Future Railway Mobile Communication System

System Requirements Specification

Source: FRMCS AT Working Group
Date: 13 December 2024
Reference: FW-AT 7800
Version: 2.0.0
No of pages: 189

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.
1.0.1	21 March 2024	Internal review in ATWG including merging of stable draft chapters. Missing chapters: 7 (partly), 19, 20, 21 and 24.
1.0.2	28 March 2024	Internal review in ATWG
1.1.0	29 March 2024	Version ready for external review
1.1.1	30 April 2024	Internal review in ATWG including minor changes
1.2.0	3 May 2024	Version ready for external review

1.2.1	27 September 2024	Correction made after external review comments including EECT agreed comments to v1.2.0
1.2.3	26 November 2024	Correction made after external review comments including EECT agreed comments to v1.2.2
1.2.4	04 December 2024	Correction made after external review comments including EECT agreed comments to v1.2.3
2.0.0	13 December 2024	Official publication.

Table of Contents

1 LIST OF ABBREVIATIONS 9

2 LIST OF DEFINITIONS 14

3 REFERENCES 22

3.1 APPLICABILITY 22
3.2 LIST OF REFERENCES 22

4 INTRODUCTION 24

4.1 BACKGROUND 24
4.2 PURPOSE OF THIS DOCUMENT 25
4.3 SCOPE 25
4.4 APPLICABILITY 25
4.5 DOCUMENT LIFE CYCLE 26

5 SYSTEM ARCHITECTURE DESIGN PRINCIPLES 27

5.1 SCOPE OF FRMCS SYSTEM AND SYSTEM ARCHITECTURE 27
5.2 PRINCIPLES FOR SYSTEM REQUIREMENTS 28

6 SYSTEM REFERENCE ARCHITECTURE AND REFERENCE POINTS 29

6.1 PREAMBLE 29
6.2 DESCRIPTION OF THE SYSTEM REFERENCE ARCHITECTURE 36
6.3 DECOMPOSITION INTO BUILDING BLOCKS 37
6.4 DESCRIPTION OF SYSTEM ARCHITECTURE REFERENCE POINTS 39
6.5 ADDRESSING 42

7 DESCRIPTION OF SUBSYSTEMS AND CONSTITUENTS 44

7.1 ON-BOARD FRMCS 44
7.2 ANTENNA FUNCTION 70

8 RADIO SPECTRUM 72

8.1 INTRODUCTION 72
8.2 OUT OF SCOPE 72
8.3 SPECTRUM PRINCIPLES 72
8.4 RMR FREQUENCY BANDS FOR EUROPE 72
8.5 PUBLIC MNO SPECTRUM IN EUROPE 73
8.6 WLAN (WI-FI) SPECTRUM IN EUROPE 76

9 GSM-R/FRMCS INTERWORKING 77

9.1 INTRODUCTION 77
9.2 OUT OF SCOPE 77
9.3 INTERWORKING INTERFACES 77
9.4 MIGRATION SCENARIOS IN EUROPE 78
9.5 INTERWORKING 79

10 NETWORK TRANSITIONS AND INTERCONNECTION 82

10.1 NETWORK TRANSITIONS 82
10.2 INTERCONNECTION 88
10.3 FS_{NNI} REQUIREMENTS 89

10.4 INTENTIONALLY DELETED 90

11 IDENTIFIERS 91

11.1 INTRODUCTION 91
11.2 SCOPE 92
11.3 IDENTIFIERS OF THE FRMCS TRANSPORT STRATUM 92
11.4 IDENTITIES OF THE FRMCS SERVICE STRATUM 94
11.5 USAGE AND DEPENDENCIES OF DIFFERENT FRMCS IDENTITIES 101
11.6 ROLE BASED IDENTIFICATION SCHEME 102

12 BEARER FLEXIBILITY 109

12.1 INTRODUCTION 109
12.2 OUT OF SCOPE 110
12.3 FRMCS MULTIPATH REQUIREMENTS 110
12.4 MULTI-OPERATOR CORE NETWORK (MOCN) 113

13 NETWORK SLICING 115

13.1 INTRODUCTION 115
13.2 OUT OF SCOPE 115
13.3 GENERAL REQUIREMENTS 115

14 QUALITY OF SERVICE AND PRIORITY 117

14.1 INTRODUCTION 117
14.2 OUT OF SCOPE 119
14.3 GENERIC REQUIREMENTS 119
14.4 FRMCS E2E QOS REQUIREMENTS 119
14.5 COMPONENT QOS PARAMETERS 122
14.6 3GPP QOS PARAMETERS 122
14.7 QOS SIGNALLING AND MONITORING 124

15 FRMCS CYBERSECURITY 125

15.1 INTRODUCTION 125
15.2 OUT OF SCOPE 125
15.3 **INTENTIONALLY DELETED.** 127
15.4 FRMCS SECURITY PRINCIPLES 127
15.5 FRMCS SECURITY REQUIREMENTS 129
15.6 MINIMUM CRYPTOGRAPHIC ALGORITHM STRENGTH USED IN FRMCS 131

16 FRMCS LOCATION AND POSITIONING SYSTEM 133

16.1 INTRODUCTION 133
16.2 OUT OF SCOPE 133
16.3 GENERAL PRINCIPLES AND SYSTEM REQUIREMENTS 133
16.4 POSITIONING AND LOCALISATION ARCHITECTURAL FRAMEWORK 137
16.5 PERFORMANCE REQUIREMENTS 138
16.6 SECURITY REQUIREMENTS 138

17 NON-FUNCTIONAL SYSTEM REQUIREMENTS 139

17.1 INTRODUCTION 139
17.2 FRMCS SYSTEM MONITORING 139
17.3 ON-BOARD FRMCS 139

18 USER EQUIPMENT 141

18.1 MOBILE EQUIPMENT 141
18.2 CONTROLLER EQUIPMENT 141
18.3 DRIVER EQUIPMENT 141

19 PROFILES IN FRMCS 142

19.1 INTRODUCTION 142
19.2 ON-BOARD FRMCS CONFIGURATION 143
19.3 FRMCS ON-BOARD APPLICATION PROFILE 146
19.4 CONFIGURATION WITHIN A FRMCS DOMAIN 147

20 FRMCS AIR INTERFACE 148

20.1 INTRODUCTION 148
20.2 GENERIC REQUIREMENTS 148

21 FRMCS COMMON FUNCTIONS 150

21.1 INTRODUCTION 150
21.2 MULTI-USER TALKER CONTROL 151
21.3 ROLE MANAGEMENT 152
21.4 AUTHORISATION OF COMMUNICATION 156
21.5 ARBITRATION 158

22 RECORDING AND LOGGING 160

22.1 INTRODUCTION 160
22.2 OUT OF SCOPE 160
22.3 GENERIC REQUIREMENTS 160

23 FRMCS TIME SERVICE 161

23.1 INTRODUCTION 161
23.2 OUT OF SCOPE 161
23.3 GENERAL PRINCIPLES, ARCHITECTURE AND SYSTEM REQUIREMENTS 161
23.4 GENERIC REQUIREMENTS 163
23.5 PERFORMANCE REQUIREMENTS 163
23.6 SECURITY REQUIREMENTS 163

24 VOICE APPLICATION SUBSYSTEM 164

24.1 GENERAL FUNCTIONAL ARCHITECTURE AND REQUIREMENTS 164
24.2 DRIVER EQUIPMENT 171
24.3 CONTROLLER EQUIPMENT 176

ANNEX A. QOS REQUIREMENT VALUES OF FRS APPLICATIONS AND ITS CLUSTERING 179

A.1 OVERVIEW OF QOS REQUIREMENT VALUES 179
A.2 DERIVATION OF QOS REQUIREMENTS BASED ON VOICE 182
A.3 DERIVATION OF QOS REQUIREMENTS FOR ETCS 183
A.4 DERIVATION OF QOS REQUIREMENTS FOR ATO 184
A.5 RESULTING DATA RATE REQUIREMENTS PER TRAIN 185
A.6 ACCEPTABLE INTERRUPTION TIME DURING IFDT 186

ANNEX B. MAPPING BETWEEN APPLICATION REGIMES AND FRS APPLICATIONS 187

ANNEX C. INTEROPERABILITY REQUIREMENTS IN EU 188

1 List of abbreviations

2D	Two-Dimensional
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
AMR	Adaptive Multi Rate
AMR-WB	AMR-Wide Band
APN	Access Point Name
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
CEP	Circular Error Probable
CEPT	European Conference of Postal and Telecommunications
CFM	Communication Functional Module
CPU	Central Processing Unit
CRUD	Create, Read, Update, Delete
CSI	Channel State Information
dB	Decibel
DNN	Data Network Name
DNS	Domain Name System
DPI	Deep Packet Inspection
DSD	Driver Safety Device
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
ECM	Entity in Charge of Maintenance
ED	End Device
EDOR	ETCS Data Only Radio
EIRENE	European Integrated Railway Radio Enhanced Network
EIRP	Equivalent Isotropic Radiated Power
EN-DC	E-UTRA New Radio – Dual Connectivity
eSIM	Embedded SIM
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EU	European Union
EVN	European Vehicle Number
EVS	Enhanced Voice Services
FA	Functional Addressing or Functional Alias
FDD	Frequency Division Duplex

FFFIS	Form Fit Functional Interface Specification
FIS	Functional Interface Specification
FN	Functional Number
FOAP	FRMCS On-board Application Profile
FQDN	Fully Qualified Domain Name
FRIOP	FRMCS Railway Interoperability On-board Profile
FRMCS	Future Railway Mobile Communications System
FROP	FRMCS Railway On-board Profile
FRS	Functional Requirements Specification
FS	FRMCS System
FS_{IWF}	FRMCS System Interworking reference point/interface
FS_{MPM}	FRMCS System MultiPath Management reference point/interface
FS_{NNI}	FRMCS System Network-Network reference point/interface
FS_{OMR}	FRMCS System OM Remote reference point/interface
FS_{ONI}	FRMCS System Other Network reference point/interface
GBFR	Guaranteed Flow Bit Rate
GCA	Group Call Area
GDPR	General Data Protection Regulation
GHz	Giga Hertz
GID	Group Call Identity
gNB	5G Base Station
GNSS	Global Navigation Satellite Systems
GoA	Grade of Automation
GPS	Global Positioning System
GPSI	Generic Public Subscription Identifier
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
HMI	Human Machine Interface
HPLMN	Home PLMN
HTTP	Hypertext Transfer Protocol
HW	Hardware
ID	IDentity
IdMS	Identity Management Server
IE	Information Element
IETF	Internet Engineering Task Force
IFDT	Inter-FRMCS Domain Transition
IFTDT	Inter-FRMCS-Transport Domain Transition
IFSDT	Inter-FRMCS-Service Domain Transition
IM	Infrastructure Manager
IMC	IMS Credentials
IMPI	IMS Private User Identity
IMPU	IMS Public User Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPUPS	Inter-PLMN User Plane Security
ISDN	Integrated Services Digital Network

iSIM	Integrated SIM
IWF	InterWorking Function
KMS	Key Management System
KPI	Key Performance Indicator
LAN	Local Area Network
MC	Mission Critical
MCC	Mobile Country Code
MCS	Mission Critical Services
MCX	Mission Critical Services
MFBR	Maximum Flow Bit Rate
MHz	Mega Hertz
MIMO	Multiple-Input Multiple-Output
MNC	Mobile Network Code
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MOTS	Modified Off The Shelf
MPF	Multipath Function
MSISDN	Mobile Station International Subscriber Directory Number
mTLS	Mutual TLS
NA	Not Applicable
NAI	Network Access Identifier
NEA	Encryption Algorithm for 5G
NEF	Network Exposure Function
NIA	Integrity Algorithm for 5G
NOTIF-IE	Notification IE
NR	New Radio
NR-DC	New Radio-Dual Connectivity
NTP	Network Time Protocol
NTT	Network Transition Trigger
OB	On-Board
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
OBF OM-SCP	On-Board FRMCS O&M Status Condition Parameters
OBF RM	On-Board FRMCS Radio Module
OC	Organisational Code
OM	Operations & Maintenance
O&M	Operations & Maintenance
OTA	Over-The-Air
P2P	Point-to-Point
PA	Public Announcement
PCC	Policy and Charging Control
PCF	Policy Control Function
PDB	Packet Delay Budget
PDR	Packet Detection Rules
PDU	Packet Data Unit
PER	Packet Error Rate
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QoS	Quality of Service

RAN	Radio Access Network
RAT	Radio Access Technology
RBC	Radio Block Centre
REC	Railway Emergency Communication
RF	Radio Frequency
RMR	Railway Mobile Radio
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
RU	Railway Undertaking
SCP	Status Condition Parameter
SD	Slice Differentiator
SDN	Software-Defined Networking
SDP	Session Description Protocol
SDS	Short Data Service
SEPP	Security Edge Protection Proxy
SIM	Subscriber Identity Module
SINR	Signal to Interference Noise Ratio
SIP	Session Initiation Protocol
SMF	Session Management Function
SMS	Short Message Service
S-NSSAI	Single Network Slice Selection Assistance Information
SRS	System Requirements Specification
SS	Synchronisation Signal
SST	Slice Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SW	Software
TCMS	Train Control Management System
TDD	Time Division Duplex
TLS	Transport Layer Security
TOBA	Telecom On-Board Architecture
TR	Technical Report
TS	Technical Specification or TrackSide
TS_{APP}	Trackside Application reference point/interface
TS_{CTRL}	Trackside Controller Application reference point/interface
TSI	Technical Specification for Interoperability
SBA	Service-Based Architecture
UDM	Unified Data Management
UE	User Equipment
UIC	Union Internationale des Chemins de Fer
UPF	User Plane Function
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UTF-8	Universal Character Set Transformation Format - 8 bits
V2X	Vehicle-to-Everything
VAS	Voice Application Subsystem
VBS	Voice Broadcast Service
VPLMN	Visited PLMN

VSWR	Voltage Standing Wave Ratio
Wi-Fi	Wireless Fidelity
WGS 84	World Geodetic System 1984
WLAN	Wireless LAN

2 List of definitions

Terms	Definitions
Active Data Path (FRMCS Multipath)	An Active Data Path carries one or more Data Flows. The availability and quality of the active Data Path can (but not always will) be measured in terms of, e.g., latency, reliability, error rate and throughput.
Administrative Domain	Domain managed by a single administrative authority (e.g., FRMCS Operator). The Administrative Domain is characterized by organizational/operator boundaries.
Address	In the Transport Stratum an address usually refers to an IP Address permitting to reach remote destinations using the data network(s) of the Transport Stratum. In the Service Stratum addresses are used equivalently and interchangeable with identifiers that are used to identify entities for the purpose of providing the functional capability expected.
Agent	An agent is a functional entity between applications in Superloose application regime and the FRMCS system.
(FRMCS) Application	According to FRS terminology [FRMCS-FRS].
Application Repository	Repository containing applications provided to the user device in need of a communication application.
Area	A geographical area.
Candidate Data Path (FRMCS Multipath)	A Candidate Data Path has the capacity to carry a specific Data Flow but it is not an Active Data Path. The availability of a Candidate Data Path can be determined by considering various aspects such as (radio) link/connection measurements (e.g., radio link quality, latency, reliability) and Multipath Policy.
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.
Concurrency	Within this specification, concurrency is defined as the capability to simultaneously manage the distribution of data flows originating Applications, by either using one single bearer, or multiple bearers for the same data flow. In case of multiple bearers for a single data flow being used, the decision on whether to duplicate the same data flow or to split it, depends on communication policies associated to operational conditions, communication profiles and area of use.
Control Plane	

Terms	Definitions
	The control plane carries signalling traffic between the network entities.
Controller	According to FRS terminology [FRMCS-FRS].
Data Communication	Exchange of information in the form of data, including video (excluding voice communication), requiring corresponding QoS treatment.
Data Flow	A flow of IP packets to which certain rules and policies can be applied. Data Flows can refer to application Media as well as to FRMCS service stratum signaling. A data Flow can be characterized by attributes (e.g., type of data: ETCS, VAS, TCMS, FRMCS signaling) and is identified via IP-5-tuples.
Data Flow Attributes	Data Flow attributes consist of the following elements: 1. Type of data flow (e.g., ETCS, VAS, TCMS, FRMCS signaling) – identified at the service layer. 2. QoS requirements (on packet latency and packet reliability) between MPF on-board and MPF trackside – provided by the trackside (FRMCS Operator) for the respective type of data.
Data Network	An IP network where multiple Hosts can be connected.
Data Network Name	According to 3GPP terminology [TS 23.003].
Data Path (FRMCS Multipath)	A Data Path is defined as a logical or physical route between a specific UE/Radio Module and a user plane endpoint within a Transport Domain, to which a Data Flow is directed. The user plane endpoint can for example be a 5G UPF of an FRMCS Transport Domain or a 5G UPF/4G PGW of a non-FRMCS Transport Domain.
Dispatcher	Synonymous to Controller. Both terms can be used interchangeably within this document.
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.
Driver Safety Device	An on-train system that monitors the alertness of the driver and provides warnings and alarms to other systems as appropriate.
Dual Connectivity	According to 3GPP terminology [TS 37.340].

Terms	Definitions
Entity in Charge of Maintenance	According to [(EU) 2016/797].
FRMCS Application Identity	The FRMCS Application Identity is an identity presented by the application to the FRMCS Service 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 Infrastructure	Composite hardware, software, network resources and services required for the existence, operation, and management of an FRMCS Domain.
FRMCS Onboard System	According to [TOBA-FRS] terminology. Note1: 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.
On-Board FRMCS Radio Function Interchangeability	Maintenance capability that enables the on-board addition or replacement of On-Board FRMCS Radio Functions without impact on the On-Board FRMCS interfaces. On-Board FRMCS Radio Function interchangeability has a dependency with On-Board FRMCS Radio Function configuration(s).
FRMCS Radio Module Interchangeability	Maintenance capability that enables the on-board addition or replacement of Radio Modules without impact on the On-Board FRMCS interfaces. FRMCS Radio Module interchangeability has a dependency with On-Board FRMCS Radio Function configuration(s).
FRMCS Service Client	An MC Service client as defined in [TS 23.280].
FRMCS Service Domain	Implementation of (parts of) the Service Stratum which belongs to and/or is operated by a unique organisation.
FRMCS Service User	An MC Service User as defined in [TS 23.280].
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 Trackside Gateway	A trackside entity exposing TS_{APP} to provide communication services for trackside applications.
FRMCS Transport Domain	

Terms	Definitions
	Implementation of (part of) the Transport Stratum which belongs to and/or is operated by a unique organisation.
FRMCS Trust Domain	
	According to [TS 103 764] definition.
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.
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.
GSM-R on-board	
	The GSM-R communication system the Voice Application Subsystem interacts with on on-board side.
Home FRMCS Domain	
	The FRMCS Domain which is considered by default as the Home of the train.
Host	
	According to 3GPP terminology as Data Host [TS 23.282].
Identity	
	Represents a person or a subscription being permitted to use the FRMCS system. An Identity is used in order to access the FRMCS system.
Identifier	
	Within the FRMCS, identities are represented by identifiers in order to warrant the correct working (and interworking) of the system.
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.
Intercom system	
	Intercom system that may be used by drivers and train staff for voice communication on-board, specified in [UIC 568-3].
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.
IT-System	
	Any IT-system providing data to support the duties of the trackside users of the Voice Application Subsystem.

Terms	Definitions
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].
Notification Function	The function within On-Board FRMCS / FRMCS Trackside Gateway which provides OB_{APP}/TS_{APP} notification services to the applications. Note: Auxilliary function and Notification function terms can be used interchangeably.
OB_{APP} Control Plane	Flow of information between applications ($_{APP}$) 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.
On-Board FRMCS	According to [TOBA-FRS] terminology. Note: FRMCS Onboard System, FRMCS on-board and On-Board FRMCS terms can be used interchangeably.
On-Board FRMCS CRUD operations	CRUD operations related to information elements stored in the On-Board FRMCS
On-Board FRMCS Gateway Function	The On-Board FRMCS Gateway Function is responsible for the coordination and management of access to the FRMCS transport services offered by the FRMCS system.
On-Board FRMCS O&M Status Condition Parameters	Necessary set of parameters to determine the possibility of entering a specific maintenance status for the On-Board FRMCS
On-Board FRMCS Package	Set of updates, upgrades, or downgrades and/or changes to firmware and/or software and/or parameters for configuration
On-Board FRMCS Radio Function	The On-Board FRMCS Radio Function is a system block of the On-Board FRMCS that implements the FRMCS Radio Function as defined in [TOBA-FRS]. An On-Board FRMCS Radio Function can be realized by one or more component(s) as part(s) of an On-Board FRMCS.
On-Board FRMCS Radio Function configuration	On-Board FRMCS Radio Function configurations (e.g., attached or detachable) intended to achieve On-Board FRMCS Radio Function interchangeability. "Attached” implies permanent HW connectivity, “detachable” implies that a connected HW can be disconnected and re-attached on-board (without factory intervention).

Terms	Definitions
On-Board FRMCS Radio Module	An onboard 5G modem supporting radio access and core capabilities of 3GPP UE.
On-Board FRMCS O&M Status Condition Parameters	On-Board FRMCS O&M Status Condition Parameters (OBF OM-SCP) is a set of parameters and conditions that when observed in conjunction can assert to a true or false condition that is used to determine if an Operations and Maintenance procedure is allowed or not.
Operation and Maintenance (O&M) user	An O&M User is a human or machine authenticated and authorised to operate on On-Board FRMCS O&M Function as an entity in charge of maintenance and operation.
Operation and Maintenance (O&M) user group	An O&M User Group is a configurable group of O&M users sharing the same access rights. O&M users can belong to multiple groups.
Policy and Charging Control	According to 3GPP terminology [TS 23.503].
Public Address	Loudspeaker system on-board used for passenger announcements, specified in [UIC 568-3],
Railway Application Stratum	Railway-specific functionalities using services offered by the FRMCS Service Stratum.
Radio Access Technology	According to 3GPP terminology [TR 21.905].
Radio Module	According to [TOBA-FRS] “FRMCS Radio Module”.
Radio Module Adapter	A Radio Module Adapter is an interface adapter that as a system component manages connectivity and interfacing with one or more radio modules.
Reference Point	According to ITU-T terminology [ITU-T M.60].
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 section [10.1.6].
Service Stratum	Communication Services and Complementary Services.
Serving FRMCS Transport/Service Domain	The FRMCS Transport/Service Domain which is currently serving the interoperable IM applications. Note: In the Inter-FRMCS-Transport-Domain transition procedure, this is the FRMCS Transport Domain before the transition.
Serving On-Board FRMCS Radio Module	In Network Transition procedures, a Serving On-Board FRMCS Radio Module is an On-Board FRMCS Radio Module carrying

Terms	Definitions
	active communication services (e.g., providing PDU session) for ETCS and/or VAS in the Serving FRMCS Transport Domain.
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.
Target FRMCS Transport/Service Domain	The FRMCS Transport/Service Domain which is the target of Network Transition. At the completion of Network Transition, the Target FRMCS Domain becomes the Serving FRMCS Domain.
Target On-Board FRMCS Radio Module	In Network Transition procedures, a Target On-Board FRMCS Radio Module is the On-Board FRMCS Radio Module which is intended to carry active communication services (e.g., providing PDU session) for ETCS and/or VAS in the Target FRMCS Transport Domain.
Trackside FRMCS	System supporting FRMCS communication to trackside applications. Trackside FRMCS is a sub-domain within the FRMCS System. Note: FRMCS trackside and Trackside FRMCS terms can be used interchangeably.
Train Interface	Interface to retrieve data from other sub-systems on-board of a train, as specified in [SUBSET-119].
Transport Stratum	Set of access functions and corresponding core functions applicable for the FRMCS system.
Update	Any major modification during service work on a subsystem or part of it which does not change the overall functional performance of the subsystem
Upgrade	Any major modification during service work on a subsystem or part of it which results in a change which improves partial or overall functional performance of the subsystem
User Equipment	According to 3GPP terminology [TR 21.905]. In this context, the Mobile Termination (MT) corresponds to the On-Board FRMCS Radio Module that enables radio capabilities within the FRMCS Transport Stratum.
User Plane	

Terms	Definitions
	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, CCS TSI Annex A applies.

3.2 List of References

[FRMCS-FRS]	UIC FU-7120: “FRMCS Functional Requirements Specification”.
[TOBA-FRS]	UIC TOBA-7510: “FRMCS Telecom On-Board System – Functional Requirements Specification”.
[FRMCS-FIS]	UIC FRMCS “Functional Interface Specification”.
[FRMCS-FFFIS]	UIC FRMCS FFFIS “Form Fit Functional Interface Specification”.
[O-8856]	UIC UGFA “Whitepaper on migration scenarios”
[O-8868]	UIC UGFA Report: “Technical aspects FRMCS RAN”.
	Intentionally deleted.
[UIC 612-04]	UIC DISPLAY SYSTEM IN DRIVER'S CABS (DDS) TRAIN RADIO DISPLAY (TRD).
[UIC 568-3]	UIC Loudspeaker and telephone systems in RIC coaches – Standard technical characteristics
[UIC 641]	UIC Conditions to be fulfilled by automatic vigilance devices used in international traffic.
[TR 21.905]	3GPP TR 21.905: “Vocabulary for 3GPP Specifications”.
[TS 22.179]	3GPP TS 22.179: “Mission Critical Push to Talk (MCPTT); 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”.
[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 23.282]	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 24.229]	3GPP TS 24.229: “IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3”.
[TS 24.482]	3GPP TS 24.482: “Mission Critical Services (MCS) identity management; Protocol specification”.
[TS 24.484]	3GPP TS 24.484: “Mission Critical Services (MCS) configuration management; Protocol specification”.
[TS 24.501]	3GPP TS 24.501: “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3”.
[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 38.331]	3GPP TS 38.331: “NR; Radio Resource Control (RRC); Protocol specification”.
[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 103 765-3]	ETSI TS 103 765-3: “Future Rail Mobile Communication System (FRMCS); Building Blocks and Functions; Part 3: Train On-Board functions and interfaces FRMCS On-Board”.
[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)”.
[EU 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”.
	Intentionally deleted.
[i.8]	ENISA, Security in 5G Specifications, Controls in 3GPP Security Specifications (5G SA).
[ISO 8601]	ISO 8601:2019: "Date and time - Representations for information interchange”.
[ITU-T E.212]	ITU-T Recommandation E.212: “International Mobile, shared codes”.
[ITU-T M.60]	ITU-T Recommendation M.60: “Maintenance terminology and definitions”.
[ITU-T X.509]	ITU-T Recommendation X.509: “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”.
[ITU-R TF.460-6]	ITU-R Recommendation TF.460-6: “Standard-frequency and time-signal emissions”.
[ITU-R TF.535-2]	ITU-R Recommendation TF.535-2: “Use of the term UTC”.
[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.).
[EIRENE-FRS]	EIRENE Functional Requirements Specification, Version 8.1.0
[EIRENE-SRS]	EIRENE System Requirements Specification v16.0.0, 21 December 2015.
[SUBSET-026]	UNISIG SUBSET-026: “ERTMS/ETCS System Requirements Specification”.
[SUBSET-037-3]	UNISIG SUBSET-037-3: “ERTMS/ETCS: EuroRadio FIS – FRMCS Communication Functional Module”.
[SUBSET-093]	UNISIG SUBSET-093: "GSM-R Bearer Service Requirements”.
[SUBSET-119]	ERTMS/ETCS, Train Interface FFFIS, Version 4.0.0
[SUBSET-126]	UNISIG SUBSET-0126: “ATO over ERTMS ATO-OB / ATO-TS Interface Specification”.
[SUBSET-147]	ERTMS Data Applications, FFFIS part: CCS Consist Network Communications Layers, Version 1.0.0
[SUBSET-148]	UNISIG SUBSET-148: “ATO-OB / ATO-TS Interface Specification Transport and Security Layers”.
[RFC-791]	IETF RFC 791 September 1981: “Internet Protocol – DARPA Internet Program Protocol Specification”.
[RFC-3261]	IETF RFC 3261 June 2022: “SIP: Session Initiation Protocol”.
[RFC-3966]	IETF RFC 3966 December 2004: “The tel URI for Telephone Numbers”.
[RFC-7542]	IETF RFC 7542 May 2015: “The Network Access Identifier”.
[RFC-8200]	IETF RFC 8200 July 2017: “Internet Protocol, Version 6 (IPv6) Specification”.
[CCS TSI]	COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919.

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 **Intentionally deleted**.

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

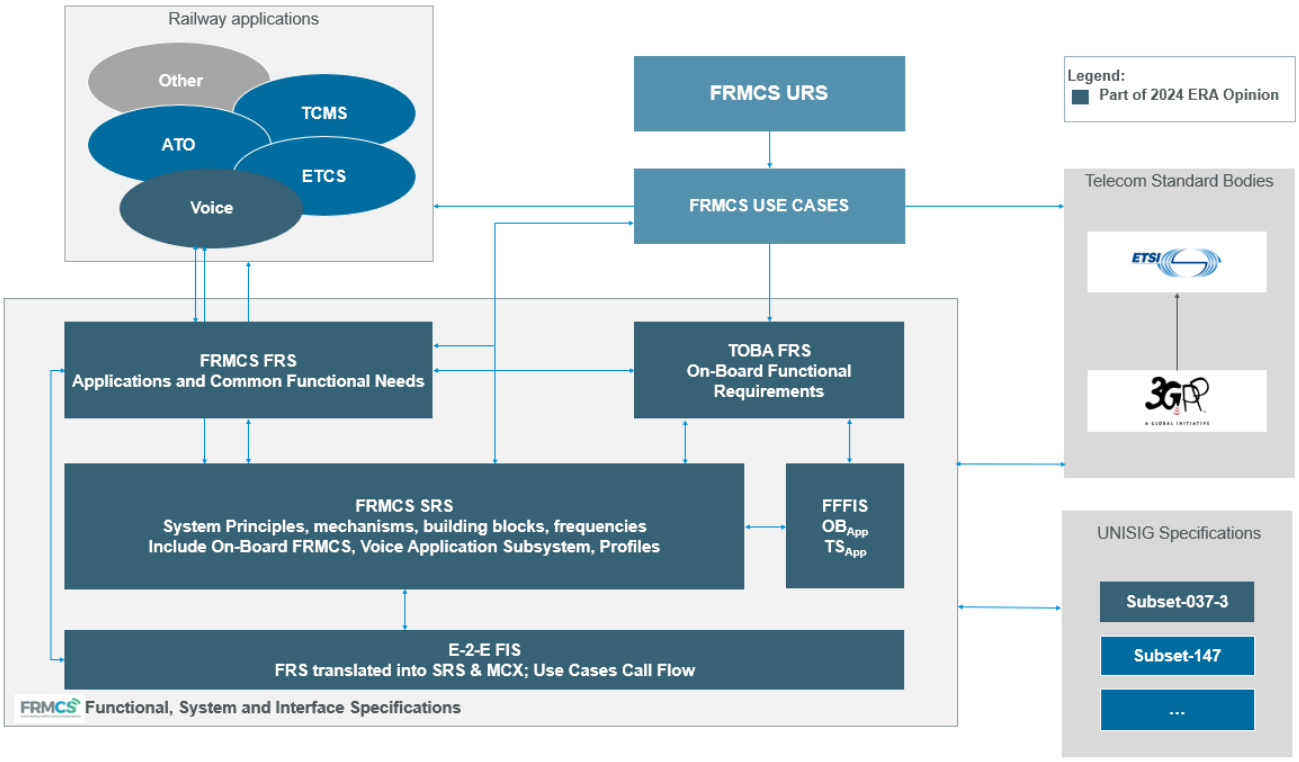


Figure 4-1: FRMCS specifications

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) enables Interoperability of rail communications within various administrative domains across geographical domains (e.g., Countries).

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

4.2.4 **Intentionally deleted**.

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 [8.4].

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 optional requirement 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 needed to be provided.

4.4.2 The following marking is applied to denote the applicability of clauses: (I)

1. Indications (M), (O) and (I) are used for clauses within the scope of the V2 specification, which is the minimum set of requirements for validation;

2. Indications (M-V3), (O-V3) and (I-V3) are used for clauses within the scope of the V3 specification. The V3 series of specification are the target version to be included in the TSI, to allow migration from the GSM-R system to the FRMCS system (FRMCS 1st edition). The V3 clauses are to be considered for information for V2;

3. Indications (M-Vx), (O-Vx) and (I-Vx) are used for clauses for a later version of the specification. These clauses are kept in the specification for readability and consistency purposes.

4. Indications (M-V3), (O-V3), (I-V3) and (M-Vx), (O-Vx), (I-Vx) may also be used for sub bullets within a clause to identify a different applicability. In this case each bullet will be indicated individually.

4.4.3 From chapter 5 onwards the category indication is included.

Editor's Note: ETSI FRMCS Technical Specifications [TS 103 764], [TS 103 765-1], [TS 103 765-2], [TS 103 765-3], [TS 103 765-4] and [TS 103 792] are to be completed in parallel to EECT process.

Editor's Note: numbers and values of all requirements from chapter 5 onwards and Annexes will be examined for at FRMCS field trials and tests. If necessary, requirements will be refined.

4.5 Document Life Cycle

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

Editor's Note: The versioning and life cycle management process of this document is out of scope for FRMCS V2.

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 shall also provide communication services applicable for operational purposes covering the following types of railways: (M-Vx)

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

5.1.3 To enable the functional requirements of [FRMCS-FRS] and [TOBA-FRS], the FRMCS System Specification defines the necessary technical building blocks and corresponding functionalities. (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)

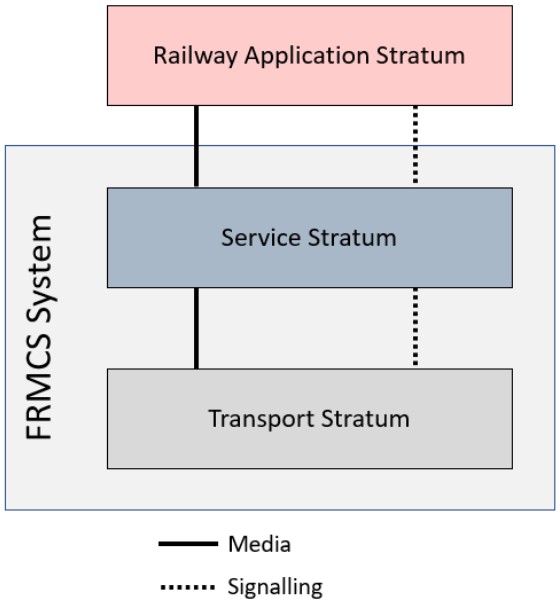


Figure 5-1 Railway Application, Service and Transport Strata

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 for 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 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 for 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., Controllers, 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 out of scope for FRMCS V2.

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)

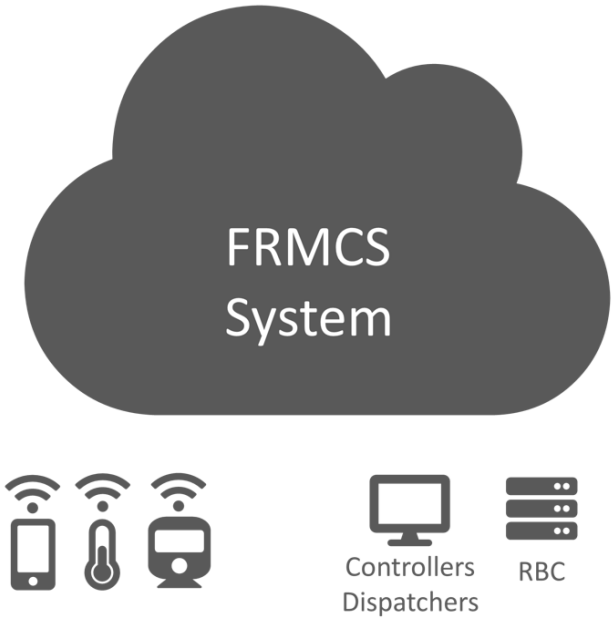


Figure 6-1 - FRMCS System and a subset of entities using communication services of the FRMCS System

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 On-Board FRMCS, 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)

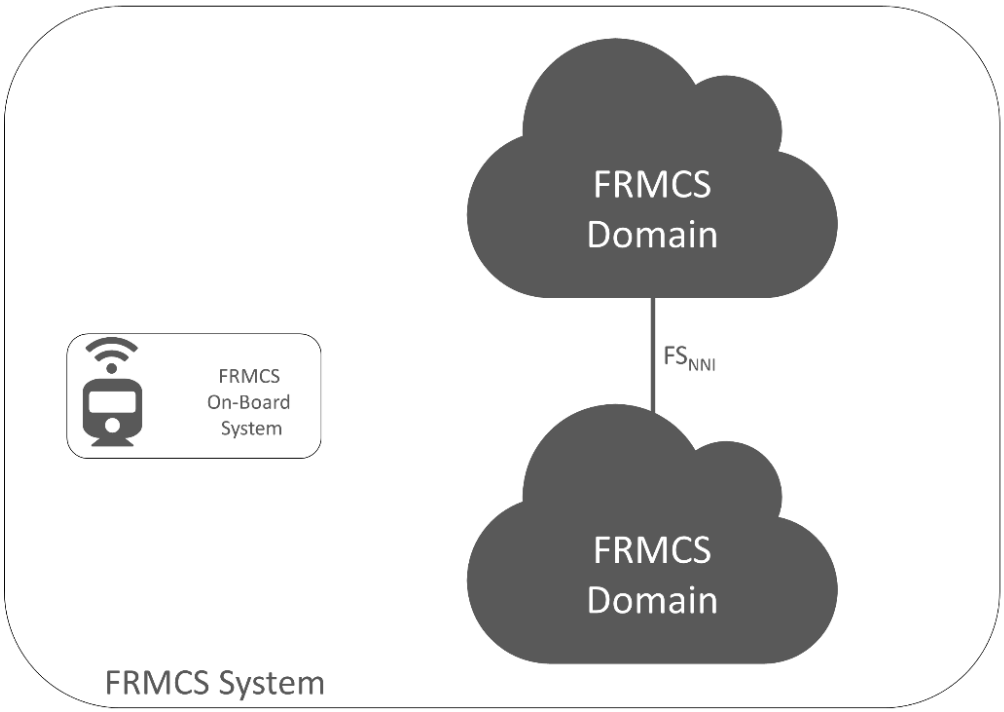


Figure 6-2 - FRMCS System and FRMCS Domains

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)

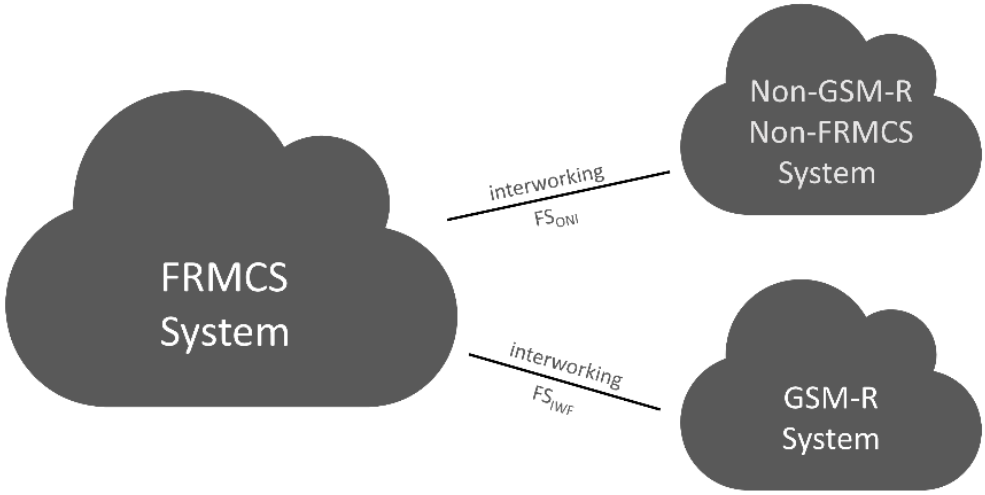


Figure 6-3 - Relation between the FRMCS System and external systems

6.1.1.5 In order to interconnect two FRMCS Domains, the FRMCS System shall support this interconnection using FS_{NNI} reference point (see 6.4.4.2). (M)

6.1.1.6 In order to interwork with GSM-R, the FRMCS System shall support this interworking using 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 using FS_{ONI} reference point (see 6.4.4.3). (O-V3)

6.1.1.8 FRMCS communication services relies: (I)

a. 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,
b. 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)

a. In the Transport Domain:
    a. A 5G Core Network,
    b. A 5G Access Network supporting the possible spectrum options as defined in section [8],
b. In the Service Domain:
    a. 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)

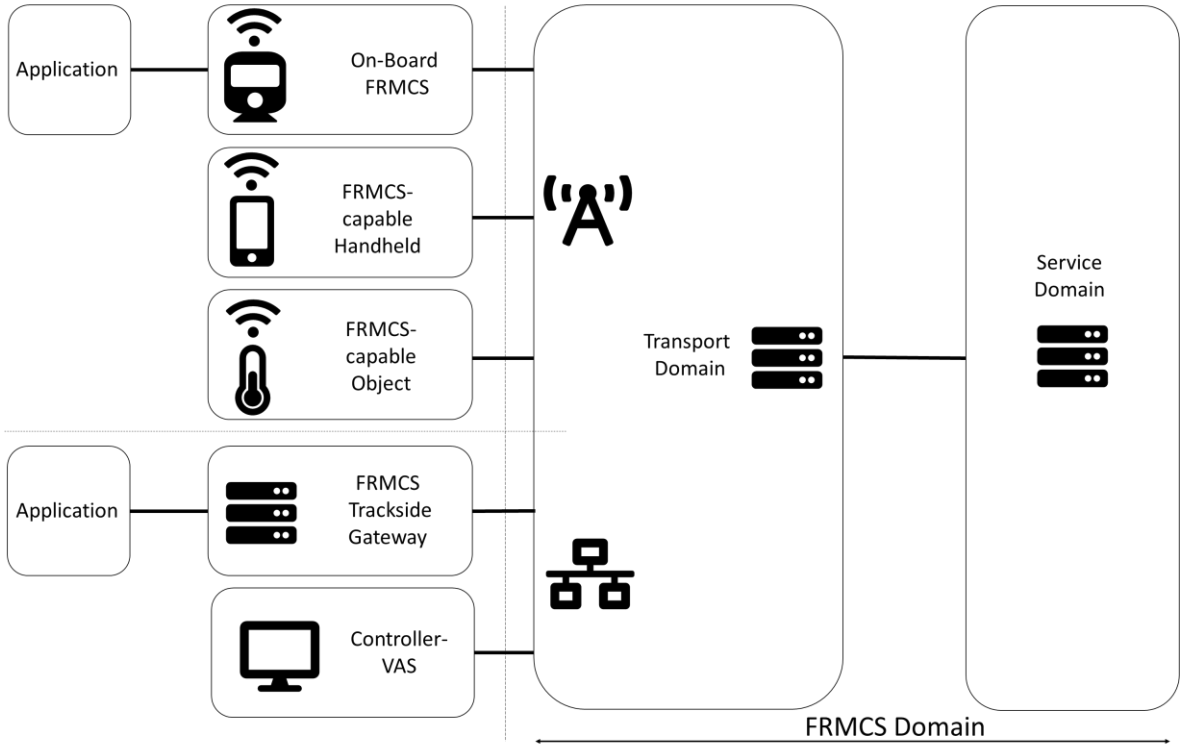


Figure 6-4 - high-level architecture diagram of communicating entities within the FRMCS system

Editor's Note: definitions and requirements of FRMCS-capable Handhelds and FRMCS-capable Objects are not in scope of FRMCS V2.

6.1.2.2 The On-Board FRMCS (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 complementary 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 not applicable to FRMCS capable handhelds and FRMCS-capable Objects.

6.1.3.1 General case

6.1.3.1.1 On-Board Applications using the FRMCS System shall use the OB_{APP}. (M)

6.1.3.1.2 Controller VAS shall use either TS_{CTRL} reference point or TS_{APP} reference point according to the requirements detailed in section [24.3.3]. (M)

6.1.3.1.3 Trackside applications other than controller VAS shall use TS_{APP}. (M)

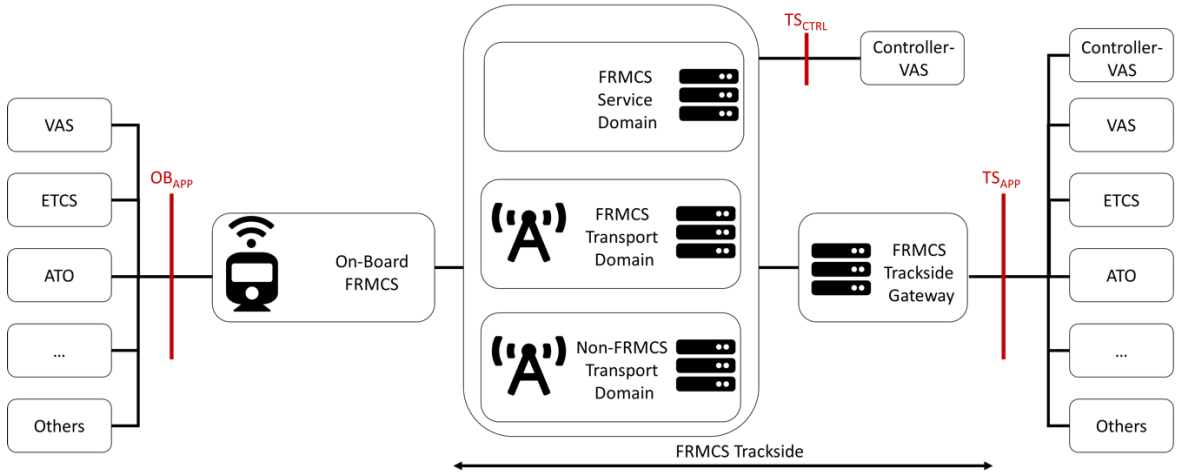


Figure 6-5 - FRMCS reference points used by application to access the FRMCS System

6.1.3.1.4 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 Client in application?	FRMCS Service Client in On-Board FRMCS / in FRMCS Trackside Gateway?
Tight	Tight	Yes	No
Loose	Loose	No	Yes
Superloose	Loose (via agent)	No	Yes

Table 6-1 Application regimes (I)

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

Editor's Note: Connecting hosts via plain IP with TS GW is for FFS.

6.1.3.1.5 The “Coupling Mode” reflects whether an application environment encompasses a FRMCS Service 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.

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

6.1.3.2 Applications leveraging a GSM-R / FRMCS 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, as defined in section [24.1.3.4]. (I)

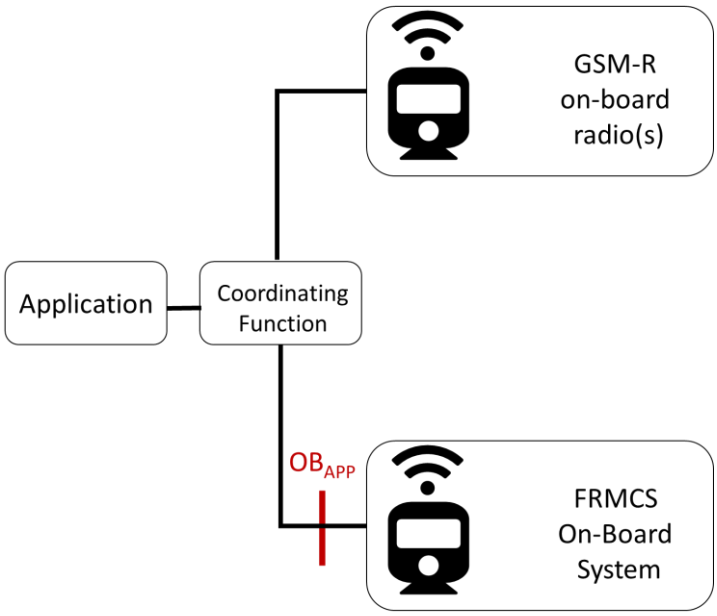


Figure 6-6 - the Coordinating Function in relation to the FRMCS System

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. (I)

6.1.3.3 Superloose Application Regime

6.1.3.3.1 Scope

6.1.3.3.1.1 Superloose application regime is defined as the application being OB_{APP}/TS_{APP}-unaware and interacting through an agent implementing OB_{APP}/TS_{APP} on behalf of the application as shown in figure 6-7. (I)

6.1.3.3.2 General principles, architecture, and system requirements

6.1.3.3.2.1 The agent for applications in Superloose application regime use OB_{APP} or TS_{APP} (I).

6.1.3.3.2.2 The agent for Superloose application regime supports loose coupling per application (I).

6.1.3.3.2.3 The agent for Superloose application regime supports an O&M interface to update credentials (e.g., for required certificates for local binding via OB_{APP}/TS_{APP}). (I)

Note 1: The interface between the agent and the application is left for implementation.

Note 2: One or many applications may use the same agent.

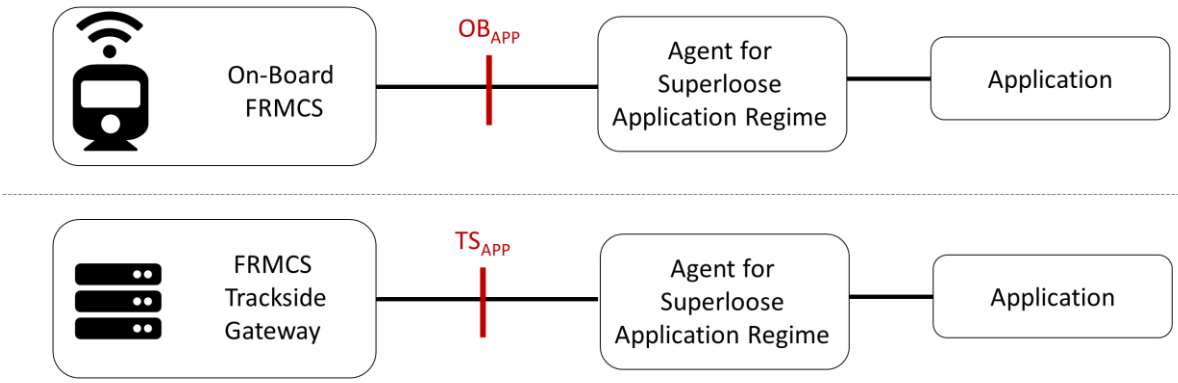


Figure 6-7 Superloose coupling mode

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

6.1.4.2.1 The application stratum encompasses applications using FRMCS communication services. (I)

6.1.4.2.2 Interconnection between application and service stratum is defined in section 6.4.1. (I)

6.1.4.3 Service Stratum

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

6.1.4.4 Transport Stratum

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

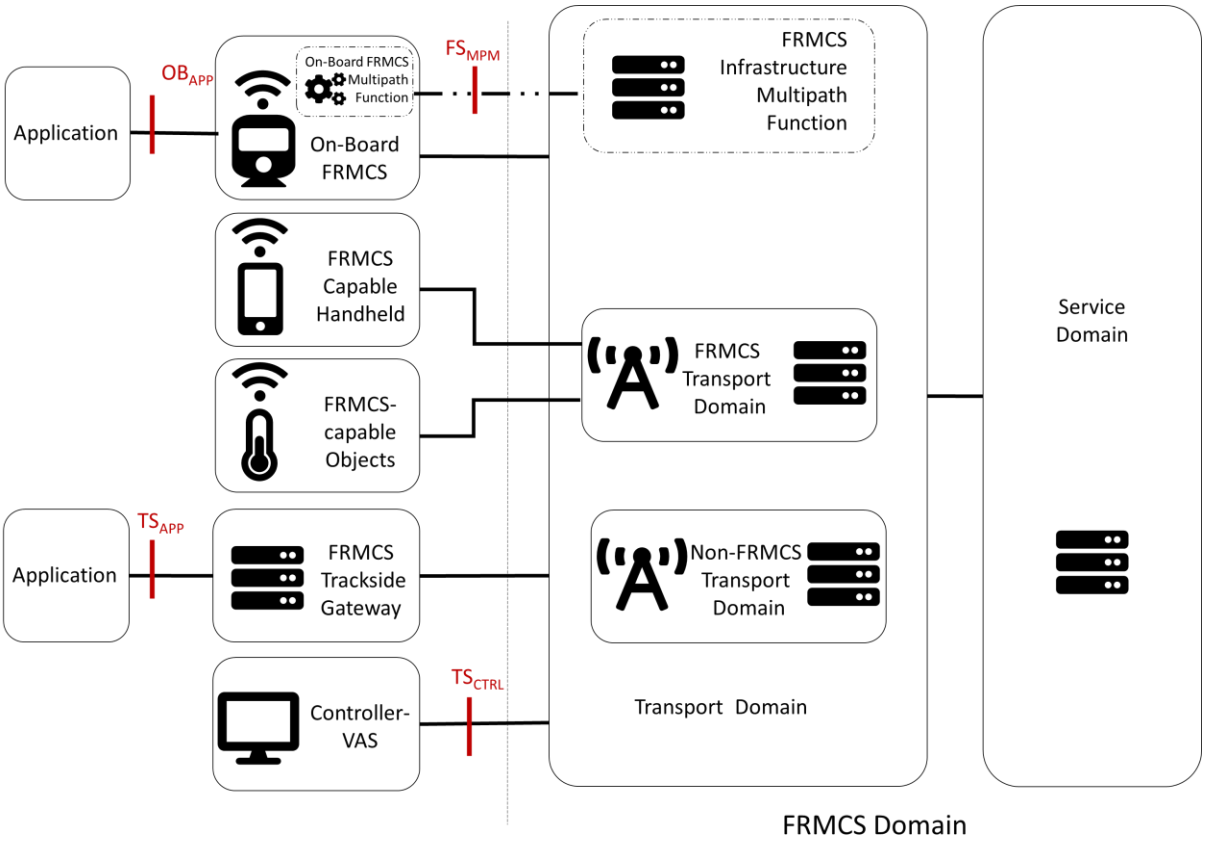


Figure 6-8 - System Reference Architecture

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), TS_{CTRL} (see 6.4.1.3), FS_{OMR} (see 6.4.3.1) and FS_{MPM} (see 6.4.2.1) are defined in subsequent sections. (I)

6.2.2 Inter-FRMCS Domain

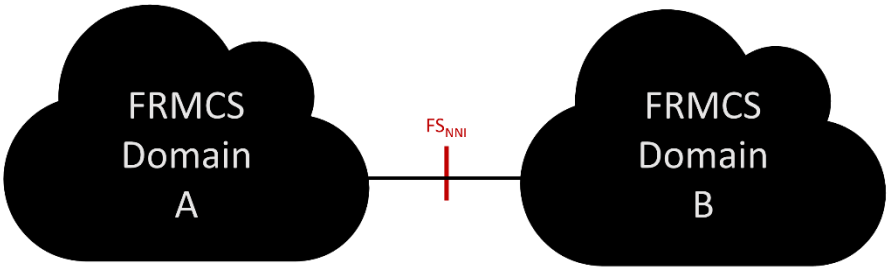


Figure 6-9 - FRMCS System: reference point between FRMCS Domains

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

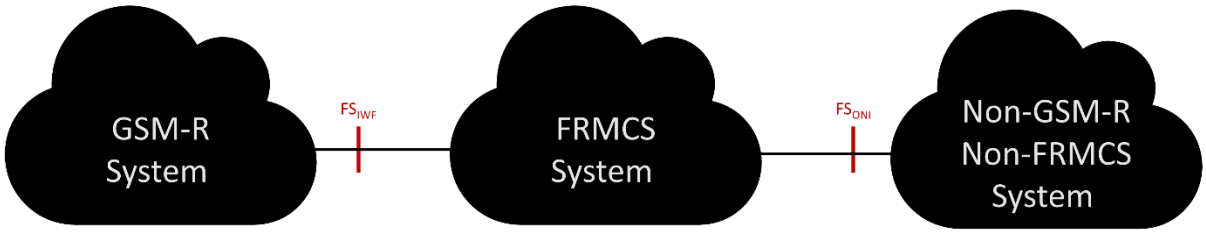


Figure 6-10 - FRMCS System: reference points towards external systems

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 out of scope for FRMCS V2.

6.3.2 On-Board FRMCS

6.3.2.1 The On-Board FRMCS 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 On-Board FRMCS include:

- Providing communication services to and from authorized onboard applications. (I)
- Providing complementary services to applications, e.g.
  - Status of the communication service
  - Positioning information
- 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 On-Board FRMCS 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 Function within the On-Board FRMCS. (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 On-Board FRMCS. (I)

6.3.4.3 The FRMCS Infrastructure Multipath Function is specified in section [12]. (I)

6.3.4.4 The concept of FRMCS Multipath is further specified 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 its own or to other interconnected Service Domains if they have been granted such right. (M)

6.3.5.2 A Service Domain shall enable communication between authorised users of its own and/or other interconnected 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) as defined in [TS 103 765-2]. (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 Intentionally deleted.

6.3.6.4 A FRMCS Transport Domain shall include a 5G Core Network and one or more Access Networks under the control of the 5G Core Network. (M-V3)

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 On-Board FRMCS and provides the means for onboard applications to make use of the communication services offered by the On-Board FRMCS. (I)

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

- Status of the communication service
- Positioning information

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 On-Board FRMCS. (I)

6.4.1.1.4 The OB_{APP} reference point shall conform to [FRMCS-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-Vx)

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-V3)

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-V3)

6.4.1.1.11 The interface defined over OB_{APP} reference point shall be accessible via the API defined in [FRMCS-FFFIS]. (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 [FRMCS-FFFIS]. (M)

6.4.1.2.4 The TS_{APP} reference point shall enable data flow between trackside applications and Trackside FRMCS. (M)

6.4.1.2.5 The interface defined over TS_{APP} reference point shall have the capability to enable confidentiality of data flow(s). (M-V3)

6.4.1.2.6 The interface defined over TS_{APP} reference point shall have the capability to enable integrity of data flow(s). (M-V3)

6.4.1.3 TS_{CTRL}

6.4.1.3.1 The TS_{CTRL} reference point provides the means for controller VAS entity to make use of FRMCS communication services provided by the FRMCS Infrastructure. (I)

6.4.1.3.2 Controller VAS interconnection via TS_{CTRL} supports cyber security measures for access to FRMCS Infrastructure. (I)

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 On-Board FRMCS 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 OBF RMs between the On-Board FRMCS 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}

6.4.3.1.1 The FS_{OMR} reference point is the system-level equivalent of the OB_{OM} reference point defined within the On-Board FRMCS. (I)

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

6.4.3.1.3 The interface over FS_{OMR} reference point shall be used for remote configuration of On-Board FRMCS. (M-V3)

6.4.3.1.4 The interface over FS_{OMR} reference point shall rely on 3GPP Mission-Critical framework. (M-V3)

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)

6.4.4.2.5 The FS_{NNI} requirements are listed in section [10.3]. (I)

6.4.4.3 FS_{ONI}

6.4.4.3.1 The FS_{ONI} reference point is defined between a FRMCS System and another system that is neither GSM-R nor FRMCS. (I)

6.4.4.3.2 The FS_{ONI} reference point should conform to [TS 103 765-1] for functionalities applicable to FRMCS Transport Domain. (O-V3)

6.4.4.3.3 The FS_{ONI} reference point should conform to [TS 103 765-2] for functionalities applicable to FRMCS Service Domain. (O-V3)

6.4.5 FRMCS Location and positioning reference points

6.4.5.1 OB_{LOC}

6.4.5.1.1 The OB_{LOC} reference point should be exposed by the onboard external source and provides the means for On-Board FRMCS to obtain Train Location Information. (O-V3)

6.4.5.2 TS_{LOC}

6.4.5.2.1 The TS_{LOC} reference point should be exposed by the trackside external source and provides the means for the FRMCS system to obtain Train Location Information. (O-V3)

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 (OB_{om}, OB_{app}, OB_{ant}, FS_{omr}, TS_{app}, TS_{ctrl} and FS_{oni}). (M)

6.5.1.3 The FRMCS System should support the IP version 4 [RFC-791] protocol suite as its key technology at external reference points (OB_{om}, OB_{app}, OB_{ant}, FS_{omr}, TS_{app}, TS_{ctrl} and FS_{oni}). (O)

6.5.2 Addressing principles

6.5.2.1 **Intentionally deleted**.

6.5.2.2 **Intentionally deleted.**

6.5.2.3 Host-to-Host (H2H) addressing scheme

6.5.2.3.1 The Host-to-Host (H2H) addressing scheme provides a transparent IP connection between two Hosts, as depicted in Figure 6-11. (I)

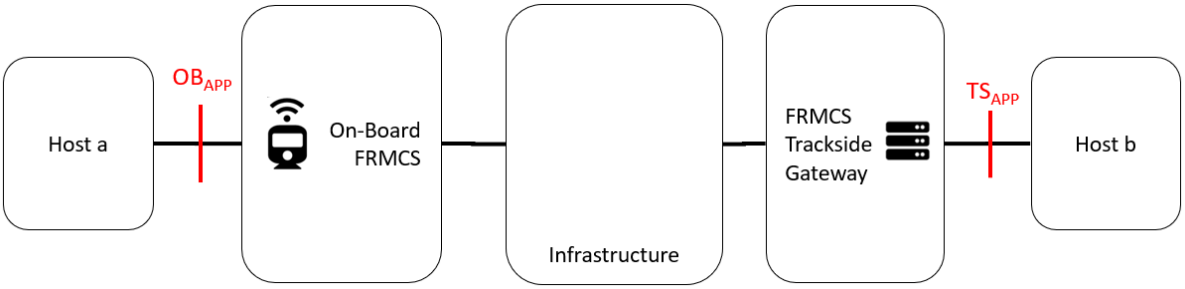


Figure 6-11: Host-to-Host (H2H) addressing principle (Loose-coupled example)

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

Editor's note: H2H for tight coupled application regime is out of scope for FRMCS V2.

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

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

6.5.2.3.5 **Intentionally Deleted**

6.5.2.3.6 The Host shall be authorized to use FRMCS services. (M)

6.5.2.3.7 The procedures for transparent IP connection in H2H approach for Loose-coupled applications shall comply to [TS 103 765-2] clause 6.2.3. (M)

Editor's note: IP layer model and IP address ranges are under investigation.

6.5.2.4 Host-to-Network (H2N) addressing scheme

6.5.2.4.1 The Host-to-Network (H2N) addressing scheme provides a transparent IP connection between a single Host and a Data Network, as depicted in Figure 6-12. (I)

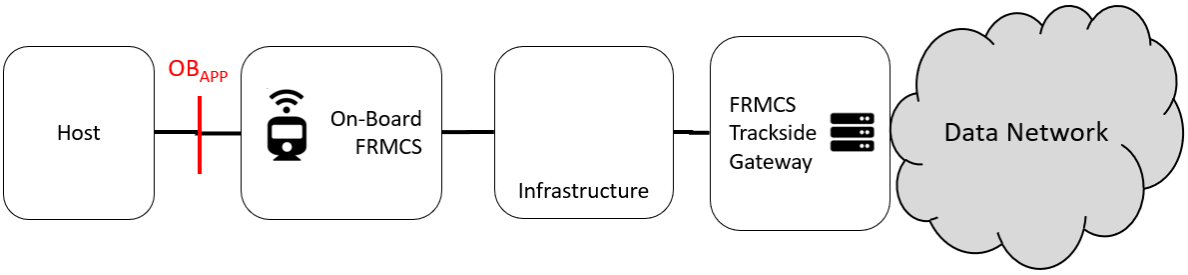


Figure 6-12: Host-to-Network (H2N) addressing principle

6.5.2.4.2 The FRMCS System shall support H2N approach for Loose-coupled and Super-loose-Coupled Applications. (M)

Editor's Note: H2N for tight coupled application regime is out of scope for FRMCS V2.

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

6.5.2.4.4 The FRMCS Trackside Gateway shall prevent Data Network hosts accessed via H2N approach to originate a session towards the remote Host. (M)

6.5.2.4.5 The procedures for transparent IP connection in H2N approach for Loose-coupled applications shall comply to [TS 103 765-2] clause 6.2.3. (M)

Editor's note: IP layer model and IP address ranges are under investigation.

7 Description of Subsystems and Constituents

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)

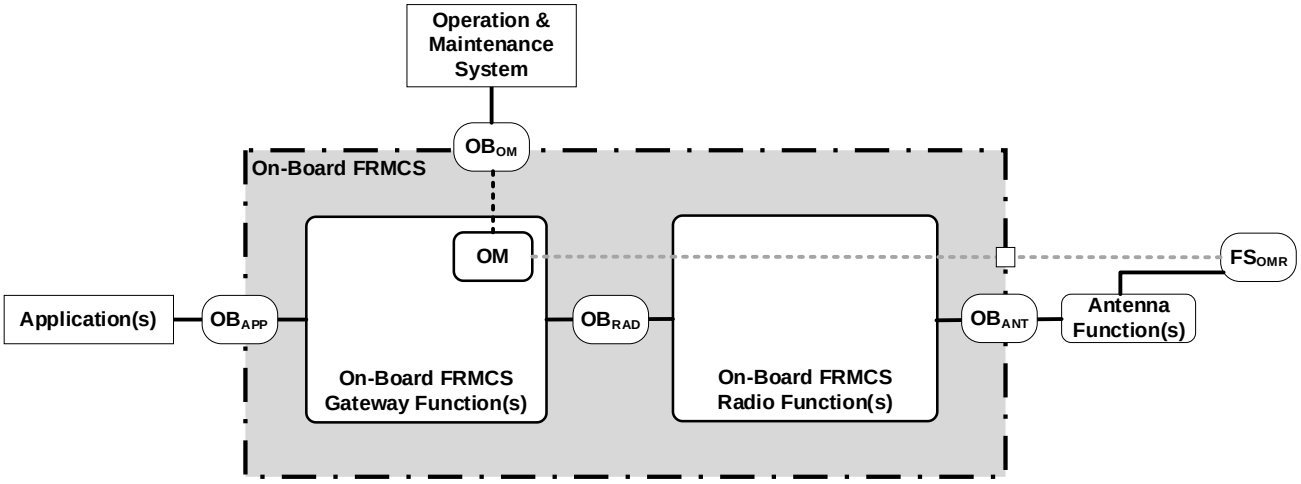


Figure 7-1: On-Board FRMCS architecture

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 [FRMCS-FFFIS].

7.1.1.2.1i The reference point between On-Board FRMCS and onboard applications is OB_{APP}. (I)

7.1.1.2.2 OB_{ant} is the reference point between On-Board FRMCS Radio Modules (as part of On-Board FRMCS Radio Function(s)) and Trackside FRMCS. (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. (I)

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 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 is 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

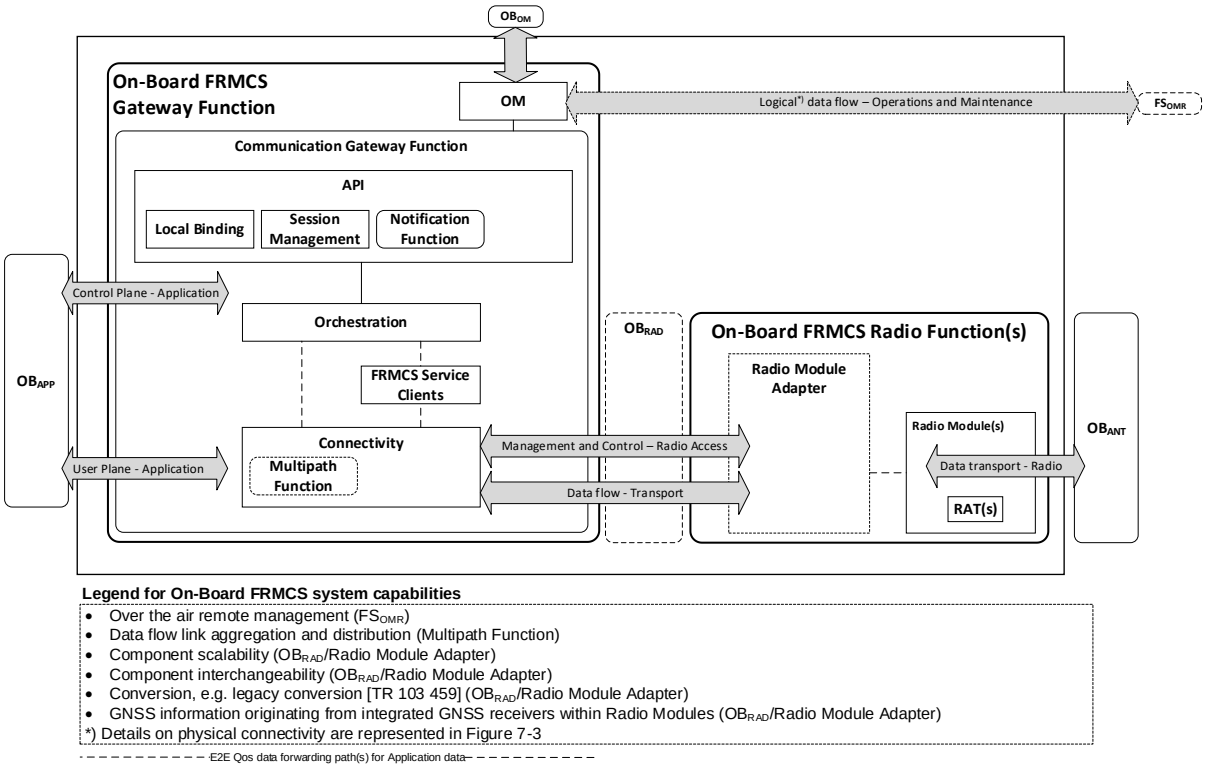


Figure 7-2: On-Board FRMCS architecture

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 v2. (I)

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

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

7.1.3.2 Architecture scope

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

- On-Board FRMCS Gateway Function ([7.1.4.2], [7.1.5])
- On-Board FRMCS Radio Function ([7.1.4.2], [7.1.5.10.2.4], [7.1.6])

7.1.3.2.2 The On-Board FRMCS Gateway Function includes the following functions (I):

- Communication Gateway Function ([7.1.5.3])
- OM ([7.1.5.11])

7.1.4 Interfaces

7.1.4.1 External Interfaces

7.1.4.1.1 OB_{APP}

7.1.4.1.1.1 The OB_{APP} interface is developed more in detail in section [6.4.1.1] of this document and in [FRMCS-FFFIS]. (I)

7.1.4.1.1.2 Physical Interface between On-Board FRMCS and the applications (OB_{APP})

7.1.4.1.1.2.1 Rationale

The on-board applications need to have connectivity in order to utilize the On-Board FRMCS. This connectivity can be of different type(s) depending on the user equipment where on-board application(s) are installed. e.g. handheld device(s) for user(s) moving within or in close proximity to a train, fixed equipment within a train or mounted on the train. (I)

7.1.4.1.1.2.2 Requirements

7.1.4.1.1.2.2.1 The On-Board FRMCS shall provide wired connectivity for devices using off the shelf technologies (e.g., Ethernet). (M)

7.1.4.1.1.2.2.2 Intentionally deleted.

7.1.4.1.1.2.2.3 The number of physical interfaces for OB_{APP} connectivity should be expandable. (O)

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)

7.1.4.1.2.1.2 OB_{ANT} implements connection of GNSS receiver and GNSS antenna. (I)

7.1.4.1.2.2 Interface Requirements

7.1.4.1.2.2.1 For each On-Board FRMCS Radio Module, the On-Board FRMCS shall provide OB_{ANT} 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 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)

7.1.4.1.2.3 Physical Interface between FRMCS Radio Modules and the antenna system (OB_{ANT})

7.1.4.1.2.3.1 Rationale

7.1.4.1.2.3.1.1 An industry-specified interface between the FRMCS Radio Modules and the antenna system, facilitates a modular implementation of the FRMCS On-Board System and increases the degrees of freedom for the fleet managers during the life cycle of the FRMCS On-Board System. (I)

7.1.4.1.2.3.2 Requirements

7.1.4.1.2.3.2.1 The OB_{ANT} physical interface shall be realised using a suitable existing industry specification. (M)

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)

7.1.4.1.3.2 Interface Requirements

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

Note: OM and associated interfaces (OB_{OM} and FS_{OMR}) are left for implementation in V3.

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

7.1.4.1.3.3 Physical Interface between local management system(s) and O&M Function of the On-Board FRMCS (OB_{OM})

7.1.4.1.3.3.1 Rationale

7.1.4.1.3.3.1.1 An industry specified physical interface between the O&M Function of the On-Board FRMCS and local management system(s) will enable and promote flexible implementation and business models in terms of fleet management with respect to the management of On-Board FRMCS. (I)

7.1.4.1.3.3.2 Requirements

7.1.4.1.3.3.2.1 The On-Board FRMCS shall provide connectivity for local O&M access using off the shelf technologies e.g. Ethernet. (M)

7.1.4.1.4 FS_{OMR}

7.1.4.1.4.1 Description

7.1.4.1.4.1.1 Interface FS_{OMR} is implemented over the FS_{OMR} reference point as defined in section [6.4.3.1] of this document. (I)

Note: The FS_{OMR} reference point is not a reference point belonging to the On-Board FRMCS scope, nevertheless the use of FS_{OMR} interface has dependencies to the On-Board FRMCS operations and maintenance.

7.1.4.1.4.1.2 Interface FS_{OMR} enables over the air gap communication between Operation and Maintenance System and On-Board FRMCS. (I)

7.1.4.1.4.2 Interface Requirements

7.1.4.1.4.2.1 The FRMCS System shall expose external interfaces at the FS_{OMR} reference point. (M-V3)

7.1.4.1.4.2.2 The On-Board FRMCS shall enable Operations and Maintenance using the FS_{OMR} interface enabled by the FRMCS System by using over the air communication. (M-V3)

7.1.4.2 Internal Interface between On-Board FRMCS Gateway Function and On-Board FRMCS 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 On-Board FRMCS Gateway Function and On-Board FRMCS 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 On-Board FRMCS 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 On-Board FRMCS Gateway Function and On-Board FRMCS Radio Function(s). (M-V3)

7.1.4.2.1.2.2 OB_{RAD} shall enable User Plane (Media) communication between On-Board FRMCS Gateway Function and On-Board FRMCS Radio Function(s). (M-V3)

7.1.4.2.1.2.3 The OB_{RAD} Control Plane shall enable relocation of established communication session(s) between On-Board FRMCS Radio Functions. (M-V3)

7.1.4.2.1.2.4 OB_{RAD} Control Plane shall enable the selection and usage of On-Board FRMCS Radio Function(s). (M-V3)

7.1.4.2.1.2.5 OB_{RAD} Control Plane will enable the selection and usage of the Radio Module(s) hosted by On-Board FRMCS Radio Function(s). (I)

7.1.4.2.1.2.6 OB_{RAD} supports in-service replacement of On-Board FRMCS 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: OB_{RAD} control plane is unrelated to OB_{APP} control plane.

Note: OB_{RAD} interface specification may use [TR 104 006] as initial input.

7.1.4.2.1.3 Physical Interface between On-Board FRMCS and the FRMCS Radio Function(s) or Radio Module(s) (OB_{RAD} physical interface)

7.1.4.2.1.3.1 Requirements

7.1.4.2.1.3.1.1 The OB_{RAD} physical interface shall support distributed deployments of FRMCS Radio Functions within a train realizing the On-Board FRMCS detachable configuration as defined in [TOBA-FRS]. (M-V3)

7.1.4.2.1.3.1.2 The OB_{RAD} physical interface shall enable sufficient performance (bandwidth, latency) to carry both the user plane traffic and the required control plane traffic without degrading the QoS of the Communication Services, as it is defined in section [14] of this document. (M)

7.1.4.2.1.3.1.3 The OB_{RAD} physical interface shall be realised using a suitable industry standard fulfilling the functional requirements stated under section [7.11] of [TOBA-FRS]. (M)

7.1.4.2.1.3.1.4 The OB_{RAD} reference point shall be able to use an existing network (e.g., CCS Consist Network as defined in [SUBSET-147]) that can provide required security and performance stated in sections [14] and [15] of this document with respect to bandwidth integrity and confidentiality. (M)

7.1.5 On-Board FRMCS Gateway Function

7.1.5.1 Introduction

7.1.5.2 An On-Board FRMCS Gateway Function encompasses Functions that enable the specification of (I):

- On-Board FRMCS system requirements related to communication service(s) enabled by FRMCS ([7.1.5.4], [7.1.5.5],[7.1.5.6], [7.1.5.7], [7.1.5.8], [7.1.5.9], [7.1.5.10]).
- System requirements related to the operation and maintenance of the On-Board FRMCS ([7.1.5.11.2.2]).

7.1.5.3 Communication Gateway Function

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

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

- API ([7.1.5.4])
- Orchestration ([7.1.5.8])
- FRMCS Service Client(s) ([7.1.5.9])
- Connectivity ([7.1.5.10])

7.1.5.4 API

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

a. Local Binding
b. Session Management
c. Notification Function

7.1.5.4.2 The API is specified by [FRMCS-FFFIS]. (I)

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:

a. Identification (M)
b. Authentication (M)
c. Integrity (M)
d. Confidentiality (M)

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

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

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

a. Identification (M)
b. Authentication (M)

Note: This is in order to be able to identify each data flow as an FRMCS Service Session and to prevent any unauthorized establishment of FRMCS Service Sessions.

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

a. Integrity (O)
b. Confidentiality (O)

Note: This is in order to provide means of data protection for Applications that have no such capability but have the need to achieve a certain level of protection.

7.1.5.5.2.6 With respect to Identification of Application instances Local Binding shall support an application registration process to the On-Board FRMCS [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-V3)

Note: Technical details of Local Binding are further specified in the [FRMCS-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, maintains 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 concurrently between any 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 Intentionally deleted.

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)

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

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 Notification Function

7.1.5.7.1 Introduction

7.1.5.7.1.1 The Notification Function is a function of the API as specified in [FRMCS-FFFIS] chapter §9.11. (I)

7.1.5.7.1.2 The Notification Function manages notifications towards the On-board applications [FRMCS-FFFIS] (I).

7.1.5.7.2 Requirements

7.1.5.7.2.1 The Notification 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 Notification Function shall provide read-only information. (M)

7.1.5.7.3 Service capabilities

7.1.5.7.3.1 The Notification Function shall have the capability to send notification information elements (NOTIF-IE) to locally bound Applications using the notification services as specified in [FRMCS-FFFIS]. (M)

7.1.5.7.3.2 The Notification Function notification feature as specified in [FRMCS-FFFIS] shall be the only feature used to send NOTIF-IE in the direction from an On-Board FRMCS to a locally bound Application. (M)

7.1.5.7.3.3 Intentionally deleted.

7.1.5.7.3.4 The provisions for sending NOTIF-IE from an On-Board FRMCS by the Notification Function using the Notification Function notification feature shall be configurable as specified in [FRMCS-FFFIS]. (M)

Note: With configurable is meant e.g. the Parameter name 'Update period for the Notification Function'.

7.1.5.7.3.5 The Notification Function shall have the capability to produce the following categories of NOTIF-IE, as specified in clause [7.1.5.7.7] (M):

a. Availability of FRMCS Transport Domain for FTD_AVL.
b. Non-availability of FRMCS Transport Domain for FTD_NAVL_NOTIF.
c. Availability of FRMCS Service Domain for FSD_AVL.
d. Non-availability of FRMCS Service Domain for FSD_AVL.

Note: Network transition state changes corresponds with Category of Notification Function information: communication Status in [FRMCS-FFFIS].

7.1.5.7.3.6 The Notification Function shall have the capability to produce the following categories of NOTIF-IE:

a. Train Location Information as defined in section 16.3.16 (M)
b. FRMCS Time Service as defined in chapter 23 (M-Vx)
c. Observed Indicative QoS (M-Vx)
d. Subscribers of identified types (M-Vx)

7.1.5.7.3.6i For Tight Coupled Applications, the Notification Function:

a. Shall be able to convey Train Location Information (M)
b. Shall be able to convey FRMCS Time Service (M-Vx)
c. Shall be able to convey Observed Indicative QoS (M-Vx)
d. Shall be able to convey Subscribers of identified types (M-Vx)

7.1.5.7.3.6ii For Loose Coupled Applications, the Notification Function:

a. Should be able to convey Train Location Information (O)

b. Shall be able to convey FRMCS Time Service (M-Vx)
c. Shall be able to convey Observed Indicative QoS (M-Vx)
d. Shall be able to convey Subscribers of identified types (M-Vx)

Editor's note: The correspondence between NOTIF-IE in the above list and Category of Notification Function as specified in [FRMCS-FFFIS] and [TOBA-FRS] is not yet completed.

7.1.5.7.3.7 Any NOTIF-IE message generated by the Notification Function and sent using Notification Function notification feature to an Application shall use the appropriate 'Value of Notification Function information' that corresponds with 'Category of Notification Function information' as specified in [FRMCS-FFFIS]. (M)

7.1.5.7.3.8 The correspondence of Category of Notification Function information with Value of Notification Function information is listed in [FRMCS-FFFIS]. (I)

7.1.5.7.4 Reliability

7.1.5.7.4.1 The reliability of the Notification Function is depending on the reliability of the data sources (e.g. Time Function or Location and Positioning Function) providing information elements as input to the Notification Function.(I)

7.1.5.7.5 Availability

7.1.5.7.5.1 The availability of the Notification Function is depending on availability of the data sources (e.g. Time Function or Location and Positioning Function) providing information elements as input to the Notification Function. (I)

7.1.5.7.6 Maintenance and troubleshooting of the Notification Function

7.1.5.7.6.1 This section concerns requirements for the purpose of providing mechanisms for trouble shooting and/or quality assurance of the Notification Function. (I)

7.1.5.7.6.2 For all sources participating in NOTIF-IE production, the Notification Function shall have the capability to monitor, maintain current status and detect changes in status of availability and non-availability. (M)

Note: The means to achieve this capability is considered out of scope of this chapter.

7.1.5.7.6.3 The Notification Function shall have the capability to produce log records for detected changes of availability status including timestamp and additional data if available. (M)

7.1.5.7.6.4 The Notification Function should have the capability to maintain a set of the latest obtained data from all sources. (O)

7.1.5.7.6.5 If the Notification Function is maintaining a set of the latest obtained data, then for all log records produced, the most recently introduced or updated record of this maintained data set shall be included as additional data associated with any log record produced. (M)

7.1.5.7.6.6 Based on a maintainable, configurable (on/off) mechanism and for all NOTIF-IE categories generated, the Notification Function should provide the capability to send the following information to the OM (O):

- Timestamp
- Train Location Information
- Application Category [FRMCS-FFFIS]
- Application On-Board identifier [FRMCS-FFFIS]
- Identifier of a session (if applicable) [FRMCS-FFFIS]
- NOTIF-IE
- Indication of successful/unsuccessful sending

7.1.5.7.7 Notifications on FRMCS availabilities

7.1.5.7.7.1 The Notification Function shall be able to notify the state transition from FTD_AVL to FTD_NAVL to an application (see section 7.1.5.12), i.e., through Notification Services defined in [FRMCS-FFFIS]. (M)

7.1.5.7.7.2 The notification in clause 7.1.5.7.7.1 is referred, as FTD_NAVL_NOTIF. (I)

7.1.5.7.7.3 The Notification Function shall be able to notify the state transition from FTD_NAVL to FTD_AVL to an application (see section 7.1.5.12), i.e., through Notification Services defined in [FRMCS-FFFIS]. (M)

7.1.5.7.7.4 The notifications in clause 7.1.5.7.7.3 is referred, as FTD_AVL_NOTIF. (I)

7.1.5.7.7.5 The FTD_AVL_NOTIF and FTD_NAVL_NOTIF messages shall include the reason of notification (e.g., “Network Transition”). (M)

7.1.5.7.7.6 If the reason of FTD_AVL_NOTIF is “Network Transition”, the notification message shall include the Target FRMCS Domain. (M)

7.1.5.7.7.7 The Notification Function shall be able to notify the state transition from FSD_AVL to FSD_NAVL to an application (see section 7.1.5.12), i.e., though Notification Services defined in [FRMCS-FFFIS]. (M)

7.1.5.7.7.8 The notifications in clause 7.1.5.7.7.7 is referred as FSD_NAVL_NOTIF. (I)

7.1.5.7.7.9 The Notification Function shall be able to notify the state transition from FSD_NAVL to FSD_AVL to an application (see section 7.1.5.12), i.e., though Notification Services defined in [FRMCS-FFFIS]. (M)

7.1.5.7.7.10 The notifications in clause 7.1.5.7.7.9 is referred as FSD_AVL_NOTIF. (I)

7.1.5.7.7.11 The FSD_AVL_NOTIF and FSD_NAVL_NOTIF messages shall include the reason of notification (e.g., “Network Transition”). (M)

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] and [FRMCS-FFFIS] chapters 5.6 and 5.7). (I)

7.1.5.8.2 Requirements

7.1.5.8.2.1 The Orchestration function shall have the capability to use data 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 FRMCS Service Client. (M)

7.1.5.8.2.3 The Orchestration Function shall manage the routing of user plane data flow inside the communication gateway using information derived from (M):

- Local Binding
- Session Management

7.1.5.8.2.4 The information used for the routing of user plane data shall encompass (M):

- Coupling Mode
- Application Identifier
- Session Identifier
- Type of communication

7.1.5.8.2.5 The routing of user plane data flow shall be implemented in a way that enables support for and QoS treatment of the applications according to Annex A, Table A.1. (M)

7.1.5.9 FRMCS Service 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 one or more FRMCS Service Clients to enable Loose Coupled communication mode. (M)

7.1.5.9.2.2 Intentionally deleted.

7.1.5.9.2.3 FRMCS Service Clients manage 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 shall contain the following function: FRMCS Multipath Function. (M-V3)

7.1.5.10.2.3 Connectivity shall provide dataflow transport resources. (M)

7.1.5.10.2.4 Connectivity shall manage and control On-Board FRMCS Radio Function(s) using OB_{RAD} if implemented. (M-V3)

7.1.5.10.3 The On-Board FRMCS Multipath

7.1.5.10.3.1 The On-Board FRMCS Multipath is a function of Communication Gateway Function. (I)

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

Note: See definition of concurrency and chapter [12] for more details.

7.1.5.10.3.3 The On-Board FRMCS Multipath Function is specified in chapter [12] of this document. (I)

7.1.5.10.3.4 The On-Board FRMCS Multipath Function will be configurable by an MPF policy received from an MPF on the infrastructure side ([12.3.27] point 3). (I)

7.1.5.10.3.5 The On-Board FRMCS Multipath Function will, according to the MPF policy, be able to transfer the data flow of a given application through a selected data path ([12.3.19], [12.3.20]). (I)

7.1.5.11 OM

7.1.5.11.1 Introduction

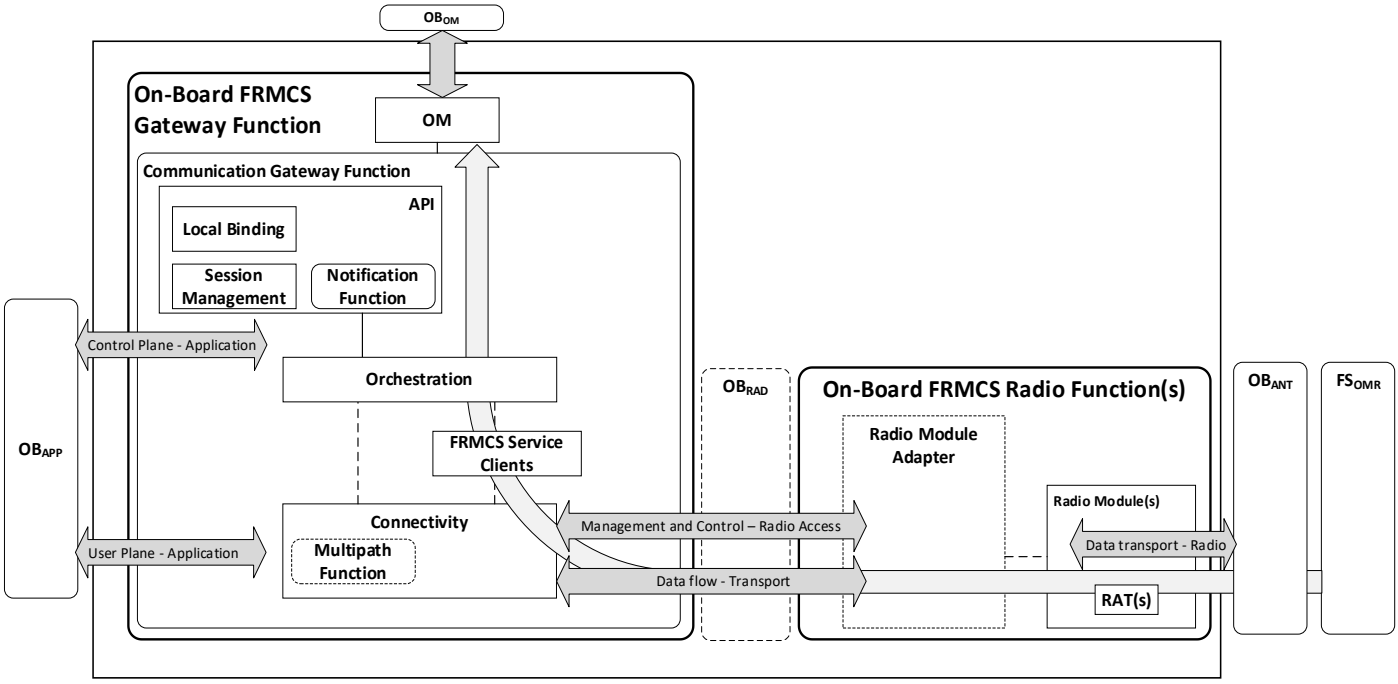


Figure 7-3: On-Board FRMCS architecture with OM

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)

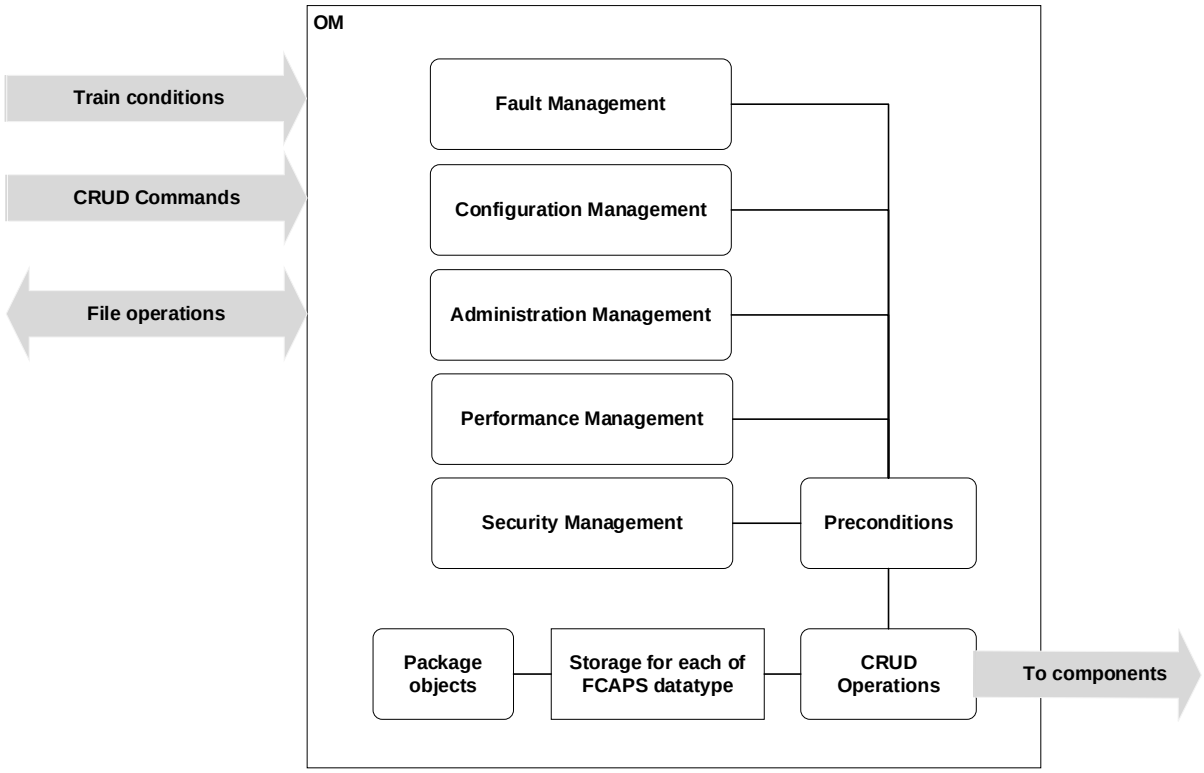


Figure 7-4: System view of OM function

7.1.5.11.2 Requirements

7.1.5.11.2.1 OM Common Requirements

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

7.1.5.11.2.1.2 The OM shall enable access to Operation and Maintenance functionalities via OB_{OM} interface (local OM access). (M)

7.1.5.11.2.1.3 Local OM access shall be available with and without available OTA connectivity. (M)

7.1.5.11.2.1.4 The OM shall enable access to Operation and Maintenance functionalities via FS_{OMR} interface (OTA OM access). (M-V3)

7.1.5.11.2.1.5 OTA OM access using an interface over FS_{OMR} reference point is expected to use OB_{ANT} and OB_{RAD} interfaces to obtain connectivity to the OM hosted by an On-Board FRMCS. (I)

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

7.1.5.11.2.2 OM Capabilities

7.1.5.11.2.2.1 The OM shall collect internal log records and data. (M)

7.1.5.11.2.2.1i The OM shall be able to receive and transfer information to external applications (local and remote) by means of a fully documented API that makes use of a standard protocol for communication (e.g, http, etc..). (M)

Note: “fully documented” in this context implies that documentation is published by the organisation that develops the API, such that it is possible for third parties to develop applications based on the same API without need to acquire additional documentation or information.

7.1.5.11.2.2.2 The OM API implements specified OM functionalities. (I)

7.1.5.11.2.2.3 The OM shall have the capability to consider the train operational status based on external information provided via OB_{OM} interface. (M-Vx)

7.1.5.11.2.2.3i The OM shall have the capability to consider the train operational status based on external information using FS_{OMR} interface. (M-Vx)

7.1.5.11.2.2.4 The OM shall have the capability of identifying train operational status based on detection mechanism(s). (M-V3)

7.1.5.11.2.2.5 The On-Board FRMCS shall have the capability to determine the possibility of entering (or not) in a specific On-Board FRMCS maintenance status based on OBF OM-SCP. (M-V3)

7.1.5.11.2.2.6 The maintenance statuses are as per the table 7-1 below. (I)

On-Board FRMCS Maintenance Status	Description

Start of Operations	Train is at the preparation phase of its operation, systems are booting up, initial information exchange are taking place
Normal Operation	Train is in normal operation, OB FRMCS is connected and some applications (Voice, ETCS, …) may be currently used
OBF Maintenance	OB FRMCS is under maintenance -undergoing a configuration, update or upgrade
GW SW Update	OB FRMCS GW is currently undergoing a software update
GW SW Upgrade	OB FRMCS GW is currently undergoing a software upgrade
Individual OBF RF SW Update	One On-Board FRMCS Radio Function is currently being updated -status need to be attached to a specific ID of the OBF RF-
Individual OBF RF SW Upgrade	One On-Board FRMCS Radio Function is currently being upgraded -status need to be attached to a specific ID of the OBF RF-
Individual OBF RM SW Update	One On-Board FRMCS Radio Module is currently being updated -status need to be attached to a specific ID of the OBF RF and OBF RM-
Individual OBF RM SW Upgrade	One On-Board FRMCS Radio Module is currently being upgraded -status need to be attached to a specific ID of the OBF RF and OBF RM-
Connectivity-affecting parameter configuration	O&M user has initiated the change of at least one parameter having an impact on connectivity (e.g., eSIM, credentials, …)
Non-Connectivity-Affecting parameter configuration	O&M user has initiated the change of at least one parameter having no impact on connectivity (e.g., application profiles, …)
Log retrieval status (background)	O&M user has initiated a query for a specific log
Audit Log retrieval status (background)	Audit log retrieval status (background): O&M user has initiated a query for a specific audit log

Table 7-1 On-Board FRMCS Maintenance Status (based on OBF OM-SCP)

7.1.5.11.2.2.7 The OM shall provide the capability of configuring combinations of conditions on the OBF OM-SCP allowing the activation of specific On-Board FRMCS maintenance statuses. (M-V3)

7.1.5.11.2.2.8 The On-Board FRMCS shall have the capability to change the On-Board FRMCS Maintenance Status only if the configured combination of conditions for the target status is verified. (M-V3)

7.1.5.11.2.3 OM Fault Management

7.1.5.11.2.3.1 The On-Board FRMCS system shall detect and classify defects within the On-Board FRMCS boundary that affect its normal operation. (M)

7.1.5.11.2.3.2 The On-Board FRMCS system shall create and send an alert and error message immediately about defects that could prevent its normal operation over the O&M interface OB_{OM}. (M)

7.1.5.11.2.3.2i The On-Board FRMCS system shall create and send an alert and error message immediately about defects that could prevent its normal operation over the O&M interface FS_{OMR}. (M-V3)

7.1.5.11.2.3.3 The monitored parameter set via the O&M function should support detecting anomalies before they develop into actual defects. (O)

7.1.5.11.2.3.4 In case of a malfunction and/or resource exhaustion, the On-Board FRMCS system should deallocate resources ([7.1.5.11.2.6.1]) associated to non-critical service sessions in case this allows the allocation of necessary resources for sustained operation of higher-priority service sessions ([FRMCS FRS] chapter 8.2.8). (O)

7.1.5.11.2.3.5 The On-Board FRMCS shall detect malfunctioning Hardware and Software components ([7.1.5.11.2.6.2]) and disable them such that they are no longer operational, without impacting critical functionalities. (M-Vx)

7.1.5.11.2.3.6 The On-Board FRMCS shall perform corrective actions (e.g., rebooting, reconfiguration, health check, etc) on individual malfunctioning components in such a way that it does not impact critical functionality. (M-Vx)

7.1.5.11.2.3.7 Only if the corrective actions taken according to [7.1.5.11.2.3.6] can result in full recovery of the malfunctioning component, the component may be used again. (I)

7.1.5.11.2.4 OM Configuration Management

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

7.1.5.11.2.4.2 The OM shall enable authenticated and authorized O&M Users to perform any one of the Create, Read, Update, Delete (CRUD) operations on the FRIOP information elements, see chapter [19.2]. (M)

7.1.5.11.2.4.3 The OM shall enable authenticated and authorized O&M Users to perform any one of the CRUD operations on the non-FRIOP information elements, see chapter [19.2]. (M)

7.1.5.11.2.4.4 The OM shall enable On-Board FRMCS Package management capabilities for On-Board FRMCS components. (M)

Note: As per definition of On-Board FRMCS Package, this can refer to a single On-Board FRMCS component, to multiple components, or to the whole On-Board FRMCS.

7.1.5.11.2.4.5 The OM shall enable O&M Users to perform any one of the CRUD operations on On-Board FRMCS Package. (M)

7.1.5.11.2.4.6 On-Board FRMCS Package management capabilities should encompass storage of On-Board FRMCS Packages in a storage facility located in the On-Board FRMCS. (O)

7.1.5.11.2.4.7 In case a storage facility for On-Board FRMCS On-Board FRMCS Packages is available, Package management capabilities shall enable any of the CRUD operations on stored On-Board FRMCS Packages. (M)

7.1.5.11.2.4.8 On-Board FRMCS Package management shall encompass package versioning with compatibility check for On-Board FRMCS Packages. (M)

7.1.5.11.2.4.9 On-Board FRMCS Package management capabilities shall have the capability to configure sources for On-Board FRMCS Packages. (M)

7.1.5.11.2.4.10 Each source for On-Board FRMCS Packages is expected to be secured. (I)

7.1.5.11.2.4.11 On-Board FRMCS Package management capabilities shall have the capability to verify the authenticity of the On-Board FRMCS Packages. (M)

7.1.5.11.2.4.12 The OM shall provide the capability of maintaining a stored current list of system components of the On-Board FRMCS including their unique IDs. (M)

7.1.5.11.2.4.12i The stored current list of system components as specified in [7.1.5.11.2.4.12] shall as a minimum consist of and by means of reference be associated with the architecture elements described and specified within chapter [7.1] of this specification: (M)

Note: With by means of reference is in this context to be understood as the capability to relate entities in a product with architectural elements in related specification(s).

7.1.5.11.2.4.12ii The content and details for the stored current list of system components shall comply to [7.1.5.11.2.4.12] (M-V3)

7.1.5.11.2.4.13 The OM shall provide the capability of retrieving the list of all the identifiable elements of the On-Board FRMCS including their unique IDs. (M)

7.1.5.11.2.4.14 The OM should provide the capability of maintaining a protected stored set of all the current parameters for the FRMCS service clients hosted by the On-Board FRMCS. (O)

7.1.5.11.2.4.15 The OM should provide the capability only to authenticated and authorized O&M Users to perform any one of the CRUD operations on information elements stored in the current parameter storage. (O)

7.1.5.11.2.5 OM Administration

7.1.5.11.2.5.1 The OM shall enable protected access for O&M Users granted with administrative rights to perform any one of the CRUD operations on OM user accounts. (M)

7.1.5.11.2.5.2 The OM shall enable protected access for O&M Users granted with administrative rights to perform any one of the CRUD operations on OM user groups. (M)

7.1.5.11.2.5.3 The OM should enable protected administrative access to configuration of assignment of OM users to OM user groups. (O)

7.1.5.11.2.5.4 The OM shall enable protected administrative access to configuration of OM user access rights. (M)

7.1.5.11.2.5.5 The OM shall grant access to O&M Users exclusively based on configured access rights. (M)

7.1.5.11.2.5.6 The OM shall provide the capability to distinguish access rights based on the type of access (local OM access or OTA OM access). (M)

7.1.5.11.2.5.7 O&M Users shall be able to perform operations and maintenance activities on On-Board FRMCS components with their associated configuration parameters. (M)

Editor's Note: A matrix of recommended access for O&M User rights related to FRIOP, non-FRIOP and Cybersecurity parameters could be provided in a later stage but not in scope of FRMCS v2.

7.1.5.11.2.5.8 The OM shall provide the capability to store a current list of all the On-Board FRMCS entities authorized to use Local Binding. (M)

7.1.5.11.2.5.8i The current list of all the On-Board FRMCS entities as specified by [7.1.5.11.2.5.8] shall be maintainable. (M)

7.1.5.11.2.5.9 The OM shall enable protected administrative access to perform any one of the CRUD operations on Local Binding credentials for FRMCS entities. (M)

7.1.5.11.2.5.10 OM should enable protected administrative access to configuration of Local Binding credentials for FRMCS entities. (O)

7.1.5.11.2.5.11 The OM shall provide the capability of maintaining a protected stored set of all the current service credentials for the FRMCS service clients hosted by the On-Board FRMCS. (M)

7.1.5.11.2.5.12 The OM shall enable protected administrative access to perform any one of the CRUD operations on records of service credentials in the current set. (M)

7.1.5.11.2.5.13 The OM shall provide the capability of maintaining a protected stored repository for transport stratum-related identifiers and parameters for:

- Radio Access (e.g., eSIM Card) (M)
- IMS/SIP Core access (M)

7.1.5.11.2.5.14 The OM shall enable protected administrative access to perform any one of the CRUD operations on records into the current repository of transport stratum-related identifiers and parameters. (M)

7.1.5.11.2.6 OM Performance Monitoring

7.1.5.11.2.6.1 The On-Board FRMCS shall monitor performance indicators related to On-Board FRMCS HW resources: (M)

- CPU load (including monitoring load)
- Memory usage
- Storage usage
- Networking load
- Networking usage type (e.g., DPI)

7.1.5.11.2.6.2 The On-Board FRMCS shall monitor performance indicators related to On-Board FRMCS components: (M)

- Gateway Function
- On-Board FRMCS Radio Function(s)
- Radio Module(s)
- SW Components
- HW Components

7.1.5.11.2.6.3 The On-Board FRMCS shall monitor performance indicators related to On-Board FRMCS interfaces: (M)

- OB_{APP}
- OB_{OM}

7.1.5.11.2.6.4 The On-Board FRMCS should monitor performance indicators related to On-Board FRMCS interfaces: (O)

- OB_{RAD}
- OB_{ANT}

7.1.5.11.2.6.5 The On-Board FRMCS should have the capability to generate performance event log records based on configurable thresholds for the monitored performance indicators. (O)

7.1.5.11.2.6.6 The On-Board FRMCS shall enable authenticated and authorised O&M users to retrieve the performance event log records relative to the monitored indicators. (M)

7.1.5.11.2.7 OM Supervision and Audit

7.1.5.11.2.7.1 The On-Board FRMCS shall include parameters that as a set, uniquely can identify a source for all generated log records. (M)

7.1.5.11.2.7.2 The On-Board FRMCS shall include time stamping in all generated log records according to chapter [23.4] of this document. (M)

7.1.5.11.2.7.3 The On-Board FRMCS shall have the capability to include location information in all generated log records according to FRMCS Location and Positioning requirements according to chapter [16.3] of this document. (M)

7.1.5.11.2.7.3i The capability as specified by [7.1.5.11.2.7.3] shall be applied whenever there is a FRMCS Service session established for any Application of Type I or Type III as defined by [10.1.3.3.4]. (M)

7.1.5.11.2.7.3ii The capability as specified by [7.1.5.11.2.7.3] should be applied whenever there is a FRMCS Service session established for any Application of Type II or Type IV as defined by [10.1.3.3.4]. (O)

7.1.5.11.2.7.4 The On-Board FRMCS shall provide the capability of protecting selected log records from alterations. (M)

7.1.5.11.2.7.5 The On-Board FRMCS shall provide the capability of configuring which log records that shall be protected from alteration. (M)

7.1.5.12 States within On-Board FRMCS

7.1.5.12.1 The On-Board FRMCS shall be able to identify in which of the following state(s) it is operating (M):

a) FRMCS Transport Domain Available (FTD_AVL)
b) FRMCS Transport Domain Not-Available (FTD_NAVL)
c) FRMCS Service Domain Available (FSD_AVL)
d) FRMCS Service Domain Not-Available (FSD_NAVL)

Note: There is one FSD-AVL / FSD_NAVL per FRMCS Service User.

7.1.5.12.2 The On-Board FRMCS shall detect the transitions between FTD_NAVL and FTD_AVL. (M)

7.1.5.12.3 The On-Board FRMCS shall detect the transitions between FSD_NAVL and FSD_AVL, per FRMCS Service User. (M)

7.1.5.12.4 The detailed definition of states in clause [7.1.5.12.1] shall comply with [TS 103 765-3]. (M)

7.1.6 On-Board FRMCS Radio Function

7.1.6.1 Introduction

7.1.6.1.1 **Intentionally deleted**.

7.1.6.1.2 The On-Board FRMCS Radio Function includes the following components (I):

- Radio Module Adapter
- Radio Module(s)

7.1.6.1.2i The On-Board FRMCS Radio Function shall enable access for the Communication Gateway Function to the FRMCS Transport Stratum. (M)

7.1.6.1.2ii The On-Board FRMCS Radio Function enables transmission of control and user plane related data. (I)

7.1.6.1.2iii The On-Board FRMCS Radio Function boundaries are given by reference points OB_{RAD} and OB_{ANT}. (I)

7.1.6.1.3 **Intentionally deleted.**

7.1.6.1.4 **Intentionally deleted**.

7.1.6.1.5 **Intentionally deleted**.

7.1.6.2 Radio Module Adapter

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

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

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

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

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

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

7.1.6.2.7 The Radio Module Adapter can encompass software. (I)

7.1.6.2.8 The Radio Module Adapter shall interface to OB_{RAD}. (M-V3)

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

7.1.6.2.10 The Radio Module Adapter interfaces with Radio Modules using suitable industrial interfaces (I)

7.1.6.3 Radio Module(s)

7.1.6.3.1 The On-Board FRMCS supports several types of Radio Modules. (I)

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

a. On-Board FRMCS Radio Module
b. MNO Radio Module
c. WLAN (e.g., Wi-Fi) Radio Module

7.1.6.3.3 **Intentionally deleted**.

7.1.6.3.4 A Radio Module has one or more external antenna interface(s), for Terrestrial Networks (TN) or Non-Terrestrial Networks (NTN) for radio access that can be either bi-directional or unidirectional. (I)

7.1.6.3.5 The On-Board FRMCS Radio Module shall comply to [TS 103 765-3]. (M)

7.1.6.3.6 The On-Board FRMCS Radio Module shall comply to requirements defined in chapter [8] of this document. (M)

7.1.6.3.7 **Intentionally deleted**.

7.1.6.3.8 For an On-Board FRMCS Radio Module, it shall be possible to disable or enable each band individually. (M-Vx)

7.1.6.3.9 For ITU region 1 and within the European Economic Area (EEA), the On-Board FRMCS Radio Module shall be capable of operating in the radio environment as defined identified per [ECC Decision (20)02]. (M)

7.1.6.3.10 The On-Board FRMCS Radio Module shall allow the implementation of National Roaming for selected railway lines. (M-V3)

7.1.6.3.11 For the purpose of National Roaming, the On-Board FRMCS Radio Module shall enable non-simultaneous usage of either RMR or MNO frequencies. (M-V3)

7.1.6.3.12 The On-Board FRMCS Radio Module shall allow the implementation of Multi-Operator Core Network (MOCN) for selected railway lines. (M-V3)

7.1.6.3.13 The MNO Radio Module shall support the frequency bands as listed in Table 8-1 of section [8] of this document. (M-V3)

7.1.6.3.13i The MNO Radio Module shall support the frequency bands as listed in Table 8-2 of section [8] of this document. (M-V3)

7.1.6.3.13ii The MNO Radio Module shall support the frequency bands as listed in Table 8-3 of section [8] of this document. (M-V3)

7.1.6.3.13iii The MNO Radio Module shall support the frequency bands as listed in Table 8-4 of section [8] of this document. (M-V3)

7.1.6.3.13iiii The MNO Radio Module shall support the frequency bands as listed in Table 8-5 of section [8] of this document. (M-V3)

7.1.6.3.14 The MNO Radio Module shall comply to requirements defined in section [8.5] of this document. (M)

7.1.6.3.15 For an MNO Radio Module, it shall be possible to disable or enable each band individually as per national configuration. (M-Vx)

7.1.6.3.16 On an OnBoard FRMCS supporting IFDT, the On-Board FRMCS Radio Module shall support carrying communications of FRMCS Service Users which are served by different FRMCS Service Domains (see chapter [10] for requirements on IFDT and interconnected FRMCS Service Domains). (M)

7.2 Antenna Function

7.2.1 Introduction

7.2.1.1 The Antenna Function is outside the boundary of the On-Board FRMCS as depicted in Figure 7-1. (I)

7.2.1.2 The Antenna Function is accessible via the OB_{ANT} interface specified in clause 7.1.4.1.2. (I)

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

7.2.2 Generic requirements

7.2.2.1 A minimum of two antenna elements shall be used for On-Board FRMCS Radio Functions (M):

- Antenna element 1 used for TX/RX
- Antenna element 2 used for RX or TX/RX

7.2.2.2 The antenna elements are implemented as individual antennas or several antenna elements in one housing (MIMO antennas). (I)

7.2.2.3 The physical setup of the antennas on the roof supports both correct functioning of each antenna and sufficient isolation between active radio systems onboard. (I)

Note: For the onboard system, to ensure the required performance of the critical RMR services, a sufficient isolation between radio systems operating simultaneously is necessary to prevent onboard interference effects (e.g., due to blocking and out-of-band emissions). A proper isolation shall be ensured between GSM-R and FRMCS in the RMR bands as well as between GSM-R and FRMCS and, if used, MNO bands. Isolation requirements for the simultaneous operation of RMR and MNO services are presented in Chapter 8.5. Measures like additional filters or disabling specific MNO bands can help to achieve the necessary isolation between the radio systems.

7.2.2.4 For the antenna function, an isotropic FRMCS onboard antenna with a minimum gain of 0dBi is assumed. (I)

7.2.2.5 For the radio network planning of band n100 of the uplink, a minimum EIRP of 25dBm in the air (at the On-Board antenna) shall be assumed. (M)

Note: This 25dBm takes into account for band n100 the UE Power Class 1 (31dBm) for the On-Board FRMCS radio modules and a maximum of 6dB losses between the radio module and the On-Board antenna (including cable losses, aging, connector losses and filter losses). As per UIC document O-8868, further interaction with industry and FRMCS projects are ongoing with the goal to achieve an EIRP level as close as possible to the regulatory maximum allowed 33dBm (31dBm UE output power plus 5dBi antenna gain minus 3 dB hardware losses).

7.2.2.6 For the radio network planning of band n101 of the uplink, a minimum EIRP of 25dBm in the air (at the On-Board antenna) shall be assumed. (M)

Note: This 25dBm takes into account for band n101 the UE Power Class 1 (31dBm) for the On-Board FRMCS radio modules and a maximum of 6dB losses between the radio module and the On-Board antenna (including cable losses, aging, connector losses and filter losses). As per UIC document O-8868, further interaction with industry and FRMCS projects are ongoing with the goal to achieve an EIRP level as close as possible to the regulatory maximum allowed 33dBm (31dBm UE output power plus 5dBi antenna gain minus 3 dB hardware losses).

7.2.2.7 The VSWR value for the On-Board FRMCS Radio Module plus the antenna plus the cable and possible other RF devices is assumed to be equal or less than 2 to reduce unwanted power reflections. (I)

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 To ensure railway interoperability and On-Board RF coexistence, sufficient isolation between RMR and MNO when operating simultaneously is necessary to mitigate On-Board interference effects. (I)

8.3.3 The performance of the On-Board Radio Modules shall not be compromised when using multiple frequency bands. (M)

8.3.4 Depending on the chosen migration- or deployment strategy, an FRMCS Operator shall support a network and/or services, using at least one or multiple of the following frequency bands for the 5G Access Network: (M-V3)

a. The RMR 900 MHz frequency band (as identified in par. 8.4.2)
b. The RMR 1900 MHz frequency band (as identified in par. 8.4.3)
c. Public MNO frequency band n28 (as identified in par. 8.5.3)
d. Public MNO frequency band n20 (as identified in par. 8.5.3i)
e. Public MNO frequency band n7 (as identified in par. 8.5.3ii)
f. Public MNO frequency band n78 (as identified in par. 8.5.3iii)

8.4 RMR frequency bands for Europe

8.4.1 [EU 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 The On-Board FRMCS shall support the use of 3GPP 5G NR technology for the paired frequency bands defined in [EU 2021/1730] of: (M)

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

Note: This frequency band is defined by 3GPP as band n100.

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

a. 1900-1910 MHz

Note: This frequency band is defined by 3GPP as band n101.

8.5 Public MNO Spectrum in Europe

8.5.1 For deployment scenarios with simultaneous On-Board operation of GSM-R, FRMCS and MNO services, an MNO frequency band in conjunction with RMR frequency bands can only be implemented if the following interference mechanisms related to On-Board antenna (including antenna gain, cable losses, aging, connector losses and filter losses) implementations will be mitigated by providing sufficient isolation: (I)

a. Blocking of On-Board FRMCS Radio Modules by one or more specific MNO band(s).
b. Out-of-band emissions into RMR bands by one or more specific MNO band(s).
c. Spurious emissions into RMR bands by one or more specific MNO band(s).

8.5.2 The EU 5G MNO frequency bands are listed in Tables 8-1 and 8-2. It is noted that: (I)

a. **Intentionally deleted**.
b. The behaviour of UE power class 1 (used for RMR bands) and UE power class 3 (typically used for MNO bands), has not yet been considered.
c. The effect of using different UE power classes on ensuring FRMCS QoS requirements (i.e., 5QI) has not yet been considered.
d. The isolation requirements listed in Tables 8-1 to 8-5, are only applied for On-Board (and not for trackside) FRMCS deployment and are only considered for the interference mechanism of blocking. In particular for cases where the isolation requirement is designated as high, coexistence studies must be performed to ensure potential coexistence between RMR (FRMCS & GSM-R) and MNO frequency bands. For this reason, these frequency bands are listed in a separate table (Table 8-5). Based on future coexistence studies and due to other interference mechanisms, the classification of the dedicated bands could change.
e. The relevant interference mechanisms have not been fully studied yet. This could imply additional restrictions or alleviations.

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.3 The On-Board FRMCS shall support band n28 with the applicable isolation requirements as defined in Table 8-1: (M-V3)

Frequency bands	Band name	Uplink/ Downlink frequency bands	Isolation requirements (for onboard scenarios with simultaneous operation of RMR and

			MNO services. Pending further On-Board coexistence studies)	
700 MHz	n28	703 MHz - 733 MHz / 758 MHz - 788 MHz	n100 Low	n101 Low

Table 8-1 Public Frequency band n28 for On-Board FRMCS deployment

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.3i The On-Board FRMCS shall support band n20 with the applicable isolation requirements as defined in Table 8-2: (M-V3)

Frequency bands	**Band name**	**Uplink/ Downlink frequency bands**	**Isolation requirements (for onboard scenarios with simultaneous operation of RMR and MNO services. Pending further On-Board coexistence studies)**	
800 MHz	n20	832 MHz - 862 MHz / 791 MHz - 821 MHz	n100 Low	n101 Low

Table 8-2 Public Frequency band n20 for On-Board FRMCS deployment

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.3ii The On-Board FRMCS shall support band n7 with the applicable isolation requirements as defined in Table 8-3: (M-V3)

Frequency bands	**Band name**	**Uplink/ Downlink frequency bands**	**Isolation requirements (for onboard scenarios with simultaneous operation of RMR and MNO services. Pending further On-Board coexistence studies)**	
2600 MHz	n7	2500 MHz – 2570 MHz / 2620 MHz – 2690 MHz	n100 Low	n101 Medium

Table 8-3 Public Frequency band n7 for On-Board FRMCS deployment

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.3iii The On-Board FRMCS shall support band n78 with the applicable isolation requirements as defined in Table 8-4: (M-V3)

Frequency bands	**Band name**	**Uplink/ Downlink frequency bands**	**Isolation requirements (for onboard scenarios with simultaneous operation of RMR and MNO services. Pending further On-Board coexistence studies)**	
3500 MHz	n78	3300 MHz – 3800 MHz (TDD)	n100 Low	n101 Medium

Table 8-4 Public Frequency band n78 for On-Board FRMCS deployment

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.4 The On-Board FRMCS supports a subset of the MNO frequency bands in use in Europe as listed in Table 8-5 for use cases not considering on board coexistence (applicable to ITU region 1): (I)

Frequency bands	**Band name**	**Uplink/ Downlink frequency bands**	**Isolation requirements (For onboard scenarios with simultaneous operation of RMR and MNO services. Pending further On-Board coexistence studies)**	
900 MHz	n8	880 MHz – 915 MHz / 925 MHz – 960 MHz	n100 High	n101 Low
1800 MHz	n3	1710 MHz – 1785 MHz / 1805 MHz – 1880 MHz	n100 Low	n101 Medium
2100 MHz	n1	1920MHz-1980MHz / 2110MHz-2170MHz	n100 Low	n101 High

Table 8-5 Public Frequency bands for On-Board FRMCS deployment (high isolation requirements)

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO services and assuming the application of FRMCS double bandpass and high bandpass RF filters.

8.5.5 To avoid blocking of band n100 by simultaneous usage of MNO bands:

a. An isolation of < 20 dB (Low) between the antennas is required for the bands n28, n20, n7, n78, n3 and n1. (I)
b. For band n8, an isolation of >= 72 dB (High) is required. (I)

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.6 To avoid blocking of band n101 by simultaneous usage of MNO bands:

a. An isolation of < 20 dB (Low) between the antennas is required for the bands n8, n20 and n28. (I)
b. For bands n3, n7 and n78 an isolation of >= 43 dB (Medium) is required. (I)
c. For band n1, an isolation of >= 72 dB (High) is required. (I)

Note: The isolation requirements regarding blocking refer to an On-Board antenna deployment scenario with simultaneous operation of FRMCS and MNO and assuming the application of FRMCS double band pass and high pass RF filter.

8.5.7 Due to the close proximity in the radio spectrum of RMR band n100 and MNO band n8 as well as RMR band n101 and MNO band n1 and taking into account standard-compliant behaviour of the involved MNO radio equipment, the highest values of isolation are required for these On-Board deployment scenarios. For band n1 and n8, an additional isolation requirement due to out-of-band emissions into RMR band n101/n100 is likely. (I)

Editor´s Note 1: Results of On-Board coexistence studies will be examined for at FRMCS field trials and (data transmission) tests. If necessary, requirements will be refined (for example exclusion of bands n8 and n1 from On-Board FRMCS systems operating simultaneously).

Editor's Note 2: The values of necessary On-Board FRMCS and MNO isolation and the relevant interference mechanism must be validated and, if necessary, reviewed before the first operational implementations of

FRMCS.

8.6 WLAN (Wi-Fi) spectrum in Europe

8.6.1 The On-Board FRMCS should support the following Wi-Fi frequency bands:

a. The 2.4 GHz band ranging from 2.400 GHz to 2.4835 GHz. (O)
b. The 5 GHz band ranging from 5.150 GHz to 5.350 GHz. (O)
c. The 5 GHz band ranging from 5.470 GHz to 5.725 GHz. (O)
d. The 5 GHz band ranging from 5.735 GHz to 5.875 GHz. (O)
e. The 6 GHz band ranging from 5.945 GHz to 6.425 GHz. (O)

9 GSM-R/FRMCS Interworking

9.1 Introduction

9.1.1 GSM-R/FRMCS interworking is the process where FRMCS users obtaining services from the FRMCS system can communicate with GSM-R users, obtaining services from the GSM-R system. (I)

9.1.2 GSM-R/FRMCS interworking is limited to FRMCS users of the VAS, which is defined in Chapter 24 of this document. (I)

9.1.3 The InterWorking Function (IWF) is a functional entity within the FRMCS system, which enables interworking between the FRMCS users and GSM-R users. (I)

9.1.4 The following section describes the interworking between GSM-R and FRMCS, based on different, possible scenarios. (I)

Note: The GSM-R/FRMCS Interworking is a trackside function located between the FRMCS and GSM-R domain and is not to be confused with the GSM-R/FRMCS Coordinating Function of CCS applications (Voice, ETCS and ATO).

9.2 Out of scope

9.2.1 The migration of ETCS (onboard & trackside) is not in scope of this document. (I)

9.2.2 Interworking between FRMCS Domains is not in scope of chapter [9]. (I)

9.2.3 MCVideo is not in scope. (I)

9.2.4 MCData services (except MCData SDS) is not in scope of chapter [9]. (I)

9.3 Interworking interfaces

9.3.1 FS_{IWF} is the generic reference point between the IWF within the FRMCS System and the GSM-R system as defined in section 6.4 and detailed in [TS 103 792]. (I)

9.3.2 Figure 9-1 depicts the reference point FS_{IWF}. (I)

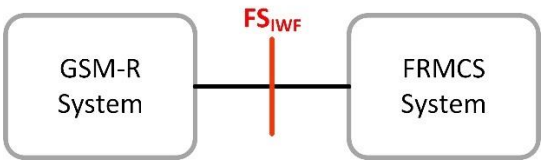


Figure 9-1 - Logical architecture IWF.

9.4 Migration scenarios in Europe

9.4.1 General requirements

9.4.1.1 Depending on the migration scenario a user can be attached to the FRMCS system, to the GSM-R system or temporarily to both. (I)

9.4.1.2 Spectrum related aspects are defined in chapter [8] of this document. (I)

9.4.1.3 [O-8856] can be used as a supplementary information source on the migration scenarios in this chapter. (I)

9.4.1.4 FRMCS is a 5G based system, as a consequence the following migration scenarios are based on this type of system. (I)

9.4.2 Intentionally deleted.

9.4.3 **Intentionally deleted.**

9.5 Interworking

9.5.1 General requirements

9.5.1.1 The IWF acts as an MC Service server which is connected to the FRMCS Service server on one side and the GSM-R Core on the other side. (I)

9.5.1.2 The main functionalities of the interworking function are routing/addressing and mapping/identity management. (I)

9.5.1.3 The IWF shall support the interworking of supplementary services, needed for the interworking between the GSM-R system and the FRMCS system according [TS 103 792]. (M)

9.5.1.4 The IWF shall provide the possibility to allow FRMCS users, independent of their role (train driver, controller…) to be reachable from the GSM-R system. (M)

9.5.1.5 The IWF shall provide the possibility to allow GSM-R users, independent of their role (train driver, controller…) to be reachable from the FRMCS system. (M)

9.5.1.6 The FRMCS system shall be able to support interworking of GSM-R priorities to the priority mechanisms of the FRMCS system and vice versa according [TS 103 792] §7 and §8. (M)

9.5.1.7 The routing of communications between the FRMCS system and GSM-R system shall be organised, within the interworking function, as defined in [TS 103 792] §6. (M)

9.5.1.8 The mapping of identities from/to the FRMCS system and to/from the GSM-R system shall be done, within the interworking function, as defined in [TS 103 792] §6. (M)

9.5.1.9 The format of the identities and addresses shall be according to chapter 11 of this document and [TS 103 792] §6. (M)

9.5.1.10 Besides the standard identities (e.g., FRMCS Service Identity, MSISDN), the IWF shall be able to map functional identities (FA and FN) as defined in [TS 103 792] §6. (M)

9.5.2 Interworking with GSM-R and FRMCS in same area

9.5.2.1 Introduction

9.5.2.1.1 For this scenario, it is assumed that both GSM-R and FRMCS are present in the same area, and the onboard system of the train supports both systems. (I)

9.5.2.1.2 The GSM-R and FRMCS coverages can be on the same line or coming from nearby railway lines (e.g., GSM-R on one line and FRMCS on parallel or crossing line). (I)

9.5.2.2 Interworking of codecs

9.5.2.2.1 In case of voice communications interworking between the GSM-R system and the FRMCS system, the AMR-WB codec shall be used for both systems. (M)

Editor's note: bit rates may be specified in later revision of the present document but not in scope of FRMCS v2.

9.5.2.2.2 [TS 103 792] §7.2.8 provides some additional information on the codec negotiation procedure with interworking. (I)

Note: Since an existing, common codec is used, the codecs within the GSM-R (Core Network/Radio Access Network/Mobile Station) won't be changed.

9.5.2.3 Performance requirements with interworking

9.5.2.3.1 The setup time of a voice communication including combination of FRMCS users and GSM-R users shall respect clause §3.4 of the [EIRENE-SRS]. (M-V3)

9.5.2.4 Point-to-Point calls

9.5.2.4.1 The FRMCS system shall give the possibility to set up a voice communication in a uniform and transparent manner between 2 users, independent of their role (train driver, controller…) and the network they are connected to. (M)

9.5.2.4.2 The call flow and identity mapping for point-to-point calls, using interworking, as defined in [TS 103 792] §8, shall be respected. (M)

9.5.2.5 Group calls & REC

9.5.2.5.1 The FRMCS system shall give the possibility to set up a voice communication in a uniform and transparent manner between 2 or more users, independent of their role (train driver, controller…) and the network they are connected to. (M)

9.5.2.5.2 The call flow and identity mapping for group calls, using interworking, as defined in [TS 103 792] §7, shall be respected. (M)

9.5.2.6 Messaging

9.5.2.6.1 The exchange of messages between the GSM-R system (SMS) and the FRMCS system (MCData SDS) shall comply with [TS 103 792] §9. (M)

9.5.2.6.2 The IWF shall be able to convert SMS into MCData SDS messages and vice versa. (M)

Note: This procedure mainly consists of the mapping of identities by the IWF and forwarding it to the corresponding network.

9.5.3 Interworking enabling transition between neighbouring GSM-R and FRMCS areas

9.5.3.1 In this scenario, only one of the two communication systems (GSM-R or FRMCS) is present in a specific area, whereas at a certain point in time a network transition from the one to the other needs to take place. (I)

9.5.3.1.1 The transition from GSM-R to FRMCS shall comply to the procedure described in §10.1.4 of this document. (M-V3)

9.5.3.1.2 The transition from FRMCS to GSM-R is described in §10.1.5 of this document. (I)

9.5.4 Security

9.5.4.1 Authorisations for the use of applications shall be transparent to the IWF. (M)

9.5.4.2 GSM-R and FRMCS have their own encryption and interworking is done by IWF, as specified in [TS 103 792]. (I)

10 Network Transitions and Interconnection

10.1 Network Transitions

10.1.1 Introduction

10.1.1.1 The Network Transition is a term used to encompass both procedures of the Inter-FRMCS-Domain Transition (IFDT) and the transition between GSM-R and FRMCS. (I)

Editor's Note: This chapter can in later versions include the 5G roaming requirements.

10.1.1.2 In Network Transition procedures, a Serving On-Board FRMCS Radio Module (OBF RM) is an OBF RM carrying active communication services (e.g., providing PDU session) at least for ATP and/or VAS in the Serving FRMCS Transport Domain (see definitions in chapter [2]). (I)

10.1.1.3 In Network Transition procedures, a Target OBF RM is the OBF RM which is intended to carry active communication services (e.g., providing PDU session) at least for ATP and/or VAS in the Target FRMCS Transport Domain (see definitions in chapter [2]). (I)

10.1.2 Trigger for Network Transition

10.1.2.1 The following information shall be available at the entity generating the Network Transition Trigger (NTT) prior to trigger decision (M-V3):

- Train's location

Note: the information can be implicitly available, e.g., a driver knows the train's location.

10.1.2.2 The following additional information shall be available at the entity generating the Network Transition Trigger (NTT) priori to trigger decision (M-V3):

- The knowledge that the train is going to cross the border (e.g., direction, if enough).
- Target FRMCS Transport Domain.

10.1.2.3 Upon the reception of the Network Transition Trigger (NTT), the On-Board FRMCS shall be able to determine the Target FRMCS Transport/Service Domain. (M-V3)

10.1.2.4 Upon the reception of NTT, the On-Board FRMCS decides, which of the following procedures shall be performed: 1) Inter-FRMCS-Domain transition (see section [10.1.3]), 2) GSM-R to FRMCS transition (see section [10.1.4]) (M-V3)

Note: the act of transition from FRMCS to GSM-R is transparent to On-Board FRMCS.

10.1.2.5 **Intentionally deleted**.

10.1.2.6 In case the On-Board FRMCS does not have a FRMCS Domain acquired, the mechanism to acquire the FRMCS Domain shall be performed by On-Board FRMCS. (M-V3)

10.1.3 Inter-FRMCS-Domain Transition for On-Board FRMCS

10.1.3.1 Introduction

10.1.3.1.1 This section describes the procedures and configurations required within FRMCS for a train which crosses the boundary between Serving FRMCS Domain and Target FRMCS Domain, as depicted in Figure 10-1. (I)

10.1.3.1.2 The two FRMCS Domains involved in this procedure might not be the Home FRMCS Domain. (I)

10.1.3.1.3 The transition between the radio coverages is bound to the radio cells' deployment along the rail line. This transition occurs at a single moment for an OBF RM which is commonly used for multiple communication services. (I)

10.1.3.1.4 However, the right moment for handing over a service from one FRMCS Service Domain to another is dependent on functional requirements of communication services and might be unsynchronized among them. (I)

10.1.3.1.5 The inter-FRMCS-domain transition is an internal FRMCS function. (I)

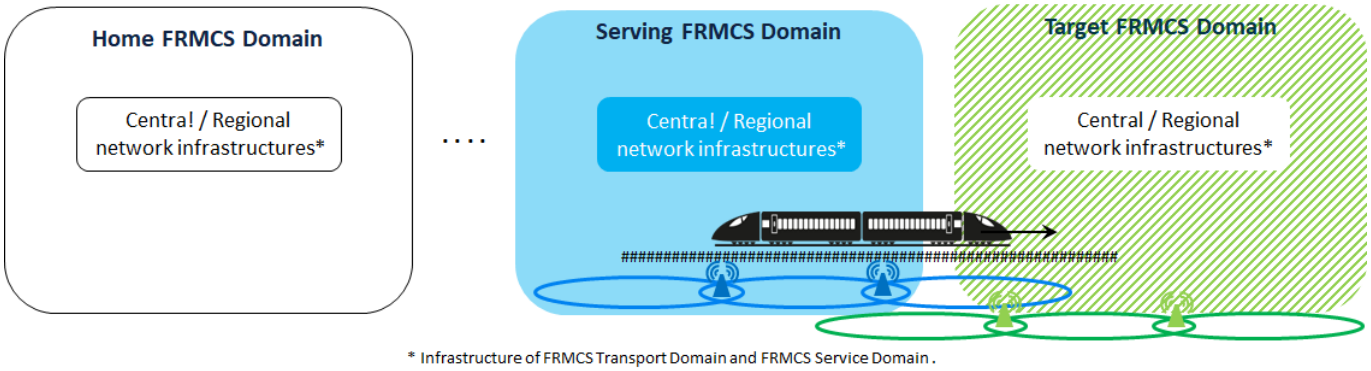


Figure 10-1. An example of an Inter-FRMCS-Domain transition

10.1.3.1.6 The Inter-FRMCS-Domain Transition is described below through two constituent procedures, namely Inter-FRMCS-*Transport*-Domain transition, and Inter-FRMCS-*Service*-Domain transition. (I)

10.1.3.2 Inter-FRMCS-Transport-Domain Transition (IFTDT)

10.1.3.2.1 The IFTDT is of one of the following types (I):

- For IFTDT Type A, the Target OBF RM is chosen among the OBF RMs which are not Serving OBF RM.
- For IFTDT Type B, the Target OBF RM is the same as Serving OBF RM.

10.1.3.2.2 For IFTDT Type A, the ongoing communication services (if any), carried by the Target OBF RM before the NTT, might be dropped during the network transition. (I)

Editor's Note: The state notifications in section [7.1.5.7.7] can be used to inform the corresponding applications (which are neither ATP nor VAS, due to requirement of IFTDT Type A in clause 10.1.3.2.1) of the dropping of the communication service due to Network Transition.

10.1.3.2.3 The procedures for IFTDT types A and B shall comply to [TS 103 765-1]. (M)

10.1.3.2.4 **Intentionally deleted**.

10.1.3.2.5 For an On-Board FRMCS supporting ATP, the IFTDT shall make use of IFTDT Type A. (M)

10.1.2.3.5i For an On-Board FRMCS supporting ATP, the IFTDT shall be either IFTDT Type A or IFTDT Type B. (M-V3)

Editor's Note: solution to support IFTDT Type B (i.e., using one OBF RM) is under investigation but not in scope of FRMCS v2.

10.1.3.2.6 For an On-Board FRMCS not supporting ATP, the IFTDT shall make use of either IFTDT Type A or IFTDT Type B. (M-V3)

10.1.3.2.7 The IFTDT of types A and B shall be supported in the FRMCS Transport Domain. (M)

10.1.3.2.8 The Inter-FRMCS-Transport-Domain transition shall be considered as completed when the FTD_AVL state is reached in the Target FRMCS Transport Domain using the Target OBF RM. (M)

Note: The states within On-Board FRMCS are defined in section [7.1.5.12].

10.1.3.3 Inter-FRMCS-Service-Domain Transition (IFSDT)

10.1.3.3.1 The Inter-FRMCS-Service-Domain Transition procedure shall rely on obtaining an authorization of an FRMCS Service User ID in the Target FRMCS Service Domain, for the FRMCS User corresponding to a locally-bound application. (M)

10.1.3.3.2 The procedure in clause [10.1.3.3.1] is referred to, in the following, as FRMCS-Service-User-Migration and at the completion of the procedure the FRMCS Service User is considered as being "Migrated". (I)

10.1.3.3.3 The procedures for IFSDT shall comply to [TS 103 765-2]. (M)

10.1.3.3.4 Following onboard application types with respect to IFSDT are considered (I):

- Type I: Interoperable IM applications (e.g., ATP, ATO, REC, driver-controller voice communication).
- Type II: Non-interoperable IM applications.
- Type III: Interoperable RU applications.
- Type IV: Non-Interoperable RU applications in the scope of FRMCS (e.g., TCMS).

Note: The “interoperability” in the above clause refer to the “railway interoperability” in Europe.

10.1.3.3.5 For locally-bound applications of Type I, at the completion of Inter-FRMCS-Domain transition, the FRMCS Service User shall be served by the Target FRMCS Service Domain (i.e., FRMCS Service User Migration to Target FRMCS Service Domain shall be performed). (M)

10.1.3.3.6 For locally-bound application(s) of Type IV, the FRMCS Service User shall be served by the Home FRMCS Service Domain (i.e., FRMCS Service User Migration shall not be performed). (M-V3)

Editor’s Note: The behaviour of applications of Type II and III with respect to the Network Transition is not known yet.

10.1.3.3.7 **Intentionally deleted**.

10.1.3.3.8 The Target OBF RM provides transport bearers for signaling and media communications of the migrated FRMCS Service Users. (I)

10.1.3.3.9 The IFSDT shall be considered as completed when the FRMCS Service User in Target FRMCS Service Domain (see clause [10.1.3.3.1]) reaches the FSD_AVL state (see section [7.1.5.12]). (M)

Editor’s Note: at certain moment, the Target FRMCS Service Domain becomes the Serving FRMCS Domain (the moment depends on the solution). For a train which is crossing one or multiple borders within its area of use, the MC Service User IDs obtained on each of the FRMCS Service Domains before this new Serving FRMCS Service Domain need to be marked as “migrated” in the corresponding MC Service Servers.

10.1.3.3.10 **Intentionally deleted**.

10.1.3.3.11 A set of notifications towards onboard applications are exposed by On-Board FRMCS in the context of Inter-FRMCS-Domain transition (see section [10.1.7]) which allow the application to recover communications as soon as FRMCS is available. (I)

10.1.3.3.12 Service continuity requirements within FRMCS (as defined in section [10.1.6]) shall be applied to REC and ATP. (M)

10.1.4 GSM-R to FRMCS Transition for On-Board FRMCS

10.1.4.1 The transition from GSM-R to FRMCS shall make use of a Target OBF RM, which is not a Serving OBF RM. (M)

Note: in a mixed scenario where, upon the reception of NTT by On-Board FRMCS, an Inter-FRMCS-Domain transition is performed for ATP communication services while GSM-R to FRMCS transition is performed for VAS, the Target OBF RM for both procedures can be the same OBF RM.

10.1.4.2 Upon the reception of the NTT implying a transition from GSM-R to FRMCS (see clause [10.1.2.4]), the On-Board FRMCS shall perform the GSM-R to FRMCS transition procedure. (M)

10.1.4.3 The transition from GSM-R to FRMCS shall be considered as completed in the transport stratum when the FTD_AVL state (see section [7.1.5.12]) is achieved in the Target FRMCS Transport Domain, using the Target OBF RM. (M)

10.1.4.4 The transition from GSM-R to FRMCS in the service stratum shall be considered as completed for a given FRMCS Service User when the FSD_AVL state (see section [10.4]) is reached for that user in the Target FRMCS Service Domain. (M)

Note: If the Target FRMCS Domain is not the Home FRMCS Domain, this procedure might include an FRMCS-Service-User-Migration.

10.1.4.5 The IMS/SIP Core credentials needed for clause [10.1.4.4] shall be available in On-Board FRMCS prior to GSM-R to FRMCS transition. (M)

10.1.4.6 The procedure for GSM-R to FRMCS transition procedure shall comply to [TS 103 765-1] and [TS 103 765-2]. (M)

Editor's Note: The NTT is sent to On-Board FRMCS when at least one FRMCS Service User needs to move to the Target FRMCS Domain. A special situation is when in the Target domain both GSM-R and FRMCS are available. ATP coordinating function by default prioritizes operating over FRMCS but this choice within VAS is left to IM/RU. Having registered users for the same application in both GSM-R and FRMCS at the same time should be prevented by implementation.

10.1.5 FRMCS to GSM-R Transition

10.1.5.1 For ATP, the transition from FRMCS to GSM-R relies on an EDOR registration in the target GSM-R network. (I)

10.1.5.2 The trigger for EDOR registration is internal to the "RBC transition FRMCS domain -> GSM-R domain" procedure defined in [Subset-026]. (I)

10.1.5.3 The FRMCS to GSM-R transition for VAS is described in clause [24.2.6.3]. (I)

10.1.6 FRMCS Service Continuity

10.1.6.1 The service continuity requirements within FRMCS, for an ongoing point-to-point communication, are only relevant as long as the application end-points are kept the same before and after transition. (I)

10.1.6.2 The service continuity requirements within FRMCS, for an ongoing group communication, are only relevant as long as the FRMCS Service User is a participant of the same group communication before and after transition. (I)

10.1.6.3 Service continuity for an ongoing group communication within FRMCS shall imply that the Inter-FRMCS-Domain transition shall be transparent to the application. (M-V3)

10.1.6.4 For a REC whose addressed area is extended over both Serving and Target FRMCS Domains, if FRMCS Service User is involved in this REC group before the IFDT, the FRMCS Service User shall rejoin the same REC group following IFDT, without any need for an action from driver. (M-V3)

10.1.6.5 If the train is moving towards the addressed area of an ongoing REC group in Target FRMCS Domain, the FRMCS Service User shall join this REC group communication following IFDT, without any need for an action from driver. (M-V3)

10.1.6.6 For ATP, the service continuity implies that: (M)

1. IFDT shall not release the opened sessions on OB_{APP} and TS_{APP} APIs for an ongoing E2E ATP connection, and
2. the interruption time of service due to IFDT is within acceptable interruption time of ATP.

10.1.6.7 The acceptable respective interruption times that shall guarantee the requirements in clauses [10.1.6.3] to [10.1.6.6] are defined in Annex A. (M-V3)

10.1.7 Notifications provided in the frame of Network Transition

10.1.7.1 The On-Board FRMCS states and the notifications, as defined in section [7.1.5.12] and [7.1.5.7.7], are used in this section. (I)

10.1.7.2 Upon achieving FTD_AVL state in the Target FRMCS Domain following the reception of an NTT, the On-Board FRMCS shall be able to send an FTD_AVL_NOTIF, with the reason set to “Network Transition” and the intended FRMCS Domain set to the Target FRMCS Domain to an application. (M)

Editor’s Note: This notification is at least exploitable by VAS in order that the corresponding FRMCS Service Client initiates the MC Service user migration in the right MC system (deduced from the information of the FRMCS Transport Domain provided in the notification).

10.1.7.3 For locally-bound TC applications of Type I (see clause [10.1.3.3.4]), the reception of FTD_AVL_NOTIF of clause [10.1.7.2] can trigger the transition of the corresponding FRMCS service users to the Target FRMCS Service Domain. (I)

10.1.7.4 Depending on the current serving technology for a given service user, clause [10.1.7.3] implies either an Inter-FRMCS-Service-Domain transition or a GSM-R to FRMCS transition has been performed. (I)

10.1.7.5 Upon achieving the FSD_AVL state in the Target FRMCS Domain following the reception of an NTT, the On-Board FRMCS shall be able to send an FSD_AVL_NOTIF, with the reason set to “Network Transition” to an application. (M)

10.1.7.6 For locally-bound LC applications of Type I, the FSD_AVL_NOTIF of clause [10.1.7.5] can be used as a trigger for re-establishing the communication on application level. (I)

10.2 Interconnection

10.2.1 Introduction

10.2.1.1 The FRMCS system provides communication services between FRMCS users belonging to two or more FRMCS Service Domains when interconnection is implemented. (I)

10.2.1.2 An FRMCS user can communicate with a FRMCS user belonging to another FRMCS domain. (I)

10.2.1.3 An FRMCS user can communicate using the private communication service (point-to-point communication) between interconnected FRMCS Service Domains. (I)

10.2.1.4 An FRMCS user can communicate using the group call communication service between interconnected FRMCS Service Domains. (I)

10.2.1.5 To allow such communication services, FRMCS domains are interconnected using FS_{NNI} as described in clause 10.3. (I)

10.2.1.6 Requirements

10.2.1.7 The following communications shall be supported between interconnected FRMCS Service Domains: (M)

1. MCPTT ad hoc group emergency alert (REC-Alert).
2. MCPTT ad hoc group communication for emergency group call (REC-Voice)
3. MCPTT ad hoc group communication for normal group call.
4. MCPTT private call

10.2.1.8 Floor control for group calls over interconnected FRMCS Service Domains shall be supported. (M)

10.2.1.9 The MCData IP Connectivity shall be supported between interconnected FRMCS Service Domains. (M)

10.2.1.10 The FRMCS system shall support the use of Functional Alias as the identifier of the initiator of a MCPTT private call between interconnected FRMCS Service Domains, for the purpose of presentation. (M)

10.2.1.11 The FRMCS system shall support the use of Functional Alias as the identifier of the recipient of a MCPTT private call between interconnected FRMCS Service Domains, for both call routing and presentation purposes. (M)

10.2.1.12 The FRMCS system shall support the use of Functional Alias as the identifier of the initiator of a group call between interconnected FRMCS Service Domains, for the purpose of presentation. (M)

10.2.1.13 The FRMCS system shall support the use of Functional Alias as the identifier(s) of the participants of a group call between interconnected FRMCS Service Domains, for the purpose of presentation. (M)

10.2.1.14 The FRMCS system shall support the use of Functional Alias as the identifier of the remote host of a MCData IP Connectivity between interconnected FRMCS Service Domains, for the purpose of routing. (M)

10.2.1.15 The FRMCS service users involved in a communication between interconnected FRMCS Service Domains are served either by their Home FRMCS Service Domain or by a Foreign FRMCS Service Domain. (I)

10.2.1.16 Each interconnected FRMCS Service Domain shall maintain only the location of its authorised FRMCS service users. (M)

10.2.1.17 The QoS and priority of communication services between interconnected FRMCS Domains shall comply with chapter 14 and Annex A. (M)

10.3 FS_{NNI} requirements

10.3.1 The FS_{NNI} shall support necessary functionalities for performing the inter-domain HTTP signaling and SIP signaling relevant for Inter-FRMCS-Domain transition (see section [10.1.3]). (M)

Note: for example, the HTTP signaling for Inter-domain MC user authentication [TS 33.180], and SIP signalling for migration to partner MC system [TS 23.280].

10.3.2 The FS_{NNI} shall support the Home-Routed communications, i.e., when OBF RM is registered to a foreign FRMCS Transport Domain, but FRMCS Service User is served on the Home FRMCS Service Domain. (M)

10.3.3 The FS_{NNI} shall support communication services between MC Service Users served by different FRMCS Service Domains (see section [10.2]). (M)

Note: One side or both sides can be a migrated MC Service User(s).

10.3.4 Based on bilateral agreement between FRMCS Operators of interconnected FRMCS domains, topology hiding may be required. (I)

10.3.5 If topology hiding between interconnected FRMCS domains is required, additional network functions shall be provided as defined in [TS 103 765-1] and [103 765-2]. (M)

10.4 Intentionally deleted.

11 Identifiers

11.1 Introduction

11.1.1 International standardisation of identifiers representing 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 railways will depend upon the railway FRMCS Domain configuration, its interconnection with other railway FRMCS Domains and its interconnection with non-FRMCS Systems, e.g., MNOs. (I)

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

11.1.5 There are different identities and addresses for all communication purposes of the FRMCS system needed, e.g., an identity defined for registration and authentication with the FRMCS system, and one or more identifiers to be provisioned for communication purposes. (I)

11.1.6 An identity can be associated with a human user, a machine type application, or a service. The identity may be used for registration, authorisation and authentication purposes. (I)

11.1.7 For identifiers which will not traverse the boundaries of the FRMCS system (internal), their structure will follow the FRMCS internal requirements. (I)

11.1.8 For identifiers which will traverse the boundaries of the FRMCS system (external) their structure will strictly follow the external requirements for interoperability. (I)

11.2 Scope

11.2.1 The scope of this chapter is: (I)

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

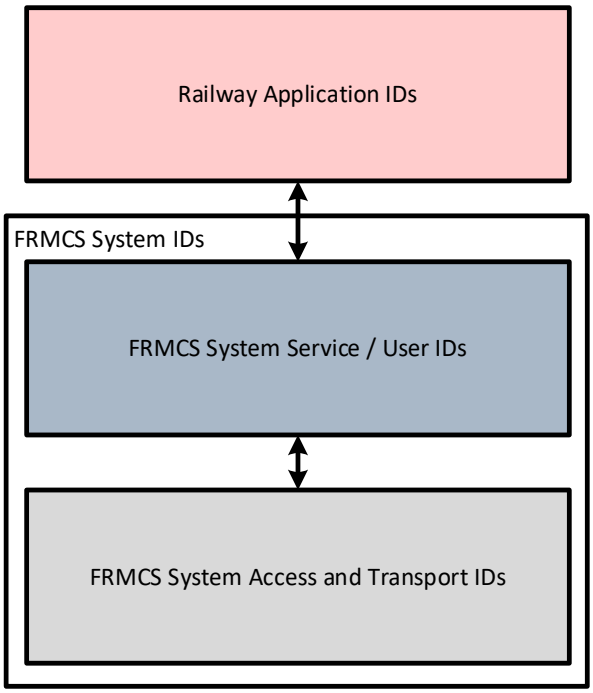


Figure 11-1: FRMCS identities

11.2.1.2 To define the structure of FRMCS System identifiers which are used to obtain communication service sessions for identified and authorized FRMCS users. (I)

11.2.1.3 To ensure that the Functional Addressing (FA) scheme as defined in the Functional Requirements Specification [FRMCS-FRS], chapter §6, is supported. (I)

11.2.1.4 The following items are out of scope for this chapter: (I)

11.2.1.5 To describe the interworking of identifiers for FRMCS ↔ GSMR and for FRMCS ↔ other networks. This is being described by ETSI in [TS 103 792], chapter §6. (I)

11.2.1.6 To define how applications are using identifiers and for which purpose. This is being described in the [FRMCS-FIS], chapter §3.1.2, and the [FRMCS-FFFIS], chapter 9. (I)

11.2.1.7 To define the format and scheme of an Application Identity. This is being described in the [FRMCS-FFFIS], chapter §9.4. (I)

11.2.1.8 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)

11.3 Identifiers 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.mnc<MNC>.mcc<MCC>.3gppnetwork.org>. (M)

11.3.1.3 A single DNN shall cover all packet 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], chapter §5.2.7 DNN = APN, and [TS 23.289], chapters §4.2.2 & 4.3.2 & A.2. (M-Vx)

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

11.3.2 Generic Public Subscription Identifier (GPSI)

11.3.2.1 The GPSI is either an MSISDN or an External Identifier [TS 23.501], chapter §5.9.8. (I)

11.3.2.2 If an MSISDN is associated with the subscription, this MSISDN shall be used as GPSI. (M)

11.3.2.3 The External Identifier, if applicable, shall have the NAI format username@realm as specified by IETF [RFC-7542]. (M)

11.3.2.4 For GPSI, applied NAI format shall be username@realm (as defined in 11.3.2.3), with (M)
username: unique identifier within domain, for security purposes masquerading username according to IETF [RFC-7542]
realm: 5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

11.3.3 Subscription Permanent Identifier (SUPI)

11.3.3.1 The SUPI shall be based on an IMSI according to [TS 23.501], chapter §5.9.2, and [TS 23.003], chapter §2.2. (M)

11.3.4 Subscription Concealed Identifier (SUCI)

11.3.4.1 The SUCI shall have the format according to [TS 33.501], chapters §5.2.5 & 6.1.2 & 6.12.1, [TS 23.003], chapter §2.2 (M):

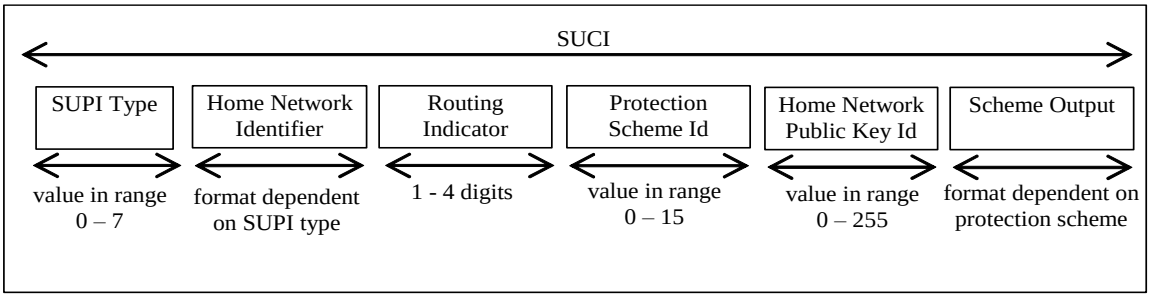


Figure 11-2: SUCI Format [TS 23.003], chapter §2.2

11.3.4.2 SUPI Type shall be 0 (indicating IMSI). (M)

11.3.4.3 Home Network Identifier shall be MCC+MNC. (M)

11.3.4.4 The other values are assigned by the FRMCS operator (no standardised value). (I)

11.3.5 Fully Qualified Domain Names (FQDN)

11.3.5.1 FQDN shall be used for addressing purpose, where standardized. (M)

11.3.6 Transport Stratum Temporary Identifiers

11.3.6.1 Temporary Identifiers of transport stratum supporting security shall be used. (M)

Editor's Note: To be clarified within the MORANE 2 validation project of FRMCS v2 specifications.

11.4 Identities of the FRMCS service stratum

11.4.1 Identification and addressing in the service stratum shall be based on one or more of:

- MC Service ID (M)
- IMS/SIP Core ID (M)

11.4.2 Identities within the FRMCS System only

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

- Mission Critical User Identity (MC ID) [TS 23.280], chapter §8.1.1
- Public Service ID
- MC Service User Identity (MC Service ID) [TS 23.280], chapter §8.1.2
- Role based identities e.g., Functional Alias
- MC Service Group ID [TS 23.280], chapter §8.1.3
- Private User ID (IMPI) [TS 23.228], chapter §4.3.3.1
- Public User ID (IMPU) [TS 23.228], chapter §4.3.3.2

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 to connect with systems outside the FRMCS System

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

- 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 Private User Identity for IMS / SIP Core

11.4.4.1.1 The FRMCS System shall make use of the Private User identities in accordance with [TS 23.003], chapter §13.3. (M)

11.4.4.1.2 The Private User Identity shall include at least MCC and MNC according to [ITU-T E.212]. (M)

11.4.4.1.3 An IMSI identifying a User of a FRMCS system shall be used as Private User Identity within FRMCS. (M)

11.4.4.1.4 An IMSI shall be composed in accordance with [TS 23.003], chapter §2.2. (M)

11.4.4.2 Public User Identity for IMS / SIP Core

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

11.4.4.2.2 The FRMCS System shall make use for Public User Identity in accordance with [TS 23.003], chapter §13.4. (M)

11.4.4.2.3 For any one provisioned Private User Identity, the following Public User Identities shall be supported: (M)

- At least one Public User Identity using SIP URI scheme as defined in [RFC-3261]
- At least one Public User Identity using Tel URI scheme as defined in [RFC-3261]

11.4.4.2.4 A Public User Identity 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 <@>

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

11.4.4.2.6 To support the use of a Public User Identity in E.164 format, the FRMCS shall associate a Tel URI with an alphanumeric SIP URI using the mechanisms specified in [TS 23.228], chapters §4.3.3.3 & 4.3.5.2 & 4.3.5.3, and [TS 24.229], chapter §4.2, in accordance with [IR 65]. (M)

Alphanumeric SIP URIs
- Example: sip:voicemail@example.com

SIP URI using E.164 format
- Example: sip:+447700900123@example.com;user=phone

Tel URI
- Example: tel:+447700900123

11.4.4.3 Public Service Identity

11.4.4.3.1 Public Service Identity shall comply with definitions specified in [TS 23.003], chapter §13.5. (M)

11.4.4.3.2 A Public Service Identity identifies a service like MCPTT, MCData, MCVideo, or a specific resource created for a service on an application server. (I)

11.4.4.3.3 A provisioned Public Service Identity shall follow one of the following URI schemes (M):
- SIP URI (see [RFC-3261])
- Tel URI (see [RFC-3966])

11.4.4.3.4 The domain part shall take the form: (M)
- ims.mnc<MNC>.mcc<MCC>.3gppnetworks.org

11.4.4.3.5 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, other Public Service Identities can be added.

11.4.4.4 Private Service Identity

11.4.4.4.1 Private Service Identity that follows definitions in [TS 23.003], chapter §13.5A does not require further specification or standardization. (I)

11.4.5 MC Identifiers

11.4.5.1 MC identifiers and addressing shall be in accordance with [TS 23.280], chapter §8. (M)

11.4.5.2 Mission Critical User Identity (MC ID)

11.4.5.2.1 MC ID shall follow definitions as specified in [TS 23.280], chapter §8.1.1. (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 Mission Critical User Service Identity (MC Service ID)

11.4.5.3.1 An MC Service ID shall always be used to identify an endpoint for MC signalling and media. (M)

11.4.5.3.2 For each MC ID, one MC service ID shall be provisioned for each MC service if applicable within a FRMCS domain. (M)

11.4.5.3.3 MC Service ID shall follow definitions as specified in [TS 23.280], chapter §8.1.2. (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 out of scope for FRMCS V2.

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 Identity (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], chapter §8.1.3. (I)

11.4.5.4.2 The MC Service Group ID for MCPTT shall be an MC Service Group ID in accordance with [TS 23.379], chapter §8. (M)

11.4.5.4.3 The following labels shall be used for MC Service group IDs for interoperability with GSM-R (M):

- <Group> defined as "group" for VGCS or "broadcast" for VBS
- <GCA> where <GCA> is defined as 5-digit group call area [EIRENE-SRS], chapter §9.9.2
- <GID> where GID is defined as 3-digit group identity [EIRENE-SRS], chapter §9.9.2

11.4.5.4.4 The following labels shall be used for MC service group IDs (M):

- <Group> defined as “group” or “broadcast”
- <Location Label> as defined in clause [11.6.3.4]
- <Group Label> consisting of 41-character maximum, defined as follows (non-exhaustive list):
    - locu (local user),
    - con (controller(s)),
    - od (other drivers),
    - atdia (all train drivers in area)
    - atdioru<RU_Name> (all train drivers of RU name) with <RU_Name> equal all operating RU trains
    - otst (other staff)
    - all (all participants reachable, only applicable in connection when Location Label is used)
    - ad (all drivers reachable, only applicable in connection when Location Label is used)
    - amw (all maintenance workers (exclusive drivers, only applicable in connection when Location Label is used)

11.4.5.4.5 The domain part of the MC Service Group ID shall be the format of the MC System ID defined in section [11.4.5.5]. (M)

11.4.5.4.6 The ad hoc MC Service Group ID for MCPTT shall comply with the following format for requests, but not to be used in a client to server request, if criteria field e.g., location is set, and no previous REC alert was initiated. (M):

- GSMR interoperability format is: <Group>.<GCA>.<GID>@<MC System ID>
- FRMCS only format is: <Group>.<Location Label>.<Group Label>@<MC System ID>

11.4.5.4.7 The pre-defined MC Service Group ID for MCPTT shall comply with the following format (M):

- GSMR interoperability format: <Group>.<GCA>.<GID>@<MC System ID>
- FRMCS only format is: <Group>.<Location Label>.<Group Label>@<MC System ID>

11.4.5.4.8 The MC Service Group ID for MCData shall be an MC Service Group ID in accordance with [TS 23.282], chapter §6A. (M)

11.4.5.5 MC System Identity (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)

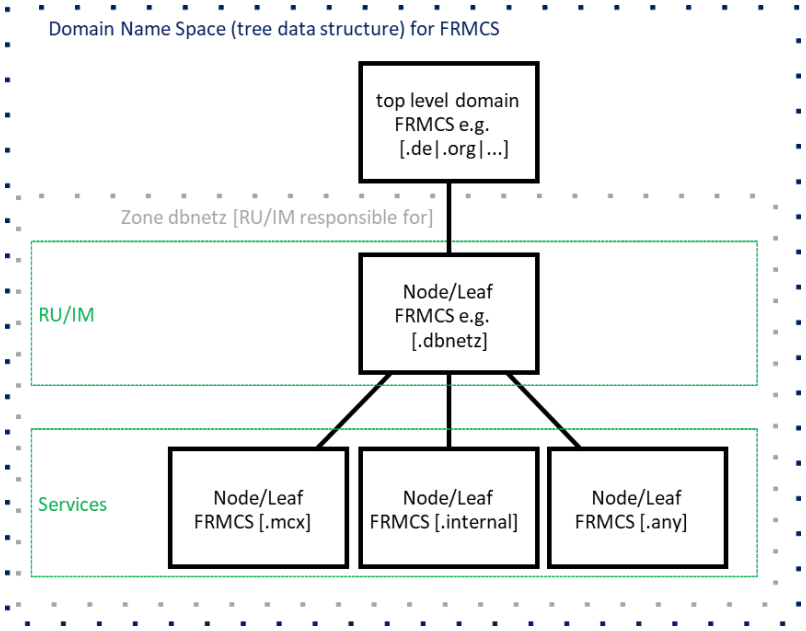


Figure 11-3: Domain Name Space for FRMCS (human-user interaction)

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)

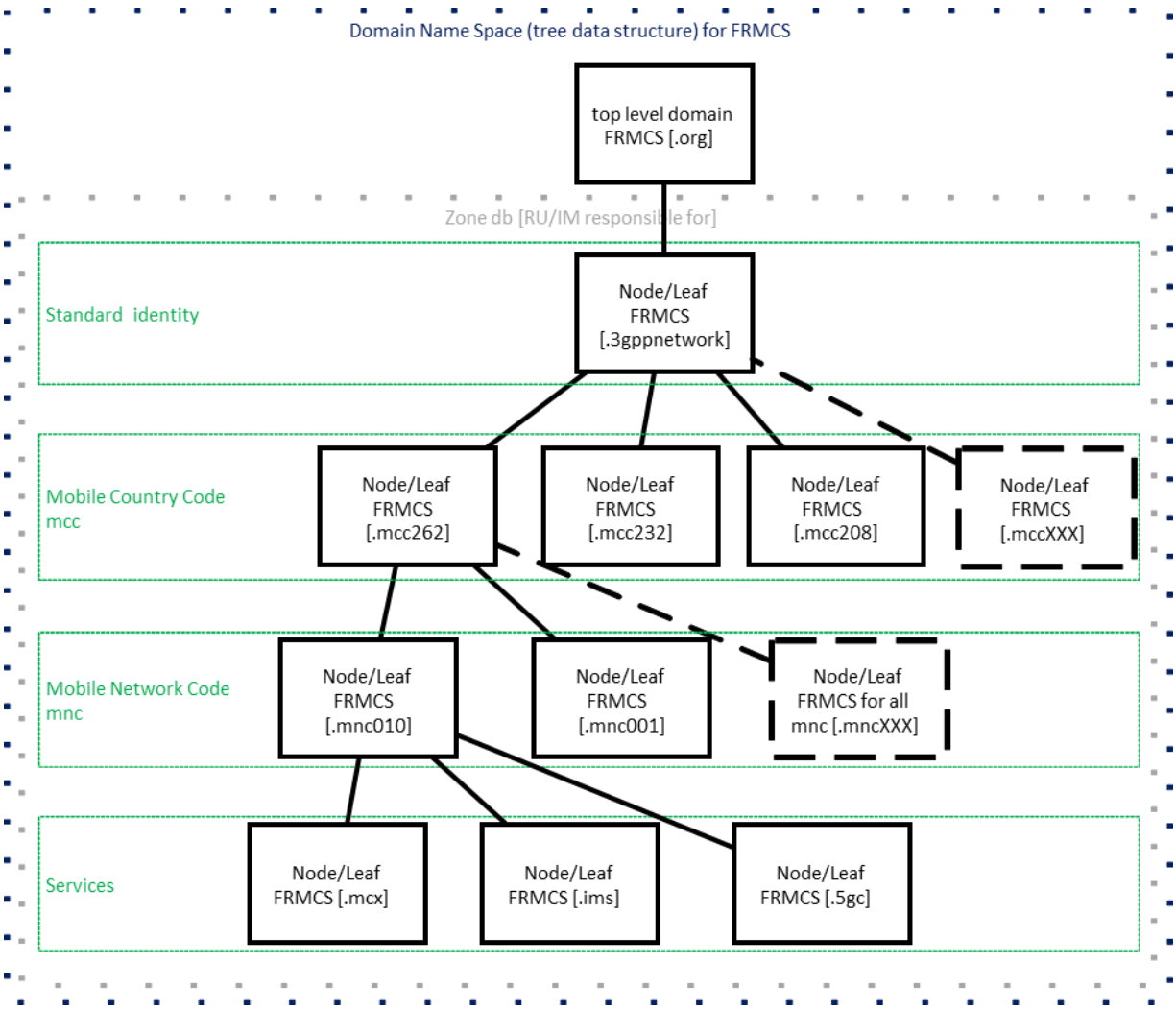


Figure 11-4: Domain Name Space for FRMCS (machine-type communication)

11.4.5.5.4 The domain of the used MC System ID for FRMCS shall be the basis for the definition of any additional sub-domain(s) within the FRMCS system. (M)

11.4.6 Service Stratum Temporary Identifiers

11.4.6.1 Temporary identifiers of service stratum supporting security shall be used. (M)

11.5 Usage and dependencies of different FRMCS identities

11.5.1 Figure 11-5 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)

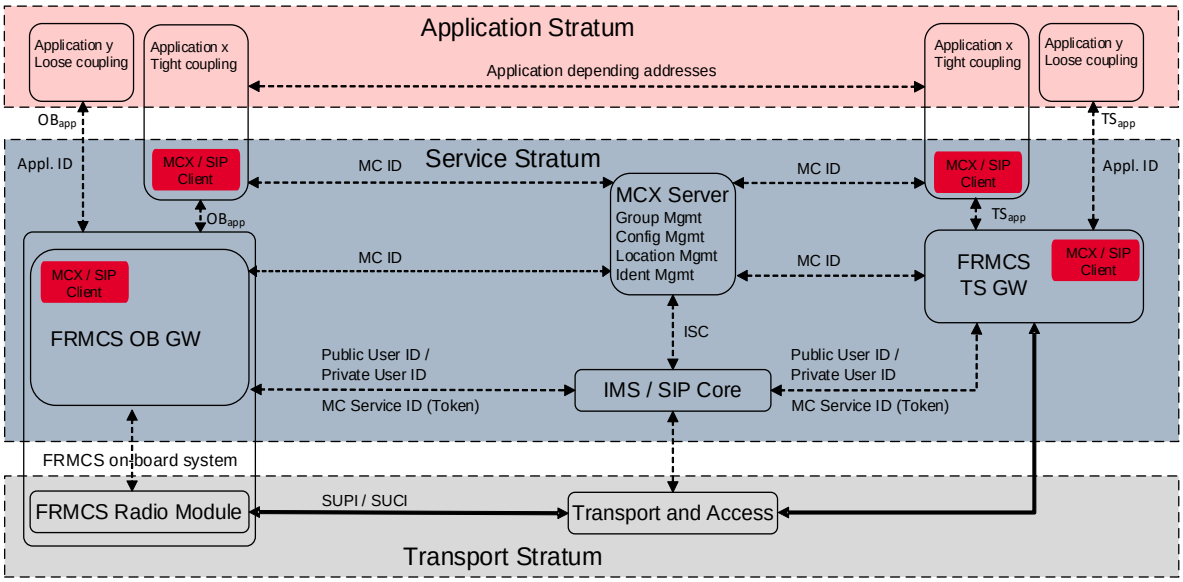


Figure 11-5: Identities and their location

11.6 Role based identification scheme

11.6.1 Identification scheme requirements

11.6.1.1 Within FRMCS, role based identification shall be based on Functional Alias in accordance with [TS 23.280], chapter §8.1.5. (M)

11.6.1.2 Within each FRMCS domain, each train number in GSM-R or Train ID in FRMCS shall be unique for the period of the journey. (M-V3)

11.6.1.3 Every rail operational function shall be identified by a unique functional label conforming with “Table 11-1: Mapping of identifiers and labels”. (M)

11.6.1.4 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)

11.6.1.5 For associating a functional label with an MC Service ID / IMPU, Functional Alias in accordance with the requirements of [FRMCS FRS], chapters §6 & App. D, and [TS 23.280], chapters §7.3.1 & 7.4.2.2.1 & 7.4.2.2.2, shall be used. (M)

11.6.1.6 The FRMCS system shall allow a FRMCS User to have zero, one or more Functional Aliases active. (M)

11.6.2 Identification scheme format

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

a. *** (for national use or for future extensions)
b. Location label
c. Identification label
d. Equipment label*
e. Function label

* Equipment label only present if Identification label used for vehicle identifier.

11.6.2.2 Location label, Identification label, Equipment label and Function label shall be used in accordance with the [FRMCS FRS], chapter 6.1. (M)

11.6.2.3 Identifiers shall have at least one of the following two formats:

a. ***Location_label.Identification_label.Equipment_label. Function_label@Organizational_code (M)
b. ***Location_label.Identification_label.Equipment_label. Function_label@<DomainName> where <DomainName> relies on section [11.4.5.5] (M)

Note: the identifiers defined in this section are not case sensitive.

11.6.2.4 It shall be possible to use the string “###” (three consecutive hashes) as wild card (i.e. with the meaning “all”) (M)

Example

FA: Railway security services chief in location area 1234 → area1234.secure01.@mcx.oebb.at

FA: Railway security team in location area 1234 → area1234.secure###@mcx.oebb.at →

using ### ← wildcard / all

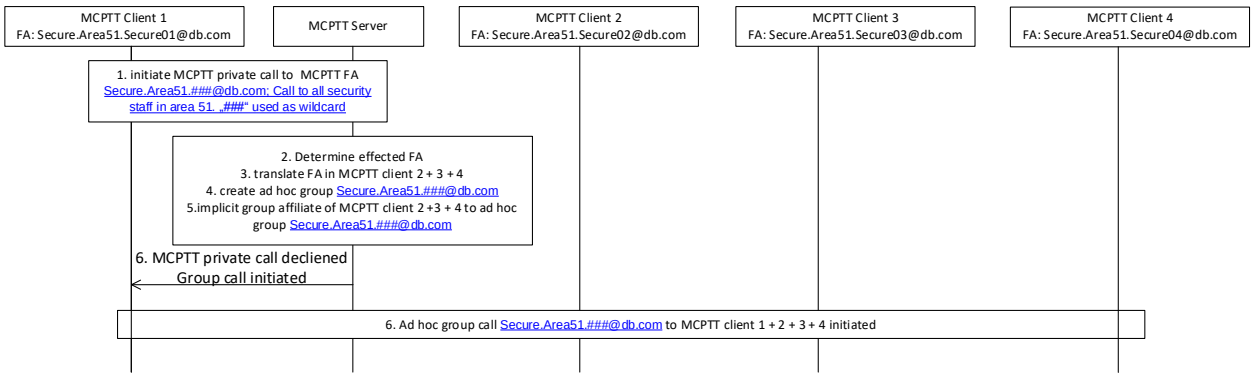


Figure 11-6: Flow wildcard

11.6.2.5 It shall be possible to use an empty (no content) label (M).

11.6.2.6 Example: FA: Train driver / Leading driver / Driver has no location (I):
ice14..Driver01@db.com

11.6.2.7 Table 11-1 shows, which labels shall be used in which identifier. (M)

		naming	Train function identity	Controller identity	Team identity	Vehicle identity	Trackside Equipment identity	Profile Addressing
Location label								
	Area ID			x	x		x	x
Identification label								
	Train ID	*National format*	x					
	Vehicle Identifier	*Nat. / Internat. format*				x		
	Shunting	Shunt			x			
	Maintenance	Maintain			x			
	Railway Security	Secure			x			
	Equipment	Equip					x	
Equipment Label		*Equip*						
	Equipment	Equip				x		
Function label							x	
	Primary controller	Control01		x				
	Secondary controller	Control02		x				
	Power supply controller	ControlPower		x				
	Train driver Leading driver Driver	Driver01	x		x			x
	Driver 2	Driver02	x					
	Driver 3	Driver03	x					
	Driver 4	Driver04	x					
	Driver 5 – reserved for Banking	Driver05	x					
	Intercom	Intercom	x					
	Public address	Public	x					
	Chief conductor	Conduct01	x					
	Second conductor	Conduct02	x					
	Third conductor	Conduct03	x					
	Fourth conductor	Conduct04	x					
	Train crew 5 – 10	Crew05 … Crew10	x					
	Catering staff chief	Cater01	x					x
	Catering 2 -10	Cater02 … Cater10	x					x
	Railway security services chief	Secure01	x		x			x
	Railway security 2 – 10	Secure02 … Secure10	x		x			x
	Switchman	Switchman		x				
	Platform inspector	Platform_Insp		x				

	Railway undertaking dispatcher	RUDispatch		x				
	Technical inspector	TechnInsp		x				
	Train preparation	TrainPrep		x				
	Emergency manager	EmergManag		x				
	All	Wholeteam						x
	Train staff	TrainStaff						x
	Shunting team leader	Shuntmem01			x			x
	Shunting team members	Shuntmem02 … Shuntmem10			x			x
	Maintenance team leader	Mainteam01			x			x
	Maintenance team members	Mainteam02 … Mainteam10			x			x
	Vehicle Equipment Function	VEF01 … VEF25				x		
	Vehicle Equipment ID	VehicleEqtFunc01 … VehicleEqtFunc25						x
	Trackside Equipment Function	*TEF01 … TEF25*					x	
	Trackside Equipment ID	*National format*					x	x
Organisation Code								
	Organisation Code	in accordance with [TAP TSI] / [TAF TSI]	x	x	x	x	x	x
Domain Name								
	Domain Name	Corresponding to sec. 11.4.5.5.2 +11.4.5.5.3						

Table 11-1: Mapping of identifiers and labels

11.6.2.8 Mapping of identifiers and labels as defined in Table 11-1 shall be extensible. (M)

11.6.3 Naming of labels

11.6.3.1 The naming of the labels shall be in accordance with “Table 11-1: Mapping of identifiers and labels”. (M)

11.6.3.2 The train identifier (train ID) shall be allocated by each Railway. (M)

11.6.3.3 Train ID shall be composed of a maximum of 41 alphanumeric characters. (M)

11.6.3.4 The Location Label shall be a

- Area Identifier (Area ID)

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

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

11.6.3.6 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)

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

11.6.3.8 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)

11.6.3.9 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)

11.6.4 Criteria Field

Editor’s Note: Criteria Field e.g. for LDA target_user=”controller of area” is out of scope for FRMCS V2.

11.6.5 Application identifiers

Editor’s Note: the trackside to onboard communication is out of scope of FRMCS v2.

11.6.5.1 The FRMCS system shall provide service to loose coupled applications which fulfil the following requirements of addressing scheme: (M)

- Global uniqueness
- Based on UTF-8

Note: FRMCS may provide mitigation procedures for applications which do not fulfil clause 11.6.5.1.

11.6.5.2 The static identifier [FRMCS-FFFIS], chapter §9.6, provided by the application within onboard local registration might be used within the authentication/authorization process, if not other FRMCS identities are provisioned withing On-Board FRMCS. (I)

11.6.5.3 For any application using FRMCS and OBapp the remote address [FRMCS-FFFIS] chapter §9.4, shall be in the following format, if not defined differently hereafter: (M)

- Unique identifier in URI-format: <identity>@<domain>

11.6.5.4 ETCS application

11.6.5.4.1 Intentionally deleted

11.6.5.4.2 FRMCS Trackside Gateway serving a RBC shall use the following format for Functional Alias activation (M):

- User part: According to [SUBSET-037-3], chapter §6.4.3.2.3
- Domain part: default domain name and if applicable the adjacent country domain name

11.6.5.4.3 FRMCS User [SUBSET-037-3] chapter §6.4.3, provided remote address [FRMCS-FFFIS], chapter §9.4, within a session start request [FRMCS-FFFIS], chapter §9.7, shall be used as user part of the target MC service URI as defined in [SUBSET-037-3], chapter §6.4.3.2.3, see figure 11-7 (M)

6.4.3.2.3 The remote address in "Session start" is:

"id<ETCS-ID>.ty<ETCS ID Type>.cc<NID_C>.ertms"

	formatted as
ETCS-ID	6-digit lowercase hex ASCII string
ETCS-ID type	2-digit lowercase hex ASCII string
NID_C	3-digit lowercase hex ASCII string

Example: id031123.ty08.cc00c.ertms

Figure 11-7: Session start parameter definition [SUBSET-037-3]

11.6.5.4.4 For CFM User application communication to trackside destination, the On-Board FRMCS shall use local domain or organisational code as domain part. (M)

Note: Selection of OC or domain or both is left for implementation.

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

12.1.3 Bearer flexibility is, in the context of this section, realised by means of FRMCS Multipath. (I)

12.1.4 **Intentionally deleted**.

12.1.5 The On-Board FRMCS shall support FRMCS Multipath. (M-V3)

12.1.6 An FRMCS Domain should support FRMCS Multipath. (O-V3)

12.1.7 If FRMCS Multipath is implemented, the requirements in this section are applicable. (I)

12.1.8 If FRMCS Multipath is not supported by the FRMCS Domain, FRMCS Multipath shall not be used by the On-Board FRMCS. (M)

12.2 Out of scope

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

12.3 FRMCS Multipath requirements

12.3.1 FRMCS Multipath shall comply with [TS 103 765-1]. (M)

12.3.2 FRMCS Multipath enables the (sequential or simultaneous) use of Data Paths over multiple Radio Modules on the same or different (transport) domains. (I)

12.3.3 FRMCS Multipath shall provide the capability to utilise Data Paths over one or multiple of the following Transport Domains: (M)

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

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

1. Public MNO networks
2. Non-terrestrial networks
3. WLAN/Wi-Fi

12.3.5 FRMCS Multipath supports the following use cases: (I)

1. Application specific Data Path selection
2. Fallback
3. Coverage extension
4. Resilience through best path selection
5. Resilience through packet replication
6. Capacity extension

12.3.6 FRMCS Multipath is handled by the FRMCS Multipath function (MPF) as illustrated in an outline of the architecture (Figure 12-1). (I)

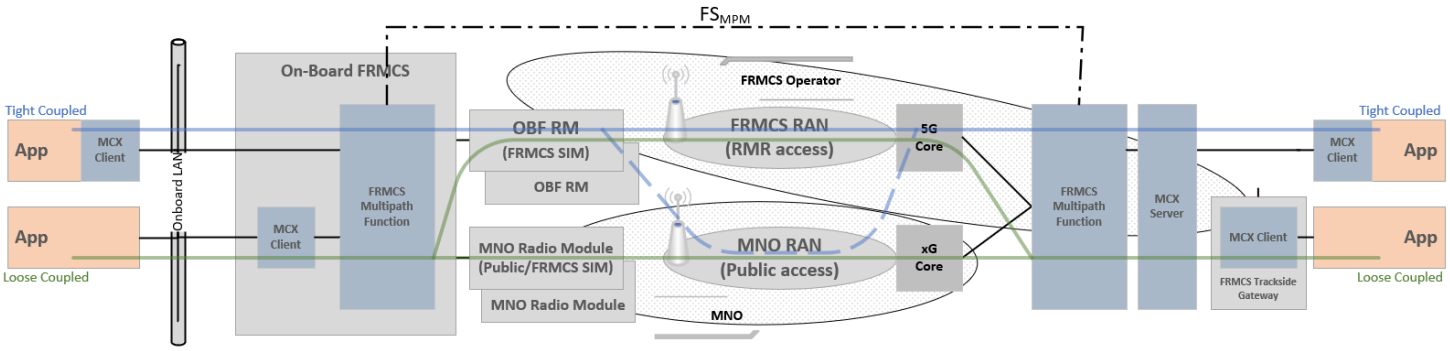


Figure 12-1 Principle of FRMCS Multipath operation (example)

12.3.7 FRMCS Multipath uses one or more Data Paths. The types of Data Paths are by example illustrated in Figure 12-1 (both the loose and tight coupled cases for the FRMCS Service client are shown): (I)

1. FRMCS Multipath uses a Data Path via the FRMCS Domain by using On-Board FRMCS Radio Modules with MOCN/RAN sharing enabled (blue lines connecting a tight coupled application). The Data Path is either established via the FRMCS RAN or via the MNO RAN, indicated by the dashed blue line.

2. FRMCS Multipath uses Data Paths via the FRMCS Domain and MNO Domain via an On-Board FRMCS Radio Module and an MNO Radio Module (green lines connecting a loose coupled application). FRMCS Multipath shall be transparent to the application, i.e. applications are unaware of FRMCS Multipath.

Note: Sharing network resources requires a bilateral agreement between FRMCS Operator and MNO.

12.3.8 The decision which Data Paths to use for a Data Flow shall be transparent to the Application Stratum (i.e. decisions on the usage of Data Paths shall be taken by FRMCS Multipath only). (M)

12.3.9 FRMCS Multipath at the On-Board FRMCS, shall provide a mechanism for selection of one or multiple Data Paths for a given Data Flow. (M)

12.3.10 FRMCS Multipath at the FRMCS Domain, should provide a mechanism for selection of one or multiple Data Paths for a given Data Flow. (O)

12.3.11 FRMCS Multipath at the On-Board FRMCS, shall provide a mechanism for transition between Data Paths of a given Data Flow. (M)

12.3.12 FRMCS Multipath at the FRMCS Domain, should provide a mechanism for transition between Data Paths of a given Data Flow. (O)

12.3.13 FRMCS Multipath at the On-Board FRMCS, should provide a mechanism for splitting of Data Paths of a given Data Flow. (O)

12.3.14 FRMCS Multipath at the FRMCS Domain, should provide a mechanism for splitting of Data Paths of a given Data Flow. (O)

12.3.15 FRMCS Multipath at the On-Board FRMCS, shall provide a mechanism for replication of data on Data Paths of a given Data Flow (M)

12.3.16 FRMCS Multipath at the FRMCS Domain, should provide a mechanism for replication of data on Data Paths of a given Data Flow (O)

12.3.17 FRMCS Multipath shall support functionality for Data Path quality evaluation measurement. Quality measurements are applicable to the On-Board FRMCS and to the FRMCS Domain, to all Active and Candidate Data Paths and to incoming and outgoing data. (M-Vx)

Editor's note: Data Path quality evaluation is out of scope of FRMCS V2 and will be specified in [TS 103 765-1] and [TS 103 765-3].

12.3.18 The MPF at the FRMCS Domain shall use, when applicable, (real-time) information obtained from an MNO (e.g., 5QI of a specific Data Flow or an estimation of transport network latency at the trackside). (M-Vx)

12.3.19 The Multipath Policy is a set of rules for mapping Data Flows to Available Data Paths (in terms of steering criteria). (I)

12.3.20 The Multipath Policy shall have the capability to define static and dynamic rules. Static rules are e.g., allowed Data Paths per Application. Dynamic rules are e.g., QoS/continuity requirements assessment based on Data Path quality measurements). (M-Vx)

12.3.21 The FRMCS Operator shall be able to configure the Multipath Policy for all applications of the FRMCS Domain under its responsibility. (M)

12.3.22 The MPF at the On-Board FRMCS and the MPF at the FRMCS Domain shall provide a mechanism to negotiate the Multipath capabilities (e.g. applicability and protocol to be used) via the FS_{MPM} reference point. (M)

12.3.23 The information elements of the FRMCS Multipath Policy are specified in [TS 103 765-1]. (I)

12.3.24 The MPF at the FRMCS Domain and the On-Board FRMCS shall apply the Multipath Policy. (M)

12.3.25 FRMCS Multipath shall support a control protocol operating using FS_{MPM} with the following functions:

1. Negotiation and selection of the FRMCS Multipath protocol and configuration to be used. (M)
2. Multipath Policy notification from FRMCS Domain to the On-Board FRMCS. (M)
3. Execution and reporting of Data Path quality evaluation measurements. (I)

12.3.26 The MPF at the On-Board FRMCS and at the FRMCS Domain shall support the multipath protocols as identified in [TS 103 765-1]. (M)

12.3.27 The MPF at the FRMCS Domain shall have the capability to negotiate the use of a single one of those protocols between On-Board FRMCS and FRMCS Domain as imposed by the FRMCS Multipath Policy. (M)

12.3.28 The MPF at the FRMCS Domain shall apply the FRMCS Multipath Policy when the On-Board FRMCS enters its domain. (M)

12.3.29 **Intentionally deleted**.

12.3.30 The Multipath Policy and configuration shall be communicated to the On-Board MPF via the FS_{MPM} reference point. (M)

12.3.31 **Intentionally deleted**.

12.3.32 **Intentionally deleted**.

12.3.33 **Intentionally deleted**.

12.3.34 To enable FRMCS Multipath, the On-Board FRMCS shall support multiple Radio Modules. (M)

12.4 Multi-Operator Core Network (MOCN)

12.4.1 MOCN allows multiple MNOs to share network infrastructure. In the context of FRMCS, the RAN of one or more MNOs are shared with the FRMCS Operator. (I)

12.4.1i A MOCN access is under the control of the 5G Core Network of an FRMCS Domain in terms of quality of service. (I)

12.4.2 MOCN requires a bilateral agreement between FRMCS Operator and MNO. (I)

12.4.3 MOCN shall support functionality as specified in [TS 103 765-1]. (M-V3)

13 Network slicing

13.1 Introduction

13.1.1 Network slicing allows to provide customised networks. (I)

13.1.2 A network slice can provide the functionality of a complete network, including radio access network functions, core network functions and IMS functions. One network can support one or several network slices. (I)

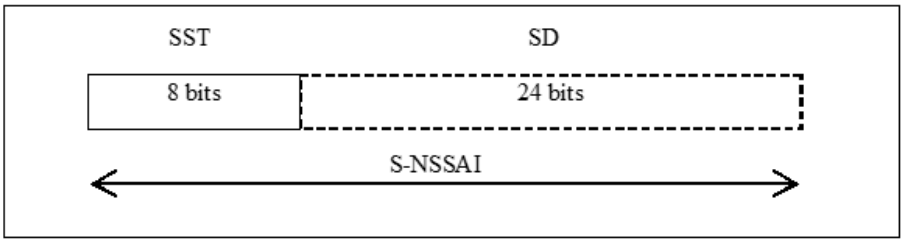
Editor's note: As Network Slicing is a mandatory feature to be supported by 5G System, the need to support Network Slicing Non-Access Stratum protocols & default S-NSSAI by FRMCS system is to be confirmed, even if network slicing is not implemented by FRMCS Operators.

13.2 Out of scope

13.3 General requirements

13.3.1 Single Network Slice Selection Assistance Information (S-NSSAI)

13.3.1.1 The S-NSSAI shall have the format according to [TS 23.003 V18.4.0] clause 28.4.2 (M-V3):



13.3.1.2 For the Slice Service Type (SST), railways shall define a dedicated default SST. (M-V3)

13.3.1.3 The Default S-NSSAI for FRMCS shall not use the Slice Differentiator (SDs) value. (M-V3)

13.3.1.4 Network slicing shall be reduced for FRMCS to use a single Default S-NSSAI (M-V3)

13.3.1.5 The 5GS subscription information shall contain the Default S-NSSAI at the 5GS UDM. (M-V3)

Editor's note: Usage of additional S-NSSAI is out of scope for FRMCS V2.

13.3.1.6 The subscription information of the Default S-NSSAI shall contain:

- one Default DNN that is used by the Default S-NSSAI (M-V3)
- the indication that the S-NSSAI is the Default S-NSSAI (M-V3)
- the indication whether the Default S-NSSAI is subject to or not "NW Slice-Specific Authentication and Authorization". (M-V3)

13.3.1.7 For a UE in a VPLMN, the UDM of the HPLMN shall provide the Default S-NSSAI only. (M-V3)

13.3.1.8 The Default S-NSSAI for FRMCS is agreed by all FRMCS system partners or an organization representing them, and the value of the Default S-NSSAI shall be a standardized value from the 3GPP [TS 23.501 V18.4.0] clause 5.15.2.2. (M-V3)

13.3.1.9 The Default S-NSSAI for FRMCS shall use the 3GPP-standardized SST value "4" vehicle to everything communication (V2X) [TS 23.501 V18.4.0] clause 5.15.2.2. (M-V3)

Editor's note: Different value of SST possible e.g., 3GPP standardized railway specific value is under investigation.

13.3.1.10 The Default S-NSSAI for MNO connectivity shall be different. (M-V3)

14 Quality of Service and Priority

14.1 Introduction

14.1.1 For operational purposes, railway applications raise individual requirements on the quality of the data exchange towards the communication system. (I)

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

14.1.3 The QoS depends on the end-to-end (E2E) path at which it is experienced/measured with clearly defined end-points. (I)

14.1.4 As illustrated in Figure 14-1, the application E2E path, i.e., experienced from railway application perspective can be subdivided into the FRMCS E2E path and the portions related to the IP networks (external to FRMCS) to interconnect the railway applications with the FRMCS system. (I)

Note1: As illustrated in Figure 14-1, the E2E QoS a human user experiences by using an application (e.g. mouth-to-ear delay for a voice call) includes the application E2E path as well as portions related to the application itself (e.g. voice processing).

Note2: The IP networks that interconnect the railway applications with the FRMCS system are outside the boundaries of FRMCS.

Note3: QoS can in principle also be applied to non-FRMCS domain networks (with reference to ETSI).

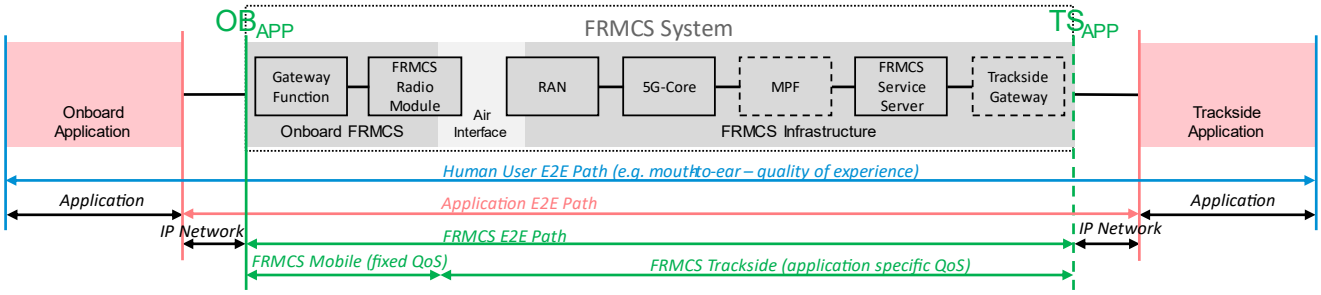


Figure 14-1: Subdivision of E2E path into sub-systems and components. For the connection of trackside applications, also TS_{CTRL} reference point is considered (see Chapter 6).

14.1.5 The FRMCS E2E path is subdivided into an onboard subsystem (On-Board FRMCS) and an infrastructure-side subsystem (FRMCS Infrastructure), which includes the air interface, and spans from the OB_{APP} reference point to the TS_{APP} reference point, as introduced in chapter 6. (I)

Note 4: Applications at trackside can be connected via TS_{APP} or TS_{CTRL} (see Chapter 6).

14.1.6 The On-Board FRMCS as well as the FRMCS Infrastructure consist of FRMCS components & subsystems, as introduced in chapter 6. Each of the components need to fulfil individual QoS requirements based on the composition of data traffic from multiple railway applications. (I)

14.1.7 Based on 3GPP QoS mechanisms, the path between the On-Board FRMCS Radio Module and the 5G Core (including the Radio Access Network and the Air Interface) can be configured with QoS per individual communication session. (I)

Note: Communication sessions can refer to application specific data exchange as well as FRMCS service stratum related signalling. An application may utilize multiple communication sessions with different QoS requirements.

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

14.1.9 To this extent, to reflect the different importance of railway applications and its associated communication sessions, priorities indicate the order at which the QoS requirements of the communication sessions should be served. (I)

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

Note: The QoS and priority handling for non-3GPP access is subject to implementation.

14.1.11 The detailed 3GPP QoS mechanisms as well as its translation to radio resource allocation is described in [TS 23.502], [TS 38.331] and references therein. (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 section (see Annex A). (I)

14.2.2 The requirements referring to the interaction with the human user (e.g., for arbitration) are out of scope of this section. (I)

14.2.3 The QoS requirements subject to the application processing is out of scope of this section. (I)

14.2.4 The QoS measurement procedures are out of scope of this section. (I)

14.3 Generic Requirements

14.3.1 To provide the required level of communication quality, the FRMCS system allocates the necessary resources by transport stratum means and harmonised RMR spectrum, targeting to fulfil the QoS requirements of the individual communication sessions. (I)

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 as described in [TS 23.501], to give preference for higher priority communication sessions. (M)

14.3.3 The FRMCS system supports various QoS parameters to reflect the different QoS requirements of the railway applications. (I)

14.3.4 The FRMCS system shall allow to associate individual QoS requirements to a communication session, independent of the QoS requirements 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)

14.4 FRMCS E2E QoS Requirements

14.4.1 Introduction

14.4.1.1 The QoS requirements towards the FRMCS system are specified based on Key Performance Indicators (KPIs). (I)

14.4.1.2 The E2E KPIs are defined between a transmitting entity called “source” and a receiving entity called “destination”, both located at the FRMCS system boundaries (e.g., OB_{APP}, TS_{APP}). (I)

14.4.2 Packet Latency and Packet Reliability

14.4.2.1 Packet 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 packet latency, to the total number of sent network layer packets. (I)

14.4.3 Data Rate

14.4.3.1 Data rate is the amount of data transmitted from the source to the destination within a specified period of time. (I)

14.4.3.2 The data rate for a communication session is coupled with a percentage (e.g., 95%) for which the data rate is achieved within a 100 meters interval. (I)

Note: The data rate is measured based on IP packets for the communication session of interest. The measurement procedure for achieving the target data rate within the 100 meters interval is out of scope of this chapter.

14.4.4 Session Setup Time

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

Note1: The session setup time includes the authorization of the QoS flow as well as the MCX session. Here MCX session setup time excludes the initial MC ID authentication, authorization and registration.

Note2: The session setup time excludes FRMCS registration as well as any application layer processing and human interaction.

Note3: For interconnecting multiple FRMCS Service Servers a deviation from the session setup times is acceptable.

14.4.4.2 The FRMCS system supports two classes, Immediate and Normal (I):

- 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 4 second for 95% of the cases. (M)

14.4.4.4 The normal communication session establishment time shall not exceed 10 seconds for 95% of the cases. (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 in accordance to [TS 22.179] 6.15.3 and 6.15.4. (M)

Note: Any application layer processing and human interaction is out of scope of this section.

14.4.6 Audio Codecs

14.4.6.1 For QoS measurement, the AMR-WB codec scheme, in accordance with [TS 103 765-2, section 5.2] and [TS 26.179, section 4.1.1] shall be supported. (M)

14.4.6.2 For QoS measurement, the EVS codec scheme, in accordance with [TS 103 765-2, section 5.2] and [TS 26.179, section 4.1.1] should be supported. (O)

14.4.7 Communication Session Specific KPI Values

14.4.7.1 The KPI target values for the individual communication sessions (e.g., referring to railway applications) shall be in accordance with Table A.1-1 Annex A. (M-V3)

Note: A deviation from the target KPIs mentioned in Annex A for special scenarios, e.g., network transition, multipath is acceptable.

14.5 Component QoS parameters

14.5.1 The packet latency for processing and packet forwarding at the On-Board FRMCS shall be considered to not exceed 15 ms for 99,9% of the packets on network layer. (M-V3)

14.5.2 The time elapsed between powering on the On-Board FRMCS Radio Module and the successful registration at the FRMCS Infrastructure (including the successful registration of the MC Service user) via an On-Board FRMCS Radio Module shall be considered to not exceed 35 s for 99% of the cases. (M-V3)

Note: The target time is under the condition that the On-Board FRMCS Radio Module is within the coverage area of FRMCS Infrastructure.

14.5.3 The packet latency for the connection between an onboard application and the On-Board FRMCS is considered to not exceed 5 ms for 99,9% of the packets. (I)

14.5.4 The packet latency for the connection between a trackside application and the FRMCS Infrastructure is considered to not exceed 50 ms for 99% of the packets. (I)

Note: the KPI values above are based on the derivations of Annex A and [SUBSET-093]

14.6 3GPP QoS Parameters

14.6.1 General

14.6.1.1 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)

14.6.1.2 The 3GPP QoS parameters describe the packet forwarding treatment that is supported between UE and 5G Core (more specifically 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 paths outside the FRMCS E2E system are subject to the respective local networks.

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

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

14.6.2 Standardized 5QI

14.6.2.1 The FRMCS system shall support the standardized 5QI values 5, 8, 65, 69 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)

14.6.2.2 The FRMCS system should support the standardized 5QI values 70. (O-Vx)

Note: Investigations are needed if e.g., chipset and other components can be met this requirement.

14.6.3 Maximum Flow Bit Rate (MFBR)

14.6.3.1 For applications associated with guaranteed bit rate (see [TS 23.501]), an MFBR is specified. (I)

14.6.4 Guaranteed Flow Bit Rate (GFBR)

14.6.4.1 For applications associated with guaranteed bit rate (see [TS 23.501]), a GFBR is specified. (I)

14.6.5 Allocation and Retention Priority (ARP)

14.6.5.1 Communication sessions require differentiation based on urgency to ensure appropriate allocation of transport resources. This allows for prioritized allocation of resources based on the criticality of each session. (I)

14.6.5.2 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)

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

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

Note 2: The mapping of ARP values is based on the considerations of [FRS]

14.6.6 Communication Session Specific 3GPP QoS Parameter Values

14.6.6.1 The 3GPP QoS parameter values that shall be applied for dedicated communication sessions are listed in Annex A (M-V3).

14.7 QoS Signalling and Monitoring

14.7.1 The QoS requirements and priorities of all relevant communication sessions (according to Annex A) shall be known to the FRMCS Infrastructure. (M)

14.7.2 The 5G System shall implement the 3GPP parameters referenced in Section 14.6 as specified in Annex A for user plane traffic. (M)

14.7.3 5G Core shall identify the required QoS and priority treatment of a communication session based on the indications provided by the MC Service Server. (M)

14.7.4 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)

14.7.5 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, as specified in Annex A. (M)

14.7.6 The QoS monitoring is subject to 3GPP mechanisms as well as to the specification of the multipath function. (I)

14.7.7 Any notifications of the QoS status towards the application is subject to the Notification Function. (I)

14.7.8 The detailed signalling and enforcement procedures of the FRMCS QoS and priority framework is based on 3GPP mechanisms defined for the 5G System in transport stratum and the Mission Critical services in service stratum and is specified within [FRMCS-FIS], [TS 103 765-1] and [TS 103 765-2], respectively. (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 **Intentionally deleted**.

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.

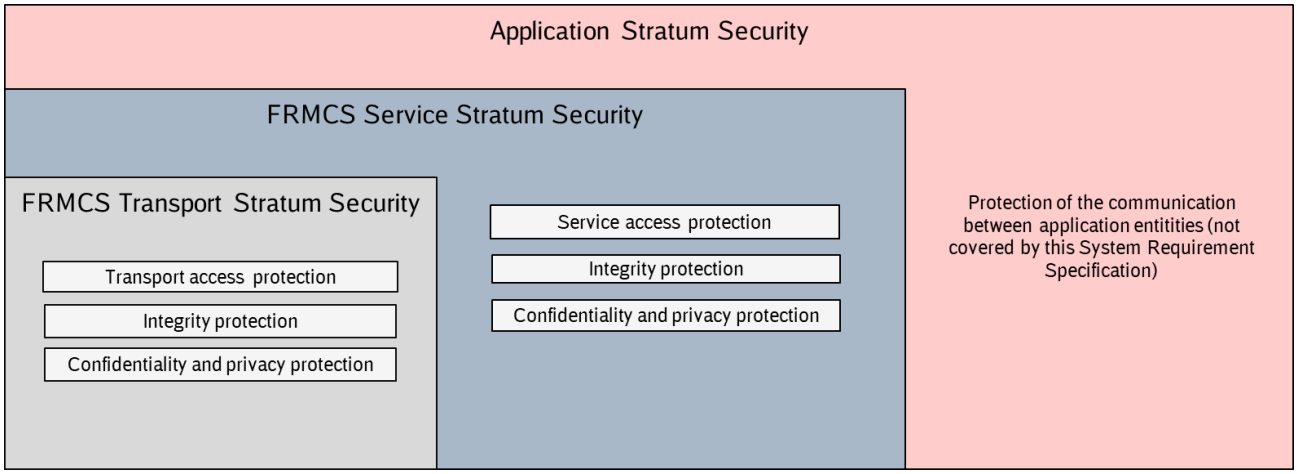


Figure 15-1 Principle multi stratum security model based on a defence in depth approach

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. (M-Vx)

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 ID, MC Service ID and MC Service 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 [TS 33.203] which is referenced in [TS 33.180].

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 15-1:

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 15-1 - 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 15-2:

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 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 15-2 - Cryptographic 5G Security Algorithms and Subscription Authentication Methods

15.6 Minimum Cryptographic Algorithm Strength used in FRMCS

15.6.1 Minimum cryptographic algorithm strength used in FRMCS is defined taking into account algorithms listed in Table 15-1 and Table 15-2. (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 15-3 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 15-3 - 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 15-3 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 FRMCS Location and positioning system

16.1 Introduction

16.1.1 Locating mobile FRMCS Users (e.g., train drivers, trackside workers) is one key element of the FRMCS System to support daily rail operations (e.g., Railway Emergency Communications, driver to controller communications based on driver's location). (I)

16.1.2 This section defines the principles, system requirements, architecture and performance requirements on the FRMCS Location and positioning system. (I)

16.2 Out of Scope

16.2.1 The location and positioning system for safety applications such as ATP is out of scope of this document. (I)

16.3 General principles and system requirements

16.3.1 The FRMCS Location and positioning system is currently limited to railway applications in Tight-Coupling mode (e.g., Railway Emergency Communication, driver to controller communications based on driver's location) and internal FRMCS System usage (e.g., FRMCS domain change), currently restricted to train positioning system. (I-V3)

16.3.2 The FRMCS Location and positioning system is currently limited to locate the train position. (I)

16.3.3 The FRMCS Location and positioning system supports various sources (producers) of Location Information, either internal or external to the FRMCS System, as depicted in Figure 16-1. (I)

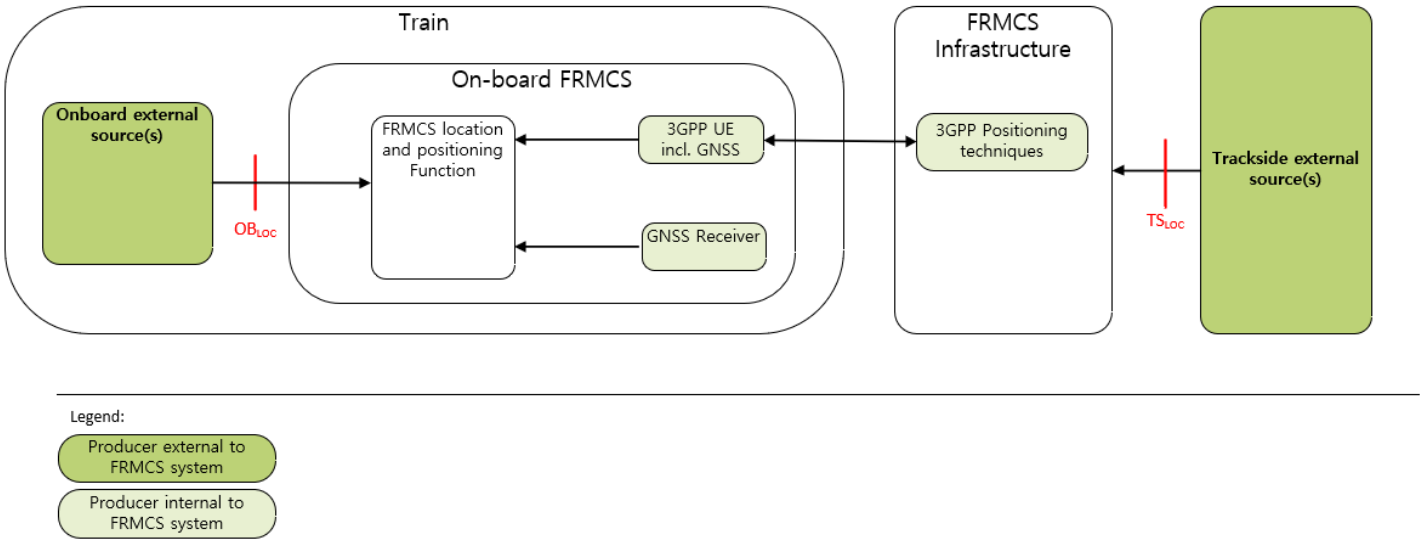


Figure 16-1 – Producers of Location Information.

16.3.4 The FRMCS Location and positioning system obtains Train Location Information from one or more source(s) internal to FRMCS System. (I)

16.3.5 The FRMCS Location and positioning system shall support obtaining Train Location Information from at least one GNSS receiver within On-Board FRMCS. (M)

16.3.6 **Intentionally deleted**.

16.3.7 When available, the FRMCS Location and positioning system should support obtaining Train Location Information from one or more source(s) external to FRMCS System, either onboard or trackside. (O-V3)

16.3.8 The best available accurate Train Location Information obtained from one or more source(s) shall be reported by the FRMCS Location and positioning function of the On-Board FRMCS respecting the following order of magnitude: (M)

a. GNSS receiver
b. Cell ID

Editor's Note: Conveyance of more than one location sources by the On-Board FRMCS should be clarified but not in scope of FRMCS v2.

16.3.9 **Intentionally deleted**.

16.3.10 For tight-coupled onboard applications, the On-Board FRMCS shall provide a Notification Function to convey Train Location Information on an event-triggered basis. (M)

16.3.11 The FRMCS Location and positioning system shall support as minimum triggers for the event-triggered basis (M):

a. Periodic reporting,
b. Distance travelled,
c. Cell change.

Note 1: cell change event is a fallback scenario as defined in 16.3.26.

Note 2: if GNSS data are not valid or not available (e.g., GNSS receiver(s) out of service), cell change will be considered.

16.3.12 The mechanism to configure the event-triggered Location reporting shall comply with MCX procedures as defined in [FRMCS-FIS]. (M)

16.3.13 The mechanism to configure event-triggered Location reporting shall support as minimum triggers (M):

a. Periodic reporting,
b. Distance travelled,
c. Cell change.

Note: cell change event is a fallback scenario as defined in 16.3.26.

16.3.14 For tight-coupled onboard applications, the On-Board FRMCS should provide a Notification Function to convey Train Location Information on demand. (O)

16.3.15 Mechanisms to convey Location information from onboard Tight-Coupled Railway Applications to the MC server shall comply with MCX procedures as defined in [TS 103 765-2]. (M)

16.3.16 The Train Location Information shall contain the following data derived from the available source(s) (M):

a. The Reference Location System e.g., the World Geodetic System 1984 (WGS 84)

Note1: only WGS 84 is currently foreseen to be supported, aligned with 3GPP and the Global Positioning System (GPS) usage.

b. The Train Geographic 2D Position (2D coordinates)
c. The Accuracy of the Train Geographic 2D Position (horizontal accuracy)
d. The Train Speed
e. The Accuracy of the Train Speed (if available by the source)

Note2: values can be “unknown”.

f. The Train Direction
g. The serving Cell ID within FRMCS Transport Domain

Note3: selecting the best serving cell when multiple UEs are attached to different serving cells is an implementation option.

h. The Time Stamp (i.e., date & time)

Note4: it is assumed that FRMCS trackside components will be synchronized e.g., 5GS and MC servers.

Note5: time stamps received from external source will be considered as synchronized sources.

16.3.17 The Train Location Information exchange format over OB_{APP} should be extensible to support additional location data (such as altitude, train acceleration). (O)

16.3.18 **Intentionally deleted**.

16.3.19 Train speed shall be obtained from one of the GNSS receivers. (M)

16.3.20 Train direction shall be obtained from one of the GNSS receivers. (M)

Note: onboard calculation is not applicable for fallback solution i.e., cell ID.

16.3.21 Calculation of distance travelled shall be supported by the FRMCS Location and positioning function of the On-Board FRMCS. (M-Vx)

Note: interface to convey distance travelled from external system (e.g., odometry) is left for implementation.

16.3.22 The FRMCS Location and positioning system shall operate under rail operational speed of the lines. (M)

a. High-speed,
b. Conventional speed.

16.3.23 The FRMCS Location and positioning system shall operate under the following rail environmental conditions: (M)

a. linear networks including confined environment such as tunnels with or without multiple tubes/segments,
b. cuttings,
c. railway stations,
d. railway crossings,
e. urban,
f. forests

16.3.24 The FRMCS Location and positioning system shall operate under the following weather conditions: (M)

a. heavy rain conditions,
b. snow,
c. foggy

16.3.25 The FRMCS system shall provide the best accuracy available for the positioning of individual FRMCS users, as depicted in figure 16-2, respecting the following order of magnitude: (M)

a. GNSS receiver
b. Cell ID

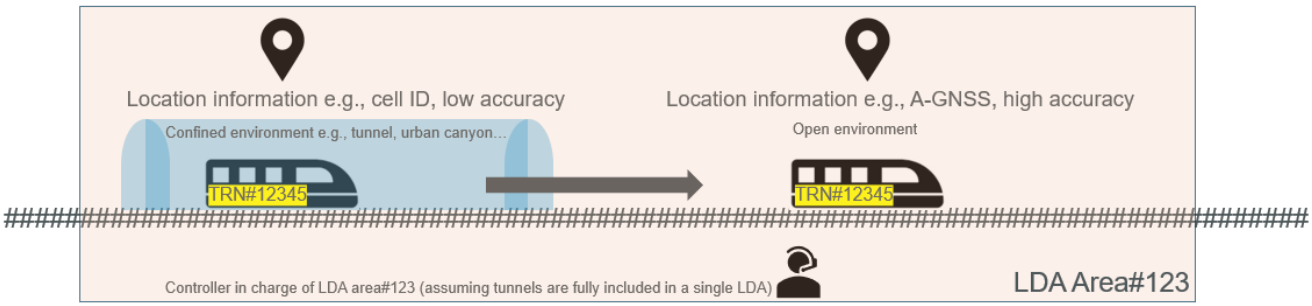


Figure 16-2 – Example of the support of best accuracy available for the positioning of a train.

16.3.26 In case of unavailability of positioning internal/external sources information for the positioning of individual FRMCS users (e.g., long tunnel), the FRMCS system shall be able to use as a fallback the serving cell ID of the FRMCS Transport Domain as positioning at minimum for applications like REC and driver to controller. (M)

16.4 Positioning and localisation architectural framework

16.4.1 The FRMCS System provides a positioning and location system as depicted in Figure 16-3. (I)

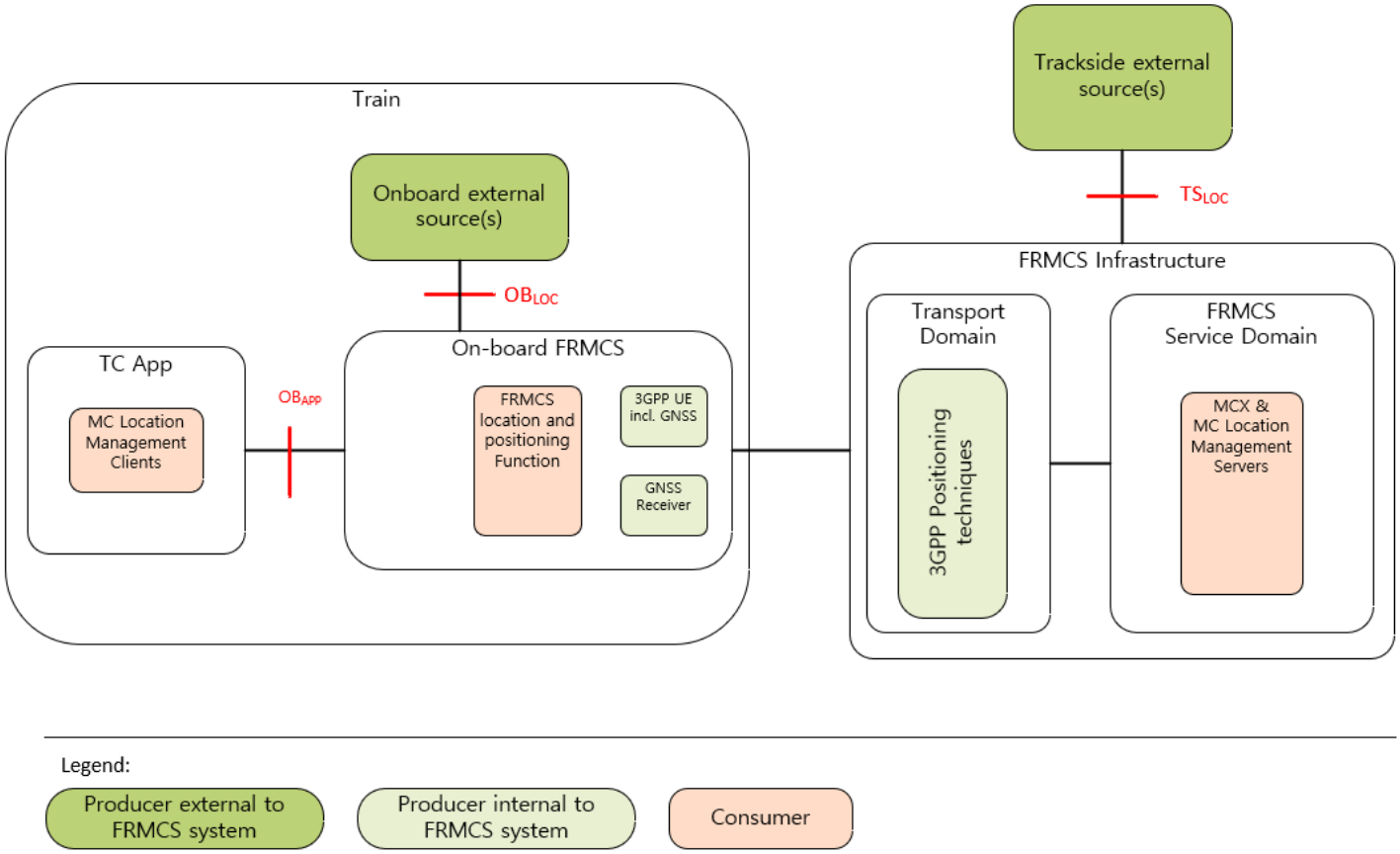


Figure 16-3 – Architecture of FRMCS Location and positioning system.

Editor's Note:

alternative architecture is under investigation (e.g., MC Location Management Client hosted by On-board FRMCS) but not in scope of FRMCS v2.

16.5 Performance requirements

16.5.1 Horizontal position accuracy is the difference between the calculated horizontal position and the actual horizontal position of a train component. (I)

16.5.2 The On-Board FRMCS shall provide a GNSS-based horizontal position accuracy of less than or equal to 4 meters CEP in open sky environment with a roof-mounted antenna. (M)

Editor's note: additional performance requirements are under investigation but not in scope of FRMCS V2.

16.5.3 The FRMCS system shall provide a horizontal position accuracy of cell ID coverage in confined environment (e.g., tunnels, urban canyons, cuttings). (M)

Note: cell change is a fallback scenario as defined in 16.3.26.

16.6 Security requirements

Editor’s Note:

list of security and privacy constraints are out of scope for FRMCS V2. Security precautionary measures to prevent knowledgeable changes of the position information of a user.

17 Non-Functional System Requirements

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 On-Board FRMCS Radio Functions, and m to the number of Gateway Functions. The notation 1:n indicates that there is one Gateway Function connected to multiple On-Board FRMCS Radio Functions. m:n indicates that multiple Gateway Functions are connected to multiple On-Board FRMCS 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 On-Board FRMCS 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)

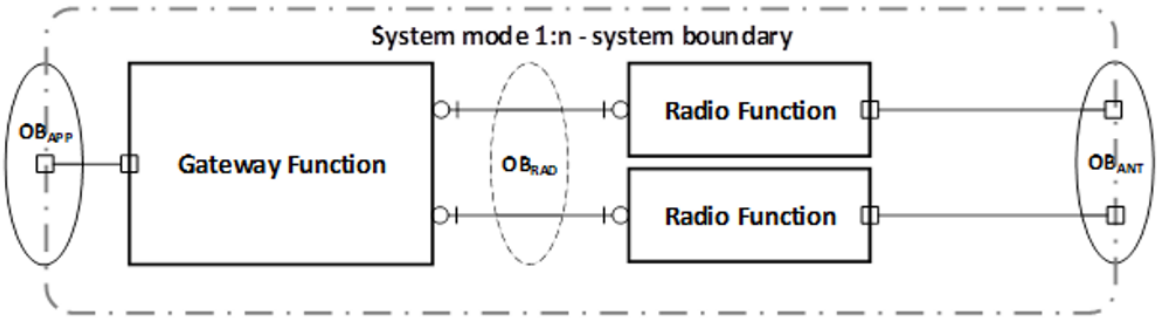


Figure 17-1: System mode 1:n. A case where 2 On-Board FRMCS Radio Functions are connected to the Gateway Function

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 out of scope for FRMCS V2.

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 On-Board FRMCS 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 On-Board FRMCS User characteristics

17.3.4.1 FRMCS Users are entities defined in chapter [2] of this document.

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 as defined in chapter [19] of this document. (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

18.1 Mobile equipment

Editor's note:

This section is out of scope for FRMCS V2.

18.2 Controller equipment

18.2.1 Controller equipment is defined in section [24.3]. (I)

18.3 Driver equipment

18.3.1 Driver equipment is defined in section [24.2]. (I)

19 Profiles in FRMCS

19.1 Introduction

19.1.1 In order to provide a consistent level of service in each railway network and, in particular, to ensure interoperability for train drivers and other users moving between domains, it is important to harmonise subscription details and other information stored in the network. (I)

19.1.2 The notion of Loose Coupling and Tight Coupling as well as the principle of strata separation in FRMCS entails that subscription information in FRMCS (i.e., “Profiles”) is much less tightly linked to the Transport Stratum (i.e. the “telecom subscriber”) and more centered around the Service Stratum (i.e. the “MCX Service User”). (I)

19.1.3 For railway interoperability, configuration in FRMCS aims at enabling the free movement of train within its area of use and usage across of the area of use of interoperable applications. (I)

19.1.4 An area of use as determined by the European Union Agency for Railways can be based on a finer granularity than a FRMCS Domain but, from a FRMCS perspective, the smallest granularity is that of a FRMCS Domain. (I)

19.1.5 In general, proper operation of applications involving a train across FRMCS Domains will rely in the On-Board FRMCS on: (I)

- FRMCS-Domain-access-related parameters, irrespective of individual applications
- Application-related parameters

19.1.6 In general, proper operation of applications involving a train across FRMCS Domains will rely outside the On-Board FRMCS on: (I)

- Application-related parameters
- Inter-domain interconnection and particularly IP routing

19.1.7 Non-interoperable applications (Types II and IV, as defined in clause 10.1.3.3.4) can still operate but shall require specific configuration to allow proper operation in a specific FRMCS Domain (in the case of Type II applications) or from a Foreign FRMCS Domain (in the case of Type IV applications). (M-V3)

19.1.8 The next sections specify the parameters, whether applications-agnostic or application-related which need to be put in place for proper operation of applications over an area of use. (I)

19.2 On-Board FRMCS configuration

19.2.1 FRMCS-Domain-access-related parameters

19.2.1.1 The FRMCS-Domain-access-related parameters to be configured on the On-Board FRMCS are based on the set of FRMCS Domains that can be encountered within the area of use. This set, excluding the Home FRMCS Domain, is referred to as Visitable FRMCS Domains. (I)

19.2.1.2 The SIM profile of each On-Board FRMCS Radio Module shall be configured with the Home FRMCS Domain as the main profile. (M-V3)

19.2.1.3 The SIM profile of each On-Board FRMCS Radio Module shall be configured for roaming in each of the FRMCS Domain within the Visitable FRMCS Domains. (M-V3)

19.2.1.4 Detailed contents of the SIM profile will be specified. (I-V3)

19.2.1.5 Each On-Board FRMCS Radio Module shall be set to "data centric" usage settings as per [TS 24.501]. (M-V3)

19.2.1.6 The On-Board FRMCS shall be configured with the FQDN or IP address of the Configuration Management Server in the Home FRMCS Service Domain as specified in [TS 24.484] clause 4.2.1. (M)

19.2.1.7 The On-Board FRMCS shall be configured with a X.509 [ITU-T X.509] TLS certificate to allow the establishment of a TLS tunnel to the authorisation endpoint of the IdMS in the Home FRMCS Service Domain (see [TS 24.482] clause 6.2.1). (M)

19.2.1.8 The On-Board FRMCS shall be configured with a X.509 [ITU-T X.509] TLS certificate to allow the establishment of a TLS tunnel to the token endpoint of the IdMS in the Home FRMCS Service Domain (see [TS 24.482] clause 6.2.2). (M)

19.2.2 Application-related parameters

19.2.2.1 For each Loose Coupled Application of Type I or III to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with: (M)

1. The X.509 certificates [ITU-T X.509] allowing the mTLS mutual authentication mandated by the Local Binding procedure specified in the [FRMCS-FFFIS]

2. The credentials associated to each MC User ID required by the application for the MC user authentication procedure specified in [TS 24.482] clause 6.3.1.
3. The scope (as specified in [TS 33.180] clause B.4.2.2) associated to each MC User ID required by the application for the MC user authentication procedure specified in [TS 24.482] clause 6.3.1.
4. The IMS/SIP Core credentials associated to each MC User ID required by the application for each FRMCS Domain within the Visitable FRMCS Domains.
5. The mapping rules enabling the transformation from the application-specific identifiers provided by the application over the OB_{APP} reference point towards MC Service User IDs.

Note: For the full list of parameters, please refer to [TS 103 765-2].

19.2.2.2 For each Loose Coupled Application of Type II to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with parameters to be specified. [M-Vx]

19.2.2.3 For each Loose Coupled Application of Type IV to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with parameters to be specified. [M-V3]

19.2.2.4 For each Loose Coupled Application to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with the mandatory parts of the FRMCS On-board Application Profile (see section 19.3). (M)

19.2.2.5 For each Tight Coupled Application (except the special case of the VAS) to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with the X.509 certificates [ITU-T X.509] allowing the mTLS mutual authentication mandated by the Local Binding procedure specified in the [FRMCS-FFFIS] (M).

19.2.3 VAS related parameters

19.2.3.1 To enable the VAS, the On-Board FRMCS shall be configured with the X.509 certificates [ITU-T X.509] allowing the mTLS mutual authentication mandated by the Local Binding procedure specified in the [FRMCS-FFFIS]. (M)

19.2.3.2 The VAS shall be configured with access information to the Home FRMCS Service Domain as per clauses 19.2.1.6 to 19.2.1.8. (M)

19.2.3.3 The VAS shall be configured with the IMS/SIP Core credentials associated to each MC User ID required by the application for each FRMCS Domain within the Visitable FRMCS Domains. (M)

19.2.3.4 The VAS shall be configured with the arbitration rules (specified in [FRMCS-FRS]) applicable for each FRMCS Domain within the Visitable FRMCS Domains. (M)

19.2.4 About FRIOP, FROP and FOAP

19.2.4.1 The FRMCS Railway Interoperability On-board Profile (FRIOP) shall be constituted of: (M)

1. The parameters identified in clauses 19.2.1.1 to 19.2.1.5.
2. For each Loose Coupled application of Types I or III, the parameters identified in clauses 19.2.2.1 and 19.2.2.4.
3. For the VAS, the parameters identified in clauses 19.2.3.1 to 19.2.3.4.

19.2.4.2 The FRMCS Railway On-board Profile (FROP) shall be constituted of: (M)

1. The parameters identified in the FRMCS Railway Interoperability On-board Profile (FRIOP), i.e., clause 19.2.4.1
2. For each Loose Coupled application of Type II, the parameters identified in clauses 19.2.2.2 and 19.2.2.4.

3. For each Loose Coupled application of Type IV, the parameters identified in clauses 19.2.2.2 and 19.2.2.4.
4. For each Tight Coupled application (except the special case of the VAS), the parameters identified in clauses 19.2.2.5.

19.2.4.3 The FRMCS On-board Application Profile (FOAP) is constituted of application-related parameters which support the execution logic of the On-Board FRMCS when interacting with the applications. The FOAP is further described in clause 19.3. (I)

19.3 FRMCS On-board Application Profile

19.3.1 For each application category to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with the following information (M):

1. The coupling mode of the application (i.e. (“Tight Coupling Mode”) or (“Loose Coupling Mode” in the present version) as defined in clause 6.1.3.1.4.
2. The type of the application (i.e. Type I, II, III or IV in the present version) as defined in clause 10.1.3.3.4.

19.3.2 For each Loose Coupled Application category to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with the following information (M):

1. Whether the application is part of the set of “Startup Applications”

Note: “Startup Applications” are applications for which the On-Board FRMCS takes specific measures as part of the FRMCS Start of Operation procedure as defined in [TS 103 764].

19.3.3 For each Loose Coupled Application category to be supported by the On-Board FRMCS, the On-Board FRMCS should be configured with the following information (O-V3):

1. Whether “Onboard-application-initiated sessions” are allowed for the Onboard application category
2. Whether “Onboard-application-terminated sessions” are allowed for the Onboard application category
3. Whether the Onboard application category is allowed to close an “Onboard-application-initiated session”
4. Whether the Onboard application category is allowed to close an “Onboard-application-terminated session”
5. Whether the usage of FRMCS Multipath is allowed for the Onboard application category
6. Whether the usage of a non-FRMCS Transport Domain is allowed for the Onboard application category
7. Whether to apply confidentiality protection on the MCX User Plane within the FRMCS Domain for the Onboard application category

Note: a default configuration can be used for specific Loose Coupled Application category that are not intended to make use of such feature.

19.3.4 For each Loose Coupled Application category of Type II or IV to be supported by the On-Board FRMCS, the On-Board FRMCS shall be configured with the following information (M):

1. The set of FRMCS Domains for which the Onboard application category is configured to operate from or in. This set is called “Domain of applicability” of the Onboard application category.

19.3.5 For each Tight Coupled Application category to be supported by the On-Board FRMCS, the On-Board FRMCS should be configured with the following information (O):

1. Whether the usage of FRMCS Multipath is allowed for the Onboard application category
2. Whether the usage of a non-FRMCS Transport Domain is allowed for the Onboard application category

19.4 Configuration within a FRMCS Domain

19.4.1 The Home FRMCS Service Domain shall be configured to authorize each MC Service User ID required by applications of Type I or III to be supported by the On-Board FRMCS. (M)

19.4.2 For each FRMCS Domain within the Visitable FRMCS Domains of an On-Board FRMCS, the Home FRMCS Service Domain shall be configured to authorize each MC Service User ID associated to that domain required by applications of Type I or III to be supported by the On-Board FRMCS. (M)

19.4.3 For each FRMCS Domain within the Visitable FRMCS Domains of an On-Board FRMCS, the FRMCS Service Domain shall be configured as a MC partner system of the Home FRMCS Service Domain of the On-Board FRMCS. (M)

19.4.4 For each FRMCS Domain within the Visitable FRMCS Domains of an On-Board FRMCS, the FRMCS Service Domain shall be configured to support the 3GPP MC migration procedure for each MC Service User ID required by interoperable applications. (M)

19.4.5 For each FRMCS Domain within the Visitable FRMCS Domains of an On-Board FRMCS, the FRMCS Domain shall ensure the reachability of IP networks that are required by applications of Type I or III and which are connected to by the application in Host-to-Network addressing mode. (M)

20 FRMCS Air Interface

20.1 Introduction

20.1.1 For the design and the dimensioning of the FRMCS air interface it is important to highlight the minimum FRMCS throughput requirement per train. As per [Annex A.5], the minimum throughput figures per running train are based on the following applications (I):

- Voice (as per section 24.1.3.2.2 & 24.1.3.2.4)
- ATP (ETCS Level 2)
- ATO (GoA2 Operation)

20.2 Generic requirements

20.2.1 The identified minimum FRMCS throughput in uplink and downlink direction per train shall be an application layer throughput of 95 kbps (M-V3).

20.2.2 For RF network design and planning, the minimum throughput requirement per train in Uplink- and Downlink direction is defined for an antenna on the roof of a train (nominally a height of 4m above the track). An isotropic antenna with a gain of 0dBi is assumed. (I)

Note: As per UIC document [O-8868], FRMCS RF network planning shall take into account a maximum of 6dB losses between the On-Board FRMCS radio module and the antenna (including cable losses, aging, connector losses and filter losses).

20.2.3 Important air interface relevant FRMCS radio network parameters for design purposes and measurements, based on the essential 5G NR specifications by 3GPP, shall be: (M-V3)

a. NR RSRP: SS-RSRP and CSI-RSRP
b. NR RSRQ: SS-RSRQ and CSI-RSRQ
c. SINR: SS-SINR and CSI-SINR

Note: SS stand for Synchronisation Signal and CSI stand for Channel State Information.

20.2.4 For considering of the FRMCS signal quality requirements especially the effects of intra system interference has to receive special attention during the radio network design of the FRMCS air interface. SINR in the worst conditions (e.g. at cell edge) is the most important RF parameter to be considered. (I-V3)

Note: See UIC document [O-8868] for more details regarding technical aspects of FRMCS RAN.

20.2.5 For the design of the FRMCS air interface the resulting data rate requirements per train as per [Annex A.5], together with the overall FRMCS QoS requirements as per section [14] and the technical background of FRMCS RAN as described per UIC document [O-8868], has to be used for the determination of the FRMCS coverage quality in the form of a minimum RSRP and SINR. (I)

Note: UIC document [O-8868] provides some examples for RF link budget calculations in the 900MHz and 1900MHz RMR frequency bands.

Editor’s Note 1: To avoid the necessity for large FRMCS radio cell overlaps to accommodate high speed train operations, optimisation of the handover process for such trains is considered necessary. Suitable algorithms, margins and RF parameter settings will be tested and refined as necessary during the FRMCS field trials.

Editor’s Note 2: The values for the FRMCS air interface concerning throughput requirements and signal quality requirements are to be validated and, if necessary, reviewed after the first operational implementation of FRMCS.

Editor’s Note 3: RF parameter values for the FRMCS air interface concerning throughput requirements and signal quality requirements shall be final specified by version 3 of UIC´s FRMCS specifications with the test results of the envisaged FRMCS projects.

21 FRMCS Common Functions

21.1 Introduction

21.1.1 FRMCS Common Functions, as per [FRMCS-FRS] concept, are a set of supporting building blocks each one providing a part of functionality used by various Railway Applications. (I)

21.1.2 The table 21-1 summarizes the FRMCS Common Functions considered in this version of the specification and presents the applicability of them, depending on the application's coupling mode, loose, tight coupled or both. It also highlights in the *implementation* column, whether this Common Function is implemented at application level (e.g., provided by the VAS) or offered by the FRMCS system. (I)

Name of the Common Function	Applicability depending on the FRMCS application coupling mode	Implementation
Multi-user talker control	Tight coupled (TC)	Application (for VAS refer to Table 24-1)
Role management and presence	Loose coupled (LC), TC	Application (for VAS refer to ch.24.1.3.3) FRMCS system
Location services	TC	FRMCS system
Authorisation of communication	LC, TC	Application (for VAS refer to ch.24.1.3.3) FRMCS system
QoS and priority	LC, TC	FRMCS system
Arbitration	TC	Application (for VAS refer to ch.24.1.3.3)

Table 21-1: List of FRMCS Common Functions

Editor's Note: Presence is not in the scope of FRMCS v2.

21.2 Multi-user talker control

21.2.1 Introduction

21.2.1.1 Multi-user talker control is applicable to designated MCPTT groups, allowing several participants talking simultaneously, during railway communication. (I)

21.2.1.2 The maximum number of simultaneous talkers of the MCPTT group can be either one or a limited number. (I)

21.2.1.3 However, in some multi-user communication (e.g. emergency communications) some relevant participants (e.g. responsible controller and initiator of the communication) need to have higher talking priorities than others and/or the exclusive right to talk during a time interval. In these cases, multi-talker control common function will apply specified priority policy and talking permissions. (I)

21.2.2 Applicability

21.2.2.1 The multi-user talker control common function is implemented in the relevant voice communication applications, listed in the [FRMCS-FRS]. (I)

21.2.3 Protocols

21.2.3.1 Floor control protocols shall be based on RTCP signaling (RTCP Application Packets) as defined in [TS 24.380]. (M)

21.2.4 Procedures

21.2.4.1 The multi-user talker control shall support the following floor control procedures, as defined in [TS 23.379]: (M)

1. Floor request
2. Floor granted
3. Floor release
4. Floor revoke, pre-emptive priority
5. Identification of the current talker based on Functional Alias

21.2.4.2 The multi-user talker control should support the following floor control procedures, as defined in [TS 23.379]: (O-V3)

1. Floor revoke, time based
2. Location of the current talker

Note : The detailed procedures are described in [FRMCS-FIS].

21.2.5 Negotiation

21.2.5.1 The FRMCS system shall provide a mechanism to negotiate the floor control capabilities including: (M-V3)

1. Floor priority supported
2. Implicit floor request supported

Note 1: The Floor control for private calls is not supported.

Note 2: Multiplexing is not supported.

21.2.5.2 The FRMCS system should provide a mechanism to negotiate the floor control capabilities including: (O)

1. Queueing of floor request supported.

21.2.6 Floor priority scheme

21.2.6.1 To allow the floor priority and queuing mechanisms of the multi-user talker control Common Function, the floor priority scheme will be defined in this specification, based on the floor priority scheme to be described in the [FRMCS-FRS]. (I-V3)

Editor's Note: The impact of the floor priority scheme on the applications' interoperable profile needs to be assessed.

21.2.7 Configuration of multi-user talker control

21.2.7.1 The decision events of the multi-user talker control common function shall be configured in the VAS: (M-V3)

1. Floor priority scheme

21.2.8 Interconnection, migration, interworking

21.2.8.1 Multi-user talker control Common Function is applicable for group calls allowing communication of FRMCS Users obtaining services from two or more interconnected FRMCS Domains, as per §10.2.2.2. (I)

Editor's Note: The behaviour of multi-user talker control common function in case of MC migration needs to be assessed. Floor priority scheme is not yet described in [FRMCS-FRS].

21.2.8.2 For group calls involving FRMCS Users and GSM-R users, the floor talker control behaviour shall comply with [TS 103 792], chapters §7.2.5 and §7.2.6. (M)

21.2.9 Cybersecurity

21.2.9.1 Confidentiality and integrity protection of RTCP signaling comply with clause 15.5.2.2. (I)

21.3 Role management

21.3.1 Introduction

21.3.1.1 The role management common function is responsible for (I):

- The processes of registration/deregistration of MC Service IDs
- The allocation and activation/deactivation of Functional alias(es)
- The addressing of users/applications based on the MC Service IDs
- The addressing of users/applications based on the Functional alias(es)

21.3.2 Out of scope

21.3.2.1 Mapping of MC identities used in FRMCS to GSM-R numbering for MCData services is out of scope, as MCData services (except MCData SDS) are out of scope of chapter §9 of this specification. (I)

21.3.3 Applicability

21.3.3.1 The role management common function is applicable for loose- and tight- coupled applications. For tight-coupled applications, part of the role management common function is implemented in the VAS, as per clause 24.1.3.3.2. The rest is implemented in the FRMCS Domain. (I)

21.3.3.2 For loose-coupled applications, part of the role management common function is implemented in the FRMCS gateways (i.e., the On-Board FRMCS and the FRMCS Trackside Gateway). The rest is implemented in the FRMCS Domain. (I)

21.3.4 Procedures

21.3.4.1 The role management common function shall support the following procedures: (M)

1. User Registration
2. Activation of one or multiple Functional Alias(es) per FRMCS User
3. De-activation of Functional Alias(es)
4. Interrogation of Functional Alias(es)
5. Presentation of the functional Alias, as an identifier of the initiator of the call
6. Intentionally deleted.
7. Notification about Functional Alias(es) activation status by other FRMCS user
8. Routing calls based on Functional Alias

21.3.4.2 User Registration

21.3.4.2.1 The logging of the user complies with the procedures described in [FRMCS-FIS], chapter § 3.1.2.1. (I)

21.3.4.2.2 Especially, for tight coupled applications, the user will be logged to the FRMCS system, using the methods described in the VAS chapter of this document, clause 24.1.2.4. (I)

21.3.4.2.3 For logging to the FRMCS system, using the MC ID, the credentials to be used and the format of them, complies with clause 11.4.5.2.2 of this document. (I)

21.3.4.2.4 The role management common function is responsible to provide an MC Service ID to the user, upon successful registration. (I)

21.3.4.2.5 The assigned MC Service ID, as outcome of the login procedure, complies with the requirements defined in the chapter §11.4.5.3 of this document. (I)

21.3.4.3 Activation of Functional Alias(es)

21.3.4.3.1 The role management common function supports the user on the assignment of functional alias(es) based on the MC Service IDs, as per clauses 11.6.1.4&11.6.1.5 of this document. (I)

21.3.4.3.2 Functional alias(es) comply with the requirements and formats, as described in chapter §11.6 of this document. (I)

21.3.4.3.3 The activation of one or multiple functional alias(es) complies with the procedures described in the [FRMCS-FIS], chapter §3.1.3.2. (I)

21.3.4.3.4 The MCX client is informed about the automatic activation of functional alias(es) by applying the subscription/notification procedures, explained in [FRMCS-FIS] chapter §3.1.3.6. (I)

21.3.4.4 De-activation of Functional Alias(es)

21.3.4.4.1 The (de)activation of functional alias(es) complies with the procedures described in the [FRMCS-FIS] chapter §3.1.3.3. (I)

21.3.4.4.2 The MCX client is informed about the automatic (de)activation of functional alias(es) by applying the subscription/notification procedures, explained in [FRMCS-FIS] chapter §3.1.3.6. (I)

21.3.4.5 Functional alias(es) interrogation

21.3.4.5.1 The interrogation of FRMCS user's functional alias(es) complies with the procedures described in the [FRMCS-FIS], chapter §3.1.3.4. (I)

21.3.4.6 **Intentionally deleted**.

21.3.4.7 Notification about functional alias(es) activation status

21.3.4.7.1 The FRMCS user shall receive updates about the status of activation of his/her functional alias (es), by other FRMCS users, as described in [FRMCS-FIS], chapter §3.1.3.6. (M-V3)

21.3.4.8 Routing calls using called Functional Alias(es)

21.3.4.8.1 Routing calls using destination Functional Alias(es) complies with the criteria defined in [FRMCS-FIS] chapters §4.4.6 for voice and §4.3.6.10 for REC. (I)

21.3.5 Configuration

21.3.5.1 The role management common function shall support the FRMCS Operator in the setting of a validity timer for deactivation of Functional aliases. (M)

21.3.5.2 The role management common function shall support the FRMCS Operator to configure the Functional aliases that will never be deactivated. (M)

21.3.5.3 The role management common function shall support the FRMCS Operator to enable or disable the automatic registration of the user. (M)

21.3.5.4 The role management common function shall support the FRMCS Operator in setting a maximum number of functional identities to be activated for an FRMCS User. (M)

21.3.5.5 The role management common function shall define: (M)

1. The list of authorised Functional Alias(es) to be activated.
2. The list of authorised Functional Alias(es) to be de-activated.

21.3.6 Migration, interworking, interconnection

21.3.6.1 For an FRMCS User migrating between FRMCS domains, the role management common function complies with the procedures described in [TS 23.280] for the usage of MC Service IDs and Functional aliases. (I)

Editor's note: The usage of Functional Alias(es) across multiple FRMCS domains is out of scope for FRMCS v2.

21.3.6.2 When moving from FRMCS to GSM-R domain and vice-versa, the registration/deregistration of the identities is handled by the coordinating function in the VAS, chapter §24.2.6.3 of this document. (I)

21.3.6.3 In addition to clause 9.5.1.10, the unicity of train ID between FRMCS and GSM-R system shall be ensured by the FRMCS system. (M-V3)

21.3.6.4 The usage of Functional Alias(es) for communications between two or more interconnected FRMCS Domains comply with the requirements of chapter §10.2.2. (I)

21.3.7 Cybersecurity

21.3.7.1 The role management applies the security Principle 3, as described in clause 15.4.3 of this document. (I)

21.4 Authorisation of communication

21.4.1 Introduction

21.4.1.1 Authorisation of communication common function allows the FRMCS Operators to control and regulate communication services for Voice, Video and Data between FRMCS Users of one or more FRMCS Domain(s). (I)

21.4.1.2 FRMCS Operators control and regulate communication services through the use of identities of the FRMCS service stratum. (I)

21.4.2 Out of scope

21.4.2.1 Authorisation of communications between FRMCS users and non-FRMCS users, except GSM-R users, is out of scope. (I)

21.4.3 Applicability

21.4.3.1 The authorisation of communication common function is applicable to loose- and tight- coupled applications. (I)

21.4.4 Procedures

21.4.4.1 The authorisation of communication shall support the following procedures:(M)

- MCX ad hoc group emergency alert procedures:

1. - Request with criteria
2. - **Intentionally deleted**
3. - Cancel
4. – Intentionally deleted.
5. – Intentionally deleted.
6. - Add participants/late entry
7. - Remove participants/move out

8. - Notification to authorised users of participants list

- MCX ad hoc group communication procedures:

9. - Voice normal group calls
10. - Voice emergency group calls
11. – Intentionally deleted.
12. – Intentionally deleted.
13. - Release
14. - Intentionally deleted
15. - **Intentionally deleted**
16. - Notification to authorised users of participants list

- Private call:

17. - Initiation in automatic commencement mode
18. - Initiation in manual commencement mode
19. - Release

- MCData IP connectivity:

20. – Point-to-point request/response
21. – Point-to-point Release

Note: The detailed procedures are described in [FRMCS-FIS].

21.4.4.2 The authorisation of communication shall support the following procedures for MCX ad hoc group emergency alert and MCX ad hoc group communications: (M-V3)

1. - Modify criteria
2. - Modify participants list
3. - Request with participants list

Note 1: Modification of participants list is only available for the initiator of an ad-hoc group call in the scope of FRMCS v2, [FRMCS-FIS] chapter §4.4.5.8.

Note 2: Request with participant list' is currently only supported via specific participant list criteria (not via participant list provided directly in MCX participant list Information element)

21.4.5 Configuration

21.4.5.1 FRMCS Operators shall control and regulate communication services through the use of MC Service User Identities, as defined in clause 11.4.5.3. (M)

Note: this is done through MC Service User Profile Configuration Data.

21.4.5.2 FRMCS Operators shall control and regulate communication services through the use of all labels of a functional alias, as defined in section 11.6. (M-V3)

Editor's note: Authorisation through MC Service User Profile Configuration Data is based on user identities. Controlling communication services through Functional Alias(es) is not supported by MCX procedures.

21.4.5.3 FRMCS Operators shall control and regulate communication services through the use of one or more labels of a functional alias (e.g., function label), as defined in section 11.6. (M-V3)

21.4.6 Interconnection, migration, interworking

21.4.6.1 Communications of FRMCS users when migrating to a partner FRMCS Domain follows the procedures of authorization from both primary and partner FRMCS Domains, as defined in [TS 23.280]. (I)

21.4.6.2 Configuration of authorizations are defined per FRMCS domain. (I)

21.4.6.3 Communications between participants of multiple FRMCS Domains complies with the authorization procedures, as defined in [TS 23.379] (I)

21.4.6.4 Communication between FRMCS and GSM-R users are authorized, following the rules described in chapter §9.5 of this document. (I)

21.5 Arbitration

21.5.1 Applicability

21.5.1.1 The arbitration common function is only applicable to tight- coupled applications. (I)

21.5.2 Configuration of Arbitration rules

21.5.2.1 Arbitration rules, specified in the [FRMCS-FRS] and configured in the VAS, are to be used for sharing communication resources of functional blocks, as defined in the VAS, clauses 24.1.2.2 and 24.1.2.3. (I)

21.5.2.2 As an outcome of the arbitration rules, putting a communication on-hold shall be a possibility offered by the VAS. (M-V3)

21.5.2.3 As an outcome of the arbitration rules, the presentation of a queued communication shall be a possibility offered by the VAS. (M-V3)

Note: The participants of a communication put on-hold or in the queue are notified.

Editor's Note: Queueing is an-going subject in the [FRMCS-FIS] with potential normative or application impact.

21.5.2.4 As an outcome of the arbitration rules, rejection of a voice communication (e.g. Private calls in manual commencement mode) shall be supported and implemented in the VAS. (M)

Note: For REC and voice communications in automatic commencement mode, rejection is not supported.

21.5.2.5 The arbitration rules, implemented in the VAS, also comply with Domain change requirements, as defined in the clause 19.2.3.4. (I)

22 Recording and Logging

22.1 Introduction

22.1.1 The purpose of recording is to record and store media (audio, video and/or data) streams. (I)

22.1.2 Note that recording may be subject of differing national laws across the European Union. (I)

22.1.3 The purpose of logging is to create a record of communication related data, called metadata (e.g., date, time, participants identities, floor requests, type of media exchanged, etc.) (I)

Note: the main purpose of recording and logging is to record media and logs for critical communications.

22.2 Out of Scope

22.2.1 Recording and logging of non-MCX communications are out-of-scope. (I)

22.3 Generic Requirements

22.3.1 The FRMCS system shall provide a mechanism to log the metadata of Railway Emergency Communications and make them available to the FRMCS operations. (M)

Editor's Note:
This requirement ensures that a feature similar to GSM-R Confirmation of High Priority Calls is supported in FRMCS system, providing all necessary metadata of a REC available for post-analysis in a central entity (MC service Server or MC Location Management Server). How to get access to those metadata by an FRMCS Operator is currently left for implementation.

22.3.2 The FRMCS system shall provide a mechanism to log the metadata of all MCX communications and store them for later inspection. (M-V3)

22.3.3 The FRMCS system shall provide a mechanism to record media data of MCX communications. (M-V3)

22.3.4 The FRMCS system shall ensure that the extraction of the recorded information is possible. (M-V3)

22.3.5 The FRMCS system shall ensure that recorded data can be persistently stored. (M-V3)

22.3.6 The function of the recording shall not impact normal FRMCS system operations. (M)
Editor's Note: Recording of encrypted data is out of scope for FRMCS V2.

23 FRMCS Time Service

23.1 Introduction

23.1.1 FRMCS relies on specific time services offered to services for optimal performance, error free operation and simply providing the basic functionality as intended. (I)

23.1.2 This version of the specification introduces the following FRMCS Time Services for the On-Board FRMCS: (I)

- Synchronization of FRMCS System Time with source,
- Providing time of day to FRMCS Time Service consumers (e.g., to be included in REC)

Editor's Note: External sources are not in scope for V2.

23.1.3 This section defines the principles and architecture, if and where gaps have been identified, and focusses otherwise on system requirements and performance requirements of the FRMCS Time Service. (I)

23.2 Out of Scope

23.2.1 Time Services for applications outside respectively beyond FRMCS are out of scope of this document. (I)

23.2.2 Such examples are: (I)

- ETCS and
- ATO

23.3 General principles, architecture and system requirements

23.3.1 FRMCS System Time is expressed in Universal Time Coordinated (UTC) [ITU-R TF.460-6] and [ITU-R TF.535-2]. (I)

23.3.2 As the architecture drawing of Figure 23-1 shows, there are two independent possible sources of reference time for synchronization. They are: (I)

- FRMCS Transport Stratum
- Global Navigation Satellite System (GNSS)

23.3.3 FRMCS Time Service shall be able to synchronize to the reference time provided by the FRMCS transport stratum. (M)

23.3.4 FRMCS Time Service system shall be able to synchronize to the reference time provided by a source as defined in 23.3.2. (M)

23.3.5 FRMCS Time Service sources shall be used simultaneously in a redundant manner protecting FRMCS Time Service against loss of time reference. (M)

Note: For the case that redundant time sources deliver differing timing the FRMCS Time Service shall have a configurable priority that decides between the redundant time sources which one to select over the other.

23.3.6 FRMCS Time Service shall provide accurate time to the FRMCS Time Service consumers. (M)

Editor's Note: Configuration selecting a source is not in scope for FRMCS V2.

23.3.7 FRMCS time service shall run with an accuracy of 10^{-6}s, i.e., 1s deviation every 10^{6}s, or better for at least one day (24 hours). (M-Vx)

23.3.8 If FRMCS time service is down, services using the FRMCS Time Service are able to continue time service, and continuously increasing numbering. (I)

23.3.9 FRMCS Time Service shall resynchronize after a loss of time sources when time sources are available again. (M)

Editor's Note: Selection of dedicated available different clocks, this includes procedure for the return to the grid is not in scope for FRMCS V2.

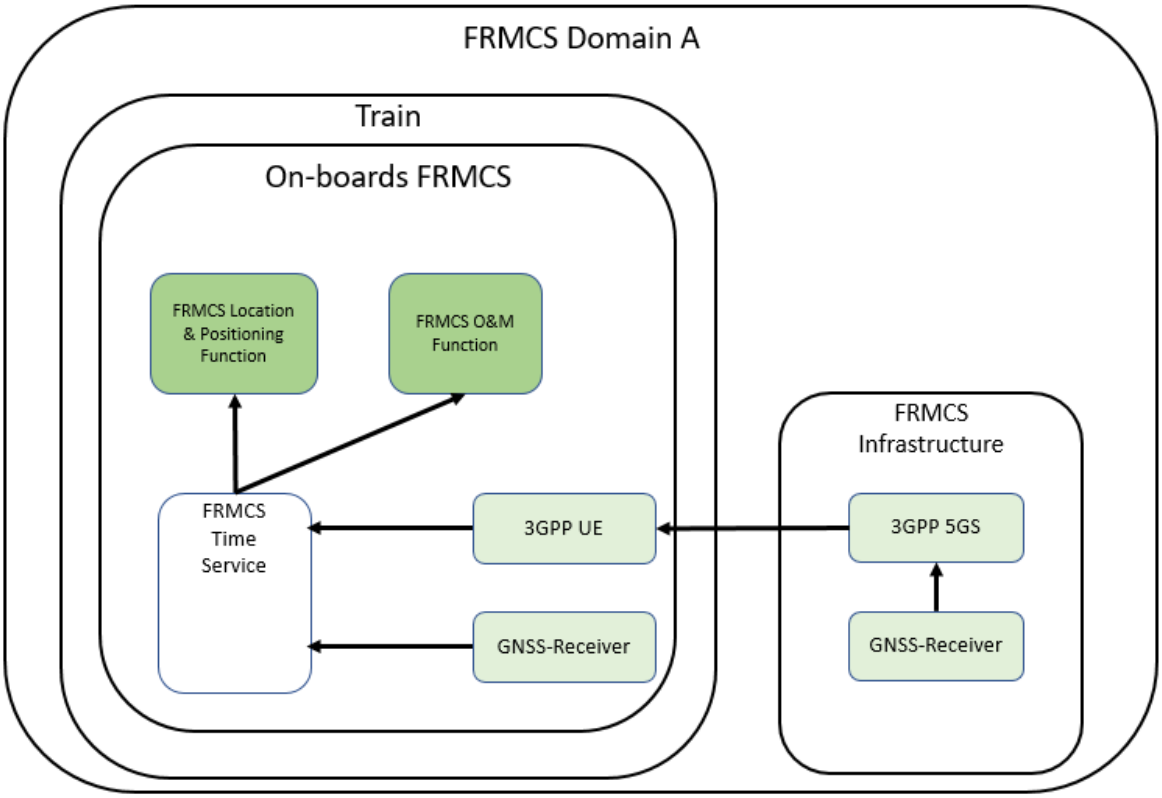


Figure 23-1 – Time Synchronization Flow

Editor's Note: Interface between 3GPP UE and Time service e.g., OBrad is not in scope for FRMCS V2.

Editor's Note: Interface between GNSS Receiver and Time service is not in scope for FRMCS V2.

Note: Usage of multiple UEs including GNSS-Receivers' is left for implementation.

23.4 Generic requirements

23.4.1 FRMCS Time Service shall provide a capability usable by FRMCS Time Service consumers to enquire the time information. (M)

23.4.2 FRMCS Time Service shall provide a capability to convey the enquired time information to consumers of the FRMCS Time Service. (M)

23.4.3 The capability of enquiring the FRMCS Time Service is based on uniform and open manner that can be used by FRMCS Time Service consumers. (I)

23.4.4 The accuracy for the time of day under regular working conditions shall be ±1ms / 24h. (M)

Editor's Note: Value needs to be verified within a validation project and is not in scope for FRMCS V2.

23.4.5 The basic UTC format shall be implemented as follows: YYYYMMDDThhmmss with [ISO 8601] (M)

- Y corresponding to year
- M corresponding to month
- D corresponding to day
- T being a separator
- h corresponding to hours
- m corresponding to minutes and
- s corresponding to second

23.4.6 For accuracy down to milliseconds additional fields should be added according to: YYYMMDDThhmmssxxx (O)

- xxx indicating 000 through 999 milliseconds.

23.5 Performance requirements

Editor's Note: Providing a list of performance requirements/constraints including between FRMCS domains is not in scope for FRMCS V2.

23.6 Security requirements

Editor's Note: Providing a list of security and privacy constraints is not in scope for FRMCS V2.

24 Voice Application Subsystem

24.1 General Functional Architecture and Requirements

24.1.1 Introduction

24.1.1.1 Figure 24-1 provides an overview of the scope of the Voice Application Subsystem (VAS). (I)

24.1.1.2 The VAS encompasses a set of functional blocks that are required to perform operational communications tasks in an interoperable manner: (I-V3)

- FRMCS Service Client
- Coordinating Function
- Common Functions
- Communication Applications
- HMI
- Interface Adapters

24.1.1.3 The VAS interacts with the FRMCS System as defined in SRS chapter [6] using the reference points OB_{APP}, TS_{APP} or TS_{CTRL}. (I)

24.1.1.4 The VAS uses tight coupled mode for OB_{APP} and TS_{APP}. (I)

24.1.1.5 The VAS may interact with: (I)

- GSM-R on-board equipment
- External systems, such as Public Address, Intercom, DSD, IT-Systems, PSTN and others.

24.1.1.6 The VAS interacts with a O&M Systems and Application Repositories through an O&M Client. (I)

24.1.1.7 General requirements applicable to the VAS are specified in chapter 24.1.2, the functional blocks inside VAS boundary are described in chapter 24.1.3. (I)

24.1.1.8 The implementation of the VAS may be in the form of an equipment installed in the cab for use by train drivers and/or an equipment for use by controllers and/or other equipment used for voice communication. (I)

24.1.1.9 The specific requirements for VAS in driver equipment are covered in section 24.2. (I)

24.1.1.10 The specific requirements for VAS in controller equipment are covered in section 24.3. (I)

24.1.1.11 The specification of VAS in equipment other than driver equipment and controller equipment is out of scope. (I)

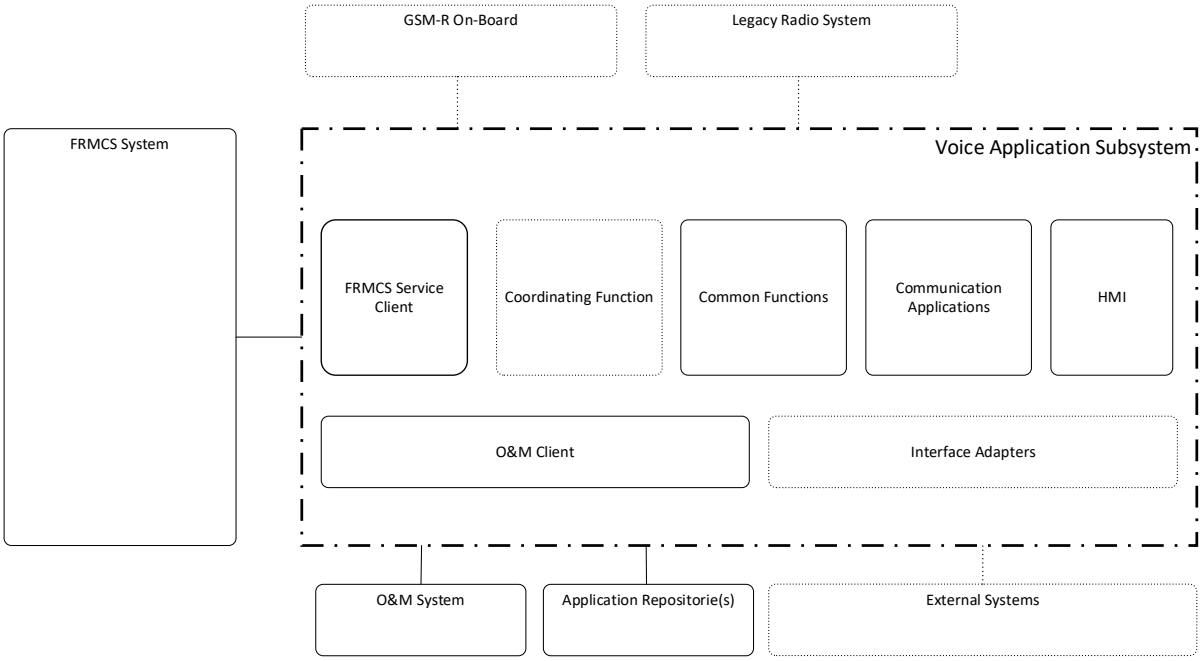


Figure 24-1: Voice Application Subsystem – General Functional Architecture (dotted lines indicate optional blocks)

24.1.2 General Requirements

24.1.2.1 The functional blocks of the VAS shall expose service primitives enabling the interaction of the functional blocks with each other. (M-Vx)

Editor's Note: In FRMCS V2 these service primitives may be vendor specific but may be harmonised in a later version of FRMCS to fully leverage the application concept. This is out of scope of FRMCS v2.

24.1.2.2 The VAS shall manage the communication application's access to resources like the functional blocks HMI, FRMCS Service Client and Interface Adapters taking into account the arbitration rules which are specified in [FRMCS-FRS]. (M)

24.1.2.3 The VAS shall prevent conflicting use of resources by the communication applications (e.g., two communication applications accessing the speaker at the same time) taking into account the arbitration rules which are specified in [FRMCS-FRS]. (M)

24.1.2.4 The VAS shall perform the user login by using one of these methods at a time:

a) preconfigured FRMCS User Identity credentials e.g., personal Smart Card or NFC tag with stored FRMCS User Identity credentials (M)
b) explicit input of FRMCS User Identity credentials by a user through the HMI (M)

24.1.2.5 Intentionally deleted.

24.1.2.6 **Intentionally deleted.**

24.1.2.7 After successful user login, the user shall be given access to the communication applications provided by the VAS, based on the user's profile (authorisation of applications). (M)

24.1.2.8 If the user login fails, the failure reason shall be displayed on the HMI. (M)

24.1.2.9 The status of the MCX user authentication, pending, success, failed, shall be continuously indicated on the HMI. (M)

24.1.3 Specification of Functional Blocks

24.1.3.1 HMI

24.1.3.1.1 The VAS encompasses an HMI suitable for driver/controller voice communication and data communication. (I)

24.1.3.1.1i A key of the HMI can be implemented as a hardware key or as a virtual key on a touch interface. (I)

24.1.3.1.2 HMI shall include as a minimum: (M-V3)

1. Display
2. Keys
3. Specific key for REC
4. Programmable keys
5. Specific Push-To-Talk key
6. Handset

24.1.3.1.3 The HMI shall provide means to the applications to mute and unmute any microphone that is part of the HMI. (M)

24.1.3.1.4 The HMI shall offer capabilities to the applications to assign shortcuts to keys to facilitate the initiation of a communication or to accept / acknowledge an incoming communication with a single user action. (M)

24.1.3.1.5 The HMI display shall offer sufficient screen space to the applications to let the user take the following actions for initiating voice communication, for transferring communications to other users and for inviting a user to join a communication:

1. enter arbitrary user identity/ies or choose user identity/ies from a list (M)
2. optionally select which user identity shall be presented to the called party/ies instead of the default identity selected by the application (M)

24.1.3.1.6 The HMI shall offer capabilities to the applications to facilitate:

1. the indication of a new incoming communication to the user visually and/or audibly (M)
2. the indication of a missed incoming communication to the user visually and/or audibly (M)
3. automatic connection of new incoming communication to the handset or the speaker (M)
4. the continuous indication of ongoing communications visually and/or audibly (M)
5. the continuous indication of a queued communications visually and/or audibly (M)
6. the update and indication of the user identity/ies of all participants in an ongoing connection upon user request (M)
7. for controller devices only: the continuous update and indication of the user identity/ies of all participants in an ongoing connection (M)

24.1.3.2 Communication Applications

24.1.3.2.1 The Communication Applications within VAS include a set of voice and data applications as defined in [FRMCS-FRS] involving driver and/or controllers. (I)

24.1.3.2.2 The following table 24-1 lists all FRS voice applications that shall be part of the Communications Applications offered by the VAS (refer to [FRMCS-FRS] for the full list of voice applications defined):

Name	FRS Ref.	Driver / Controller	Category
Voice communication functions	10.1	both	M
Generic voice communication	10.2	both	M
On-train outgoing voice communication from the train driver towards the controller(s) of the train	10.3	both	M
On-train incoming voice communication from the controller towards a train driver	10.4	both	M
Multi-Train voice communication for drivers	10.5	both	M
Banking voice communication	10.6	both	M-V3
Trackside maintenance voice communication	10.7	controller	M-Vx
Shunting voice communication	10.8	both	M-V3
Ground to ground voice communication	10.10	controller	M
Railway emergency communication [1)]	10.11	both	M

Name	FRS Ref.	Driver / Controller	Category
Public train emergency communication [1)]	10.13	both	M-Vx
On-train outgoing voice communication from train staff towards a ground user	10.15	controller	M-V3
On-train incoming voice communication from a ground user towards train staff	10.16	controller	M-V3
Railway staff emergency communication [1)]	10.17	both	M-Vx
Urgent on-train outgoing voice communication from the train driver towards the controller(s) of the train	10.18	both	M
Urgent multi-train voice communication for drivers	10.19	both	M
On-train voice communication towards passengers (Public Address)	10.23	both	O-V3

Table 24-1: Voice applications mandatory for the Voice Application Subsystem

1) Voice & Data application.

24.1.3.2.3 Although the scope is the Voice Application Subsystem, some data/video applications are as well required for one of the following reasons: (I)

1. Pre-requisite for the voice application to work as designed including fulfilling a general FRMCS requirement (e.g. Role Management and Presence)
2. To potentially substitute a voice application (e.g. Train Departure Communication)
3. Allowing data applications to use resources of the Voice Application Subsystem (e.g. DSD, Messaging Services)

24.1.3.2.4 The following table 24-2 lists all FRS data applications that shall be part of the Communications Applications offered by the VAS (refer to [FRMCS-FRS] for the full list of data applications defined):

Name	FRS Ref.	Driver / Controller	Category
Data communication functions	11.1	both	M
Generic data communication	11.2	both	M-V3
Role management and presence application (only role management part)	11.3	both	M
Access to recording of communications	11.10	both	M-Vx
Critical Advisory Messaging services – safety related data communication	11.15	both	M-V3
Train driver advisory – train performance	11.25	both	M-Vx
Train Departure data communications	11.26	both	M-Vx
Messaging Services	11.27	both	M-V3
Transfer of Data	11.28	both	O-V3
On-train safety device to ground communication	11.34	both	M-V3

Table 24-2: Data applications mandatory for the Voice Application Subsystem

24.1.3.2.5 Following the application concept [FRMCS-FRS, chapter 5] it shall be possible to add further communication applications. (M-Vx)

24.1.3.2.6 The communication applications shall choose the identity of a user by applying the following priorities: (M)

1. Temporary Functional Aliases
2. Permanent Functional Aliases
3. MC Service User Identity

24.1.3.2.7 The communication applications provided by VAS shall allow individual users participating in communications to terminate an on-ongoing communication depending on the type of communication and the user's role. (M)

24.1.3.2.7i The communication applications provided by VAS shall allow individual users participating in communications to put on hold, queue, leave, re-join an on-ongoing communication depending on the type of communication and the user's role. (M-V3)

24.1.3.2.8 The rules to terminate, put on hold, queue, leave, re-join an on-ongoing communication are covered in [FRMCS-FRS] per communication application, the methods are defined in [FRMCS-FIS]. (I)

24.1.3.2.9 The [FRMCS-FIS] provides means to inform all parties of a communication when a new user joins or a user is no longer participating in a communication. (I)

24.1.3.3 Common Functions

24.1.3.3.1 The VAS shall provide or make use of the common functions required by the communication applications included in VAS. (M)

24.1.3.3.2 The common functions are limited to (refer to [FRMCS-FRS] for the full list of common functions defined): (I)

- Role management and presence (only Role Management part)
- Location services
- Authorisation of communications
- QoS and priority
- Arbitration
- Multi-user talker control

24.1.3.4 Coordinating Function

24.1.3.4.1 For multi-mode driver equipment, the VAS hosts the Coordinating Function responsible for executing the change of operation modes FRMCS and GSM-R, or Class B train radio system. (I)

24.1.3.4.2 The requirements for the Coordinating Function are specified in the driver equipment specific section [24.2.4.4]. (I)

24.1.3.5 FRMCS Service Client

24.1.3.5.1 The VAS shall host one or several embedded FRMCS Service Client(s) (M)

24.1.3.6 Interface Adapters

24.1.3.6.1 Interface Adapters may be used to connect the VAS to systems external of FRMCS. (I)

24.1.3.6.2 The requirements for Interface Adapters are specified in the equipment specific sections [24.2.4.6] and [24.3.4.5]. (I)

24.1.3.7 O&M Client

24.1.3.7.1 The O&M Client shall interact with the Application Repository to install / update / remove applications in a controlled and secure way. (M-Vx)

Editor's Note: The interface used is out of scope of FRMCS v2.

24.1.3.7.2 There maybe be multiple Application Repositories (e.g. IM operated and RU operated repositories. (I)

24.1.3.7.3 The O&M Client shall support remote administration and configuration via an O&M System: (M)

- Retrieval of FRIOP (only applicable to driver equipment)
- Communication Applications configuration
- Common Functions configuration
- O&M for remote-management (e.g., SW-Update)

24.1.3.7.4 The management and configuration of the VAS applications or of the VAS functional blocks shall be done in a controlled and secure way. (M)

24.1.3.7.5 The O&M Client shall interact with an O&M System of the IM through an O&M Interface. (M-V3)

Editor's Note: The interface used is out of scope of FRMCS v2.

24.1.3.7.6 The O&M Client shall use FRMCS Services for connecting to the O&M System. (M-V3)

24.1.3.7.7 The O&M Client should interact with an O&M Entity of an RU. (O)

Note: The interface used is left to implementation.

24.1.3.7.8 The O&M Client should provide a local interface to a allow an O&M user to perform O&M tasks locally. (O)

Note: The interface used is left to implementation.

24.2 Driver Equipment

24.2.1 Introduction

24.2.1.1 The driver equipment is an entity providing access to communications services offered by FRMCS system for a driver by use of the VAS. (I)

24.2.1.2 A driver equipment is operated by an IM or an RU. (I)

24.2.2 Functional Architecture

24.2.2.1 The functional architecture of VAS in a driver equipment is shown in Figure 24-2. (I)

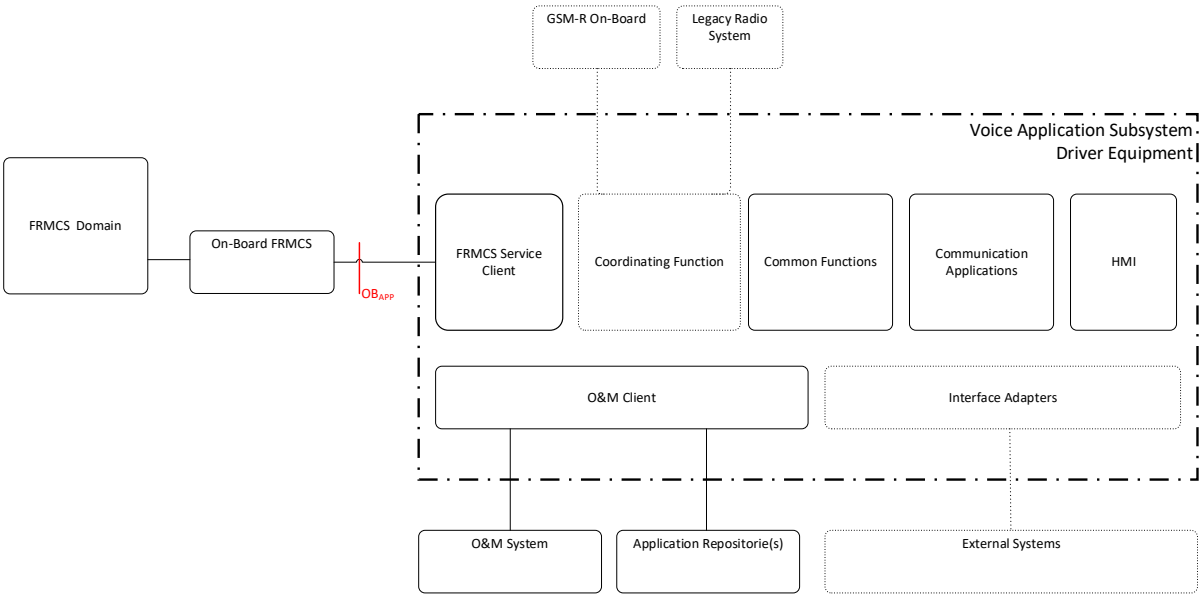


Figure 24-2: VAS Functional Architecture - Driver Equipment (dotted lines indicate optional blocks)

24.2.3 General Requirements

24.2.3.1 Requirements specified in chapter 24.1.2 shall apply. (M)

24.2.3.2 The VAS shall securely store the parameters specified in SRS chapter [19.2.3] retrieved from the FRIOP. (M)

24.2.3.3 The VAS shall use OB_{APP} in tight coupled mode as defined in [FRMCS-FFFIS]. (M)

24.2.3.4 The VAS shall perform the local binding procedure with OB FRMCS as specified in [FRMCS-FFFIS] which includes subscription to the general notification service. (M)

24.2.3.5 The VAS should subscribe to additional OB_{APP} API Services as defined in [FRMCS-FFFIS]. (O)

24.2.3.6 The VAS shall provide the information received from OB_{APP} API Services to other components of VAS (e.g. by a publish/subscribe method). (M)

Note: How to realize the information exchange is left to implementation.

24.2.3.7 After the user has provided the user login credentials using one of the methods specified in clause 24.1.2.4, the VAS shall temporarily cache the credentials locally in a secure way, if the IdMS is temporarily not reachable (e.g. due to being out of FRMCS coverage). (M)

24.2.3.8 If temporary caching of credentials was used due to temporary unavailability of IdMS (24.2.3.7), the user authentication with the IdMS shall be performed as soon as the IdMS can be reached. (M)

24.2.3.9 If temporary caching of credentials was used due to temporary unavailability of IdMS (24.2.3.7), the cached user credentials shall be deleted after authentication with IdMS has been performed. (M)

24.2.3.10 Any user credentials stored in the cache shall be deleted upon powering off or restarting the driver equipment. (M)

24.2.4 Specification of Functional Blocks

24.2.4.1 HMI

24.2.4.1.1 Requirements specified in section 24.1.3.1 shall apply. (M)

24.2.4.1.2 The ergonomics of the HMI shall comply with [UIC 612-04]. (M-V3)
Note: [UIC 612-04] may need to be updated to cover FRMCS

24.2.4.1.3 The HMI may be hosted on a different physical entity than the physical entity hosting the other functional blocks of VAS. (I)

24.2.4.1.4 The connectivity of such detached HMI is out of scope. (I)

24.2.4.1.5 In case FRMCS and GSM-R and/or Class B train radio system modes of operation are supported, the HMI shall provide the user the possibility to trigger the switch of operation modes between FRMCS, GSM-R and Class B train radio system (e.g. via a key). (M)

24.2.4.1.6 In case more than one HMI is connected to the same VAS instance, the following shall apply: (M-V3)

1. On each HMI, one user can login.
2. Each logged-in user can use the communication applications of the VAS based on this user's profile.
3. An HMI where no user has logged in, provides limited access to communication applications of the VAS.

24.2.4.2 Communication Applications

24.2.4.2.1 Requirements specified in chapter 24.1.3.2 shall apply. (M)

24.2.4.3 Common Functions

24.2.4.3.1 Requirements specified in chapter 24.1.3.3 shall apply. (M)

24.2.4.4 Coordinating Function

24.2.4.4.1 The Coordinating Function shall retrieve information about GSM-R network availability from the GSM-R On-board. (M)

Note: How to retrieve this information is left to implementation.

24.2.4.4.2 The procedures for selecting and changing the mode of operation between FRMCS and GSM-R are specified in chapter 24.2.6. (I)

24.2.4.4.3 The procedures for selecting and changing to a mode of operation other than FRMCS and GSM-R are left for implementation. (I)

24.2.4.5 FRMCS Service Client

24.2.4.5.1 Requirements specified in chapter 24.1.3.5 shall apply. (M)

24.2.4.6 Interface Adapters

24.2.4.6.1 The driver equipment Interface Adapters should be used to connect on-board communication systems such as Public Address, Intercom, etc. as well as any other (optional) on-board train systems such as DSD, train borne recorder, etc. to the VAS. (O)

Note: Alternatively, these systems may connect directly to OB FRMCS in loose or super loose coupling mode.

24.2.4.6.2 The driver equipment Interface Adapters shall connect to the consist network as defined in [SUBSET-147]. (M-Vx)

24.2.4.6.3 If implemented the driver equipment Interface Adapters shall connect to devices complying with the following specifications: (M-V3)

- [UIC 568-3] for Public Address and Intercom
- [UIC 641] for Driver Safety Device
- [SUBSET-119] for Train Interface

24.2.4.7 O&M Client

24.2.4.7.1 Requirements specified in chapter 24.1.3.7 shall apply. (M)

24.2.5 Interworking with GSM-R

24.2.5.1 The VAS in a driver equipment shall either use FRMCS or GSM-R. (M)

24.2.5.2 During transition from/to FRMCS the VAS may be connected to both systems for a short period of time. (I)

24.2.5.3 The mapping of identities from/to the FRMCS system and to/from the GSM-R system is done by the IWF as specified on SRS chapter [9.5] (I)

24.2.5.4 In case no mapping of a functional ID (FA / FN) can be done, the user ID (FRMCS Service User Identity / MSISDN) of the initiator of the communication shall be presented on the HMI. (M)

24.2.6 Specific Procedures for FRMCS/GSM-R Dual Mode Implementations

24.2.6.1 Power-up / Start of Mission

24.2.6.1.1 At power up, the Voice Application Subsystem shall follow the following procedure to select FRMCS or GSM-R mode of operation.

1. The VAS performs the local binding procedure with On-Board FRMCS as specified in [FRMCS-FFFIS]. (I)
2. The user shall be prompted to execute the FRMCS user login via the HMI. (M)
3. Mode of operation:
   a) The user shall be prompted to select a mode of operation (M).
   b) Auto-selection by external system or by configuration shall be used alternatively (M-Vx).
4. If GSM-R Mode of operation is selected, the Coordinating Function shall grant the GSM-R On-Board access to the HMI, the further network selection (PLMN ID) and registration procedures shall follow [EIRENE-FRS]. (M)
5. If FRMCS Mode of operation is selected, the Coordinating Function shall grant the VAS access to the HMI, the further registration procedures shall follow [FRMCS-FIS]. (M)
6. The selection of the FRMCS domain is performed by the OB FRMCS and is transparent to the user. As fallback a manual selection of the FRMCS domain by the user shall be offered. (M)
7. The user shall be informed in a visual and audible manner if the selected communication system has been successfully activated. (M)

24.2.6.2 Selection Mode of Operation after Network Loss

Editor's Note: To be further developed but not in scope of FRMCS V2.

24.2.6.3 Transition from/to FRMCS to/from GSM-R mode of operation

24.2.6.3.0 A manual mode switch is used for both transition directions, i.e. the service transition to FRMCS is not auto coupled to the NTT received by the OB FRMCS.

Therefore, the transition of voice services is not synchronized with the transition of ATP/ATO communication. (I)

24.2.6.3.1 Upon reception of a trigger (e.g. button pressed on HMI) the Coordinating Function shall transition the mode operation. (M)

24.2.6.3.2 Transition from FRMCS to GSM-R shall follow the sequence defined here:

1. Mode switch trigger is received from HMI. (I)
2. The VAS shall leave or, if initiator of the communication, shall terminate any ongoing FRMCS communication service. (M)
3. The VAS shall deregister the FRMCS user IDs and related functional aliases. (M)

Note: The procedure assumes sufficient coverage overlap to ensure the deregistration can be performed before the FRMCS coverage ends. De-registration of FRMCS IDs under GSM-R coverage via IWF would be a more robust approach.

4. The GSM-R cab radio application gets exclusive access to the HMI. (I)
5. The user shall be prompted to choose a GSM-R network (PLMN ID) (M)
6. The GSM-R on-board shall be requested to perform functional registration of the equivalent Functional Number(s) without any user intervention required. (M)
7. The re-establishment of a previously ongoing communication service is left to the previously involved users. (I)

24.2.6.3.3 Transition to FRMCS from GSM-R follows the sequence defined here:

1. Mode switch trigger is received from HMI. (I)
2. If FRMCS is available (FTD_AVL_NOTIF received from OB FRMCS), the mode switch operation proceeds, otherwise the mode switch shall be rejected and be signalled to the HMI. (M)

Note: It is assumed that the On-Board FRMCS has received an NTT at a certain point in time and independent of the mode switch trigger. Upon reception of the NTT the OB FRMCS prepares the transport layer services and thereafter issues an FTD_AVL notification.

3. The selection of the FRMCS domain is performed by the OB FRMCS and is transparent to the user. As fallback a manual selection of the FRMCS domain by the user shall be offered. (M)
4. The GSM-R on-board is requested to leave or, if initiator of the communication, shall terminate any ongoing GSM-R communication service. (M)
5. The GSM-R on-board shall be requested to de-register the assigned Functional Numbers. (M)

Note: The procedure assumes sufficient coverage overlap to ensure the deregistration can be performed before the GSM-R coverage ends. De-registration of GSM-R FNs under FRMCS coverage via IWF would be a more robust approach.

1. The VAS gets exclusive access to the HMI. (I)
2. The VAS shall perform the MCX user authentication procedure and retrieve the equivalent functional aliases without any user intervention required. (M)
3. The re-establishment of a previously ongoing communication service is left to the previously involved users. (I)

24.3 Controller Equipment

24.3.1 Introduction

24.3.1.1 The controller equipment is an entity providing access to the FRMCS system for a controller by use of the VAS. (I)

24.3.1.2 A controller equipment is operated by an IM or an RU. (I)

24.3.2 Functional Architecture

24.3.2.1 The functional architecture of VAS in a controller equipment is shown in Figure 24-3. (I)

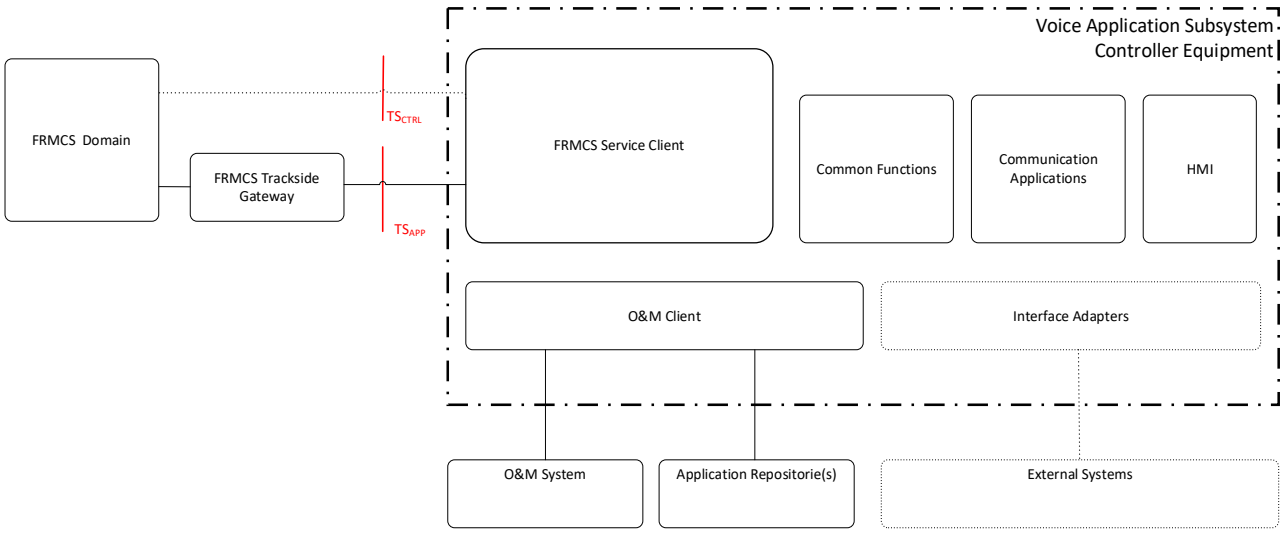


Figure 24-3: VAS Functional Architecture - Controller Equipment (dotted lines indicate optional blocks)

24.3.3 General Requirements

24.3.3.1 Requirements specified in chapter 24.1.2 shall apply. (M)

24.3.3.2 The VAS of a controller equipment supporting TS_{APP} shall interconnect with the FRMCS service domain using TS_{APP} in tight couple mode. (M)

24.3.3.3 The VAS of a controller equipment not supporting TS_{APP} shall interconnect with the FRMCS service domain using TS_{CTRL} (M)

24.3.3.4 A VAS of a controller equipment using TS_{CTRL} or TS_{APP} shall not use the other reference point simultaneously. (M)

24.3.4 Specification of Functional Blocks

24.3.4.1 HMI

24.3.4.1.1 Requirements specified in section 24.1.3.1 shall apply. (M)

24.3.4.1.2 For implementations where FRMCS and GSM-R co-exists and are interconnected, a single HMI shall offer access to FRMCS and GSM-R services without the need of a mode switch. (M-V3)

24.3.4.1.3 The HMI may be hosted on a different physical entity than the physical entity hosting the other functional blocks of VAS. (I)

24.3.4.1.4 The connectivity of such detached HMI is out of scope. (I)

24.3.4.2 Communication Applications

24.3.4.2.1 Requirements specified in chapter 24.1.3.2 shall apply. (M)

24.3.4.3 Common Functions

24.3.4.3.1 Requirements specified in chapter 24.1.3.3 shall apply. (M)

24.3.4.4 FRMCS Service Client

24.3.4.4.1 Requirements specified in chapter 24.1.3.5 shall apply. (M)

24.3.4.5 Interface Adapters

24.3.4.5.1 The controller equipment Interface Adapters should be used to connect to systems external to FRMCS. (O)

24.3.4.5.2 Such external systems may include a railway disposition system or any other business-supporting IT-systems. (I)

24.3.4.5.3 Interface Adapters may also be used to interconnect the controller equipment to communication services provided by GSM-R, business telephony systems or PSTN in case such interconnection is not offered by an FRMCS IWF. (I)

24.3.4.6 O&M Client

24.3.4.6.1 Requirements specified in chapter 24.1.3.7 shall apply. (M)

24.3.5 Interworking with GSM-R

24.3.5.1 The VAS of a controller equipment can be serving a GSM-R or FRMCS exclusive area as well as an area having both systems. (I)

24.3.5.2 The VAS of a controller equipment serving an area with GSM-R and FRMCS, shall be interconnected to both systems (e.g., through IWF), however functionally registered in only one system. (M)

24.3.5.3 The mapping of identities from/to the FRMCS system and to/from the GSM-R system is done by the IWF as specified on SRS chapter [9.5] (I)

24.3.5.4 In case no mapping of a functional ID (FA / FN) can be done, the user ID (FRMCS Service User Identity / MSISDN) of the initiator of the communication shall be presented on the HMI. (M)

24.3.6 Non-Functional Requirements

Editor's Note: the specification of non-functional requirements is out of scope for FRMCS V2.

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

A.1 Overview of QoS Requirement Values

The Table A.1-1 lists the FRMCS E2E QoS parameter values for all relevant communication sessions (based on FRS applications) as well as the mapping towards 3GPP QoS parameters. Comments w.r.t. to the communication sessions are listed below. The numbers hold for inner-domain communication session, for inter-domain communication and domain transitions derivations from the target numbers are expected.

Communication Session					FRMCS E2E QoS Parameters (Section 14.4)							3GPP QoS Parameters (Section 14.6)			
Communication Session Category (1)	Grade of Automation (see Note)				Peak Data Rate per Connection		Data Rate Aggregation		FRMCS E2E Packet Latency (FRMCS E2E Packet Reliability)	Session Setup Time	Acceptable Communication Session Interruption Time (see Section 10)	Flow Bit Rates		5QI	ARP
	GoA0	GoA1	GoA2	GoA3/4	UL	DL	Single conn. per cell (2)	All conn. per cell (3)				MFBR	GFBR		
FRMCS Signalling (4)	x	x	x	x	20 kbps (95%)	20 kbps (95%)	-	x	200 ms (95%)	Normal	t.b.d.	n/a	n/a	5 / 69	1
Pre-defined Default (5)	x	x	x	x	n/a	n/a	n/a	n/a	n/a	Normal	t.b.d.	n/a	n/a	8	8
Emergency Voice (6)	x	x	x	x	45 kbps (95%)	45 kbps (95%)	-	x	200 ms (95,0001%)	Immediate	t.b.d.	45 kbps	10 kbps	65 (GBR)	2
Voice (7)	x	x	x	x						Normal	t.b.d.	45 kbps	10 kbps	65 (GBR)	3-8
Urgent Data (8)	x	x	x	x	10 kbps (90%)	10 kbps (90%)	-	x	1s (98%)	Immediate	t.b.d.	n/a	n/a	8	3, 5
General Data (9)	x	x	x	x					1s (95%)	Normal	t.b.d.	n/a	n/a	8	5, 6
TCMS (10)	x	x	x	x	-	-	-	-	-	Normal	t.b.d.	n/a	n/a	8	7
ATP Regular Data (11)	-	x	x	x	10 kbps (95%)	10 kbps (95%)	-	x	1s (99%)	Immediate	t.b.d.	10 kbps	1 kbps	4 (GBR)	4
ATP Compl. Data (12)	-	x	x	x	10 kbps (90%)	10 kbps (90%)	x	-	1s (95%)	Normal	t.b.d.	n/a	n/a	8	6
ATO (13)	-	-	x	x	10 kbps (95%)	10 kbps (95%)	-	x	1s (95%)	Normal	t.b.d.	n/a	n/a	8	6
	-	-	x	x	-	100 kbps (90%)	x	-							

Comments
(1) FRS Applications not yet covered : 10.7, 10.8, 10.9, 10.13–10.17, 10.20–10.22, 10.24, 10.25, 11.6 – 11.8, 11.11 – 11.14, 11.16, 11.17, 11.20 – 11.26, 11.29 - 11.32, 12.1 – 12.5
(2) Sufficient to serve a single train at a time per cell for the respective application
(3) All trains within a cell shall be served simultaneously for the respective application
(4) “FRMCS Signalling” refers to the FRMCS internal signalling (related to MCX and 5G)
(5) 5QI=8 for predefined data applies for MCData only,w.r.t. clause 14.7.5
(6) “Emergency Voice” includes FRS applications 10.11
(7) “Voice” include FRS applications 10.18-10.19 (ARP=3), 10.3-10.6 (ARP=5), 10.10+10.23 (ARP=6), 10.2 (ARP=8). The data rate is based on codec rate + RTP/UDP/IP header information
(8) “Urgent Data” includes FRS applications 11.15 (ARP=5), 11.34 (ARP=3)
(9) “General Data” includes FRS applications 11.3 (ARP=5), 11.9 (ARP=6). The data rate is considered to include overhead w.r.t. TCP/IP header information.
(10) “TCMS” includes FRS applications 11.19
(11) “ATP Regular Data” refers to ETCS on-board – ETCS trackside communication and includes FRS applications 11.4. The data rate is considered to include overhead w.r.t. TCP/IP header information.
(12) “ATP Complementary Data” refers to, but not restricted to, ETCS complementary services (e.g, KMS) and includes FRS applications 11.18. The data rate is considered to include overhead w.r.t. TCP/IP header information.
(13) “ATO” include FRS applications 11.5 (see further explanation in Annex A.4. The data rate is considered to include overhead w.r.t. TCP/IP header information.

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

Note: The columns for Grade of Automation (GoA) refer to the dimensioning of the FRMCS trackside, e.g., to support GoA2, all applications with an “x” in the GoA2 column should be considered. To calculate the respective data rates, the column data rate aggregation is to be considered, i.e., if the data rate of the communications session is to be considered for every connection (e.g., every train) within a radio cell or just for a single connection (considering that the support of parallel connections is not required for an appropriate dimensioning).

The mapping of FRS Applications to the communication session categories included in Table A.1-1 follows the logic in Table A.1-2.

Parameter	FRS Indication	SRS QoS Value
Latency	LOW	≤200msec
	NORMAL	>200msec ≤1sec
	BEST EFFORT	>1sec
Reliability	HIGH	≥99%
	MEDIUM	<99% & >95%
	NORMAL	≤95%
Throughput	LOW	≤50kbps
	MEDIUM	>50kbps

Table A.1-2 – Mapping of FRS Indications to SRS QoS Values

A.2 Derivation of QoS Requirements Based on Voice

For enabling acceptable voice quality, the mouth-ear-delay shall not exceed 300 ms (95%) based on [TS 22.179]. To fulfil the requirement, the critical path is considered, which is the path from an onboard device to the service server and back to another onboard device (see Figure A.2-1). Based on the components illustrated in the figure A.2-1 the values listed in Table A.2-1 for packet latency and packet reliability are derived.

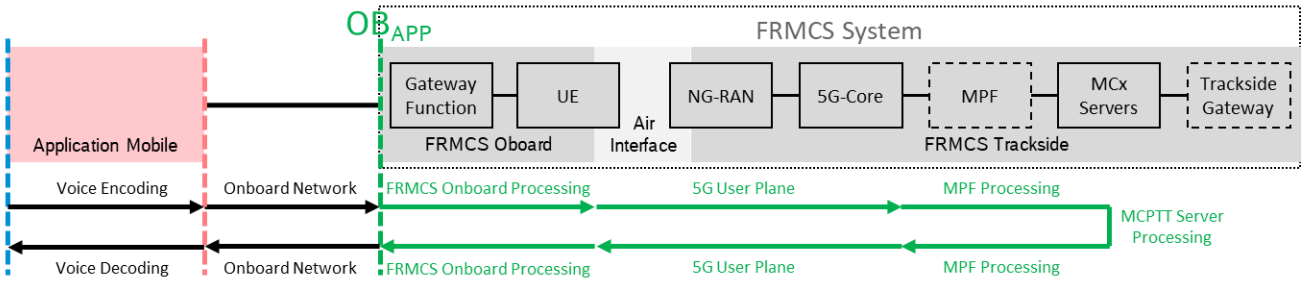


Figure A.2-1: Human User E2E Path for voice communication considering the most critical path (onboard - onboard via server)

Component	Packet Latency (Packet Reliability)	Derivation / Comments
Voice Encoding	45 ms (99,9%)	2x frame size (20 ms) + look ahead time (5 ms) [3GPP TS 26.171; TS 26.190]
Voice Decoding	45 ms (99,9%)	2x frame size (20 ms) + look ahead time (5 ms) [3GPP TS 26.171; TS 26.190]
Onboard Network	5 ms (99,9%)	Based on [Subset-147] 8.4.4.1.2 for process data
On-Board FRMCS Processing	15 ms (99,9%)	Remaining packet latency (packet reliability) is split between On-Board FRMCS Processing and Server Processing
5G User Plane	75 ms (98%)	Based on [TS 23.289], MCPTT shall use 5QI=65. Based on [TS 23.501], 5QI=65 refers to 75 ms (98% holds for all GBR packets)
Server Processing (MPF+ MCPTT)	20 ms (99%)	Remaining packet latency (packet reliability) is split between On-Board FRMCS Processing and Server Processing

Table A.2-1: Derived values for packet latency (packet reliability)

A.3 Derivation of QoS Requirements for ETCS

The QoS requirements for packet latency and packet reliability for ETCS are derived from [Subset-093], as the parameters in there need to be translated for FRMCS and cannot be applied right away. The derivations in this section are based on [Subset-093] Section 6.7.5, which specifies the Transaction Transfer Delay (TTD) with 2.6 s (99%). Figure A.3-1 shows how the complete path of the TTD is sub-divided into several components, while Table A.3-1 lists the derived values on packet latency and packet reliability.

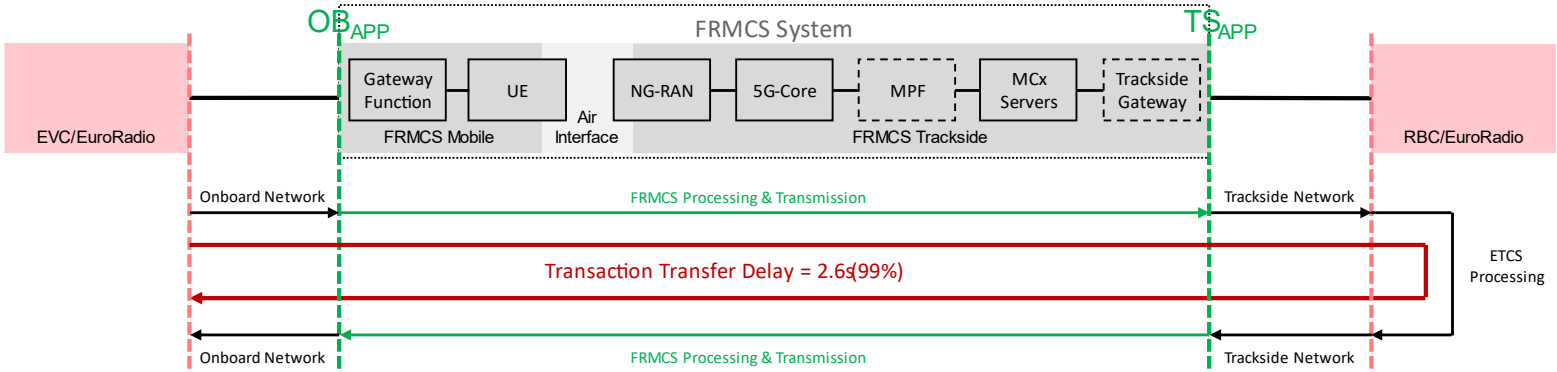


Figure A.3-1: E2E path for transaction transfer delay for ETCS

Component	Packet Latency (Packet Reliability)	Derivation / Comments
Onboard Network	5 ms (99,9%)	Based on [[SUBSET-147] 8.4.4.1.2 for process data
Trackside Network	50 ms (99,9%)	Packet latency based on [SUBSET-093] 6.7.5.6 assuming an equal split of UL and DL Packet reliability is distributed over the components
ETCS Processing (RBC)	30 ms (99,9%)	Packet latency based on [SUBSET-093] 6.7.5.5. Packet reliability is distributed over the components
FRMCS Processing & Transmission	1,23 s (99,7%) → 1 s (99%)	Remaining packet latency (packet reliability) is based on [SUBSET-093] 6.7.3 and considering an equal split of UL and DL. The translation from 99,7% towards 99% is subject to validation.

Table A.3-1: Component wise values of packet latency and packet reliability.

A.4 Derivation of QoS Requirements for ATO

The derivation of the data rate for ATO is based on the messages defined in [SUBSET-126] as well as indications provided by [SUBSET-148]. For the exchange of regular data of ATO (frequent messages), [SUBSET-148] Section 6.2.1.1.5 is considered, resulting in 10 kbps as upper bound. In addition to that a maximum of 100 kbps is considered for the transmission of less regular Journey Profiles and Segment Profiles (only a few per hour). Due to the rare transmission, it is considered that the transmission does not need to happen for all trains/connections within a cell in parallel but at least for a single train/connection per cell.

A.5 Resulting Data Rate Requirements per Train

This section provides the summarized data rate figures for several GoA equipment levels per train as well as per single additional connection per cell.

Grade of Automation	Applications	Data Rate			
		Uplink (all connections per cell)	Uplink (single connection per cell)	Downlink (all connections per cell)	Downlink (single connection per cell)
GoA0	FRMCS Signalling	20 kbps		20 kbps	
	Voice/Emergency Voice	45 kbps		45 kbps	
	Basic Data	10 kbps		10 kbps	
	Summary	**75 kbps**		**75 kbps**	
GoA1	FRMCS Signalling	20 kbps		20 kbps	
	Voice/Emergency Voice	45 kbps		45 kbps	
	Basic Data	10 kbps		10 kbps	
	ATP Regular Data	10 kbps		10 kbps	
	ATP Compl. Data		10 kbps		10 kbps
	Summary	**85 kbps**	**10 kbps**	**75 kbps**	**10 kbps**
GoA2	FRMCS Signalling	20 kbps		10 kbps	
	Voice/Emergency Voice	45 kbps		45 kbps	
	Basic Data	10 kbps		10 kbps	
	ATP Regular Data	10 kbps		10 kbps	
	ATP Compl. Data		10 kbps		10 kbps
	ATO Regular Data	10 kbps		10 kbps	
	ATO Compl. Data				100 kbps
	Summary	**95 kbps**	**10 kbps**	**95 kbps**	**110 kbps**

Table A.5-1: Component wise values of packet latency and packet reliability.

A.6 Acceptable interruption time during IFDT

This annex provides the maximum acceptable interruption time per application. For that the service continuity within FRMCS be satisfied, the service interruption due to IFDT needs to be within this limit.

Application	Acceptable interruption time of application	Comment
ATP (clause 10.1.6.6)	5 sec (99,9%)	The service interruption due to IFDT is the time from the initiation of IFDT until the completion of the recovery of an ongoing ATP connection.
REC in case of clause 10.1.6.4	40 sec (99%)	The service interruption due to IFDT is the time from the release of the ongoing voice communication of the REC group (in the context of clause 10.1.6.4) until the successful recovery of the voice communication for the same REC group.

Annex B. Mapping between application regimes and FRS applications

Applications		FRS	Application regime	OB_{APP} coupling mode	TS_{APP} coupling mode
Automatic Train Protection communication		11.4	Loose	Loose	Loose
Automatic Train Operation communication (up to ATO GoA2)		11.5	Loose	Loose	Loose
Key Management System		11.18	Superloose	Loose	Loose
Public Key Infrastructure		N/A	Superloose	Loose	Loose
Railway Emergency Communication		10.11	Tight	Tight	Tight
Applications supported by VAS of Controller Equipment		10.3, 10.4	Tight	N/A	Tight

Annex C. 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.

Printed by

International Union of Railways

16, rue Jean Rey 75015 Paris - France

March 2024

Legal deposit March 2024

ISBN 978-2-7461-3119-4