain. (I)

12.5.2 A UE with FRMCS Multi Access capability shall support 3GPP 5G NAS signaling for the involved access technologies. (M)

12.5.3 The Transport Stratum supports the multiple access technologies as specified in accordance to [TS 103 765-1]. (I)

Note: the list of access technologies will not be discussed in the context of Bearer flexibility.

Examples of Access Technologies are:

- Terrestrial 3GPP access – 5G NR;
- Terrestrial Non-3GPP access – Wi-Fi/WLAN;
- Non-Terrestrial 3GPP access – 5G NR Satellite;
- Non-Terrestrial Non-3GPP access – Satellite;
- Wireline 5G access network.

12.5.4 The FRMCS Multi Access capability enables the simultaneous use of 3GPP and non-3GPP RATs in accordance with [TS 103 765-1] and shall encompass at least the combination of terrestrial 5G NR RAT or terrestrial Non-3GPP RAT. (M)

12.5.5 To enable FRMCS Multi Access, the FRMCS On-Board System should provide at least one UE supporting FRMCS Multi Access. (O)

12.5.6 FRMCS Multi Access should be supported by the infrastructure. (O)

12.5.7 The FRMCS Multi Access capability of the UE (including e.g., RAT combinations) shall be notified to the infrastructure. (M)

12.5.8 FRMCS Multi Access shall support the selection of the appropriate access technology. (M)

12.5.9 FRMCS Multi Access shall support the transition between Access Technologies (inter-RAT) for an ongoing communication. (M)

12.5.10 FRMCS Multi Access shall be based on 3GPP 5G system standard (e.g., ATSSS). (M)

12.5.11 For FRMCS Multi Access a rule set is applicable which governs the selection of one or more Access Technologies. (I)

12.5.12 FRMCS Multi Access should be supported by the UE. (O)

12.6 FRMCS Intra-RAT

12.6.1 FRMCS Intra-RAT capability shall support the selection, in a single UE, of either 5G NR terrestrial access making use of RMR spectrum or 5G NR terrestrial access making use of spectrum allocated to PMNO's (i.e., RAN Sharing with a public MNO). (M)

12.6.2 FRMCS Intra-RAT capability shall support the inter-frequency transition for 5G NR terrestrial access (intra-RAT) between RMR spectrum and spectrum allocated to PMNO's for an ongoing communication. (M)

12.6.3 FRMCS Intra-RAT capability shall be provided based on 3GPP 5G system capabilities (e.g., Intra-RAT Inter-frequency cell selection/handover). (M)

12.6.4 FRMCS Intra-RAT capability should be supported by the infrastructure. (O)

12.7 For further study

12.7.1 The set of access/transport policies is defined by the FRMCS Operator. This policy may differ from FRMCS Operator to FRMCS Operator. (I)

12.7.2 The responsibility for access/transport policies (IM or RU) when crossing the border needs to be clarified. (I)

12.7.3 Carrier aggregation and dual connectivity as specified by 3GPP. (I)

12.7.4 The solution choice(s) for FRMCS Multipath based on evolved standards is to be clarified in later release of this SRS. (I)

13 Network slicing

Editor’s note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

14 Quality of Service and Priority

14.1 Introduction

14.1.1 Railway applications exhibit different requirements on quality characteristics of communication sessions, e.g., in terms of latency or reliability. (I)

14.1.2 The fulfilment of Quality of Service (QoS) requirements can impact the rail operation performance and the entire utilisation of the track system. (I)

14.1.3 If the available radio resources are insufficient to handle the overall communication demands, congestion occur and not all QoS requirements can be fulfilled at the same time. (I)

14.1.4 In order to reflect the different importance of railway applications and its associated communication sessions, priorities indicate the obligation to serve the application and/or an order for recommended QoS fulfilment. (I)

14.1.5 This section defines the requirements on the FRMCS Quality of Service and Priority framework, the mapping towards the 3GPP mechanisms and its utilization. (I)

14.2 Out of Scope

14.2.1 An analysis of the operational requirements as well as a translation into system requirements is out of scope of this document. (I)

14.2.2 The description of the detailed 3GPP QoS mechanisms as well as its translation to radio resource allocation is out of scope of this document. (I)

14.2.3 The identification of the application by the FRMCS Service Server in order to apply the corresponding QoS and priority is out of scope of this section. (I)

14.3 Generic Requirements

14.3.1 In order to provide the required level of communication quality, the FRMCS system shall allocate the necessary resources by transport stratum means, reflecting the QoS requirements of the individual communication sessions. (M)

14.3.2 If the QoS requirements of all the simultaneous communication sessions cannot be fulfilled at the same time, the FRMCS system shall utilize priorities to give preference for higher priority applications. (M)

14.3.3 The FRMCS system shall support various QoS parameters in order to sufficiently reflect the different QoS requirements of the railway applications. (M)

14.3.4 The FRMCS system shall allow to associate individual parameter values to a communication session, independent of the QoS parameter values of other communication sessions. (M)

14.3.5 If the FRMCS system is not able to associate specific QoS requirements or priorities with a communication session, it shall be able to apply a predefined default. (M)

14.3.6 The QoS of a communication session is impacted by the configuration of the FRMCS onboard system, the FRMCS trackside system as well as local network components which are not subject to FRMCS specification. (I)

14.3.7 The signalling and enforcement procedures of the FRMCS QoS and priority framework shall be based on 3GPP mechanisms defined for the 5G System in transport stratum and the Mission Critical services in service stratums. (M)

Note: the interworking with multipath and different types of core networks is FFS.

14.4 QoS Requirements

14.4.1 Introduction

14.4.1.1 The requirements on FRMCS from an application perspective are specified based on the following Key Performance Indicators (KPIs). (I)

14.4.1.2 For those KPIs, an end-point refers to an application entity, which uses FRMCS to communicate with another application entity of the same type (e.g., ETCS, ATO). The transmitting application entity is called “source”, the receiving application entity is called “destination” in the following definitions. (I)

14.4.1.3 The KPIs are measured at the reference point between application entity and FRMCS (e.g., OB_App, TS_App). (I)

14.4.2 Latency and Packet Reliability

14.4.2.1 Latency is the time it takes to transfer a given network layer packet from a source to a destination. (I)

14.4.2.2 Packet Reliability is the ratio of the amount of sent network layer packets successfully delivered to the destination within the defined latency, to the total number of sent network layer packets. (I)

14.4.2.3 The respective QoS requirement values on latency and packet reliability for defined railway applications are indicated by the functional requirement description of [FRMCS-FRS] and the indications given in [TR 22.889, TR 22.989] Section 12.10 as well as [TS 22.289]. (I)

Note: the values of the referenced documents are subject to modifications in updated versions

14.4.3 Data Rate

14.4.3.1 Data rate is the data volume transmitted from the source to the destination within a given time. (I)

14.4.4 Session Setup time

14.4.4.1 The setup time of a communication session is the elapsed time between the communication establishment request transmission and the reception of the indication of successful communication session establishment at the source of the request. (I)

Note: The session setup time exclude any application layer processing and human interaction.

14.4.4.2 The FRMCS system supports two classes:

- Immediate
  The application requires immediate setup of the communication session. (I)
- Normal
  Normal communication session setup time range does not harm the use of the application. (I)

14.4.4.3 The immediate communication session establishment time shall not exceed 1 second for 99% of the cases (99%-ile). (M)

14.4.4.4 The normal communication session establishment time shall not exceed 3 seconds for 99% of the cases (99%-ile). (M)

14.4.5 Talker assignment time

14.4.5.1 Talker assignment time comprises the timeframe between talker request and the permission to talk. (I)

14.4.5.2 The talker assignment time shall be lower than 300 ms for 99% of the emergency cases (99%-ile). (M)

14.4.5.3 The talker assignment time shall be lower than 300 ms for 95% of the other cases (95%-ile). (M)

14.4.6 Audio Codecs

14.4.6.1 The supported audio codecs for voice calls are specified in [TS 103 765-2]. (I)

14.4.6.2 The audio codecs to be supported by the FRMCS system shall be in accordance with [TS 26.179]. (M)

14.4.7 Application Specific KPI Values

14.4.7.1 The KPI values for the railway applications defined in [FRMCS-FRS] should be in accordance with Table 22-1 (Annex A). (O)

Note: Table 22-1 (Annex A) of this FRMCS SRS version considers only an FRS application subset (ATP, ATO, REC) and is subject to extensions and modifications in updated versions of the FRMCS SRS.

14.5 3GPP Parameters

14.5.1 General

14.5.1.1 The FRMCS system considers the QoS requirements of specific applications (as indicated in Section 14.4). For an adequate provisioning of transport resources, the FRMCS system assigns corresponding 3GPP QoS parameters (in accordance with, e.g., [TS 23.501] Section 5.7.2 and [TS 23.289]) towards the related communication sessions. (I)

14.5.1.2 The 3GPP QoS parameters describe the packet forwarding treatment that is supported between UE and UPF of the FRMCS transport stratum, while the QoS requirements of Section 14.4 are defined end-to-end (see Figure 14-1). (I)

Note: The path between application entity and UE as well as the path between application entity and UPF are subject to, e.g., the respective local networks.

14.5.1.3 The network entities outside the scope of 5G system are dimensioned to support congestion free communication. (I)

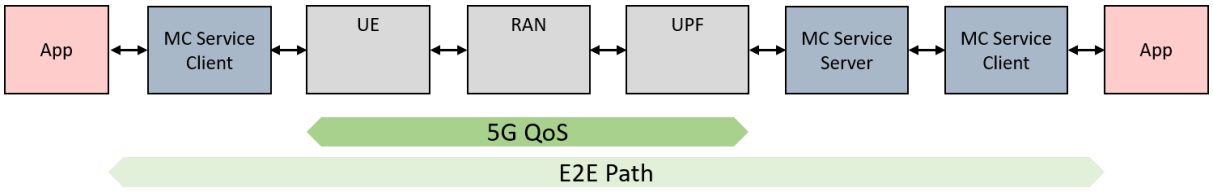


Figure 14-1: QoS in 5G versus E2E

14.5.1.4 The 3GPP QoS parameters introduced in the following include the 5G QoS Identifier (5QI), the Guaranteed Flow Bit Rates (GFBR) and the Allocation and Retention Priority (ARP). (I)

Note: Section 14.5 covers transport stratum QoS and priorities only, service stratum parameters are FFS.

14.5.2 Standardized 5QI

14.5.2.1 The FRMCS system shall support the set of standardized 5QI values as listed in Table 14-1 in accordance with the definitions in [TS 23.501] Section 5.7.4 (see Table 5.7.4-1 including its notes) and [TS 23.289] for MC services in order to reflect the requirements on latency and packet reliability given in Section 14.4.7. (M)

Standardized 5QI
5
7
65
67
69
76

Table 14-1: Standardized 5QI values to be supported by the FRMCS system and its utilization

14.5.3 Guaranteed Flow Bit Rate (GFBR)

14.5.3.1 For applications associated with guaranteed bit rate (see [TS 23.501]), a GFBR should be defined. (O)

Note: the specification of GFBR values for the FRS applications is FFS.

14.5.4 Allocation and Retention Priority (ARP)

14.5.4.1 Different communications between two or more applications need to be distinguished in their urgency, in order to appropriately or less preferably allocate corresponding transport resources. ARPs are used when resources are scarce and a decision needs to be taken with respect to which communication has precedence for allocation of these resources at a given point in time with a given QoS. (I)

14.5.4.2 The FRMCS system shall apply the ARP values 1 to 8, based on the definition in [TS 23.501] Section 5.7.2.2. (M)

Note 1: ARP values 9-15 are a national matter.

Note 2: the mapping of ARP values towards FRS application is FFS.

14.6 QoS Signalling

14.6.1 The 5G Core shall implement PCC rules in accordance with the QoS requirements referenced in Section 14.4 and QoS parameters referenced in Section 14.5. (M)

14.6.2 The PCF of the 5G Core shall identify the required QoS and priority treatment of a communication session based on the indications by the MC Service Server. (M)

14.6.3 At communication session establishment, the MC Service Server shall be able to identify the QoS requirements and priority associated with the communication session based on procedures specified in [TS 103 765-2]. (M)

14.6.4 If the MC Service Server is not able to identify the specific QoS requirement or priority for the session request for establishment, it shall indicate a predefined default. (M)

14.6.5 The QoS signalling relevant for at communication session establishment is illustrated in Figure 14-2. (I)

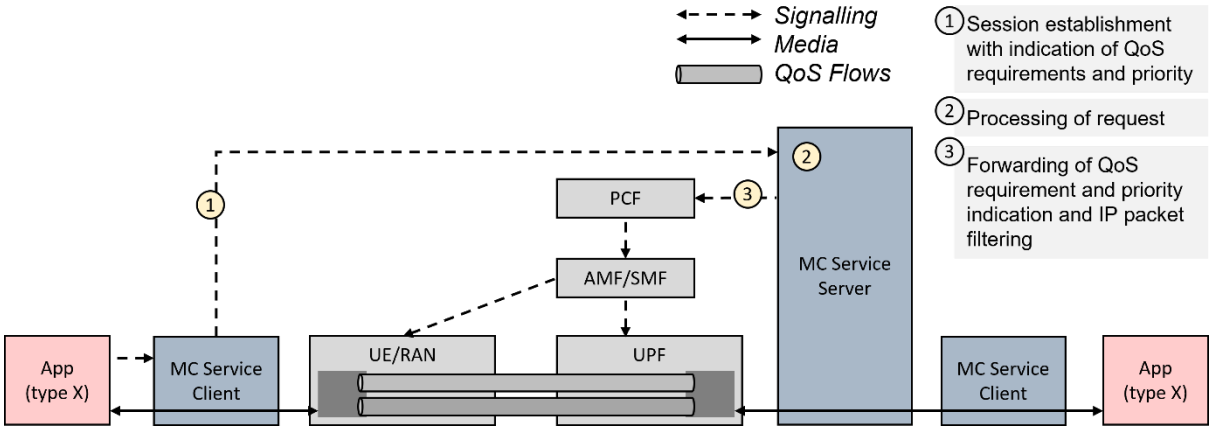


Figure 14-2: 3GPP QoS signalling relevant for interoperability

14.7 For Further Study

14.7.1 The specification of alphabets for MCData short data services (SDS) is FFS. (I)

14.7.2 The QoS requirement values for the FRS applications not listed in Table 22-1 as well as the revision of the requirement values listed in Table 22-1 is FFS. (I)

14.7.3 The priorities on the FRS applications of [FRMCS-FRS] is FFS. (I)

14.7.4 The mapping of QoS requirements towards appropriate 3GPP QoS parameters as well as the utilization of the 3GPP priority framework for transport stratum and service stratum (e.g., presentation priority for arbitration as well as floor priority) is FFS. (I)

14.7.5 The specification of alternative 3GPP QoS parameters (as defined by [TS 23.501] Section 5.7.1.2a) for each application type is FFS. (I)

14.7.6 The distinction of QoS contributions of FRMCS onboard system and FRMCS trackside system is FFS. (I)

14.7.7 The dynamic adjustment of QoS parameters (i.e., context aware QoS) for an already established communication session is FFS. (I)

14.7.8 The utilization of QoS and priorities in context of FRMCS Multipath is FFS. (I)

14.7.9 The interworking with core networks other than 5G Core in context of QoS is FFS. (I)

14.7.10 The requirements on a mechanism for real-time monitoring and logging of QoS of the individual communication sessions is FFS. This includes the notification of the service stratum and the notification of the application itself in case the QoS is not satisfied. (I)

14.7.11 The procedure and location of endpoints for QoS measurements is FFS. (I)

14.7.12 The definition of Maximum Flow Bit Rate (MFBR) is FFS. (I)

14.7.13 The definition of harmonised default QoS and priority figures as introduced in 14.3.5 are FFS. (I)

14.7.14 The dimensioning of network entities outside the scope of 5GS as introduced in 14.5.1.3 are FFS. (I)

15 FRMCS Cybersecurity

15.1 Introduction

15.1.1 The term cybersecurity refers: (I)

- to the condition of system resources being free from unauthorised access and from unauthorised or accidental change, destruction or loss [i.1]; and
- to collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect users, networks, devices, software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks as well as to protect organization and user's assets.

15.1.2 Cybersecurity related terms, like e.g., the security attributes confidentiality, integrity, privacy and authenticity are defined in [i.3]. (I)

15.1.3 In the following, the term cybersecurity is used only in the context of FRMCS security and is thus equated with that term. (I)

Note 1: Generally, the term security should not be confused with the term safety. Safety refers to the freedom from unacceptable risk, which is related to human health or to the environment [i.4].

15.2 Out of Scope

15.2.1 Regulation, governance, policy, management, updating, patching, testing, maintenance, backup, life cycle, logging, monitoring, configuration, operation and implementation related topics in the context of FRMCS security, e.g., needed for fraud protection, physical protection, anomaly detection, incident response, incident recovery and forensic analysis are very important and should be covered, e.g., by complementary FRMCS security guidelines, outside of this System Requirement Specification. (I)

Note 2: [**i.**5] aims at the implementation of a consistent approach to the management of the security of a railway system, provides cybersecurity design principles and provides to the railway operators, system integrators and product suppliers, with guidance and specifications on how cybersecurity will be managed in the context of the lifecycle process.

15.2.2 FRMCS security relevant configurations, design shaping details and categorizations, for example (I)

- cryptographic algorithms;
- key lengths; and
- requirement categories (mandatory vs. optional) of the protection of security attributes like data integrity, confidentiality, authenticity and privacy

are depending on risk assessments by consideration of different aspects like hazard potential (related to threats and vulnerabilities) and damage potential) [i.5]. **Risk assessments are not covered by this System Requirement Specification.**

15.2.3 TOBA local security aspects are not covered by this System Requirement Specification. (I)

15.2.4 Trackside local data network security aspects are not covered by this System Requirement Specification. (I)

15.2.5 Implementation specific security aspects are not covered by this System Requirement Specification. (I)

15.2.6 Application stratum security is out of scope of this System Requirement Specification. (I)

15.3 For further Study

Detailed FRMCS security aspects particularly in the context of:

- sequentially or simultaneously used FRMCS multipath and FRMCS multi access;
- trusted and untrusted non-3GPP access;
- non-terrestrial access;
- wireline access;
- interconnected FRMCS service domains;
- interconnected FRMCS transport domains;
- interconnection and interworking with other / external systems, networks and domains;
- off-network communication; and
- fall back to PMNO and GSM-R

are for further study and will consider primarily to be finalized ETSI Technical Specifications in the context of the FRMCS architecture incl. building blocks and functions [TS 103 764], [TS 103 765-1], [TS 103 765-2] as well as secondarily 3GPP specifications [TS 33.180] and [TS 33.501]. (I)

15.4 FRMCS Security Principles

15.4.1 Principle 1: The FRMCS security applies a defence in depth approach [i.5] in which multiple layers of security are utilizing a combination of various security measures. Such an approach addresses many different attacks and threats using several independent methods for: (I)

- data protection: protecting data from network attackers and malicious actors;
- transparency: having knowledge of which parties have what access to the data; and
- access control: allowing endpoints meaningfully to grant access to parties with this knowledge.

15.4.2 Principle 2: The FRMCS service stratum security and the FRMCS transport stratum security are complementary and functionally independent from each other. (I)

15.4.3 Principle 3: The FRMCS security applies features, mechanisms and cryptographic algorithms according to ETSI and 3GPP technical specifications that require managed unique identities, identifiers, credentials, certificates and keys. (I)

15.4.4 Principle 4: Application stratum security functions may be used, additionally. (I)

15.4.5 Principle multi stratum security model: Figure 15-1 shows the principle multi-stratum security model with its protection functions following a defence in depth approach. The term “depth” is here related to a model that from application stratum’s point of view the service stratum is logically placed below the application stratum and the transport stratum is logically placed below the service stratum. (I)

The FRMCS service stratum security protects: (I)

- access to the FRMCS service stratum based on authentication and authorization; and
- data in the FRMCS service stratum in the context of integrity, confidentiality and privacy.

The FRMCS transport stratum security protects: (I)

- access to FRMCS transport stratum based on authentication and authorization; and
- data in the FRMCS transport stratum in the context of integrity, confidentiality and privacy.

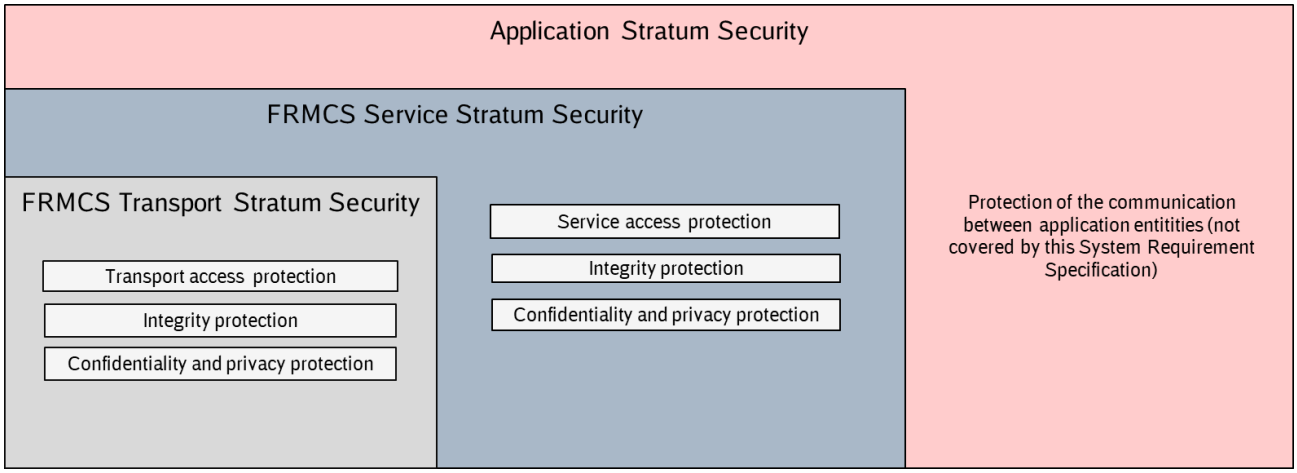


Figure 15-1 Principle multi stratum security model based on a defence in depth approach

15.5 FRMCS Security Requirements

15.5.1 Service Stratum and Transport Stratum

15.5.1.1 [TR 22.889] lists requirements of the security framework for FRMCS. (I)

15.5.1.2 The FRMCS service stratum security and the FRMCS transport stratum security shall provide functions to fulfil requirements resulting from the GDPR [i.7]. (M)

15.5.2 Service Stratum

15.5.2.1 [TS 33.180] applies for the FRMCS service stratum security in the following context:

- The FRMCS service stratum security shall provide functions for the MCX user authentication. (M)
- The FRMCS service stratum security shall provide functions for the MCX user service authorisation that validate whether an MCX user has the authority to access certain MC services. (M)
- The FRMCS service stratum security shall provide functions for the protection of the confidentiality and integrity of media / data payload as well as of signalling data. (M)
- The FRMCS service stratum security should provide functions for the protection of the authenticity of data payload. (O)
- The FRMCS service stratum security shall provide functions for the protection of the privacy of data, like e.g., MC user ID, MCPTT ID, MCVideo ID, MCData ID and MCX Group ID. (M)

Note 3: IMS / SIP security features and mechanisms, e.g., in the context of subscriber authentication, data integrity and data confidentiality are specified in [TS33.203] which is referenced in [TS33.180].

15.5.2.2 The FRMCS service stratum security shall be able to protect the confidentiality, integrity and authenticity as well as to authenticate MCX users based on cryptographic algorithms and MCX user authentication framework according to table 6:

Confidentiality of the RTP media stream for MCPTT shall be protectable by AEAD_AES_128_GCM. (M)
Integrity of the RTP media stream for MCPTT should be protectable by AEAD_AES_128_GCM. (O)
Confidentiality of the RTP media stream for MCVideo shall be protectable by AEAD_AES_128_GCM. (M)
Integrity of the RTP media stream for MCVideo should be protectable by AEAD_AES_128_GCM. (O)
Confidentiality of the RTCP signalling for MCPTT should be protectable by AEAD_AES_128_GCM. (O)
Integrity of the RTCP signalling for MCPTT shall be protectable by AEAD_AES_128_GCM. (M)
Confidentiality of the RTCP signalling for MCVideo should be protectable by AEAD_AES_128_GCM. (O)
Integrity of the RTCP signalling for MCVideo shall be protectable by AEAD_AES_128_GCM. (M)
Confidentiality and integrity of the data payload for MCDATA shall be protectable by AEAD_AES_128_GCM. (M)
Confidentiality and integrity of signalling data for MCDATA shall be protectable by AEAD_AES_128_GCM. (M)
Confidentiality and integrity of the data payload for MCDATA should be protectable by AEAD_AES_256_GCM. (O)
Confidentiality and integrity of signalling data for MCDATA should be protectable by AEAD_AES_256_GCM. (O)
Authenticity of data payload for MCDATA should be protectable by ECCSI. (O)
MCX UE and MC system shall support OpenID Connect 1.0 framework for MCX user authentication. (M)
Note 1: According to [TS 33.180] the protection of the integrity of the RTCP signalling is mandatory.
Note 2: As stated in [TS 33.180] the protection of both confidentiality and integrity of the data payload and signalling data for MCDATA is mandatory.
Note 3: For MCDATA it is recommended by security experts to demand AEAD_AES_GCM_256 as AEAD_AES_GCM_128 will become vulnerable within the foreseeable lifespan of FRMCS.

Table 6 - Cryptographic MCX Security Algorithms and MCX user authentication framework

15.5.3 Transport Stratum

15.5.3.1 [TS 33.501] applies for the FRMCS transport stratum security in the following context:

- The FRMCS transport stratum security shall provide functions for subscription and serving network authentication. (M)
- The FRMCS transport stratum security shall provide functions for the UE and serving network authorization. (M)
- The FRMCS transport stratum security shall provide functions for the protection of the confidentiality and integrity of user data as well as of signalling data. (M)
- The FRMCS transport stratum security shall provide functions for the protection of the privacy of data, e.g., for the identifier SUPI. (M)

15.5.3.2 The FRMCS transport stratum security shall be able to protect the confidentiality and integrity as well as to authenticate subscriptions based on cryptographic algorithms and subscription authentication methods according to table 7:

Confidentiality of the user data between the UE and the gNB shall be protectable by 128-NEA1. (M)
Confidentiality of the user data between the UE and the gNB should be protectable by 128-NEA2. (O)
Confidentiality of the user data between the UE and the gNB should be protectable by 128-NEA3. (O)
Confidentiality of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively shall be protectable by 128-NEA1. (M)
Confidentiality of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively should be protectable by 128-NEA2. (O)
Confidentiality of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively should be protectable by 128-NEA3. (O)

Integrity of the user data between the UE and the gNB shall be protectable by 128-NIA1. (M)
Integrity of the user data between the UE and the gNB should be protectable by 128-NIA2. (O)
Integrity of the user data between the UE and the gNB should be protectable by 128-NIA3. (O)
Integrity of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively shall be protectable by 128-NIA1. (M)
Integrity of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively should be protectable by 128-NIA2. (O)
Integrity of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively should be protectable by 128-NIA3. (O)
UE and serving network shall support EAP-AKA' and 5G AKA subscription authentication methods. (M)
UE and serving network should support the EAP-TLS subscription authentication method. (O)
Note 1: According to [TS 33.501] the protection of the integrity of the RRC and NAS-signalling between the UE and gNB and between UE and AMF, respectively is mandatory.

Table 7 - Cryptographic 5G Security Algorithms and Subscription Authentication Methods

15.6 Minimum FRMCS Security Level

15.6.1 A minimum FRMCS security level is defined taking into account algorithms listed in Table 6 and Table 7. (I)

Note 4: The minimum FRMCS security level does not yet take into account the results of risk assessments, as these do not yet exist.

15.6.2 The set of cryptographic algorithms, MCX user authentication framework and 5G subscription authentication methods according to Table 8 shall be implemented and applied. (M)

FRMCS Service Stratum Security		
Scope	***Security Item***	***Cryptographic Algorithm and MCX User Authentication Framework according to [TS 33.180]***
Voice	Confidentiality of MCPTT (media payload)	AEAD_AES_128_GCM
	Integrity of MCPTT (signalling data)	AEAD_AES_128_GCM
Video	Confidentiality of MCVideo (media payload)	AEAD_AES_128_GCM
	Integrity of MCVideo (signalling data)	AEAD_AES_128_GCM
Data	Confidentiality of MCDATA (data payload)	AEAD_AES_128_GCM
	Integrity of MCDATA (data payload)	AEAD_AES_128_GCM
	Confidentiality of MCDATA (signalling data)	AEAD_AES_128_GCM
	Integrity of MCDATA (signalling data)	AEAD_AES_128_GCM
Authentication	MCX user authentication	OpenID Connect 1.0

FRMCS Transport Stratum Security		
Scope	***Security Items***	***Cryptographic Algorithms and Subscription Authentication Methods according to [TS 33.501]***
User Data	Confidentiality of user data	128-NEA1
	Integrity of the user data	128-NIA1
Signalling Data	Confidentiality of the RRC and NAS-signalling	128-NEA1
	Integrity of the RRC and NAS-signalling	128-NIA1
Authentication	Subscription authentication	EAP-AKA' and 5G AKA

Table 8 - Set of cryptographic algorithms, MCX user authentication and subscription authentication methods to be **implemented and applied** for the minimum FRMCS security level

Note 5: The set of cryptographic algorithms listed in Table 8 for the FRMCS transport security follows the finding 1 in chapter 15.1 of [i.8], which states "To protect data from interception and alteration, apply by default a strong, not-NULL ciphering and integrity protection algorithms (e.g., 128-NEA1 or stronger and 128-NIA1 or stronger, respectively) for both user and signalling data exchanged between the UE and the network.".

16 Positioning and localisation

Editor's note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

16.1 Introduction

16.2 General principles and system requirements

16.3 Positioning and localisation architectural framework

16.4 Accuracy

16.5 Security

Editor's note:
Provide a list of security and privacy constraints. Security precautionary measures to prevent knowledgeable changes of the position information of a user.

16.6 Integrity

Editor's note:
Provide the level of integrity of positioning information.

16.7 Reference points (coordination system)

Editor's note:
Provide a definition of the reference points of the positioning system.

17 Non-Functional System Requirements

Editor's note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

17.1 Introduction

17.2 FRMCS System monitoring

17.3 On-Board FRMCS

17.3.1 System modes and states

17.3.1.1 Introduction

17.3.1.1.1 2 system modes are foreseen: (I)

a) System mode 1:n
b) System mode m:n

Note: n corresponds to the number of Radio Functions, and m to the number of Gateway Functions. The notation 1:n indicates that there is one Gateway Function connected to multiple Radio Functions. m:n indicates that multiple Gateway Functions are connected to multiple Radio Functions.

17.3.1.1.2 System mode m:n is intended for the implementation of (Gateway Function) redundancy. (I)

17.3.1.2 System mode 1:n

17.3.1.2.1 System mode 1:n is the main mode of the On-Board FRMCS, where one Gateway Function is connected to one or several Radio Function(s), as depicted in Figure 17-1. (I)

17.3.1.2.2 System mode 1:n is applicable both for integrated and distributed architectures. (I)

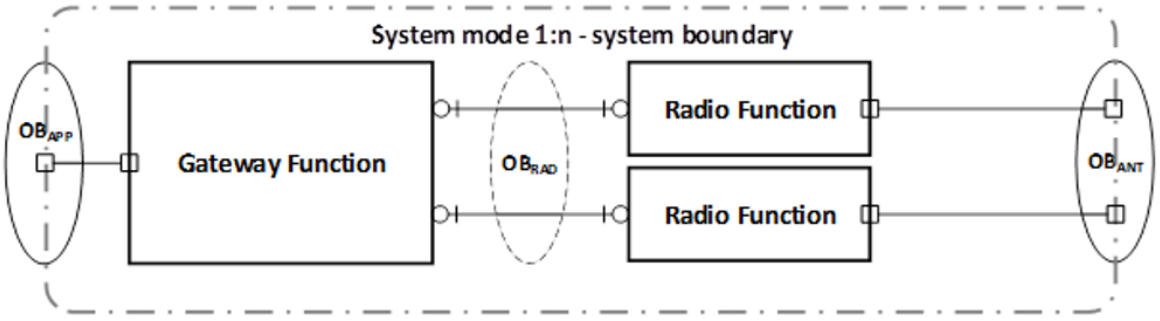


Figure 17-1: System mode 1:n. A case where 2 radio Functions are connected to the Gateway Function

17.3.1.2.3 The 1:n system mode shall be possible. (M)

17.3.1.3 System mode (m:n)

Editor's note: This topic is FFS and subsequent ones.

17.3.2 Major system capabilities

17.3.2.1 The On-Board FRMCS accommodates shared usage of radio access resources for concurrent critical and performance applications. (I)

17.3.2.2 The On-Board FRMCS enables two coupling modes [TOBA FRS] (I):

- Loose Coupling Mode
- Tight Coupling Mode

17.3.2.3 The On-Board FRMCS shall enable Operation and Maintenance. (M)

17.3.2.4 The On-Board FRMCS shall enable at least one Gateway Function. (M)

17.3.2.5 Each Gateway Function shall contain at least one Communication Gateway. (M)

17.3.2.6 The On-Board FRMCS shall contain at least one Radio Function. (M)

17.3.3 External Constraints

17.3.3.1 The following external constraints should be considered: (I)

- Existing national frequency plans
- Coexistence with GSM-R in 900 MHz
- Coexistence with MNOs in neighbouring frequency blocks
- Coexistence with other systems (e.g., SRD, UAS, DECT)
- Cross border Synchronization (TDD)

17.3.4 FRMCS User characteristics

17.3.4.1 FRMCS Users are entities that can have access to the On-Board FRMCS (I), e.g.:

- Human
- Machine

17.3.4.2 Entities have access to the On-Board FRMCS through FRMCS-enabled applications. (I)

17.3.4.3 An FRMCS User shall be uniquely identifiable. (M)

17.3.4.4 An FRMCS User’s profile should define the system capabilities made available to the user. (O)

17.3.4.5 An FRMCS User shall be identified by the On-Board FRMCS using profiles. (M)

17.3.4.6 An FRMCS User shall have the capability to establish a communication session with any other user(s) of the system, as long as it has the right to do so. (M)

18 User equipment

Editor's note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

18.1 Mobile equipment

18.2 Controller equipment

19 Subscriber configuration

Editor’s note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

20 System configuration

Editor’s note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

21 Off-Network communication

Editor's note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS. This section may refer to [TR 22.990].

22 Miscellaneous

Editor’s note:
This section will not be addressed in version 1.0.0 of the FRMCS SRS.

Annex A. QoS Requirement Values of FRS applications and its Clustering

The Table 22-1 illustrates a mapping of FRS applications and the functional requirements (as stated in the URS – light grey columns) to system requirement values on latency, packet reliability and data rate as introduced in this specification document (light blue columns). The system requirements are input for the mapping towards 3GPP parameters.

UIC URS v5.0 / FRS v1.0.0			**Service Type**			**Latency**		**Packet Reliability**		**Data Rate**		**Session Setup Time**
Applications	URS	FRS	Voice	Video	Data	Funct. requ.	Service value	Funct. requ.	Service value	Funct. requ.	Service value	Funct./ System requ.
Automatic Train Protection communication (up to ETCS L2) Note: Further ATP evolutions (e.g., ETCS L3) is FFS (see 14.7.2)	5.9	11.4			x	Low	100 ms – 500 ms	High	99.9%	Low	4 kbps - 10 kbps	Immediate
Automatic Train Operation communication (up to ATO GoA2)	5.10	11.5			x	Low	100 ms – 500 ms	High	99.9%	Low	ffs	Immediate
Railway Emergency Communication	5.15	10.11	x			Low	100 ms – 500 ms	High	99%	Low	ffs	Immediate
					x	Low	100 ms – 500 ms	High	99.9%	Low	4 kbps - 10 kbps	Immediate

Table 22-1 - Mapping of FRS application to QoS system requirements and attribute values

Annex B. Mapping between application regimes and URS applications

UIC URS v5.0 / FRS v1.0.0			Application regime	OB_{APP} coupling mode	TS_{APP} coupling mode
Applications	URS	FRS			
Automatic Train Protection communication (up to ETCS L2) Note: Further ATP evolutions (e.g., ETCS L3) is FFS (see 14.7.2)	5.9	11.4	Loose	Loose	Loose
Automatic Train Operation communication (up to ATO GoA2)	5.10	11.5	Loose or Superloose	Loose	ffs
Key Management System	8.9	11.18	Superloose	Loose	ffs
Public Key Infrastructure	N/A	N/A	Superloose	Loose	ffs
Railway Emergency Communication	5.15	10.11	Tight	Tight	ffs

Annex C. Mapping of FRS Requirements to SRS Requirements

Editor's note: The complete mapping of FRS Requirements to SRS Requirements will be provided in later revision.

FU-7120 - FRS		FW-AT-7800 - SRS	
Clause	Requirement	Clause	Covered by relevant SRS Requirement
2	List of abbreviations		
3	List of definitions		
4	Introduction		
4.1	Background		
4.2	Purpose of this document		
4.3	Scope		
4.4	Applicability		
5	Application concept		
5.1	Goal		
5.2	Principles		
5.3	Applications framework		
6	FRMCS functional addressing		
6.1	Introduction		
6.2	Generic requirements		
6.3	Functional identities		
7	Introduction to common functions and applications		
8	Common functions		
8.1	Introduction		
8.2	Common functions		
8.2.2	Assured voice communication common function (URS 8.1)		To be completed
8.2.2.1	Introduction		
8.2.2.2	Generic requirements		

8.2.2.3	Requirements for interworking with GSM-R		
8.2.2.4	Requirements for off-network		
8.2.2.5	Requirements for network maintenance, configuration and monitoring		
8.2.2.6	Attributes (inputs/outputs)		
8.2.3	Multi user talker control common function (URS 8.2)		To be completed
8.2.3.1	Introduction		
8.2.3.2	Generic requirements		
8.2.3.3	General behaviour granting permission to talk		
8.2.3.4	Requirements for interworking with GSM-R		
8.2.3.5	Requirements for off-network		
8.2.3.6	Requirements for network maintenance, configuration and monitoring		
8.2.3.7	Attributes (inputs/outputs)		
8.2.4	Role management and presence common function (URS 8.3)		To be completed
8.2.5	Location services common function (URS 8.4)		
8.2.5.1	Introduction		
8.2.5.2	Generic requirements		
8.2.5.2.1	The location service common function shall be able to provide, on request, the location information of a user device at any time.	16	To be completed
8.2.5.2.2	The location information shall be accessible by an application or an external system.	16	To be completed
8.2.5.2.3	The location service common function shall support the following elements: a) User's geographical horizonal position; b) User's geographical horizonal and vertical position; c) User's velocity (speed and direction in the horizontal space); d) User's acceleration; e) Railway infrastructure element(s) linked to the user (e.g. track section ID, station ID, signal box ID, track kilometre marking)	16	To be completed
8.2.5.2.4	The system is able to support the elements above, but at some time not all the information might be available	16	To be completed

8.2.5.2.5	Each location information element shall be accompanied by: a) The level of accuracy of the location information element; b) The time stamp of the location information element.	16	To be completed
8.2.5.2.6	The location services common function shall allow external source(s) to be location information sources, to enhance the accuracy or to add other type of location information.	16	To be completed
8.2.5.2.7	The external source(s) providing location information can be e.g. interlocking system, ATC, sensor, RFID, information from MCx or external GPS/Galileo.	16	To be completed
8.2.5.2.8	The location services common function shall provide, upon request, the identity/ies of the user(s) matching the following criteria: a) User's geographical position included in a given polygon; b) User's velocity included in a given range; c) User's geographical position linked to a railway infrastructure element(s) (such as a balise or a level crossing); d) User's functional identity in a given range (e.g. leading driver of company AA).	16	To be completed
8.2.5.3	Requirements for interworking with GSM-R	9	To be completed
8.2.5.4	Requirements for off-network		
8.2.5.4.1	The location services common function shall be able to operate in off-network mode	21	To be completed
8.2.5.5	Requirements for network maintenance, configuration and monitoring		
8.2.5.6	Attributes (inputs/outputs)		
8.2.5.6.1	The FRMCS system shall support the following input attributes: a) The identity of the user; b) The range of positions (polygon including geographical coordinates); c) The velocity in a given range; d) The set of railway infrastructure elements; e) The range of function identities.		To be completed

8.2.5.6.2	The FRMCS system shall support the following output attributes: a) The user's position (geographical position); b) The user's velocity; c) The user's acceleration; d) The set of railway infrastructure elements linked to user's position; e) The level of accuracy; f) Time stamp of the location information; g) The identities of the users matching the request criteria.		To be completed
8.2.6	Authorisation of communication common function (URS 8.5)		
8.2.6.1	Introduction		
8.2.6.2	Generic requirements		
8.2.6.3	Requirements for interworking with GSM-R		
8.2.6.4	Requirements for off-network		
8.2.6.5	Requirements for network maintenance, configuration and monitoring		
8.2.6.6	Attributes (inputs/outputs)		
8.2.7	Authorisation of application common function (URS 8.7)		To be completed
8.2.8	QoS Class negotiation common function (URS 8.8)		
8.2.8.1	Introduction		
8.2.8.2	Generic requirements		
8.2.8.2.1	The QoS negotiation common function shall assign to each communication a QoS category.	14	To be completed
8.2.8.2.2	The application shall be able to request a QoS category upon the initiation of a communication.	14	To be completed
8.2.8.2.3	The allowed QoS categories shall be allocated to each application by the network operator.	14	To be completed
8.2.8.2.4	In case the requested QoS category is granted by the system, the communication is established.	14	To be completed
8.2.8.2.5	If the requested QoS category cannot be granted, the system shall be able to perform any of the following actions based on network operator setting: a) Establish the communications with a lower QoS category, or; b) Reject the request for communication.	14	To be completed

8.2.8.2.6	The QoS category assigned shall be constantly monitored by the system.	14	To be completed
8.2.8.2.7	If the assigned QoS category during an ongoing communication becomes lower than the requested one, the system shall be able to perform any of the following actions based on network operator setting: a) The application accepts the lower QoS category and the ongoing communications continues, or; b) Stop the ongoing communication.	14	To be completed
8.2.8.2.8	When no QoS category is requested upon the initiation of a communication, the system shall apply the predefined QoS category.	14	To be completed
8.2.8.2.9	The QoS negotiation common function shall assign to each communication a priority level which will be used by the system during the assignment of resources to a communication.	14	To be completed
8.2.8.2.10	The application shall be able to request a priority level upon the initiation of a communication.	14	To be completed
8.2.8.2.11	The maximum allowed priority level shall be allocated to each application by the network operator.	14	To be completed
8.2.8.2.12	The default priority level shall be allocated to each application by the network operator.	14	To be completed
8.2.8.2.13	When no priority level is requested, the system shall apply the default priority level.	14	To be completed
8.2.8.2.14	If the requested priority level is accepted, the system shall assign this priority level for this communication.	14	To be completed
8.2.8.2.15	If the requested priority level is not accepted, the system shall assign the maximum allowed priority level for this communication and notify the assigned priority level to the application.	14	To be completed
8.2.8.2.16	In the case of a lack of resources upon the initiation of a communication, based on the priority level of the related communications, the FRMCS system shall: a) Downgrade other ongoing communication(s) to a lower QoS category, or; b) Release other communication(s), or; c) Reject the initiation of the communication.	14	To be completed

8.2.8.2.17	In the case of a lack of resources during an ongoing communication, based on the priority level of the related communications, the FRMCS system shall: a) Downgrade other ongoing communication(s) to a lower QoS category, or; b) Release other communication(s), or; c) Release the ongoing communication.	14	To be completed
8.2.8.3	Requirements for interworking with GSM-R		
8.2.8.3.1	For user-to-user/multi-user communication, in the direction from GSM-R to FRMCS, the GSM-R priority level is exchanged. Mapping of GSM-R priority level to FRMCS priority level shall be performed in the FRMCS system.	9	To be completed
8.2.8.3.2	For user-to-user/multi-user communication, in the direction from FRMCS to GSM-R, the GSM-R priority level is exchanged. The priority level from FRMCS shall be mapped to GSM-R priority level by the FRMCS system.	9	To be completed
8.2.8.4	Requirements for off-network		
8.2.8.5	Requirements for network maintenance, configuration and monitoring		
8.2.8.5.1	The system shall allow the network operator to get statistics about the communication pre-emption, QoS category degradation and occurrences of denials.		To be completed
8.2.8.5.2	A user shall not experience any interruption or divergent behaviour in the usage of an application due to a transition between networks (seamless user experience).		To be completed
8.2.8.6	Attributes (inputs/outputs)		
8.2.8.6.1	The QoS negotiation common function shall support the following input attributes: a) QoS Category; b) Priority level.		To be completed
8.2.8.6.2	The QoS negotiation common function shall support the following output attributes: a) Assigned QoS category; b) Assigned priority level. c) Release a communication.		To be completed
8.2.9	Assured data communication common function (URS 8.10)		To be completed
8.2.9.1	Introduction		

8.2.9.2	Generic requirements	
8.2.9.3	Requirements for interworking with GSM-R	
8.2.9.4	Requirements for off-network	
8.2.9.5	Requirements for network maintenance, configuration and monitoring	
8.2.9.6	Attributes (inputs/outputs)	
8.2.10	Inviting-a-user common function (URS 8.11)	To be completed
8.2.10.1	Introduction	
8.2.10.2	Generic requirements	
8.2.10.3	Requirements for interworking with GSM-R	
8.2.10.4	Requirements for off-network	
8.2.10.5	Requirements for network maintenance, configuration and monitoring	
8.2.10.6	Attributes (inputs/outputs)	
8.2.11	Arbitration common function (URS 8.12)	To be completed
8.2.12	Billing information common function (URS 10.1)	To be completed
8.2.12.1	Introduction	
8.2.12.2	Generic requirements	
8.2.12.3	Requirements for interworking with GSM-R	
8.2.12.4	Requirements for off-network	
8.2.12.5	Requirements for network maintenance, configuration and monitoring	
8.2.12.6	Attributes (inputs/outputs)	
8.2.13	Time synchronisation common function (URS 8.13)	To be completed
8.2.13.1	Introduction	
8.2.13.2	Generic requirements	
8.2.13.3	Requirements for interworking with GSM-R	
8.2.13.4	Requirements for off-network	
8.2.13.5	Requirements for network maintenance, configuration and monitoring	
8.2.13.6	Attributes (inputs/outputs)	
9	Introduction to applications	
9.1	Introduction	

9.2	Applications
10	Voice applications
10.1	Basic voice communication functions
10.2	Generic HMI aspects
10.3	Basic voice communication
10.3.1	Introduction
10.3.2	Generic requirements
10.3.3	HMI requirements
10.3.4	Requirements for interworking with GSM-R
10.3.5	Requirements for off-network
10.3.6	Requirements for network maintenance, configuration and monitoring
10.3.7	Involved common functions
10.4	On-train outgoing voice communication from the train driver towards the controller(s) of a train (URS 5.1)
10.4.1	Introduction
10.4.2	Generic requirements
10.4.3	HMI requirements
10.4.4	Requirements for interworking with GSM-R
10.4.5	Requirements for off-network
10.4.6	Requirements for network maintenance, configuration and monitoring
10.4.7	Involved common functions
10.5	On-train incoming voice communication from the controller towards a train driver (URS 5.2)
10.5.1	Introduction
10.5.2	Generic requirements
10.5.3	HMI requirements
10.5.4	Requirements for interworking with GSM-R
10.5.5	Requirements for off-network
10.5.6	Requirements for network maintenance, configuration and monitoring
10.5.7	Involved common functions

10.6	Multi-train voice communication for drivers including ground user(s) (URS 5.3)
10.6.1	Introduction
10.6.2	Specific pre-conditions
10.6.3	Requirements
10.6.4	HMI requirements
10.6.5	Requirements for interworking with GSM-R
10.6.6	Requirements for off-network
10.6.7	Requirements for network maintenance, configuration and monitoring
10.6.8	Involved common functions
10.7	Ground to ground voice communication (URS 5.8)
10.7.1	Introduction
10.8	Railway Emergency Communication (URS 5.15)
10.8.1	Introduction
10.8.2	Generic requirements
10.8.3	HMI requirements
10.8.4	Requirements for interworking with GSM-R
10.8.5	Requirements for off-network
10.8.6	Requirements for network maintenance, configuration and monitoring
10.8.7	Involved common functions
11	Data applications
11.1	Data communication functions
11.2	Basic data communication
11.2.1	Introduction
11.2.2	Generic requirements
11.2.3	HMI requirements
11.2.4	Requirements for interworking with GSM-R
11.2.5	Requirements for off-network
11.2.6	Requirements for network maintenance, configuration and monitoring
11.2.7	Involved common functions

11.3	Role management and presence application
11.3.1	Introduction
11.3.2	Generic requirements
11.3.3	Functional identity handover
11.3.4	HMI requirements
11.3.5	Requirements for interworking with GSM-R
11.3.6	Requirements for off-network
11.3.7	Requirements for network maintenance, configuration and monitoring
11.3.8	Involved common functions
11.4	Automatic Train Protection communication (URS 5.9)
11.4.1	Introduction
11.4.2	Generic requirements
11.4.3	HMI requirements
11.4.4	Requirements for interworking with GSM-R
11.4.5	Requirements for off-network
11.4.6	Requirements for network maintenance, configuration and monitoring
11.4.7	Involved common functions
11.5	Automatic Train Operation communication (URS 5.10)
11.5.1	Introduction
11.5.2	Generic requirements
11.5.3	HMI requirements
11.5.4	Requirements for interworking with GSM-R
11.5.5	Requirements for off-network
11.5.6	Requirements for network maintenance, configuration and monitoring
11.5.7	Involved common functions
11.6	Safety key management data communication (URS 5.31)
11.6.1	Introduction
11.6.2	Generic requirements
11.6.3	HMI requirements

11.6.4	Requirements for interworking with GSM-R		
11.6.5	Requirements for off-network		
11.6.6	Requirements for network maintenance, configuration and monitoring		
11.6.7	Involved common functions		
12	Video applications		
12.1	Basic video communication functions		
13	(VOID)		
14	Terminal requirement		
14.1	Use case: Deported control of applications		
15	System management and configuration aspects		
15.1	Introduction		
15.2	Network management and configuration		
15.3	User equipment management and configuration		
16	Digital resilience		
16.1.1	The FRMCS shall provide precautionary measures to prevent unauthorised and potential malicious access and acts affecting the use of the communication system and any associated data.	15	To be completed
16.1.2	Certain applications require strong authentication, encryption and key management methods and the communication system shall support these when required.	15	To be completed
16.1.3	The system, its design, use, and ecosystem shall be and remain resilient against (cyber) security threats.	15	To be completed
17	To do list		
	The user shall be able to move an existing communication (connected or queued) to another of its device having the corresponding application active.		
18	References		
Appendix A	URS Pr's and GN's covered in FRS		
Appendix B	Traceability to URS and Use cases		
Appendix C	Regional requirements		

	European Union		
	Asia		
	US		
Appendix D	Mapping of functional addressing with GSM-R		
		9	To be completed
Appendix E	Call handling		
I.	User-to-user communication – example 1		
II.	Multi-user communication – example 1		
III.	Multi-user communication – example 2		
IV.	Multi-user communication – example 3		
V.	Multi-user communication – example 4		
VI.	Multi-user communication – example 5		

Annex D. Interoperability requirements in EU

This annex is the placeholder for identifying the requirements relevant for interoperability in the European Union, i.e. the requirements, with respect to the authorisation in the EU according to the TSI, that are considered in the European Directives to be relevant for interoperability as fulfilling the essential requirements for the Control-Command and Signalling (CCS) subsystem related to safety and technical compatibility which must be met by the rail system, the subsystems, and the interoperability constituents, including interfaces according to the corresponding conditions set out in Directive (EU) 2016/797. It is mandatory that each railway subsystem in the EU meets these requirements on lines under the scope of the Directive and the CCS TSI to ensure technical compatibility between Member States and safe integration between train and track.

At this stage, the version of this specification is not considered complete for the purpose of tendering On-Board FRMCS equipment, and the identification of all requirements relevant for interoperability is for further study.

This annex is therefore only informative.