Grant agreement
No 951725

Deliverable D2.1

TOBA Architecture Report

Disclaimer:

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

No part of this document may be copied, reproduced, disclosed or distributed by any means whatsoever, including electronic without the express permission of the author(s). The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

5GRAIL

5G for future RAILway mobile communication system

D2.1 - TOBA Architecture Report

Due date of deliverable: 30/04/2021

Actual submission date: 31/01/2023

Leader/Responsible of this Deliverable: KONTRON / Farid BAZIZI

Reviewed: Y

Document status

Revision	Date	Description
0.1	11/05/2021	First issue - open points to be addressed in revision 2
0.2	12/05/2021	Inputs from the different workstreams merged by WP Leader
0.3	18/05/2021	Update from WP leader based on comments from members of the WP
0.4	21/05/2021	Revised version from Coordinator
1.0	26/05/2021	Additional updates and consolidation of the first deliverable version
1.1	05/07/2021	Additional updates from review comments and open points progresses
1.2	18/10/2021	Additional updates from review comments and open points progresses
2.0	15/03/2022	Revision from Coordinator of the second deliverable version. Modifications following E.C comments Modifications and corrections of OBAPP API Corrections following comments from WP2 partners Version submitted

3.0	16/01/2023	Details regarding border-crossing function Various API corrections Version submitted

Project funded from the European Union’s Horizon 2020 research and innovation program

Dissemination Level		
PU	Public	✓
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/11/2020 Duration: 30 months

Executive Summary

5GRAIL aims to demonstrate prototypes of the 5G FRMCS ecosystem and to validate the FRMCS/5G specifications, including the compliance of railway essential operational services such as railway ETCS, ATO, Voice, TCMS, video and PIS.

This document provides the architecture details to support the development of prototypes within WP2 that aims to be rolled out in Europe for a series of FRMCS/5G pilot tests (in labs & in the field) to demonstrate how these technical solutions can be integrated, to validate their feasibility and to evaluate their performance under a combination of environmental conditions in various test-sites (France, Hungary and Germany).

The main challenge was to address the key design paradigms for the FRMCS/5G gateways prototypes:

- Decoupling of Applications and Communication Services/Transport
- Bearer Flexibility (i.e. variety of bearers or Radio Access Technologies simultaneously)
- Resource Sharing (e.g. providing transport services for multiple applications of any category using the same FRMCS on-board system considering the individual QoS requirements of the application and possibly priorities among applications)

Overall, this has been solved with 5G technology and MCX services. Indeed, for each design paradigms, a technology enabler has been considered, studied and whenever the technology ecosystem was not mature enough, alternative solutions have been elaborated to support the execution of 5GRAIL trials. This is summarized in the below table.

Table 1: Technology enablers for FRMCS/5G TOBA architecture

FRMCS gateway design paradigm	Technology enabler	Technology maturity	5GRAIL focus
Decoupling Service/Transport	MCX services	Standardized & available	MC Services and MC DATA IPConn. Introduced in 2.2.1 and 2.2.4
Bearer Flexibility	5G ATSSS	Standardized, not available (UE and 5GCore not available)	Multiconnectivity. Introduced in 2.2.5
Resources Sharing	5G 5QI	Standardized, not available (UE and 5GCore not available)	5QI based. Introduced in 2.2.3

Moreover, due to the partial availability of specifications, there is a set of assumptions listed in the chapter 3 3and considered for the proposed phased design of the modules.

On top of these assumptions, there were also technical open points that emerged naturally during the architecture elaboration. These open points are in general due to FRMCS/5G specifications gaps. All these open points have been addressed with this revision, either by considering the specification work advance, or by agreeing within the Consortium assumptions.

Abbreviations and Acronyms

Abbreviation	Description
3GPP	3rd Generation Partnership Project
5G NSA	5G Non StandAlone
5G SA	5G StandAlone
API	Application Programmable Interface
AS	Application Server
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATSSS	Access Traffic Steering, Switching and Splitting
CA	Certificate Authority
CAM	Connected and Automated Mobility
CCS	Control Command and Signalling
CCTV	Closed Circuit TeleVision
CP	Control Plane
CSCF	Call/Session Control Functions
CSFB	Circuit Switched Fall Back
DN	Domain Name
DRCS	Data Radio Communication System
DSCP	Differentiated Services Code Point
DSD	Driver Safety Device
EDOR	ETCS Data Only Radio
ETCS	European Train Control System
EU	European Union
FFFIS	Form Fit Functional Interface Specification
FIS	Functional Interface Specification
FRMCS	Future Railway Mobile Communication System
FRS	Functional Requirements Specification

GA	Grant Agreement
GCG	Ground Communication Gateway
GNSS	Global Navigation Satellite System
GoA	Grade of Automation
GRE	Generic Routing Encapsulation (RFC8086) -> Tunnel GRE
GTW or GW	GaTeWay or GateWay
H2020	Horizon 2020 framework program
HSS	Home Subscriber System
IMPI	IP Multimedia Private Identity
IMPU	IMS Public User Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IWF	Inter Working Function
JSON	JavaScript Object Notation
MCG	Mobile Communication Gateway
MCx	Mission Critical
MPTCP	MultiPath Transmission Control Protocol
MNO	Mobile Network Operator
MQTT	Message Queuing Telemetry Transport
mTLS	Mutual Transport Layer Security
N3IWF	Non-3GPP Inter Working Function
NR	New Radio
NSA	Non-Stand Alone (5G Core architecture)
OB	On Board
OB_GTW	On-Board Gateway
OBA	On-Board Application (e.g. ETCS on-board, ATO on-board)
OBU	On-Board Unit
OM	Operation & Maintenance

OTA	Over The Air
OTT	Over The Top
PCB	Printed Circuit Board
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PKI	Public Key Infrastructure
PSS	Process Safety System
QoS	Quality Of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RBC	Remote Block Centre
REST	REpresentational State Transfer
RPC	Remote Procedure Call
RF	Radio Frequency
SA	Stand Alone (5G Core architecture)
S-CSCF	Servicing-CSCF (Correspondence IMPU - @ IP)
SIP	Session Initiation Protocol
SMA	Subminiatures version A, type of coaxial RF connectors
SRS	System Requirements Specification
TCMS	Train Control Management System
TCN	Train Communication Network
TLS	Transport Layer Security
TOBA	Telecom On-Board Architecture
TRDP	Train Realtime Data Protocol (see IEC 61375)
TS	Track Side
TS_GTW	TrackSide Gateway
TSE	Track Side Entity (e.g. RBC, KMC, ATO trackside)
TSI	Technical Specification for Interoperability

UE	User Equipment
UIC	Union Internationale des Chemins de fer
UP	User Plane
URLLC	Ultra-Reliable Low-Latency Communications (5G)
URS	User Requirements Specification
VPN	Virtual Private Network
WP2	Work Package 2

Definitions

Term	Term Definition
Application	Provides a solution for a specific communication need that is necessary for railway operations. In the context of this document, an application is interfacing with the FRMCS on-board system, through the OB_{APP} reference point, to receive and transmit information to ground systems, (for example, ETCS, DSD, CCTV, passenger announcements, etc.).
Application Coupled mode	It defines if an application is aware of the services used in the FRMCS service layer.
Loose Coupling mode	Coupling mode for an application which is not 3GPP MCx aware
Tight Coupling mode	Coupling mode for an application which is 3GPP MCx aware
Application Service	Application part responsible of the UP management
Bearer Flexibility	The FRMCS on-board system shall be capable of providing transport services using a variety of bearers (i.e. Radio Access Technologies) [FRMCS On-network communication shall support the flexible use of different radio bearers]
Channel	Specific logical or physical communication link between assets (IEC)
Communication Services	Services enabling the exchange of information between two or more applications
Communication service availability	Percentage value of the amount of time the end-to-end communication service is delivered according to an agreed QoS, divided by the amount of time the system is expected to deliver the end-to-end service according to the specification in a specific area.
Communication service reliability	Ability of the communication service to perform as required for a given time interval, under given conditions.
Compliance authorities	Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations (NF EN IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2 : technical security requirements for IACS components, 2019-04).
Conduit	Logical grouping of communication channels that share common security requirements connecting two or more zones (IEC)
Control Plane	The control plane carries signalling traffic between the network entities.

Data communication	Exchange of information in the form of data, including video (excluding voice communication).
Domain	The highest-level group of functional entities (e.g., FRMCS is a domain, whereas PLMNs operated by different operators are administrative domains).
End-to-end latency	The time that takes to transfer a given piece of information unidirectional from a source to a destination, measured at the communication interface, from the moment it is transmitted by the source to the moment it is successfully received at the destination.
FRMCS On-board gateway function	It is an on-board gateway function responsible for the coordination and managing of access to the FRMCS transport services offered by the FRMCS system.
FRMCS On-Board Application Client	Enables authorization of an application to the FRMCS Gateway.
FRMCS Radio Module	Modem with one or more 3GPP or/and non-3GPP radio access technologies supported by the FRMCS system.
FRMCS Service Client	Enables the use of the Communication Services and/or Complementary Services for the railway applications.
Harmonized Frequency	Harmonized communications (900 / 1900 MHz) (ETCS, ATO, Voix) Interoperability requirements
Infrastructure network	Access & core networks + MCx & IMS
Interworking	Interworking is the functionality of two networks to talk to each other enabling services to be delivered across the two networks
“Flat-IP” Coupling Mode	This is a sub-mode of Loose-coupling type with static configuration of the requested session. Hence, flat-IP applications can only use the static session configured in FRMCS OB_GTW and TS_GTW.
Network slice	A set of network functions and corresponding resources necessary to provide the required telecommunication services and network capabilities.
Non-Harmonized Frequency	Frequencies used for specific needs of infrastructure managers (telediags, data offload in stations, not for passengers). This spectrum cannot be used for interoperability
Priority service	A service that requires priority treatment based on operator policies.
Product	System, subsystem or component that is manufactured, developed or refined for use by other products (IEC 62443-4-1)
QCI (or 5QI)	A scalar that is used as a reference to a specific packet forwarding behavior (e.g. packet loss rate, packet delay budget) to be provided to a SDF. This may be implemented in the access network by the QCI referencing node specific parameters that control packet forwarding treatment (e.g. scheduling weights,

	admission thresholds, queue management thresholds, link layer protocol configuration, etc.), that have been pre-configured by the operator at a specific node(s) (e.g. eNodeB)
Reliability	In the context of network layer packet transmissions, percentage value of the amount of sent network layer packets successfully delivered to a given system entity within the time constraint required by the targeted service, divided by the total number of sent network layer packets.
Service continuity	The uninterrupted user experience of a service that is using an active communication when a UE undergoes an access change without, as far as possible, the user noticing the change.
Steering	Choosing the best available network based on data plan, speed, cost or latency.
Splitting	Splitting the traffic over two networks to achieve higher speeds. Networks can be combined to increase download speed, upload speed or both.
System under consideration	Defined collection of IACS assets that are needed to provide a complete automation solution, including any relevant network infrastructure assets
Switching	Moving seamlessly from one network to another. For instance, when a user leaves their home Wi-Fi network and joins the cellular network or roams from Wi-Fi hotspot to another.
Transfer interval	Time difference between two consecutive transfers of application data from an application via the service interface to 3GPP system.
Transport Service	It is a service that provides transport of user information and control signals between corresponding reference points considering the required QoS for the individual communication.
User Equipment	An equipment that allows a user access to network services via 3GPP and/or non-3GPP accesses.
User plane	The user plane (sometimes called data plane or bearer plane), carries the user/application traffic.
Voice Communication	Exchange of information in the form of voice requiring corresponding QoS treatment, regardless of the transmission method.
Zone	Grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization (IEC)

CONTENTS

Executive Summary 4

Abbreviations and Acronyms 5

Definitions 9

1 INTRODUCTION 24

1.1 Project Context 24

1.2 Project Objectives 26

1.3 Prototype’s deliveries 27

1.4 The selected Use cases 27

1.4.1 On-Board and Track Side Gateways 29

1.4.2 ETCS Application 31

1.4.3 ATO Application 32

1.4.4 VOICE Application 33

1.4.5 TCMS Application 34

1.4.6 CCTV Application 35

1.4.7 PIS Application 36

2 SYSTEM ARCHITECTURE 37

2.1 Architecture System Principles 37

2.2 Architecture System Functionalities 39

2.2.1 FRMCS Service stratum 40

2.2.2 Loose vs Tight Coupled Application 42

2.2.3 Quality of Service (QoS) and priority 44

2.2.4 Session Management and Addressing/routing 45

2.2.5 Bearer Flexibility 46

2.2.6 FRMCS to GSM-R Switching 47

2.2.7 Positioning 48

2.2.8 Location 49

2.2.9 Timestamping & Synchronization 50

2.2.10 Availability / Redundancy - Resilience 50

2.2.11 Cybersecurity 51

2.2.12 FRMCS On-Board & Track Side gateways Interfaces 51

2.2.13 Auxiliary function 54

2.2.14 RF switching/combiner antenna 54

2.2.15 FRMCS border-crossing 55

3 ASSUMPTIONS FOR 5G RAIL PROJECT EXECUTION 58

3.1 Assumption table 58

4 FRMCS 5G MODEMS 62

4.1 Modem description 62

4.1.1 Directives 62

4.1.2 European type approval 63

4.1.3 Requirements of quality 63

4.2 Safety precautions note 63

4.3 Modem’s design 64

4.4 Modem characteristics 65

4.4.1 Throughput 66

4.4.2 Quality of service (QoS) 67

4.4.3 GNSS 67

4.4.4 Modem table 68

4.5 Modem integration in TOBA On Board gateway 70

4.6 Modem antenna interface 73

4.7 Summary 74

4.8 Risks update (Modem status from 10th September 2021) 75

4.9 Schedule 76

5 FRMCS GATEWAY SERVICES IN THE SYSTEM VIEW 77

5.1 FRMCS Gateway services – principles overview 78

5.2 FRMCS On Board gateway 78

5.2.1 Architecture of OB_GTW 78

5.2.2 Functionalities 82

5.2.3 Interfaces 104

5.2.4 Prototype deliverable 107

5.3 FRMCS Track Side Gateway 109

5.3.1 Architecture 109

5.3.2 Functionalities 111

5.3.3 Interfaces 115

5.3.4 Prototype deliverable 117

5.4 Other On-board and Trackside components 119

5.4.1 O&M client and server 119

5.4.2 RF combining & switching 119

6 APPLICATIONS & FRMCS GATEWAYS INTERFACES 125

6.1 Application coupling mode 126

6.2 OB_{APP} interface 127

6.2.1 Functions 127

6.2.2 Physical interface 129

6.2.3 Protocol stack 129

6.2.4 API version and Websocket URI 132

6.2.5 Loose coupled interface 132

6.2.6 Tight coupled interface 144

6.3 TS_{APP} interface 146

6.3.1 Functions 146

6.3.2 Physical interface 147

6.3.3 Protocol stack 147

6.3.4 Loose coupled interface 149

6.3.5 Tight coupled interface 149

7 Applications 150

7.1 ALSTOM ETCS 150

7.1.1 APPLICATION ARCHITECTURE PROPOSAL 150

7.1.2 INTERFACES 155

7.1.3 INTERWORKING WITH GSM-R 156

7.2 CAF ETCS & TCMS 156

7.2.1 ARCHITECTURE PROPOSAL 156

7.2.2 INTERFACES 160

7.2.3 INTERWORKING WITH GSM-R 163

7.3 ATO 163

7.3.1 APPLICATION ARCHITECTURE PROPOSAL 163

7.3.2 INTERFACES 167

7.3.3 INTERWORKING WITH GSM-R 168

7.4 VOICE 168

7.4.1 APPLICATION ARCHITECTURE PROPOSAL 168

7.4.2 INTERFACES 174

7.4.3 INTERWORKING WITH GSM-R 177

7.4.4 CYBERSECURITY 177

7.5 PIS 177

7.5.1 APPLICATION ARCHITECTURE PROPOSAL 177

7.5.2 INTERFACES 186

7.5.3 INTERWORKING WITH GSM-R 188
7.5.4 CYBERSECURITY 188
7.6 CCTV 190
7.6.1 APPLICATION ARCHITECTURE PROPOSAL 190
7.6.2 INTERFACES 198
7.6.3 INTERWORKING WITH GSM-R 199
7.6.4 CYBERSECURITY 199
7.7 REMOTE VISION 199
7.7.1 Remote Vision APPLICATION ARCHITECTURE PROPOSAL 199
7.7.2 INTERFACES 204
8 CONCLUSIONS 205
9 APPENDICES 206
9.1 Appendix 1 – Communication attributes to QoS 206
9.2 Appendix 2 - End to end dataflows 207
9.3 Appendix 3 – Application type and application profile 211
9.4 Appendix 6 – Example to illustrate the virtual session IP address 212
9.5 Appendix 7 – ID to be used in WP3 and WP4 219
9.5.1 For WP3 219
9.5.2 For WP4: 220
9.6 Appendix 8 – Cybersecurity 221
9.6.1 ZCR 1: Identify the System Under Consideration 221
9.6.2 ZCR 2: Initial cyber security risk assessment 229
9.6.3 ZCR 3: Partition the SUC into zones and conduits 246
9.7 Appendix 9 – PKI and certificate management for local binding 247
10 STANDARDS DOCUMENTS 249
11 REFERENCES DOCUMENTS 251

12 CYBERSECURITY STANDARDS AND REFERENCES DOCUMENTS 252

Table of figures

Figure 1: WP2 execution timeline 24
Figure 2: WP2 prototypes 25
Figure 3: WP2 architecture baseline 26
Figure 4: WP2 prototypes/components in FRMCS ecosystem 27
Figure 5: WP2 Prototype/component deliveries and targeted LAB and FIELD WPs 27
Figure 6: Architecture overview (Component's list) 37
Figure 7: Application, Services and Transport Stratums (FRMCS SRS) 40
Figure 8: FRMCS services: the central part of the architecture 41
Figure 9: FRMCS Service Stratum – MCx Clients & MCx Server 41
Figure 10: Loose-coupling vs tight-coupling for applications 43
Figure 11: End to end view of loose and tight coupling for applications 43
Figure 12: QoS function 45
Figure 13: IP connectivity model 46
Figure 14: Bearer Flexibility function 47
Figure 15: FRMCS to GSM-R switching 48
Figure 16: OBapp interface 52
Figure 17: OBant interface 53
Figure 18: TSapp interface 53
Figure 19: RF switching/combiner antenna. 55
Figure 20: Network crossing function 56
Figure 21: Border crossing function 56
Figure 22: FRMCS principle architecture 62

Figure 23: Modem design overview 65

Figure 24: ES1 photos 68

Figure 25: Modem mechanical dimensions 71

Figure 26: Modem SIM card 72

Figure 27: FRMCS Gateway services – Principles overview 78

Figure 28: FRMCS on board gateway – Building blocks 79

Figure 29: Kontron Multiconnectivity function 86

Figure 30: Kontron Multiconnectivity based on MPTCP 86

Figure 31: Alstom multiconnectivity - User Plane 87

Figure 32: Alstom multiconnectivity - MCx signalling plane – possible implementation 88

Figure 33: 2 steps in local binding 91

Figure 34: User plane management 92

Figure 35: Session state diagram – outgoing session 94

Figure 36: Session state diagram - Incoming session 96

Figure 37: MCx authentication and authorization 98

Figure 38: Border-crossing “ATO-like” 101

Figure 39: Border-crossing "ETCS-like" 101

Figure 40: Border-crossing details in 5GRAIL 102

Figure 41: N-type connector 106

Figure 42: SMA connector 106

Figure 43: TOBA trackside gateway - Building blocks 109

Figure 44: User plane management 114

Figure 45: TS_GTW-A 118

Figure 46: Antennas implementation 119

Figure 47: recommendation of connection 120

Figure 48: RF switch 121

Figure 49: Power combiner 121

Figure 50: update of the electrical schematic to introduce the hardware redundancy 122

Figure 51: advanced electrical schematic 123

Figure 52: OB$_{APP}$/TS$_{APP}$ location 125

Figure 53: End to end communication for tight coupled applications 126

Figure 54: End to end communication for loose coupled applications 126

Figure 55: Tight coupled application OB$_{APP}$ protocol stack 130

Figure 56: Loose coupled application OB$_{APP}$ protocol stack 131

Figure 57: OBapp global exchanges 134

Figure 58: Connection Status management 141

Figure 59: OB$_{APP}$ global exchanges in tight coupled mode 145

Figure 60: Tight coupled application TS$_{APP}$ protocol stack 148

Figure 61: Loose coupled application TS$_{APP}$ protocol stack 149

Figure 62: ETCS system architecture with both on board and track side parts 151

Figure 63: ETCS system using simulator 153

Figure 64: Overview of simulators 154

Figure 65: Overall TCMS and ETCS architecture 157

Figure 66: Proposed architecture for implementation testing environment 157

Figure 67: Overall TCMS architecture 158

Figure 68: Overall ETCS architecture - detailed 158

Figure 69: Overall TCMS and ETCS architecture - detailed 160

Figure 70: Overall TCMS architecture - detailed 161

Figure 71: Overall ETCS architecture - detailed 162

Figure 72: ATO over FRMCS 163

Figure 73: Hardware platform 166

Figure 74 Front view of the ITA-5231 166

Figure 75: Simulator 167

Figure 76: Dual Mode GSM-R/FRMCS Voice Application........ 169

Figure 77: Siemens’ hardware platform 170

Figure 78: SVR400+ front panel 170

Figure 79: Console Unit front panel........ 172

Figure 80: Console Unit rear panel 172

Figure 81: Gland Box 173

Figure 82: Power Supply Unit........ 173

Figure 83: Graphical Driver’s Control Panel........ 175

Figure 84: PIS application architecture overview. 178

Figure 85: APIS on-board server (Front panel). 178

Figure 86: VIPA-HOST........ 180

Figure 87: On-board TFT display device........ 182

Figure 88: Trackside microphone........ 184

Figure 89: APIS software components........ 185

Figure 90: Location simulator for PIS........ 186

Figure 91: Multi-Channel Message: selection of several channels........ 187

Figure 92: Text message scheduling window. 188

Figure 93: Audio message scheduling window........ 188

Figure 94: CCTV system architecture overview. 190

Figure 95: Human Machine Interface (HMI)........ 191

Figure 96: Mobile Network Video recorder........ 193

Figure 97: Streaming server........ 196

Figure 98: CCTV VMS software components. 197

Figure 99: Global Architecture of the remote driving system in the FRMCS........ 200

Figure 100: Onboard Logical Diagram........ 200

Figure 101: TrackSide Logical Diagram 201

Figure 102: Photo of the Heavy version of the Remote Driving Desk 203

Figure 103: Software Platform of the PC Vision System 203

Figure 104: FRMCS principle architecture 222

Figure 105: FRMCS Gateway services – Principle overview 222

Figure 106: Focus on FRMCS OB 223

Figure 107: FRMCS on board gateway – Building blocks 223

Figure 108 : FRMCS TS architecture principle 225

Figure 109: TOBA trackside gateway - Building blocks 226

Figure 110: WP2 Prototype/component deliveries and targeted LAB and FIELD WPs 236

Figure 111: Needs for TLS connection 247

Figure 112: certificate generation with client generating its private key 248

Figure 113: Certificate generation with CA generating the private key for the client 248

List of tables

Table 1: Technology enablers for FRMCS/5G TOBA architecture 4

Table 2: Reference documents inputs for WP2 execution 25

Table 3: WP1 Use case list candidates for WP3, WP4 and WP5 28

Table 4: WP2 Functions derived from WP1 use cases 29

Table 5: On-Board ad Track Side Gateways Use Cases 30

Table 6: ETCS Application Use Cases 31

Table 7: ATO Application Use Cases 32

Table 8: VOICE Application Use Cases 33

Table 9: TCMS Application Use Cases 34

Table 10: CCTV Application Use Cases 35

Table 11: PIS Application Use Cases 36

Table 12: From use cases to system functionalities ... 39

Table 13: System functionalities to components mapping... 39

Table 14: Critical applications Priority and Coupling Type ... 44

Table 15: Assumption table ... 61

Table 16: Modem characteristics... 66

Table 17: Modem DL throughput ... 66

Table 18: Modem UL throughput ... 66

Table 19: Modem ES summary ... 68

Table 20: Modem RF antenna interface ... 73

Table 21: Modem bandwidths ... 74

Table 22: Allocation to building blocks ... 84

Table 23: Pinout of the RF connectors... 106

Table 24: Function traceability ... 112

Table 25: Allocation to building blocks ... 113

Table 26: Application coupling mode ... 127

Table 27: OB$_{APP}$ functions... 127

Table 28: FRMCS_GTW_REGISTER parameters ... 135

Table 29: FRMCS_GTW_DEREGISTER parameters... 137

Table 30: FRMCS_GTW_SESSION_START parameters... 137

Table 31: FRMCS_GTW_SESSION_END parameters ... 139

Table 32: FRMCS_GTW_SESSION_STATUS parameters... 139

Table 33: FRMCS_GTW_SERVICE_REQUEST parameters ... 140

Table 34: FRMCS_APP_INCOMING_SESSION parameters... 141

Table 35: FRMCS_APP_SESSION_STATUS_SESSION_NOTIF ... 142

Table 36: FRMCS_APP_SESSION_STATUS_CHANGED parameters... 143

Table 37: TS$_{APP}$ functions... 146

Table 38: SVR400+ Specification 171

Table 39: Graphical Driver’s Control Panel hard keys legend 176

Table 40: Graphical Driver’s Control Panel soft keys legend 176

Table 41: Description of the front panel description of the APIS on-board server. 180

Table 42: Hardware description of the VIPA-HOST server. 181

Table 43: Hardware description of the on-board display device. 183

Table 44: Hardware description of the microphone. 184

Table 45: Hardware of the APIS trackside server. 184

Table 46: Human Machine Interface Technical data 192

Table 47: Mobile Network Video recorder Technical data 193

Table 48: Technical data 195

Table 49: Translation table from comm_profile to QoS 206

Table 50: Application type list 211

Table 51: Example of application_profile 212

Table 52: Initial FRMCS risk matrix 244

1 INTRODUCTION

5GRAIL aims to demonstrate prototypes of the 5G FRMCS ecosystem and to validate the FRMCS specifications, including the compliance of railway essential operational services such as railway ETCS, ATO, Voice, TCMS, video and PIS.

This document focuses on the development of prototypes within WP2 that aims to be rolled out in Europe for a series of pilot tests (in labs & in the field) to demonstrate how these technical solutions can be integrated, to validate their feasibility and to evaluate their performance under a combination of environmental conditions in various test-sites (France, Hungary and Germany).

This document is the deliverable "D2.1 Architecture Report" as depicted in the "Figure 1: WP2 execution timeline".

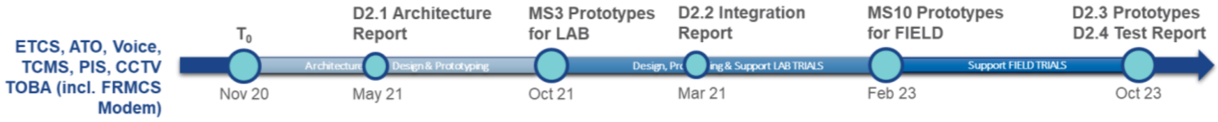


Figure 1: WP2 execution timeline

1.1 Project Context

As shown in "Figure 2: WP2 prototypes", there are two types of WP2 prototypes:

- The Applications, already rolled out in GSM-R which needs to be ported over the new FRMCS systems. Main evolution is the compliancy with the new FRMCS standardized reference points OBapp for the onboard part and TSapp for the trackside part.
- The so-called TOBA system that is declined into the two FRMCS gateways for on-board and trackside. These prototypes are developed from scratch being a new node of FRMCS.

The key design paradigm for the FRMCS/5G gateways prototypes expected are:

- Decoupling of Applications and Communication Services/Transport;
- Bearer Flexibility (i.e. variety of bearers or Radio Access Technologies simultaneously);
- Resource Sharing (e.g. providing transport services for multiple applications of any category using the same FRMCS on-board system considering the individual QoS requirements of the application and possibly priorities among applications).

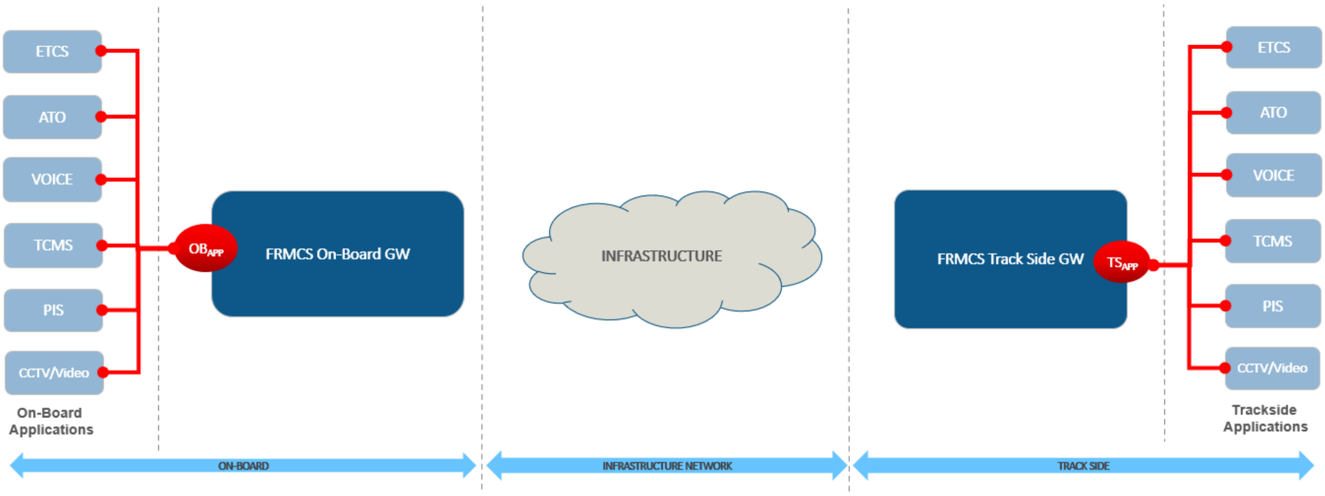


Figure 2: WP2 prototypes

The prototype will respect the FRMCS specs as far as possible. If some of them are still under discussion, assumptions will be made – refer to Table 2: Reference documents inputs for WP2 execution

Table 2: Reference documents inputs for WP2 execution

Body	Specification Name	Reference	Current Release	Current Status	Public or Confidential	Scope / High Level Content	Date of publication
UIC	FRMCS Principle Architecture	MG-7904	0.3.0	Stable draft	CO	FRMCS Principle Architecture	January 2021
UIC	ETCS over FRMCS Principle Architecture	MG-7904-1	0.0.2	Early draft	CO	ETCS over FRMCS Principle Architecture	January 2021
UIC	FRMCS On-Board Functional Requirements Specification (TOBA FRS)	TOBA-7510	1.0.15	Stable draft	CO	Mapping FRMCS URS regarding on-board functions	nov.-21
UIC	FRMCS System Requirements Specification (FRMCS SRS)	FW-AT-7800	0.3.1	Stable draft	CO	System principles (QoS, Security, Frequencies, User Addressing, handhelds, devices, trackside, etc). Mapping FRMCS FRS Usage of Building Blocks from 3GPP/ETSI (consolidated by ETSI) Interworking with GSM-R Priority 1: QoS, Spectrum, Security, Bearer agility, Identification, Adressing Priority 2: Interconnection, Border-crossing & roaming, Localization & positioning, Migration	oct.-21
UIC	FRMCS On-Board System Requirements Specification (TOBA SRS)	TOBA-7530	0.0.8	Stable draft	CO	Mapping TOBA FRS Usage of Building Blocks from 3GPP/ETSI (consolidated by ETSI)	nov.-21
UIC	FRMCS Functional Interface Specification (FRMCS FIS)	FIS - 7900	0.0.4	Early draft	CO	E-2-E for Control Plane (mapping of URS to MCX) Dependency on TOBA & FRMCS SRS	nov.-21
UIC	FRMCS Form-Fit Functional Interfaces (FRMCS FFFIS)	FFFIS -7900	0.1.4	Stable draft	CO	OB$_{APP}$ and TS$_{APP}$ Specifications Dependency on TOBA & FRMCS SRS	2 August 2021
UNITEL	OnBoard train antenna system study	-	3	Stable draft	CO	Presentation on OBant: GSM-R & FRMCS technologies working simultaneously	Feburary 2021
EUG	ETCS over FRMCS; principles and functional requirements	20E136	1.0		CO	This document defines the principles and functional requirements for the use of FRMCS as a standalone radio data bearer for ETCS	April 2021

Consequently, the WP2 prototyping requirements have to be derived and elaborated according to the following methodology:

- Use cases selected in WP1 for WP3, WP4 and WP5 execution;
- Assumptions derived from the available specification inputs.

This layered methodology is represented in the "Figure 3: WP2 architecture baseline" below. Each of the upper layer is derived from the lower one. The Use Case list is described in the chapter 1.2 and the Assumptions in the chapter 3.

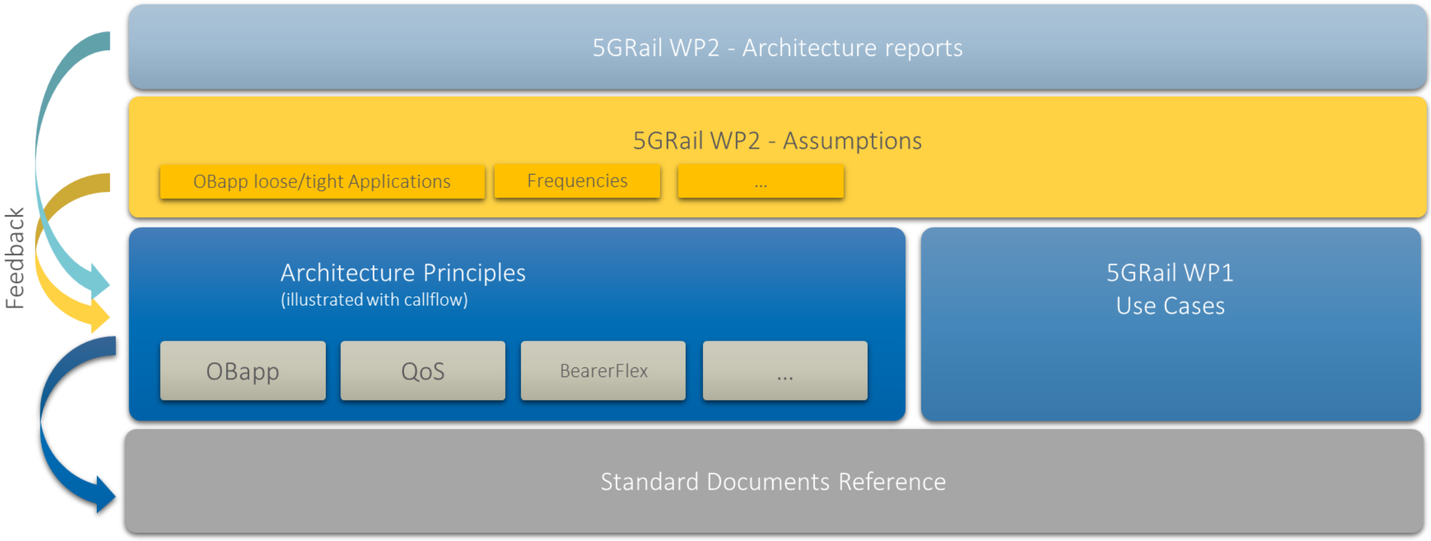

5GRail WP2 - Architecture reports
5GRail WP2 - Assumptions
OBapp loose/tight Applications
Frequencies
...
Architecture Principles
(illustrated with callflow)
OBapp
QoS
BearerFlex
...
5GRail WP1
Use Cases
Standard Documents Reference
Feedback

Figure 3: WP2 architecture baseline

1.2 Project Objectives

The "Figure 4: WP2 prototypes/components in FRMCS ecosystem" articulates a further detailed view of the FRMCS ecosystem and the various components with the one marked as "WP2". This view is considered to be consistent with MG-7904 which gives the high-level architecture principles.

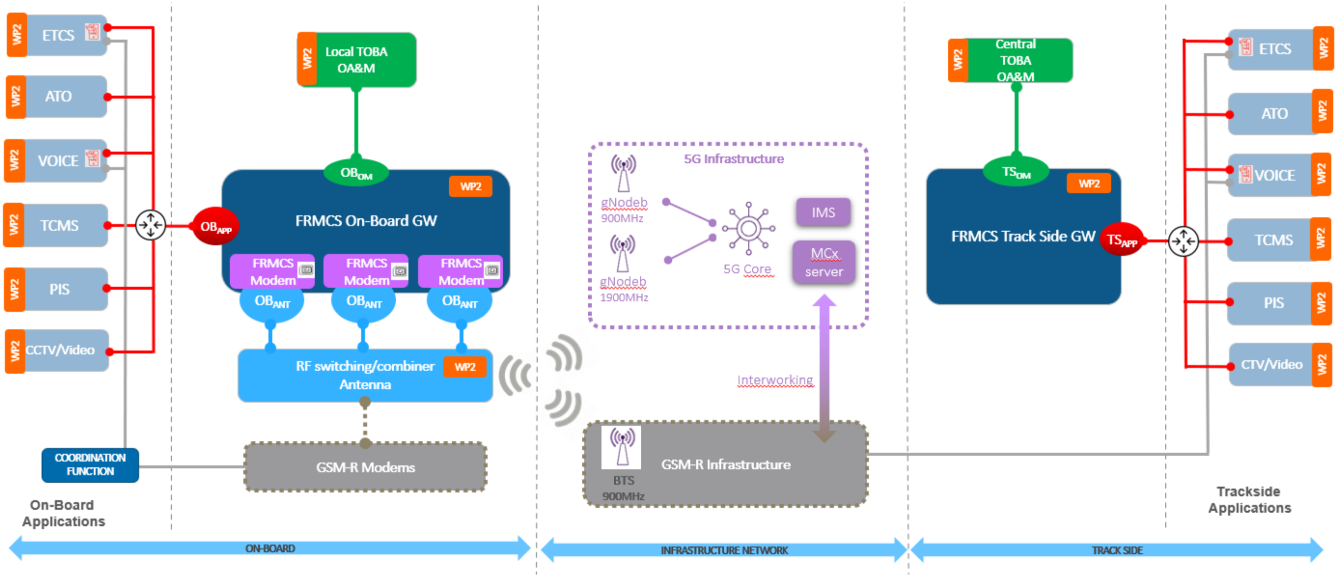
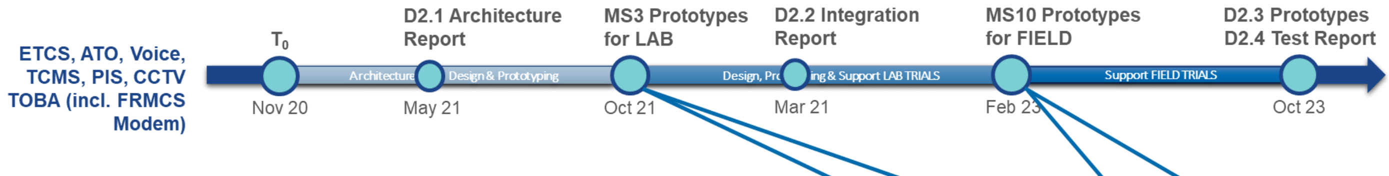


Figure 4: WP2 prototypes/components in FRMCS ecosystem

1.3 Prototype's deliveries

The "Figure 5: WP2 Prototype/component deliveries and targeted LAB and FIELD WPs" shows the list of the prototypes that will be delivered as per WP2 and indicates the targeted LAB and FIELD test WPs. All these prototypes are described in the next chapters.

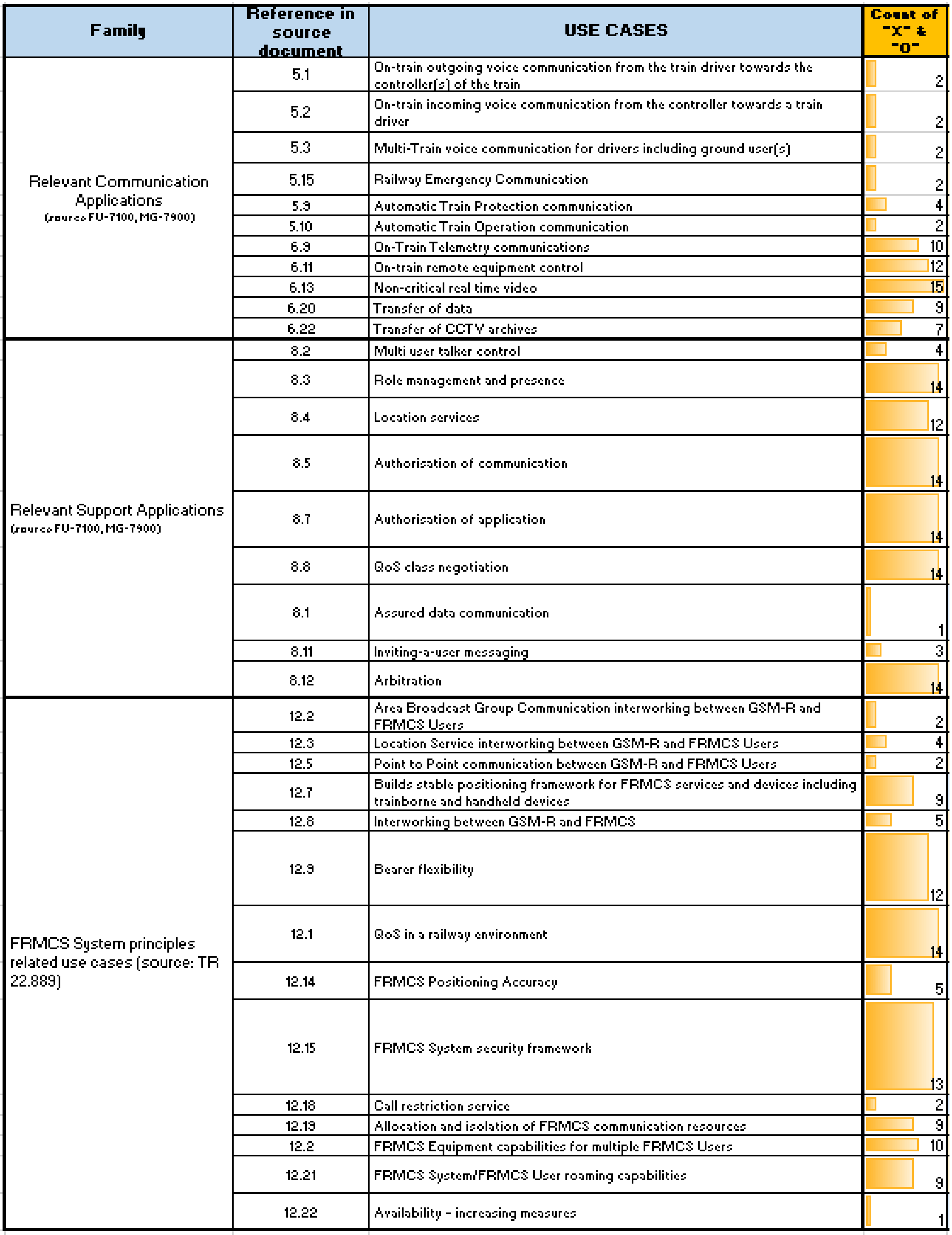


WP2 Components								Integration WPs			
Participant	Efforts	Tasks	Deliverables	Onbard		Wayside		WP3 LAB NOKIA	WP4 LAB KT	WP5 FIELD DB	WP5 FIELD SNCF
				HW	SW	HW	SW				
KONTRON	96	T2.1	TOBA K-Prototype	✓(Radio)	✓		✓	✓	✓ (P1)	✓	✓
THALES	38	T2.1.1	FRMCS 5G Radio module	✓(USB Modem)				✓ (early lab derisk)	✓ (early lab derisk)		
			Cybersecurity	Study/Assessment							
			PIS	✓	✓	✓	✓		✓		
ALSTOM	80	T2.3	ETCS upgraded to FRMCS	✓	✓		✓(Simu)		✓		✓
			ATO upgrade to FRMCS	✓	✓		✓(Simu)		✓		✓
			TOBA A-Prototype	✓(Radio)	✓		✓		✓ (P2)		
SIEMENS	35	T2.2	Train Radio Voice application	✓(Audio/Display)	✓	× Using MCx server from 5G infra		✓		✓	
CAF	19	T2.4	ETCS upgraded to FRMCS	✓(Simu)	✓(Simu)		✓(Simu)	✓		✓	
			TCMS	✓	✓		✓(Simu)	✓		✓	
TELESTE	10	T2.4	CCTV/Video	✓	✓	✓	✓	✓		✓	

Figure 5: WP2 Prototype/component deliveries and targeted LAB and FIELD WPs

1.4 The selected Use cases

The use case list targeted for WP3, WP4 and WP5 has been elaborated within WP1 and is consolidated in the "Table 3: WP1 Use case list candidates for WP3, WP4 and WP5". Note the 4th column is a rough indicator of the frequency of usage of these support applications and requirements for the communication applications. (i.e., 1 means less often required than 4 for communications applications) .'X" is meant for mandatory and "O" for optional.

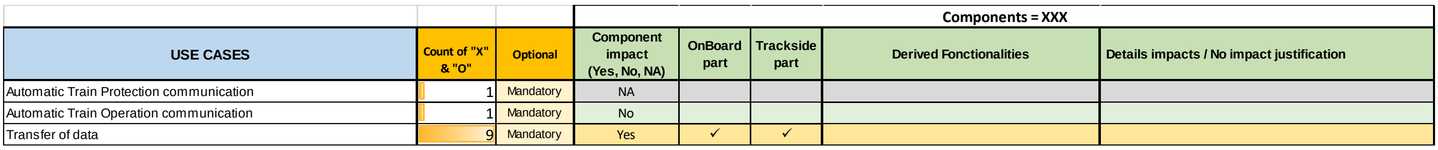


Family	Reference in source document	USE CASES	Count of "X" & "O"
Relevant Communication Applications (source FU-7100, MG-7900)	5.1	On-train outgoing voice communication from the train driver towards the controller(s) of the train	2
	5.2	On-train incoming voice communication from the controller towards a train driver	2
	5.3	Multi-Train voice communication for drivers including ground user(s)	2
	5.15	Railway Emergency Communication	2
	5.9	Automatic Train Protection communication	4
	5.10	Automatic Train Operation communication	2
	6.9	On-Train Telemetry communications	10
	6.11	On-train remote equipment control	12
	6.13	Non-critical real time video	15
	6.20	Transfer of data	9
	6.22	Transfer of CCTV archives	7
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4
	8.3	Role management and presence	14
	8.4	Location services	12
	8.5	Authorisation of communication	14
	8.7	Authorisation of application	14
	8.8	QoS class negotiation	14
	8.1	Assured data communication	1
	8.11	Inviting-a-user messaging	3
	8.12	Arbitration	14
FRMCS System principles related use cases (source: TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2
	12.3	Location Service interworking between GSM-R and FRMCS Users	4
	12.5	Point to Point communication between GSM-R and FRMCS Users	2
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9
	12.8	Interworking between GSM-R and FRMCS	5
	12.9	Bearer flexibility	12
	12.1	QoS in a railway environment	14
	12.14	FRMCS Positioning Accuracy	5
	12.15	FRMCS System security framework	13
	12.18	Call restriction service	2
	12.19	Allocation and isolation of FRMCS communication resources	9
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10
	12.21	FRMCS System/FRMCS User roaming capabilities	9
	12.22	Availability – increasing measures	1

Table 3: WP1 Use case list candidates for WP3, WP4 and WP5

The methodology applied is to derive the needed functions for the prototypes to support these use cases. These functions will be used as requirements and will be described later in this document.

Precisely, the template from “Table 4: WP2 Functions derived from WP1 use cases” is further on derived for each of the WP2 prototypes/components and shown in the next paragraphs.



			Components = XXX				
USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Automatic Train Protection communication	1	Mandatory	NA				
Automatic Train Operation communication	1	Mandatory	No				
Transfer of data	9	Mandatory	Yes	✓	✓		

Table 4: WP2 Functions derived from WP1 use cases

1.4.1 On-Board and Track Side Gateways

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory					
	5.1	Automatic Train Operation communication	1	Mandatory					
	6.2	Transfer of data	9	Mandatory					
	6.13	Non critical real-time video	15	Mandatory					
	6.22	Transfer of CCTV archives	7	Mandatory					
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory	No				
	8.3	Role management and presence	14	Mandatory	Yes	✓	✓	TOBA_F1.3: Session management-Loose TSGTW_F1.3: Session management-Loose TOBA_F1.1:Expose an OBAPP API TSGTW_F1.1: Expose a TSAPP API	Management of functional ID see requirements in URS chap 8.3 Obapp and Tsapp for registration
	8.4	Location services	12	Mandatory	Yes	✓		TOBA_F7: Obtain localization information, and provide it to the applications	Capture and store location for a location and share with others entity… see requirements in URS chap 8.4
	8.5	Authorisation of communication	14	Mandatory	Yes	✓	✓	TOBA_F1.5: Authenticate the on-board applications TSGTW_F1.5: Authenticate the TS applications TOBA_F1.3: Session management-Loose TSGTW_F1.3: Session management-Loose TOBA_F1.8: Session proxying-Tight TSGTW_F1.8: Session proxying-Tight	Control the access to some communications from user ID Session management-Loose function has to control the authorization for a requested communication
	8.7	Authorisation of application	14	Mandatory	Yes	✓	✓	TOBA_F1.5: Authenticate the on-board applications (OBAUTH) TSGTW_F1.5: Authenticate the TS applications TOBA_F1.3/TSGTW_F1.3: Session management-Loose TOBA_F1.8/TSGTW_F1.8: Session proxying-Tight	Control the access to some communications for the applications Session management-Loose function has to control the authorization for a requested communication
	8.8	QoS class negotiation	14	Mandatory	Yes	✓	✓	TOBA_F1.4/TSGTW_F1.4: Provide to the application the required communication attributes	
	8.1	Assured data communication	1	Optional	Yes	✓	✓	TOBA_F1.7/TSGTW_F1.7: Expose link supervision information to the applications which request it	to be confirmed with the applications view if necessary for TS but it seems the case in the URS description.
	8.11	Inviting-a-user messaging	3	Mandatory	No				Managed in applications
	8.12	Arbitration	14	Mandatory	Yes	✓		TOBA_F1.4: Provide to an application the required communication attributes	
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory	No				
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory	No				
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory	No				do not agree with this use case. For us it is not applicable at all
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional	Yes	✓		TOBA_F7.1: Obtain positioning and time information TOBA_F7.2: Provide positioning information to the applications	F7.2 to be confirmed whether it is really in TOBA scope
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory	No				Switching between GSM-R / FRMCS done at application level.
	12.9	Bearer flexibility	12	Mandatory	Yes	✓	✓	BearFlex transparent for Onboard applications TOBA_F1.2/TSGTW_F1.2: Multipath/BearerFlex TOBA_F2: Support multiple modem and radio technologies TOBA_F3/TSGTW_F1.3: Connect to multiple networks TOBA_F1.1: Expose an OBAPP API to the OB application TSGTW_F1.1: Expose a TSAPP API to the TS application	Onboard and Trackside gateway needs to implement OBAPP API is the service level which ensure decoupling of application and transport levels
	12.1	QoS in a railway environment	14	Mandatory	Yes	✓	✓	OBapp and TSapp QoS services based on 5QI TOBA_F1.4/TSGTW_F1.4: Provide to an application the required communication attributes	Mapping of 5QI from 5G infrastructure into OBapp/Tsapp.
	12.14	FRMCS Positioning Accuracy	5	Optional	Yes	✓		TOBA_F7.1: Obtain positioning and time information TOBA_F7.2: Provide positioning information to the applications	Location services interface to be defined… GPS/GNSS?Consolidate positioning sources to provide a location for the train F7.2 to be confirmed whether it is really in TOBA scope
	12.15	FRMCS System security framework	13	Mandatory	Yes	✓	✓	TOBA_F1.5: Authenticate the on-board applications (OBAUTH) TSGTW_F1.5: Authenticate the TS applications TOBA_F1.3: Session management-Loose TSGTW_F1.3: Session management-Loose	The requirements for full system security framework (threat and attack detection, fraud detection, traffic monitoring,…) is out of scope for TOBA (to be considered as an external cybersecurity component) Session management-Loose function has to control the authorization for a requested communication
	12.18	Call restriction service	2	Optional	No				Managed in applications
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory	Yes	✓	✓	TOBA_F1.3/TSGTW_F1.3: Session management-Loose TOBA_F1.8/TSGTW_F1.8: Session proxying-Tight	Segregate communications ressources from the different applications
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory	Yes	✓	✓	TOBA_F1.3/TSGTW_F1.3: Session management-Loose TOBA_F1.8/TSGTW_F1.8: Session proxying-Tight	Establish many session for multiple application
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory	Yes	✓		TOBA_F6: FRMCS roaming capability	ensure continuity of service during roaming scenario ensure that each RBC (for ETCS example) will be joignable from any FRMCS network
	12.22	Availability – increasing measures	1	Optional	Yes	✓	✓	TOBA_F1.2/TSGTW_F1.2: Multipath/BearerFlex TOBA redundancy ???	open question: does this mean that there is a requirement for 2 TOBA in the train?

Table 5: On-Board ad Track Side Gateways Use Cases

The derived functions are described in the chapter 5

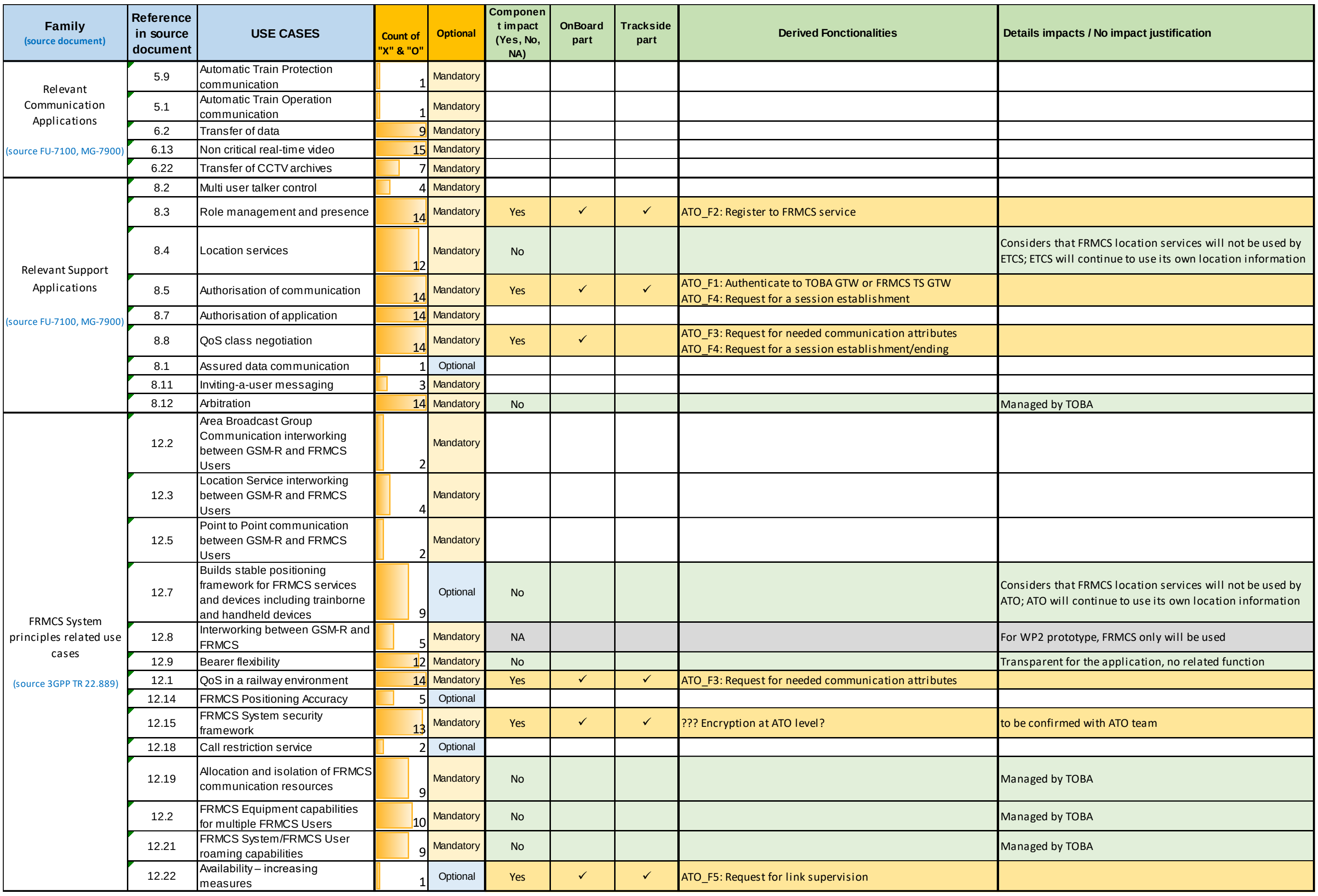
1.4.2 ETCS Application

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory					
	5.1	Automatic Train Operation communication	1	Mandatory					
	6.2	Transfer of data	9	Mandatory					
	6.13	Non critical real-time video	15	Mandatory					
	6.22	Transfer of CCTV archives	7	Mandatory					
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory					
	8.3	Role management and presence	14	Mandatory	Yes	✓	✓	ETCS_F2: Register to FRMCS service	
	8.4	Location services	12	Mandatory	No				Considers that FRMCS location services will not be used by ETCS; ETCS will continue to use its own location information
	8.5	Authorisation of communication	14	Mandatory	Yes	✓	✓	ETCS_F1: Authenticate to TOBA GTW or FRMCS TS GTW ETCS_F4: Request for a session establishment	
	8.7	Authorisation of application	14	Mandatory					
	8.8	QoS class negotiation	14	Mandatory	Yes	✓		ETCS_F3: Request for needed communication attributes ETCS_F4: Request for a session establishment/ending	
	8.1	Assured data communication	1	Optional					
	8.11	Inviting-a-user messaging	3	Mandatory					
	8.12	Arbitration	14	Mandatory	No				Managed by TOBA
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory					
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory					
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory					
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional	No				Considers that FRMCS location services will not be used by ETCS; ETCS will continue to use its own location information
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory	NA				For WP2 prototype, FRMCS only will be used
	12.9	Bearer flexibility	12	Mandatory	No				Transparent for the application, no related function
	12.1	QoS in a railway environment	14	Mandatory	Yes	✓	✓	ETCS_F3: Request for needed communication attributes	
	12.14	FRMCS Positioning Accuracy	5	Optional					
	12.15	FRMCS System security framework	13	Mandatory	Yes	✓	✓	to be completed…	to be further discussed with ETCS team
	12.18	Call restriction service	2	Optional					
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory	No				Managed by TOBA
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory	No				Managed by TOBA
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory	No				Managed by TOBA
	12.22	Availability – increasing measures	1	Optional	Yes	✓	✓	ETCS_F5: Request for link supervision	

Table 6: ETCS Application Use Cases

The derived functions are described in the chapter 7.1

1.4.3 ATO Application



Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory					
	5.1	Automatic Train Operation communication	1	Mandatory					
	6.2	Transfer of data	9	Mandatory					
	6.13	Non critical real-time video	15	Mandatory					
	6.22	Transfer of CCTV archives	7	Mandatory					
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory					
	8.3	Role management and presence	14	Mandatory	Yes	✓	✓	ATO_F2: Register to FRMCS service	
	8.4	Location services	12	Mandatory	No				Considers that FRMCS location services will not be used by ETCS; ETCS will continue to use its own location information
	8.5	Authorisation of communication	14	Mandatory	Yes	✓	✓	ATO_F1: Authenticate to TOBA GTW or FRMCS TS GTW ATO_F4: Request for a session establishment	
	8.7	Authorisation of application	14	Mandatory					
	8.8	QoS class negotiation	14	Mandatory	Yes	✓		ATO_F3: Request for needed communication attributes ATO_F4: Request for a session establishment/ending	
	8.1	Assured data communication	1	Optional					
	8.11	Inviting-a-user messaging	3	Mandatory					
	8.12	Arbitration	14	Mandatory	No				Managed by TOBA
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory					
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory					
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory					
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional	No				Considers that FRMCS location services will not be used by ATO; ATO will continue to use its own location information
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory	NA				For WP2 prototype, FRMCS only will be used
	12.9	Bearer flexibility	12	Mandatory	No				Transparent for the application, no related function
	12.1	QoS in a railway environment	14	Mandatory	Yes	✓	✓	ATO_F3: Request for needed communication attributes	
	12.14	FRMCS Positioning Accuracy	5	Optional					
	12.15	FRMCS System security framework	13	Mandatory	Yes	✓	✓	??? Encryption at ATO level?	to be confirmed with ATO team
	12.18	Call restriction service	2	Optional					
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory	No				Managed by TOBA
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory	No				Managed by TOBA
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory	No				Managed by TOBA
	12.22	Availability – increasing measures	1	Optional	Yes	✓	✓	ATO_F5: Request for link supervision	

Table 7: ATO Application Use Cases

The derived functions are described in the chapter 7.3.

1.4.4 VOICE Application

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Functionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory	No				
	5.1	Automatic Train Operation communication	1	Mandatory	No				
	6.2	Transfer of data	9	Mandatory	No				
	6.13	Non critical real-time video	15	Mandatory	No				
	6.22	Transfer of CCTV archives	7	Mandatory	No				
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory	Yes	✓		Private and group calls	Set the number of simultaneous talkers, Set initial talker permissions and priorities, Request permission to talk, Grant permission to talk, Revoke permission to talk
	8.3	Role management and presence	14	Mandatory	Yes	✓		User Profile Management and aliasing	Registration & Deregistration of a functional identity, User login to the system, User logout from the system, Presentation of identities, Interrogation of identities within a certain context
	8.4	Location services	12	Mandatory	Yes	✓		Private, group and emergency calls	Provide location information, Request for location information, Request for identities based on location
	8.5	Authorisation of communication	14	Mandatory	Yes	✓		Permit / deny communication	Permit / deny communication - Common with loose coupling
	8.7	Authorisation of application	14	Mandatory	Yes	✓		Enabling / Disabling applications	Enabling/Disabling applications - Common with loose coupling
	8.8	QoS class negotiation	14	Mandatory	Yes	✓		QoS	Requesting/(re)negotiating QoS classes - Common with loose coupling
	8.1	Assured data communication	1	Optional	No				
	8.11	Inviting-a-user messaging	3	Mandatory	Yes	✓		Dynamic Group Affiliation/De-affiliation	Receiving an invitation to a voice communication, Accepting an invitation to a voice communication, Rejecting an invitation to a voice communication, Ignore an invitation to a voice communication
	8.12	Arbitration	14	Mandatory	Yes	✓		Arbitration	Arbitration for communication presentation and initiation, auto-connection and auto-merging. Done at the application level
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory	Yes	✓		Group Affiliation/De-affiliation between GSM-R and FRMCS users	Receiving an invitation to a voice communication, Accepting an invitation to a voice communication, Rejecting an invitation to a voice communication, Ignore an invitation to a voice communication
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory	Yes	✓		Private, group and emergency calls between GSM-R and FRMCS users	Provide location information, Request for location information, Request for identities based on location
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory	Yes	✓		Private calls between GSM-R and FRMCS users	
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional	Yes	✓		Private, group and emergency calls	Alternative to GNSS to obtain the position of the FRMCS equipment
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory	Yes	✓		Switching between GSM-R / FRMCS systems	Done at the application level
	12.9	Bearer flexibility	12	Mandatory	Yes	✓		BearFlex transparent for Onboard applications	Onboard and Trackside gateway needs to implement
	12.1	QoS in a railway environment	14	Mandatory	Yes	✓		OBapp and TSapp QoS services based on 5QI	Mapping of 5QI from 5G infrastructure into OBapp/Tsapp.
	12.14	FRMCS Positioning Accuracy	5	Optional	Yes	✓		Private, group and emergency calls	Provide location information, Request for location information, Request for identities based on location
	12.15	FRMCS System security framework	13	Mandatory	Yes	✓		Authentication to the FRMSC Gateway	
	12.18	Call restriction service	2	Optional	Yes	✓		Private and group calls based on a user identity and/or location	Permit / deny communication
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory	No				
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory	Yes	✓		Private, group and emergency calls	Multiple FRMCS Users in the vehicle/train shall be able to use one FRMCS Equipment simultaneously
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory	Yes	✓		Private, group and emergency calls	FRMCS system shall allow communication services between FRMCS Users that are belonging to different administrative realms of the FRMCS System
	12.22	Availability – increasing measures	1	Optional	No				

Table 8: VOICE Application Use Cases

The derived functions are described in the chapter 7.4.

1.4.5 TCMS Application

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory					
	5.1	Automatic Train Operation communication	1	Mandatory					
	6.20	Transfer of data	9	Mandatory	Yes	✓	✓		Pending UIC decission if file transfer will be done in TCMS too as it is done in CCTV
	6.9	On-Train Telemetry communications	1	Mandatory	Yes	✓	✓		Main use cases of TCMS
	6.11	On-train remote equipment control	1	Mandatory	Yes	✓	✓	This implies Trackside intiated conectivity to a onboard equipment	
	6.13	Non critical real-time video	15	Mandatory					
	6.22	Transfer of CCTV archives	7	Mandatory					
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory					
	8.3	Role management and presence	14	Mandatory	Yes	✓	✓	TCMS_F2: Register to FRMCS service	
	8.4	Location services	12	Mandatory	No				Considers that FRMCS location services will not be used by TCMS. TCMS for now will continue to use its own location information but it could be useful for monitoring purposes in the future. From TCMS perspective ir could be useful to have it but not mandatory and will not be tested in the prototype
	8.5	Authorisation of communication	14	Mandatory	Yes	✓	✓	TCMS_F1: Authenticate to TOBA GTW or FRMCS TS GTW TCMS_F4: Request for a session establishment	
	8.7	Authorisation of application	14	Mandatory	Yes	✓	✓	TCMS_F1: Authenticate to TOBA GTW or FRMCS TS GTW TCMS_F4: Request for a session establishment	
	8.8	QoS class negotiation	14	Mandatory	Yes	✓	✓	TCMS_F3: Request for needed communication attributes TCMS_F4: Request for a session establishment/ending	On TCMS we need to communicate from trackside to onboard too
	8.1	Assured data communication	1	Optional					
	8.11	Inviting-a-user messaging	3	Mandatory					
	8.12	Arbitration	14	Mandatory	No				Managed by TOBA
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory					
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory					
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory					
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional	No				Considers that FRMCS location services will not be used by TCMS. TCMS for now will continue to use its own location information but it could be useful for monitoring purposes in the future. From TCMS perspective ir could be useful to have it but not mandatory and will not be tested in the prototype
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory	NA				For WP2 prototype, FRMCS only will be used
	12.9	Bearer flexibility	12	Mandatory	Yes	✓	✓		Pending if bearer flex will be tested in TCMS. For the prototype it can be assumed that it is transparent for the application
	12.1	QoS in a railway environment	14	Mandatory	Yes	✓	✓	TCMS_F3: Request for needed communication attributes	
	12.14	FRMCS Positioning Accuracy	5	Optional					
	12.15	FRMCS System security framework	13	Mandatory	Yes	✓	✓		Trackside initiated communication shall be allowed
	12.18	Call restriction service	2	Optional					
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory	No				Managed by TOBA
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory	No				Managed by TOBA
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory	No				Managed by TOBA
	12.22	Availability – increasing measures	1	Optional					

Table 9: TCMS Application Use Cases

1.4.6 CCTV Application

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication	1	Mandatory					
	5.1	Automatic Train Operation communication	1	Mandatory					
	6.2	Transfer of data	9	Mandatory					
	6.13	Non critical real-time video	15	Mandatory	Yes	✓	✓	QoS support in TOBA	TOBA needs to support QoS for loose coupled and non-MCx applications
	6.22	Transfer of CCTV archives	7	Mandatory	Yes	✓	✓	QoS support in TOBA	TOBA needs to support QoS for loose coupled and non-MCx applications
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control	4	Mandatory					
	8.3	Role management and presence	14	Mandatory					
	8.4	Location services	12	Mandatory					
	8.5	Authorisation of communication	14	Mandatory					
	8.7	Authorisation of application	14	Mandatory					
	8.8	QoS class negotiation	14	Mandatory					
	8.1	Assured data communication	1	Optional					
	8.11	Inviting-a-user messaging	3	Mandatory					
	8.12	Arbitration	14	Mandatory					
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	2	Mandatory					
	12.3	Location Service interworking between GSM-R and FRMCS Users	4	Mandatory					
	12.5	Point to Point communication between GSM-R and FRMCS Users	2	Mandatory					
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	9	Optional					
	12.8	Interworking between GSM-R and FRMCS	5	Mandatory					
	12.9	Bearer flexibility	12	Mandatory					
	12.1	QoS in a railway environment	14	Mandatory					
	12.14	FRMCS Positioning Accuracy	5	Optional					
	12.15	FRMCS System security framework	13	Mandatory					
	12.18	Call restriction service	2	Optional					
	12.19	Allocation and isolation of FRMCS communication resources	9	Mandatory					
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users	10	Mandatory					
	12.21	FRMCS System/FRMCS User roaming capabilities	9	Mandatory					
	12.22	Availability – increasing measures	1	Optional					

Table 10: CCTV Application Use Cases

1.4.7 PIS Application

Family (source document)	Reference in source document	USE CASES	Count of "X" & "O"	Optional	Component impact (Yes, No, NA)	OnBoard part	Trackside part	Derived Fonctionalities	Details impacts / No impact justification
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	~~Automatic Train Protection communication~~	~~1~~	~~Mandatory~~					
	5.1	~~Automatic Train Operation communication~~	~~1~~	~~Mandatory~~					
	6.20	Transfer of data	9	Mandatory	No				
	6.13	~~Non critical real-time video~~	~~15~~	~~Mandatory~~					
	6.22	~~Transfer of CCTV archives~~	~~7~~	~~Mandatory~~					
Relevant Support Applications (source FU-7100, MG-7900)	~~8.2~~	~~Multi user talker control~~	~~4~~	~~Mandatory~~					
	8.3	Role management and presence	14	Mandatory	No				
	8.4	Location services	12	Mandatory	Yes	✓		TRAIN_LOCATION_FUNC	onboard transit interface
	8.5	Authorisation of communication	14	Mandatory	No				it's assumed there is always an authorisation to communicate
	8.7	Authorisation of application	14	Mandatory	Yes	✓	✓	APIS_GW_AUTH: Authenticate to FRMCS OB GTW or FRMCS TS GTW APIS_GW_SESSION: Request for a session establishment	APIS trackside & onboard FRMCS interfaces
	8.8	QoS class negotiation	14	Mandatory	Yes		✓	APIS_GW_SESSION: Request for a session establishment with the appropriate QoS class	Everytime a session is established the application needs to provide its QoS profile
	~~8,10~~	~~Assured data communication~~	~~1~~	~~Optional~~					
	~~8.11~~	~~Inviting-a-user messaging~~	~~3~~	~~Mandatory~~					
	8.12	Arbitration	14	Mandatory	No				Managed by FRMCS GWs
FRMCS System principles related use cases (source 3GPP TR 22.889)	~~12.2~~	~~Area Broadcast Group Communication interworking between GSM-R and FRMCS Users~~	~~2~~	~~Mandatory~~					
	~~12.3~~	~~Location Service interworking between GSM-R and FRMCS Users~~	~~4~~	~~Mandatory~~					
	~~12.5~~	~~Point to Point communication between GSM-R and FRMCS Users~~	~~2~~	~~Mandatory~~					
	~~12.7~~	~~Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices~~	~~9~~	~~Optional~~					
	~~12.8~~	~~Interworking between GSM-R and FRMCS~~	~~5~~	~~Mandatory~~					
	~~12.9~~	~~Bearer flexibility~~	~~12~~	~~Optional~~					
	12,10	QoS in a railway environment	14	Mandatory	Yes		✓	APIS_GW_SESSION: Request for a session establishment with the appropriate QoS class	Everytime a session is established the application needs to provide its QoS profile
	~~12.14~~	~~FRMCS Positioning Accuracy~~	~~5~~	~~Optional~~					
	12.15	FRMCS System security framework	13	Mandatory	No				After the authentication of the application, we assume there is no additional effort to secure. It's also assume that the FRMCS System security framework requirements are not applicable to APIS application since they are more related to FRMCS services (FRMCS GWs)
	~~12.18~~	~~Call restriction service~~	~~2~~	~~Optional~~					
	~~12.19~~	~~Allocation and isolation of FRMCS communication resources~~	~~9~~	~~Mandatory~~					
	~~12.2~~	~~FRMCS Equipment capabilities for multiple FRMCS Users~~	~~10~~	~~Mandatory~~					
	~~12.21~~	~~FRMCS System/FRMCS User roaming capabilities~~	~~9~~	~~Mandatory~~					
	~~12.22~~	~~Availability – increasing measures~~	~~1~~	~~Optional~~					

Table 11: PIS Application Use Cases

2 SYSTEM ARCHITECTURE

This paragraph is a summary of the "Telecom On-Board Architecture (TOBA)", described in various standardization documents (UIC, 3GPP, etc.), available at the time of writing this report. It allows to know the main characteristics of the product which will be available in a few years and serve as input data for the realization of the prototypes, object of the present document.

2.1 Architecture System Principles

An overview of the current understanding of the architecture is depicted on “Figure 6: Architecture overview (Component’s list)”.

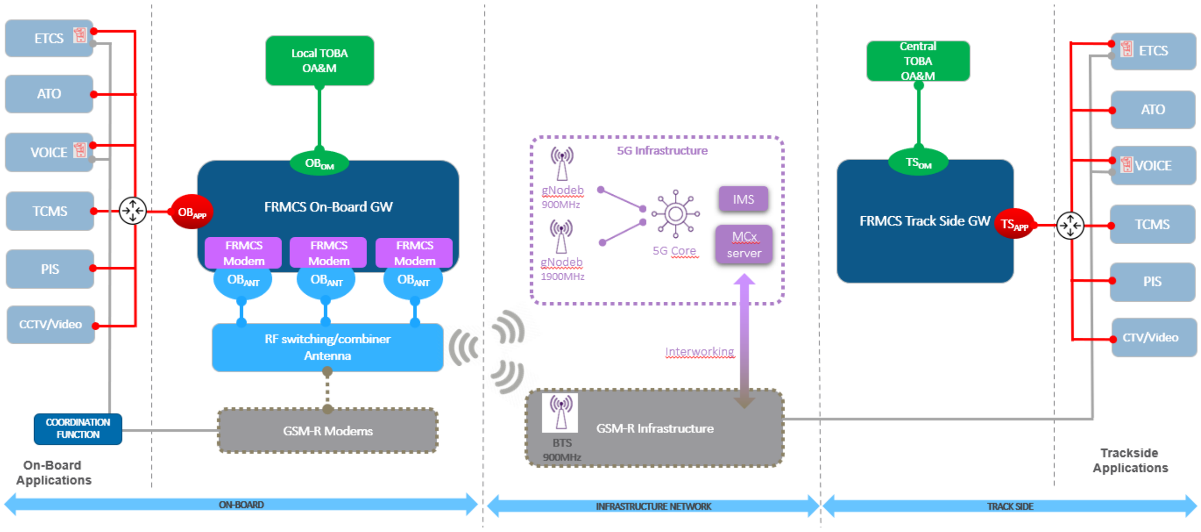


Figure 6: Architecture overview (Component’s list)

As shown on the figure, the applications are implemented in two parts:

- One part on board side;
- One part on track side.

Connections between the on board side and the trackside sides of each application go through two gateways, located on both side of the 5G infrastructure:

- The FRMCS on board gateway (OB_GTW), connected to the applications through OBapp interface and to the 5G radio access networks, through a set of FRMCS modems;
- The FRMCS trackside gateway (TS_GTW), connected to the applications through TSapp interface and to the 5G core infrastructure.

As the number of antennas on the roof of a train is limited by the available space, a “radio frequencies combining/switching” function will be inserted between antenna outputs of the modems and the antennas. Obrad is not mentioned on figure 6 as it is considered as an internal interface for 5G Rail OB GW prototypes (See assumptions ID#34 in assumptions table, paragraph 3.1).

Both gateways (OB_GTW & TS_GTW) are managed through a dedicated interface, respectively named OBom and TSom.

All the above components will be part of the work package 2 (WP2) deliveries as previously shown on "Figure 4: WP2 prototypes/components in FRMCS ecosystem". It is important to note that OB and TS gateways are new components, introduced by the FRMCS TOBA architecture and are therefore to be specified from scratch unlike the applications that already existed in the previous ERTMS version, used for train control. Thus, the main impact on applications is to adapt them to use the OBapp and TSapp interfaces to access the FRMCS service layers and the underlying 5G infrastructure.

Due to the absence of finalized specifications documents at the time of the 5GRail project, the details of the functionalities to be offered by the gateways and are limited to the already specified impacts on the applications. -

To mitigate this lack of specifications and be able to move forward on the project, the FRMCS uses cases, described in *[S6]* and *[S7]*, has been used to list the main awaited system functionalities, as explained in paragraph "1.4 The selected Use cases ". In addition to the use cases list, the following draft versions of standard documents were also used:

- *[S8]* - UIC MG-7904 - FRMCS Principle Architecture – Version 0.3.0 (Draft) – 14/12/2020
- *[S9]* - UIC TOBA FRS-7510 - FRMCS Telecom On-Board System – Functional Requirements Specification (FRS) – Version 0.2.0 (Draft) – 14/04/2020

The Table 12: From use cases to system functionalities below provide the list of system functionalities and mentions, for each of them, the source (standard documents or use cases) from which it is extracted.

			SYSTEM FUNCTIONALITIES													
			FRMCS Service Stratum	Loose vs Tight	QoS	Session Mngt Adressing	BearerFlex	GSM-R Interworking	Positionning	Timestamping Synchro	Availability Redundancy Resilience	Cynbersecurity	FRMCS OB & TS GW interfaces	Auxiliary Function	RF switching Combining	FRMCS Roaming Capability
DOC. STANDARD		DOCUMENT TITLE														
MG-7904		FRMCS Principle Architecture	x	x	x	x	x						x	x		
FRS 7510		Telecom On-Board System – Functional Requirements Specification	x												x	
Family (source document)	Reference in source document	USE CASES														
Relevant Communication Applications (source FU-7100, MG-7900)	5.9	Automatic Train Protection communication														
	5.1	Automatic Train Operation communication														
	6.2	Transfer of data														
	6.13	Non critical real-time video														
	6.22	Transfer of CCTV archives														
Relevant Support Applications (source FU-7100, MG-7900)	8.2	Multi user talker control														
	8.3	Role management and presence														
	8.4	Location services							x							
	8.5	Authorisation of communication				x										
	8.7	Authorisation of application				x										
	8.8	QoS class negotiation			x											
	8.1	Assured data communication														
	8.11	Inviting-a-user messaging														
	8.12	Arbitration														
FRMCS System principles related use cases (source 3GPP TR 22.889)	12.2	Area Broadcast Group Communication interworking between GSM-R and FRMCS Users														
	12.3	Location Service interworking between GSM-R and FRMCS Users							x							
	12.5	Point to Point communication between GSM-R and FRMCS Users														
	12.7	Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices							x							
	12.8	Interworking between GSM-R and FRMCS						x								
	12.9	Bearer flexibility					x									
	12.1	QoS in a railway environment			x											
	12.14	FRMCS Positioning Accuracy							x							
	12.15	FRMCS System security framework										x				
	12.18	Call restriction service														
	12.19	Allocation and isolation of FRMCS communication resources														
	12.2	FRMCS Equipment capabilities for multiple FRMCS Users														
	12.21	FRMCS System/FRMCS User roaming capabilities														x
	12.22	Availability – increasing measures									x			x		

Table 12: From use cases to system functionalities

Thus, the solution delivered by WP2 will have to implement the above system functionalities, mandatory for the validation of use cases.

Each of the system functionalities is described in a paragraph below.

2.2 Architecture System Functionalities

This paragraph describes each of the system functions identified above, specifying which components are impacted.

"Table 13: System functionalities to components mapping" specifies which components are impacted for each of the system functionalities.

COMPONENT	ARCHITECTURE SYSTEM FUNCTIONALITIES													
	FRMCS Service Stratum	Loose vs Tight	QoS	Session Mngt Adressing	BearerFlex	GSM-R Interworking	Positionning	Timestamping Synchro	Availability Redundancy Resilience	Cynbersecurity	FRMCS OB & TS GW interfaces	Auxiliary Function	RF switching Combining	FRMCS Roaming Capability
GATEWAYS														
FRMCS OB GTW	x	x	x	x	x	x	x	x	x	x	x	x	x	x
FRMCS TS GTW	x	x	x	x	x			x	x	x	x			
APPLICATIONS														
ETCS		x	x			x			x	x	x	x		
ATO		x	x			x			x	x	x	x		
VOICE	x	x	x	x		x	x		x	x	x	x		
CCTV		x	x						x	x	x	x		
TCMS		x	x						x	x	x	x		
PIS		x	x						x	x	x	x		

Table 13: System functionalities to components mapping

2.2.1 FRMCS Service stratum

FRMCS service stratum is a key principle of the TOBA architecture, used to interconnect on-board and trackside parts of the application.

Another key principle of the TOBA architecture is the decoupling between railway application stratum and transport, so that the transport layer can evolve (to support a new radio technology, for example) without impacting the application layer.

The logic of stratums is illustrated in "Figure 7: Application, Services and Transport Stratums (FRMCS SRS)" below.

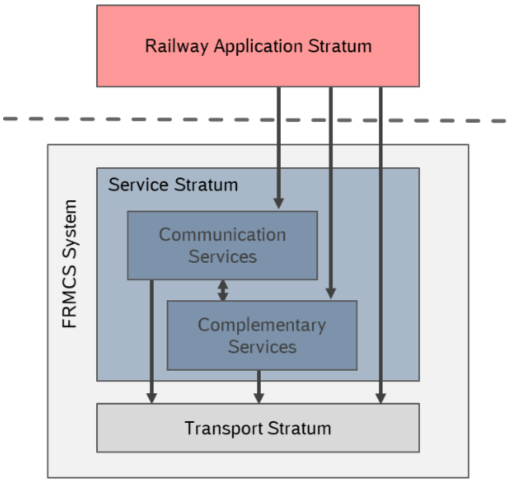


Figure 7: Application, Services and Transport Stratums (FRMCS SRS)

This logical view implies that:

- Both gateways (on-board and trackside) are in charge of service and transport stratums;
- All applications in the "railway application stratum" must interface with FRMCS system.

The key role played by the FRMCS services (part of the service stratum) in the TOBA architecture is detailed in "Figure 8" and explain how on-board and trackside part of an application can exchange information:

- Application will only use facilities exposed by FRMCS Services;
- All FRMCS modems will be part of the transport stratum, on the on-board gateway;
- FRMCS services will be in charge of processing application requests using the facilities offered by the transport layer.

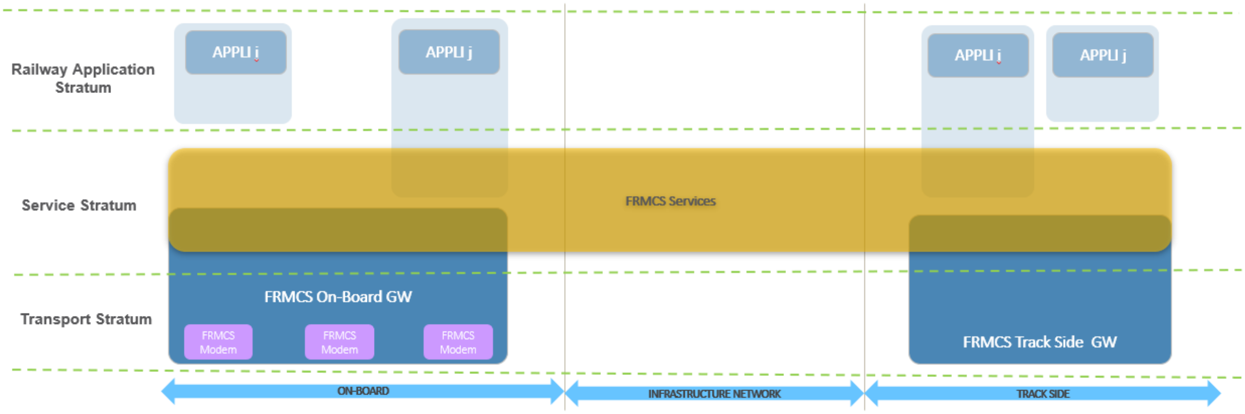


Figure 8: FRMCS services: the central part of the architecture

The implementation of FRMCS services is based on one MCx server, located in the infrastructure, and MCx clients, on each side of the infrastructure FRMCS. These MCx server and MCx clients are used to interconnect both part of an application and it is a key principle of the TOBA architecture.

“Figure 9” shows that MCx clients are still part of the service layer but two integration options are possible:

- either the MCx client is embedded in the bottom part of the application;
- or the MCx client is embedded in the upper part of the gateways.

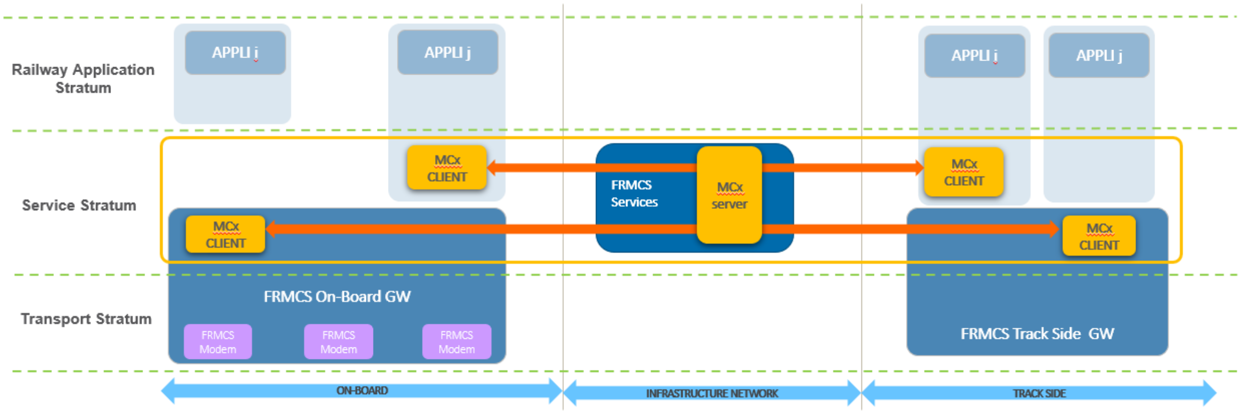


Figure 9: FRMCS Service Stratum – MCx Clients & MCx Server

Depending on where the MCx client is embedded, the coupling between the application and the gateway will be different. The specifications of the coupling seen from the application in both modes are described in the following paragraph.

More details the different stratums can be found in *[S8]*.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.2 Loose vs Tight Coupled Application

As part of the transition from the old version of the train control system (ERTMS) to the new FRMCS generation, existing applications will have to be migrated to make them compatible with the FRMCS system, especially to manage the MCx logic.

In this application migration, as explained in the previous paragraph, both coupling modes are to be considered:

1. Applications that are aware of their transport service requirements and that are able to request those from the FRMCS system;
2. Applications that are not aware of their transport service requirements and that are therefore not able to request those.

For both coupling mode, the exchanges will be managed by the FRMCS system, involving the use of a MCx client. Only the location of the MCx client is different and the notion of tight and loose coupling is introduced:

- For **tight** coupling, the MCx client is embedded in the application,
- For **loose** coupling, the MCx client is embedded in the FRMCS On-Board and Trackside Gateway.

This implies different messages will be sent, depending on the type of coupling of the application, for the interface exposed by on-board gateways to the applications. For on-board gateway, this interface is named OBapp and described below in paragraph “2.2.12 FRMCS On-Board & Track Side gateways Interfaces”.

The two modes of application coupling are summarized in “Figure 10”.

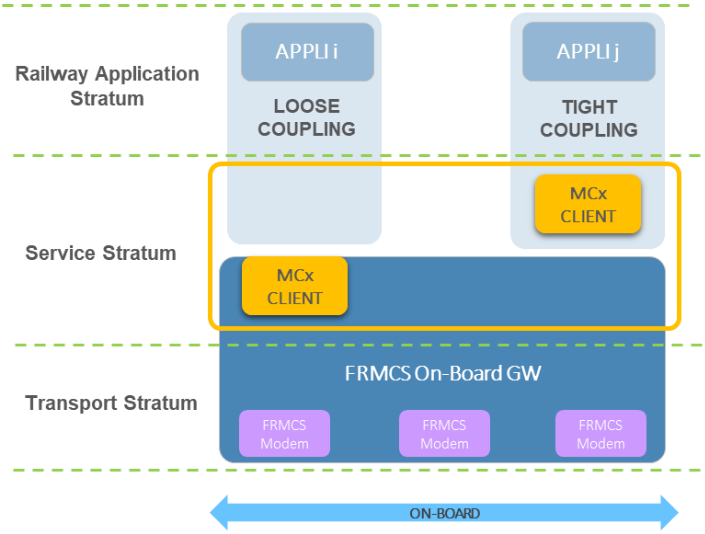


Figure 10: Loose-coupling vs tight-coupling for applications

Obviously, the main advantage for the applications is to rely on a standardized MCx logic and, in turn, to be independent of possible changes introduced in the transport layer.

The same approach is applicable to the trackside. The interface between applications and track-side gateway is named TSapp and described below in paragraph "2.2.12 FRMCS On-Board & Track Side gateways Interfaces".

The end-to-end view of loose and tight coupling for applications is summarized in "Figure 11".

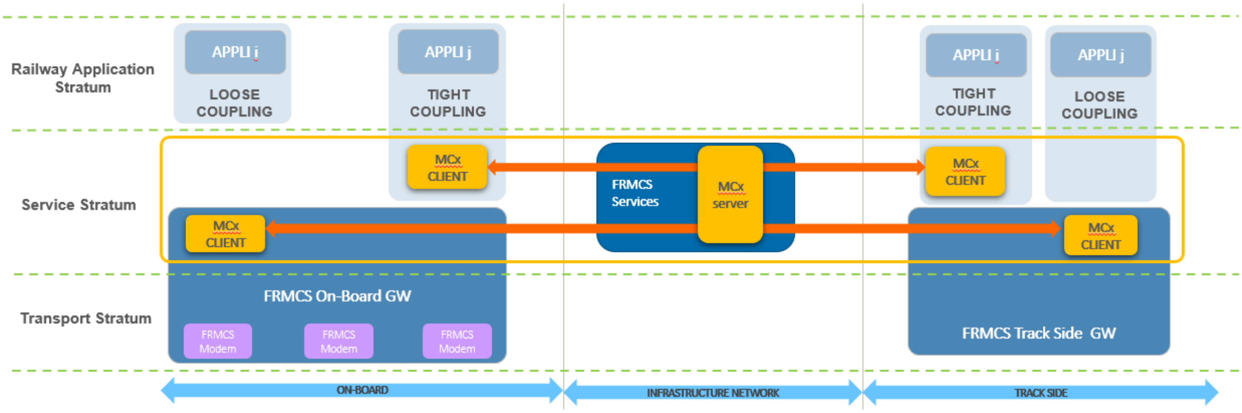


Figure 11: End to end view of loose and tight coupling for applications

The coupling type for critical applications is the following:

- Only the VOICE application will use **tight coupling** mode;
- All other applications (ETCS, ATO, TCMS, CCTV/Video, PIS) will use **loose coupling** mode.

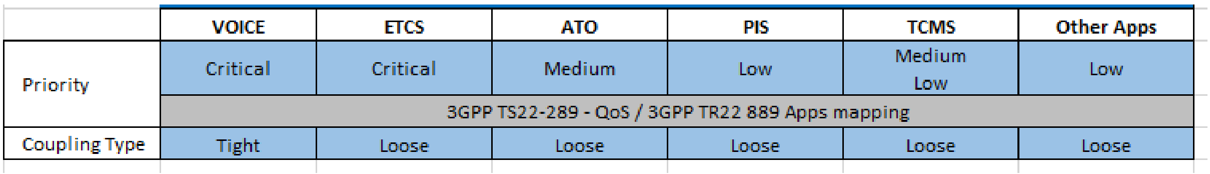
“Arguments for loose coupling of data centric Railway Applications” are provided in *[S12]* document.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.3 Quality of Service (QoS) and priority

Railway applications exhibit different characteristics, e.g., in terms of latency or reliability. On the other hand, the FRMCS System offers bearer services with different characteristics. The main purpose of the Quality of Service (QoS) is to specify the list of attributes applicable to the FRMCS bearer service.

Application categories describe the data transfer characteristic to be achieved by a bearer service. In order to reach the QoS applicable for each application category, also transport priority levels are required to differentiate among the communication urgency. Priority handling of communication service encompasses the assignment of a priority to a communication and involves the seizing of resources, which are in use by a communication having a lower ranking in the absence of idle resources. Priority handling includes as well discontinuation of an ongoing communication having a lower priority to allow an incoming communication of higher priority. Priority handling needs to be provided to a FRMCS User for all communications. The priority of application is summarized in Table 14 below.



	VOICE	ETCS	ATO	PIS	TCMS	Other Apps
Priority	Critical	Critical	Medium	Low	Medium Low	Low
	3GPP TS22-289 - QoS / 3GPP TR22 889 Apps mapping					
Coupling Type	Tight	Loose	Loose	Loose	Loose	Loose

Table 14: Critical applications Priority and Coupling Type[1]

The QoS will be based on FRMCS MCx services using 5G QoS so called 5QI, from FRMCS modems and 5G core, as illustrated in “Figure 12” (See orange boxes).

[1] For VOICE, the table mentions only critical priority, which the strongest requirement. Obviously, additional QoS and priority requirements are needed to differentiate railway emergency call and low voice priority call, for example. Details are available in the application profiles description, described later in this document.

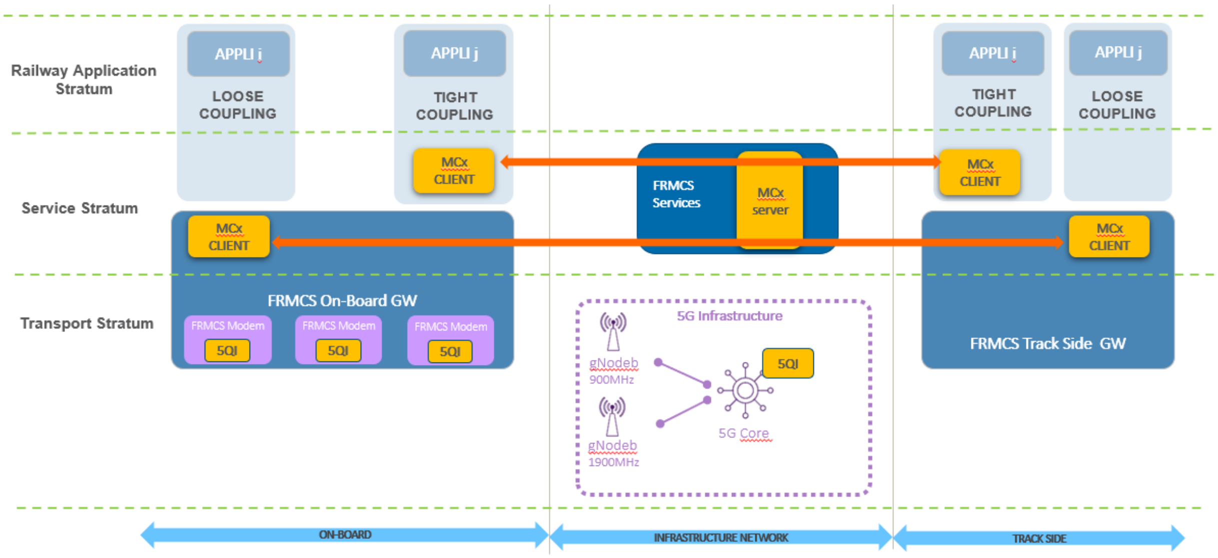


Figure 12: QoS function

It is important to note that QoS is only managed for FRMCS modems (not for 4G, Wi-Fi, etc.); the framework for Quality of Service within the FRMCS System is used.

For more detail, the use case "QoS in a railway environment" is described in detail in *[S7]*. Refer to 9.1 (Appendix 1) for details on communication attributes to QoS translation.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.4 Session Management and Addressing/routing

FRMCS system uses the IP protocol suite as its key technology; both at internal and external interfaces.

The purpose of this function is to authenticate the application by FRMCS OB GTW, before opening end to end session, between on-board and track side part of the application.

The proposed solution will rely on Mission Critical services as described in the 3GPPP standardization documents; in particular MCData. MCData is a suite of services which utilizes the common functional architecture defined in 3GPP TS 23.280 to support MC services including the common services core. One service of the MCData services suite is IP Connectivity, illustrated in '' Figure 13" (extracted from *[S11]*, page 23).

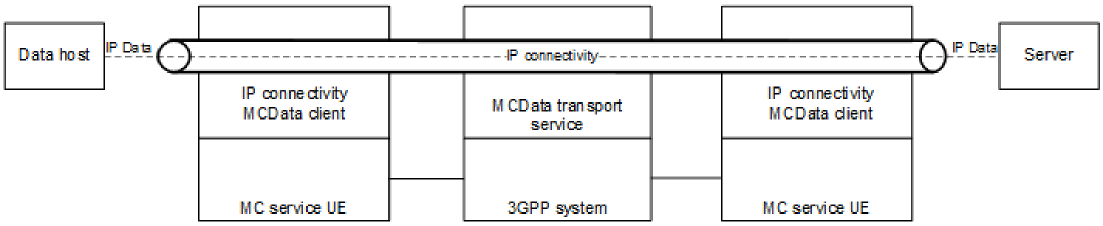


Figure 13: IP connectivity model

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality: OB & TS gateways and tight coupled applications (i.e. VOICE).

2.2.5 Bearer Flexibility

As explained in the use case “bearer flexibility” from *[S7]* document, FRMCS envisages bearer flexibility to allow a certain level of independence between Railway Applications and the underlying transport system. FRMCS includes wireless and wireline access. It comprises multiple access systems and shall support various voice and data applications.

The rationale behind these requirements is that the lifecycle of railway applications is in general much longer than the lifecycle of telecommunication access/transport systems. Moreover, bearer flexibility aims at improving service availability and performance.

The characteristics of bearer flexibility are:

1. A Railway Application may use one or one of several access systems as appropriate.
2. Connection of FRMCS Equipment to different access systems is dynamic (i.e. the most appropriate 3GPP or non-3GPP access technologies are selected automatically, potentially using multiple access technologies for one or more Railway Applications).
3. The set of access systems chosen meets the defined QoS and the service requirements e.g. FRMCS User mobility and connectivity which are necessary to guarantee the functionality.
4. The introduction of a new access system should not negatively impact existing Railway Applications (Principe of transparency for the applications)

The approach taken within FRMCS allows the integration of 3GPP and non-3GPP radio access evolution.

For 5GRail execution, non FRMCS modems (4G) are only used to demonstrate bearer flexibility function. In addition, for non FRMCS modems, QoS will not be managed.

The bearer flexibility function is managed by the two FRMCS gateways, which implement the transport stratum, as shown in “Figure 14: Bearer Flexibility function”.

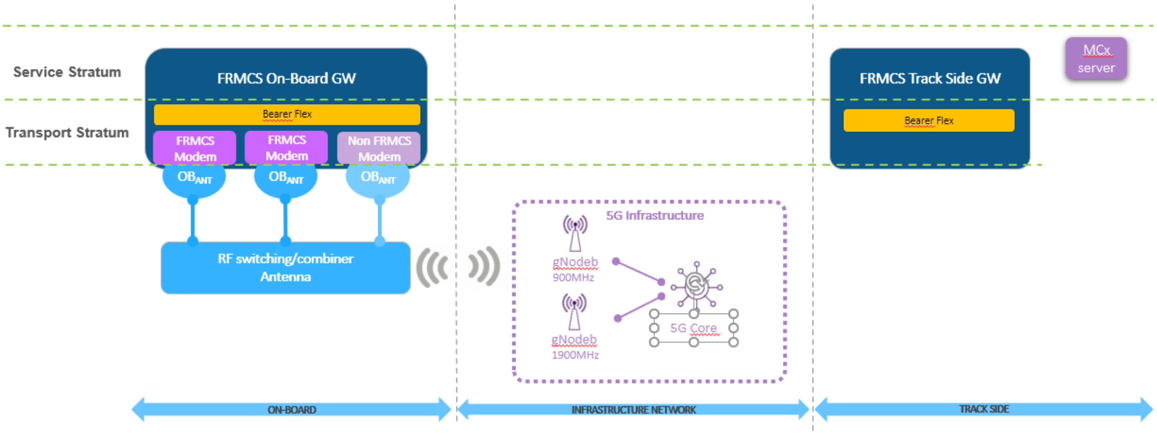


Figure 14: Bearer Flexibility function

It is important to note that the trackside gateway is mandatory to implement the bearer flexibility, although this gateway is not described in the standardization documents. In the context of 5GRAIL, it is important to notice that bearer flexibility is managed by two gateways (OB GW & TS GW) to support multi-connectivity (i.e., multiple transport domains). Thus, **bearer flex is understood as multi-connectivity** (i.e., multiple transport domains) in the context of 5GRAIL and not as multiple-access domains. The bearer flexibility feature described in this architecture report document only include the integration of multiple access technologies, while a parallel usage of multiple 5G Core systems is not covered, but part of the FRMCS target architecture (as e.g., described in *[S12]*). The bearer flexibility is therefore only a subset of the complete multi-connectivity functionality.

Two multi-connectivity use cases will be tested : links redundancy (of fallback) and links aggregation, using 4G or/and 5G networks in laboratories and fields.

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality, related to the transport stratum: OB & TS gateways.

2.2.6 FRMCS to GSM-R Switching

Switching from FRMCS to GSM-R[2] will be managed at application level, through the coordination function, as described in “Figure 15: FRMCS to GSM-R switching”.

[2] Do not confuse “switching from FRMCS to GSM-R” with “FRMCS/GSM-R interworking”. FRMCS/GSM-R interworking allows a user from one domain to communicate to another user from another domain. This feature should be transparent for the users and not managed at application level.

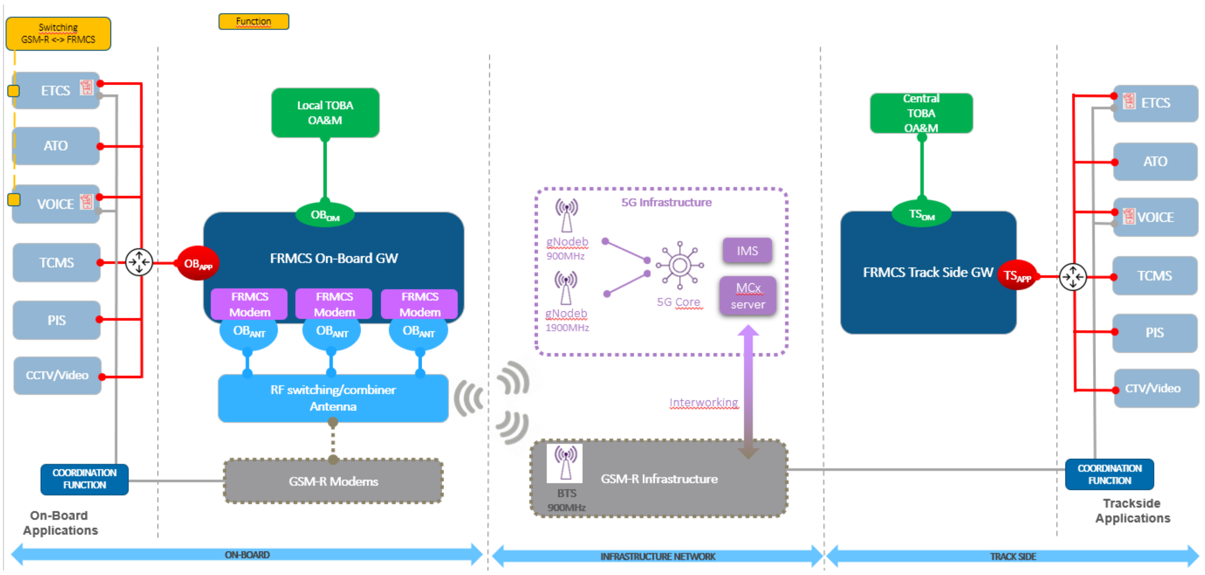


Figure 15: FRMCS to GSM-R switching

The use case “Service Interworking and service continuation between GSM-R and FRMCS” is described in detail in *[S7]*.

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality: ETCS, ATO and VOICE applications.

2.2.7 Positioning

The European railway sector concluded these last years to the necessity to evolve the European Railway Traffic Management System (ERTMS) and particularly to provide an enhanced positioning of trains.

Positioning services are part of the global train CCS (Command-Control System), particularly key for ETCS, ATO and FRMCS Voice Operational Services. In general, positioning accuracy will become a major building block to increase the automation level of train operation (See use case “FRMCS Positioning Accuracy” in *[S7]*).

Some information about “Positioning” can be found in document *[S12]*; in particular, terms definitions:

- **Positioning** is a functionality that captures the current physical location, speed and optionally the direction vector. A distinction is made between absolute and relative positioning.
- An **absolute position** corresponds to the geographical position at the time of determining the position.
- Consolidated position. The consolidated positioning information i.e. the location information resulting from the combination of all positioning sources available to the FRMCS System.

At least, absolute position is needed for on-board gateway, in order to add them to the measurements made by the O&M function.

Several sources are possible to retrieve the positioning information:

- Positioning service available on-board and used by the on-board gateway,
- Dedicated GNSS device embedded in on-board gateway,
- Reused of embedded GNSS from FRMCS 5G modem hosted by the on-board gateway.

Option 1 would have the advantage of providing a single positioning source that could be used by both on-board gateway and applications. Unfortunately, the availability of such a service is not currently confirmed. Therefore, options 2 and 3 could be used as an alternative for internal on-board gateway needs. For all options, the impacts on the interfaces of the on-board gateway will be studied.

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality: OB gateway and VOICE application.

2.2.8 Location

Location Services are the capability of the FRMCS system to store and provide the location of the user(s) or devices.

Location Services shall be able to provide a mechanism for obtaining high accuracy Location information by integrating position information from multiple external sources (e.g. magnetometers, orientation sensors, GNSS).

Location information as a consolidated position shall be based on the most accurate available information, for example taking into account track position and running/moving direction. The provisioning of localization assisting data (e.g. GNSS RTK correction data, digital map data, etc.) by devices and external systems shall be supported.

The location service shall support the following elements:

- User's geographical horizontal position;
- User's geographical horizontal and vertical position;
- User's velocity (speed and direction in the horizontal space);
- User's acceleration;
- Railway infrastructure element(s) linked to the user (e.g. track section ID, station ID, signal box ID, track kilometer marking).

Each location information element shall be accompanied by:

- The level of accuracy of the location information element;

- The time stamp of the location information element.

The location services shall provide, upon request, the identity/ies of the user(s) matching the following criteria:

- User's geographical position included in a given polygon;
- User's velocity included in a given range;
- User's geographical position linked to a railway infrastructure element(s);

2.2.9 Timestamping & Synchronization

At least, timestamping is needed for on-board gateway, in order to add them to the measurements made by the O&M function. In addition, for cybersecurity needs, information from all system log files can be retrieved and their analysis is simplified if all data has been timestamped with a common time source.

Several sources, provided by the system or by a node of the system, are possible to retrieve the time for information timestamping:

- Service available on-board and used by On-Board Gateway,
- Common NTP server,
- On-Board gateway local NTP server.

For all options, the impacts on the interfaces of the on-board gateway will be studied.

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality: OB & TS gateways.

2.2.10 Availability / Redundancy - Resilience

For certain applications, especially but not exclusively the critical ones, a high availability, reliability and resilience of the connection to the trackside may be instrumental in establishing redundant nodes (avoiding single points of failures) and/or redundant radio links. The usage of multiple Mobile Radios and/or multiple Trackside Transport domains may here be an important component to addressing the stated KPIs.

This is an important functionality of the whole system unfortunately not yet described in the standardization documents.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.11 Cybersecurity

The European railway sector concluded these last years to the necessity to evolve the European Railway Traffic Management System (ERTMS) and particularly to increase cybersecurity measures.

The FRMCS Architecture & Technical Work group (ATWG) oversees the global FRMCS architecture, the SRS (System requirements Specification), the System Use Cases for 3GPP standardization, the cybersecurity aspects and the technology orientation. Currently, work is still in progress and no "Cybersecurity Specification" document is available.

Obviously, the embedded FRMCS gateway, based on the new Telecom On-Board architecture ("On-Board router") will have to include some cybersecurity material protections. More generally, cybersecurity must be addressed at the system level and its implementation will potentially impact all nodes of the solution.

Some information about "System Security" can be found in document *[S3]*. Existing FRMCS cybersecurity specifications to be considered for 5GRAIL are:

- UIC URS v5 Paragraph 8
- 3GPP TR 22.889 v17.3.0 Section 12.15 (also called system use cases for 3GPP standardization)
- TOBA FRS 7510 v1.0.12 section 7.6 (This document is not yet published – Not present in reference document paragraph)

For 5GRail project execution, in the absence of specification documents for system cybersecurity, the focus will be on MCX service security framework further detailed in 5.2.2.4.10 and OBapp/TSapp Local Binding function described in 5.2.2.4.5.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.12 FRMCS On-Board & Track Side gateways Interfaces

As explained above in this document, the on-board gateway is a new entity in the Telecom On-Board Architecture (TOBA), in charge of achieving a decoupling between application and communication service as well as transport service. Thus, the interface named OBapp, between the On-Board gateway and the applications, whatever the coupling mode used, is a key interface (see "Figure 16: OBapp interface").

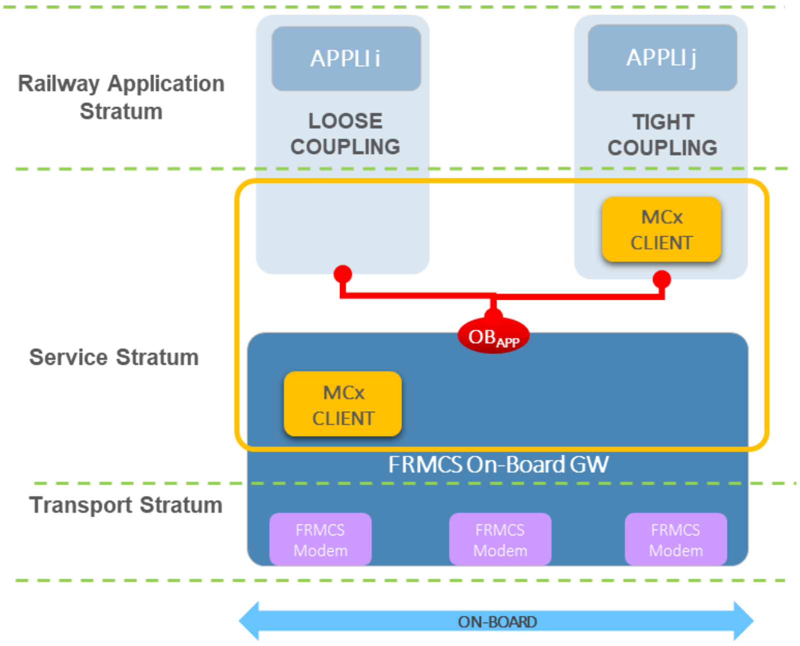


Figure 16: OBapp interface

OBapp is the functional interface between applications and FRMCS on-board system and all applications shall use the FRMCS on-board system through this interface. Several guidelines for his OBapp interface are available in document *[S9]*. However, although this interface should be standardized, the specification documents are not yet available.

In order to move forward on the project, a version of this OBapp interface has been defined in chapter 6.2.

OBom will not be standardized. A proposal for these interfaces has been defined in chapter 5.2.3.

The OBant antenna is a physical interface that connects the outputs of the modems to the antennas (see “Figure 17: OBant interface”), arranged on the roof of the train. This interface is realized using suitable existing industry standard, like SMA.

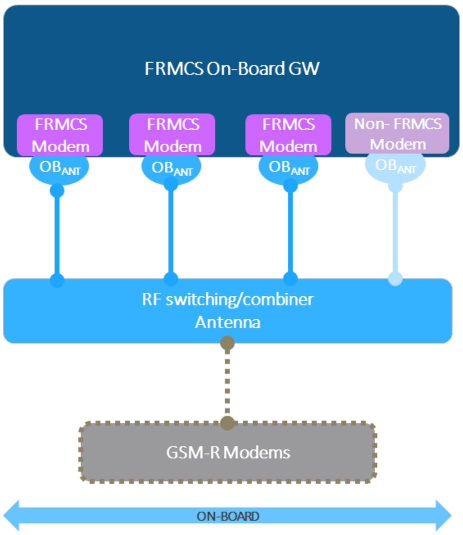


Figure 17: OBant interface

The same logic is applicable for the track side gateway, except for OBant interface as no FRMCS modems are embedded on track side. The interface name is prefixed by TS instead of OB. Thus, OBapp is renamed TSapp, as shown in "Figure 18".

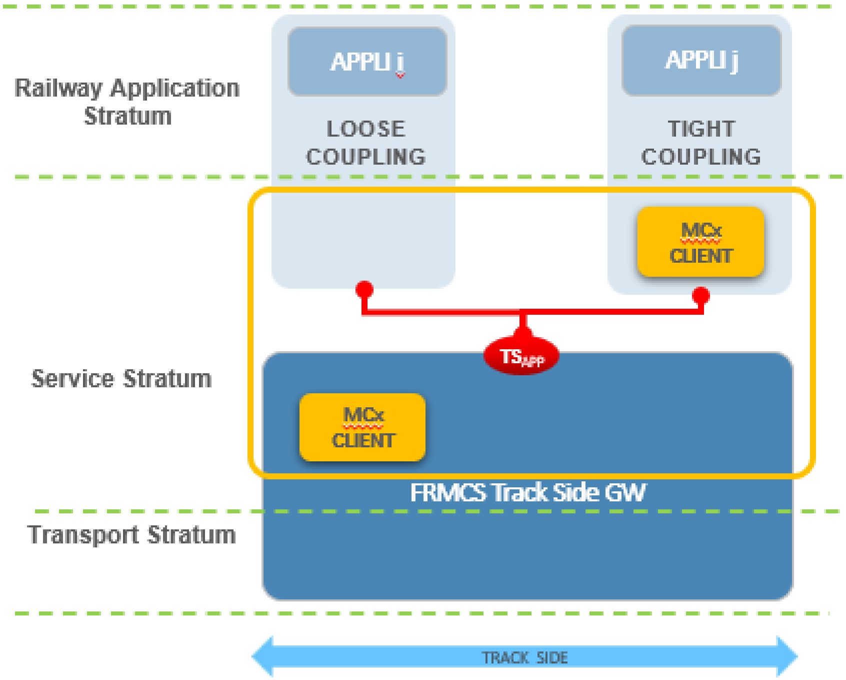


Figure 18: TSapp interface

As for the OBapp interface, no specification document is currently available. A version of this TSapp interface has been defined in chapter 6.3.

The same applies to TSom and TSinfra interfaces; where TSinfra is the Core Network interface of the track-side gateway. A proposal for these interfaces has been defined in chapter 5.3.3.

All components of the WP2 deliveries (i.e. OB & TS gateways and all applications) are impacted to support this system functionality.

2.2.13 Auxiliary function

Auxiliary function is described in *[S8]* document as follow:

> "This function is the instantaneous collector of certain status information and is necessary for shared association mode and a potential option in the loose coupled approach in dedicated mode. »

Thus, auxiliary function is mainly there to provide status of the connectivity i.e. return of information from user equipment (UE) to applications (Modem failure, link supervision, etc.).

From WP2 deliveries point of view, only a subset of components is impacted to support this system functionality: OB gateway and all applications. For TS gateway, still need to confirm if it is concerned as the function is linked to modems and radio access links management.

2.2.14 RF switching/combiner antenna

In railway environment, the space for antennas, on the roof of the train, is limited.

Therefore, whenever possible, antenna has to be shared across the used technologies and frequencies (5G, 4G, Wi-Fi, GSM-R, GNSS). For that, it is possible to combine or switch antennas.

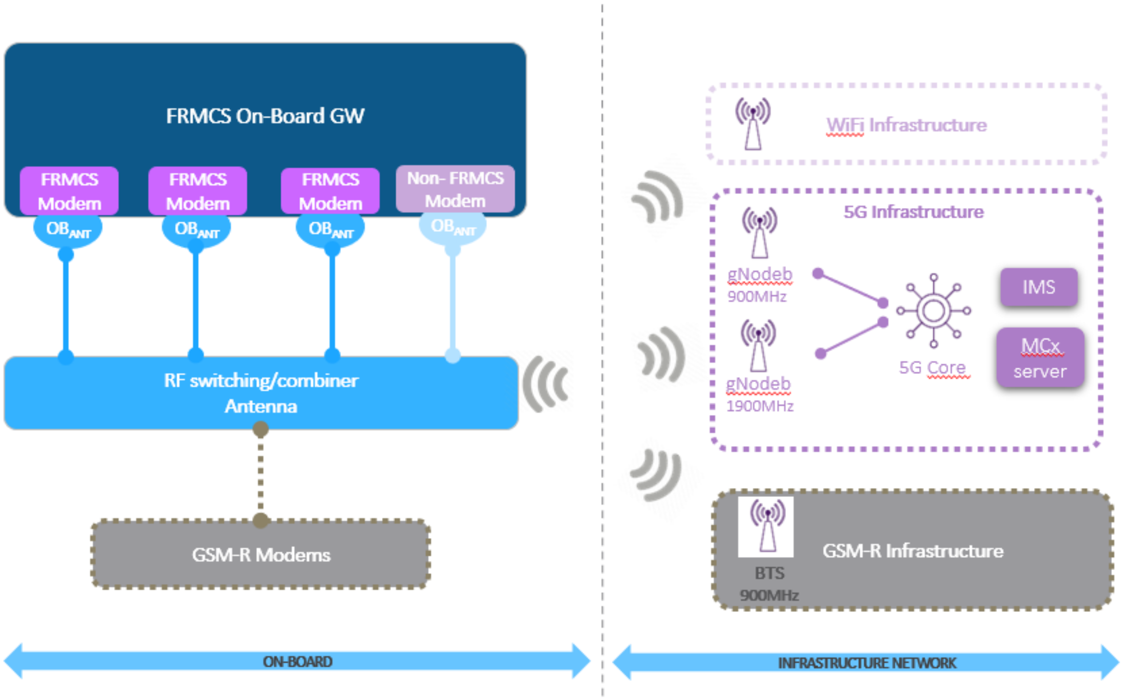


Figure 19: RF switching/combiner antenna.

In 5GRAIL context, there are three use cases to be considered and detailed in:

- FRMCS 5G placing in GSM-R train,
- FRMCS 5G modems hardware redundancy,
- Bearer Flexibility.

From WP2 deliveries point of view, only one component is impacted to support this system functionality: OB gateway. It is the only component that embeds modems, connected to antennas.

2.2.15 FRMCS border-crossing

As GSM-R, FRMCS is based by construction on a multi-tenant seamless architecture, as the liberalization of railway business in Europe makes that trains have to run on different national or regional architectures, with a fully interoperable level of service for essential operational communications.

Additionally, with the concept of global interconnection derived from GSM-R and extended in the frame of FRMCS 5G, the vehicles will run in a European railway cloud supporting Europe-wide identical Connected and Automated Mobility (CAM) services.

The inter-network roaming feature must support both national and international roaming, as illustrated by “Figure 20: Network crossing function”:

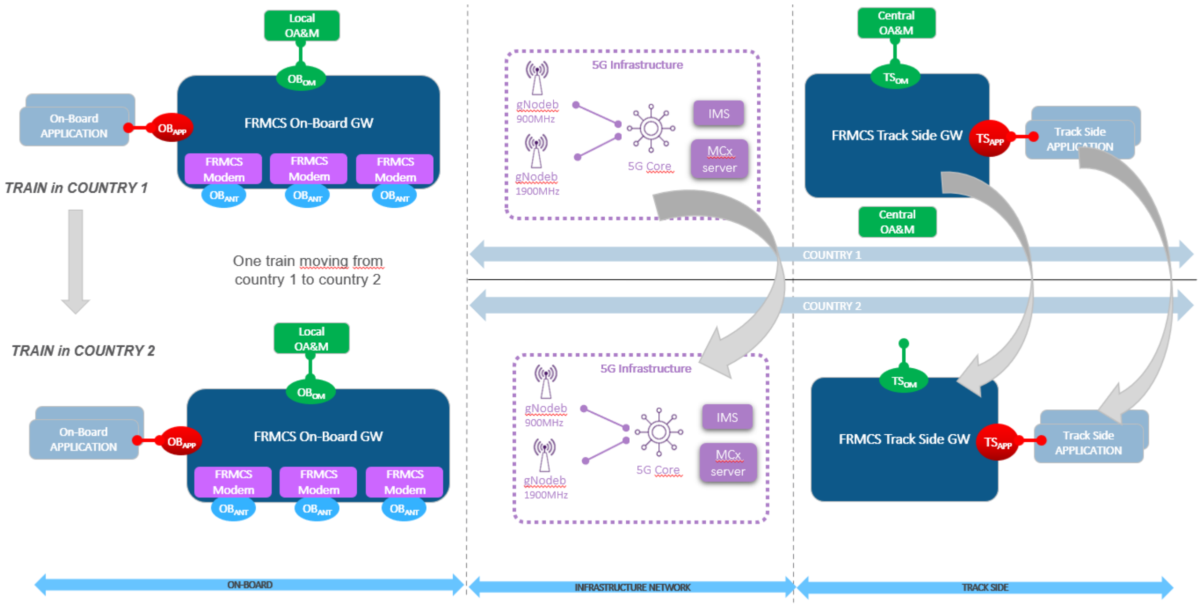


Figure 20: Network crossing function

and “Figure 21: Border crossing function”:

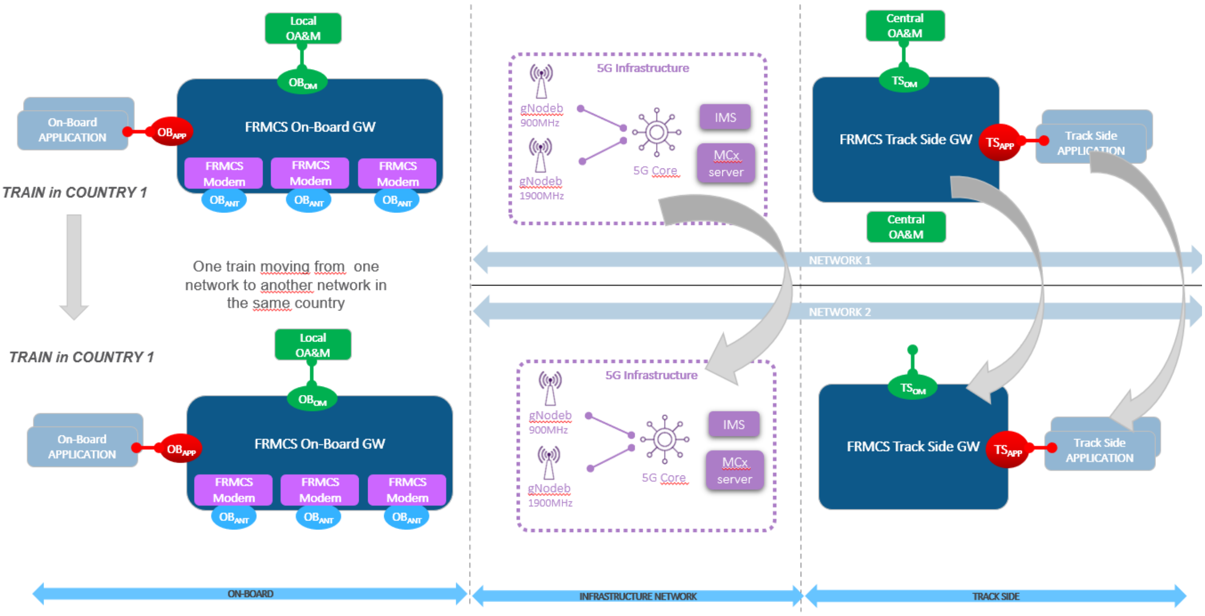


Figure 21: Border crossing function

From WP2 deliveries point of view, only one component is impacted to support this system functionality: OB gateway. It is the only component that embeds modems, connected to different radio access networks, using different radio access technology.

3 ASSUMPTIONS FOR 5G RAIL PROJECT EXECUTION

The previous paragraph described the product architecture based on currently available standardization documents.

The objective of the 5G Rail project is to implement prototypes on the basis of the current FRMCS specifications including for architecture and to validate the correct behavior of the system.

As part of the project execution, the prototypes developed will only support a subset of the product functionalities. The objective is to be able to provide an implementation in the given time and supporting the necessary functions, to validate the concepts of the TOBA architecture.

This paragraph lists the assumptions made and the limitations introduced for the project execution. These assumptions are intended to fill gaps where specifications are not yet available. It is important to note that approbation of assumptions by all 5G Rail contributors (i.e. contributors to all work packages) is a critical milestone for 5GRail project execution. This will determine the specifications baseline to implement prototypes of gateways and applications, awaited as deliveries of work package 2 (WP2).

In cases where objectives cannot be met, variances between expectations and achievement will be explained. In addition, if standardization documents become available before the end of the project, a gap analysis between the content of the architecture report and the FRMCS specifications will be provided.

3.1 Assumption table

The following table summarizes the assumptions finally considered for 5GRAIL execution.

ID	Owner	Technical Architecture Assumptions to support WP2 execution
1	Kontron	TOBA prototype supports connection with Loose and tight Coupled applications.
3	Kontron	TOBA prototype (OB and TS) supports IPv4 connections, on standard ETH socket (802.3) for OBAPP and OBOM. Only IP4 is selected to minimize complexity of implementation so that OB & TS gateways prototypes can be delivered more quickly. This assumption is mainly to reduce development duration and is acceptable for prototypes. Obviously, IPv6 is considered as a future-proof technology and will be part of the final products
4	Kontron Siemens	For tight coupled applications OB_{APP} and TS_{APP} interface is based on MCx framework
5	Siemens	Voice application will be delivered using tightly coupled approach
6	Siemens	The voice application will be cyber security tested in accordance with Siemens PSS process. Any additional requirements from the cyber security assessment will need to be addressed once it is available.
7	Siemens	Principle architecture shows dual mode coordination between GSMR & FRMCS. Assumption is this will need to be developed, with minimal coordination function. It is assumed it will be either in an GSM-R environment or FRMCS environment

8	Siemens	QoS management within FRMCS boundary will be common between tight and loose coupling, in the sense it will both be based on MCX.
9	Siemens	Authentication interface will be common between tight and loose coupling
10	Siemens	Voice arbitration will be done at the application level. Tables 5A.1.1 Call arbitration table for incoming new calls (MI) and 5A.1.2 Call arbitration table for outgoing new calls (MI) of the EIRENE SRS v16.0.0 will be used for the 5GRail project
11	CAF	There will be a counterpart on the trackside equivalent to wayside for Loose Coupled approach.
12	CAF	As there is no decision for TCMS, TCMS and ETCS will follow the same approach for resource efficiency, using both applications the same client implementation.
13	CAF	Bidirectional communication between trackside and wayside is allowed.
14	Alstom	To enable the ETCS application (loose-coupled) to receive necessary information about the link between train and trackside and the link between gateway and EVC, the Auxiliary function is used. To monitor the link between gateway and EVC, another mechanism in OBapp API shall be used
15	Alstom	Name resolution: TOBA gateway is responsible for sending to the application the remote IP address to be used by the application for user plane. In the session establishment request, the OB ETCS application sends the FQDN of the RBC to be joined or the RBC ID, TOBA will use this information to establish the session with the relevant TS_GTW
16	Alstom	For on-board applications: no local authentication for the 1st prototype (in other words, OBauth will not be implemented). At the end, we suppose a local authentication using TLS within OBAPP API. Valid for ETCS and ATO
18	Alstom	The first prototype will consider FRMCS only (no switching between FRMCS and GSM-R). Valid for ETCS and ATO
19	Alstom	Assumption on hold waiting for clarification : Cross-border scenario not clear yet (pure roaming? Conservation of MCData-Ipconn session?). RBCs will be reachable from any FRMCS network. Thus, at border crossing between countries A and B, ETCS application will not request to FRMCS to establish a second communication service on the network of country B before terminating the communication service on the network of country A. This refers also to the second note in TOBA_FRS chapter 7.5.2, the underlying requirements become obsolete. Valid for ETCS and ATO. This assumption is based on [S9] - UIC TOBA FRS-7510 - FRMCS Telecom On-Board System – Functional Requirements Specification (FRS) – Version 0.2.0 (Draft) – 14/04/2020. Be aware, according to chapter 7.5.1 of TOBA FRS 7510 version 1.0.12 (21/05/2021 - This document is not yet published – Not present in reference document paragraph), it should be possible to be connected to RBC in country A and RBC in country B at the same time, while the transport connection only needs to be established to a single PLMN.
20	Alstom	ATO and ETCS is a loose-coupled application
21	Alstom	Name resolution: TOBA gateway is responsible for sending to the application the remote IP address to be used by the application for user plane. In the session establishment request, the ATO-OB application sends the FQDN of the ATO-TS, TOBA will use this information to establish the session with the relevant TS_GTW

22	Alstom	Assumption on hold waiting for clarification : Cross-border scenario not clear yet (pure roaming? Conservation of MCData-Ipconn session?). ATO-TS will be reachable from any FRMCS network. Thus, at border crossing between countries A and B, ATO-OB application can request to FRMCS to establish a second communication service to a second ATO-TS even if TOBA is not attached yet on the network of country B. In other words, the application is not responsible to request to FRMCS a change of network. This refers also to the second note in TOBA_FRS chapter 7.5.2, the underlying requirements become obsolete.
23	Alstom	OBAUTH is a local authentication between TOBA and on-board applications, it does not rely on a trackside server. We suppose a local authentication using TLS within OBAPP API
24	Alstom	FRMCS will need a trackside gateway in front of TOBA (at least for loose-coupled applications)
26	Alstom	ETCS dev will be phased that way : - 1st phase: ETCS will support flat IP approach only - 2nd phase : ETCS will implement loose couple interface (Obapp) - 3rd phase : ETCS will implement switch-over between FRMCS and GSM-R -Flat IP approach has to be considered for ETCS trackside simulator (no implementation of Tsapp for 5GRail project)
27	SNCF	Remote vision app will use flat IP only interface for 5GRail project aligned with phasing approach
30	Thales	PIS will need a trackside auxiliary function to interop with FRMCS service function via TSAPP
31	Thales	PIS prototype supports connection with Loose Coupled applications
32	Thales	Security requirement on Obapp / Tsapp : U_p, C_p , O&M and logs data streams from applications separation on OBAPP and TSAPP interfaces. This will be prototyped by PIS application within 5GRAIL.
33	Thales	Bidirectional communication between trackside and wayside is allowed.
34	Thales	For on-board PIS application: local authentication will be implemented via OBAUTH (local binding)
35	Thales	For trackside PIS applications: local authentication will be implemented via TSAUTH
36	Thales	Bidirectional PIS data streams to be only handled by FRMCS connectivity (not via GSM-R)
39	Kontron	TOBA prototype QoS will be based on static QoS flow statically provisioned by network infrastructure.
40	Kontron	TOBA prototypes integrate 1900MHz FRMCS 5G modem - (900MHz - currently not feasible)
41	Kontron Thales	TOBA prototypes integrate WIFI and 4G modem to support potential fallback/bearflex Test cases
42	UIC	5GRAIL critical applications shall make use of MCX Services
43	UIC	FRMCS Trackside Gateway Functions should be either implemented over a dedicated product (new H/W and S/W) or part of an existing 5GC Network Elements (new S/W only)
44	UIC	FRMCS Trackside Gateway Functions shall be interoperable with FRMCS Onboard Gateway (i.e., TOBA). However, this is not considered with 5GRAIL prototypes.
45	UIC	The Auxiliary functions (i.e., accessibility of FRMCS Service via a link status) shall be within the FRMCS boundaries
46	UIC	ETCS and ATO shall make use of MCData IP Connectivity (IPCONN) Service type
47	Alstom	The OB_GTW embeds a gnss receiver or use the gnss capabilities included in Thales modem. Please also see chapter 5.2.1.9.

49	Alstom	For synchro: OB GTW can use the time information from GNSS receiver for its own needs (e.g. timestamping) but at this stage there is no requirement for OB GTW to distribute time to the applications through NTP
50	Teleste	CCTV live streaming: IP stream is provided from onboard CCTV camera, through Video Management System (VMS). VMS is interfacing with onboard FRMCS GW through OBapp. On the trackside there is another VMS, which is interfacing through Tsapp
51	Teleste	Transfer of CCTV archives (i.e., CCTV offload)application shall requires QoS support from Obapp
52	Teleste	CCTV applications (including CCTV live streaming) are Loose coupled.
53	Kontron	QoS is only managed for FRMCS modem (No QoS for Wi-Fi, 4G, etc.)
54	Alstom	The OB_GTW can obtain GNSS positioning only, but it is not responsible for a consolidated positioning (i.e. location information resulting from the combination of all positioning sources available to the FRMCS system) or its distribution to the applications. The consolidated positioning and its distribution would be performed by a dedicated on-board equipment, not in the scope of the WP2 architecture report.
55	Nokia	Nokia will provide 3GPP standardized connectivity between dispatcher and MC Server (as defined in 3GPP SA6 TS23.280). So dispatcher will not be connected to the TS_GW and not use TSAPP. In this implementation of tight application, TSAPP=OBAPP is not assumed anymore
56	Kontron	In the context of 5GRAIL, it is important to notice that bearer flexibility is managed by two gateways (OB GW & TS GW) to support multi-connectivity (i.e., multiple transport domains). Thus, bearer flex is understood as multi-connectivity (i.e., multiple transport domains) in the context of 5GRAIL and not as multiple-access domains
57	CAF	On TCMS, for prototype purposes "auto_accept" mode will be used

Table 15: Assumption table

4 FRMCS 5G MODEMS

Referring to the **FRMCS PRINCIPLE ARCHITECTURE-PRIMARY STRATUM FUNCTIONAL BLOCKS** from the FRMCS 5G modem is in the red circle.

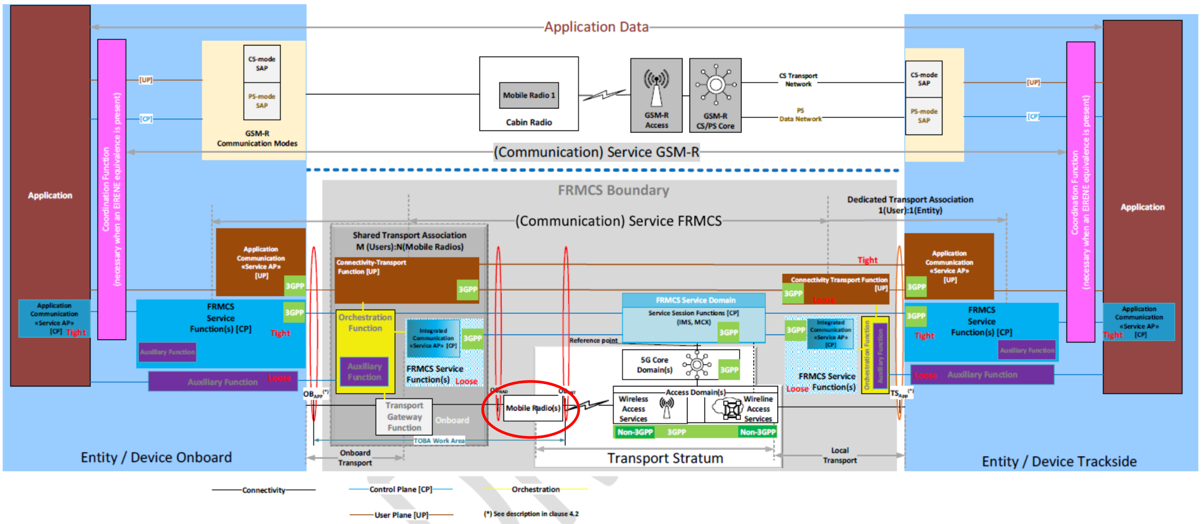

Application Data
Application
Coordination Function
(necessary when an EIRENE equivalence is present)
[UP]
[CP]
CS-mode SAP
PS-mode SAP
GSM-R Communication Modes
Mobile Radio 1
Cabin Radio
GSM-R Access
GSM-R CS/PS Core
CS Transport Network
PS Data Network
(Communication) Service GSM-R
FRMCS Boundary
(Communication) Service FRMCS
Shared Transport Association M (Users):N(Mobile Radios)
Dedicated Transport Association 1(User):1(Entity)
Application Communication «Service AP» [UP]
3GPP
Application Communication «Service AP» [CP]
Tight
FRMCS Service Function(s) [CP]
Auxiliary Function
Loose
Connectivity-Transport Function [UP]
Orchestration Function
Integrated Communication «Service AP» [CP]
FRMCS Service Function(s)
Transport Gateway Function
Onboard
TOBA Work Area
OB_{APP} (*)
OB_{RAD}
OB_{ANT}
Mobile Radio(s)
Reference point
FRMCS Service Domain
Service Session Functions [CP] (IMS, MCX)
5G Core Domain(s)
Access Domain(s)
Wireless Access Services
Wireline Access Services
Non-3GPP
Connectivity Transport Function [UP]
TS_{App} (*)
Entity / Device Onboard
Onboard Transport
Transport Stratum
Local Transport
Entity / Device Trackside
Connectivity
Control Plane [CP]
Orchestration
User Plane [UP]
(*) See description in clause 4.2

Figure 22: FRMCS principle architecture

The Mobile Radio (the Modem) complies with major FRMCS requirements in terms of frequency band and output power, allowing the execution of the 5G Rail test cases in lab environment and on track. It is designed to be integrated into the TOBA Onboard Device. Several Modems can be integrated side-by-side into one Device.

4.1 Modem description

The FRMCS mobile Radio is a complete device, capable to be approved standalone. It targets the compliance of the hardware with the regulatory and standards requirements, although for the purpose of lab and track tests on the private network frequency range FRMCS-1900MHz there will be no special regulatory approval and operator certification.
It will be ensured that the modem do not harm adjacent networks.

The modem is based on an approved Cinterion® MV31-W data card with several hardware and software changes.
The data card is reworked and with a new baseband it gets the name **MR21-SR**. Together with an external PA it builds a device **FGR21-SR** with 31dBm output power to fulfil the basic requirements for the FRMCS-1900 frequency band.

4.1.1 Directives

- 2014/53/EU - Directive of the European Parliament and of the council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the

market of radio equipment and repealing Directive 1999/05/EC.
The device is labelled with the CE conformity mark.

- 2002/95/EC (RoHS 1) 2011/65/EC (RoHS 2) - Directive of the European Parliament and of the Council of 27 January 2003 (and revised on 8 June 2011) on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)

4.1.2 European type approval

- For the prototypes it is not foreseen and regulatory approval or operator certification.

4.1.3 Requirements of quality

- IEC 60068 Environmental testing
- DIN EN 60529 IP codes

4.2 Safety precautions note

Do not operate the cellular modem in the presence of flammable gases or fumes. Switch off the cellular terminal when you are near petrol stations, fuel depots, chemical plants or where blasting operations are in progress. Operation of any electrical equipment in potentially explosive atmospheres can constitute a safety hazard.

Your cellular modem receives and transmits radio frequency energy while switched on. Remember that interference can occur if it is used close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always switch off the cellular terminal or mobile wherever forbidden, or when you suspect that it may cause interference or danger.

SOS IMPORTANT!
Cellular terminals or mobiles operate using radio signals and cellular networks. Because of this, connection cannot be guaranteed at all times under all conditions.
Therefore, you should never rely solely upon any wireless device for essential communications, for example emergency calls.
Remember, in order to make or receive calls, the cellular terminal or mobile must be switched on and in a service area with adequate cellular signal strength. Some networks do not allow for emergency calls if certain network services or phone features are in use (e.g. lock functions, fixed dialling etc.). You may need to deactivate those features before you can make an emergency call. Some networks require that a valid SIM card be properly inserted in the cellular terminal or mobile.

4.3 Modem's design

The modem is designed as a complete module using hardware for standard data card MV31-W and adaptations to the FRMCS requirements. The 5G cellular platform is delivered by Qualcomm.

The adaptations include:

1. Change the base band on the MV31-W underlying chipset from SDX55 to QCX315, because only this new chipset from Qualcomm can be upgraded to support the frequency band FRMCS-1900MHz. The radio module with QCX315 base band is named **MR21-SR**.
   It will replace the currently used SDX55 platform.
   The **MR21-SR** module has a m.2 NGFF.
2. Adding an output power booster for increase the output power to 31dBm on the antenna port.
3. Adding rail quality connectors (SMA antenna connector, USB-C, Power Connector, System connector) for attaching the TOBA hardware.
4. All electronics is mounted on a Carrier PCB designed for attachment to a heat sink (not included). The size of the PCB is 80 x 100mm.
5. The PCB is mounted on a solid aluminium 8mm (max 10mm) block for best heat spreading to the heat sink.
   The mounting concept is with threaded holes from the bottom of the block and is to be defined yet.

There will be number of devices for use with the FRMCS TOBA Onboard Devices.

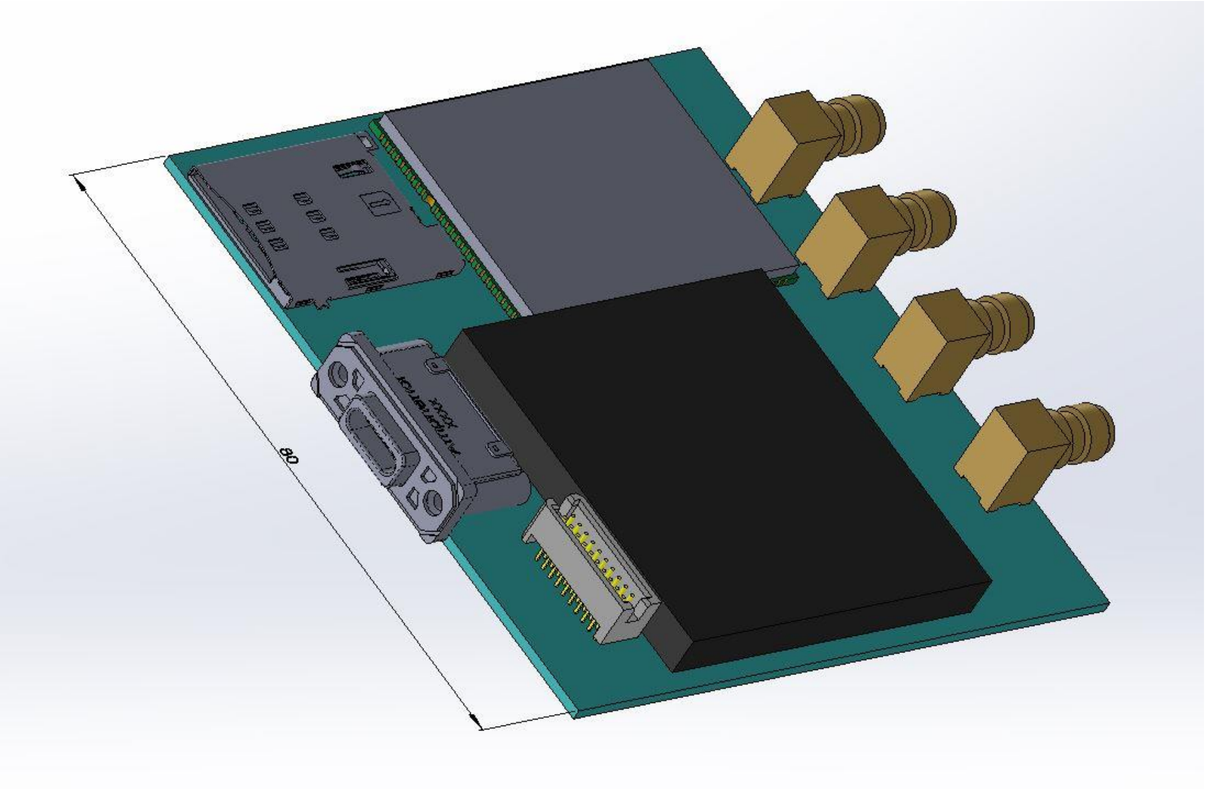


Figure 23: Modem design overview

The firmware of the modem is also adapted to the FRMCS-1900MHz frequency band (n39).

4.4 Modem characteristics

The modem will be “data only”-modem (no VoLTE, no VO NR, no emergency call and no integrated MCx client)

Feature area	Sub feature	MV31-W For comparison (5G)	MR21-SR
3GPP compliance		Rel.15 (LTE and 5G)	Rel.15
Component carrier	Max number of CC	1 (no CA)	1 (no CA)
	Maximum bandwidth	100MHz	40MHz
Carrier spacing numerology	Subcarrier spacing	15kHz (FDD) 30 kHz (TDD)	30kHz (TDD)
Modulation TDD	Maximum QAM order	DL – 256-QAM	DL – 64-QAM

		UL – 256-QAM	UL – 64 QAM
MIMO	DL	4 x 4 MIMO	2 x 2
	UL	2 x 2 MIMO	No MIMO
Duplex mode		TDD FDD	TDD FDD
Core network options		Option 3X, 3A and Option 2	Option 2
RF band support		World band coverage, see datasheet	n39

Table 16: Modem characteristics

5QI is supported as network initiated QoS. This is the same as of XDS55.

4.4.1 Throughput

The throughput is calculated as follows.

Sub-6 DL configuration	DL throughput (Mbps)	
	75% duty cycle	95% duty cycle
N39: 40MHz (64-QAM, 2x2 MIMO)	214	308
FRMCS: 10MHz (64-QAM, 2x2 MIMO)	54	77

Table 17: Modem DL throughput

Sub-6 UL configuration	UL throughput (Mbps)	
	25% duty cycle	92.5% duty cycle
N39: 40MHz (64-QAM, no UL MIMO)	44	160
FRMCS: 10MHz (64-QAM, no UL MIMO)	11	40

Table 18: Modem UL throughput

More modem capabilities are detailed in the AT commands description [3].
We recommend using the standardized AT commands to make the modem swap easy. If not possible introduce RIL (Radio Interface Layer) to make all specific adaptations on one limited place.

4.4.2 Quality of service (QoS)

About usage of 5G QoS, Qualcomm stated:

1. The UE supports only Network initiated QoS not UE initiated QoS (same as SDX55)

2. ATCOP Command support – following are not supported as they were not mandatory for passing conformance (same as SDX55)

- AT+C5GQOS
- AT+C5GQOSRDP

There is an AT command to setup the Traffic Flow Template: AT+CGTFT.
The write command looks like:

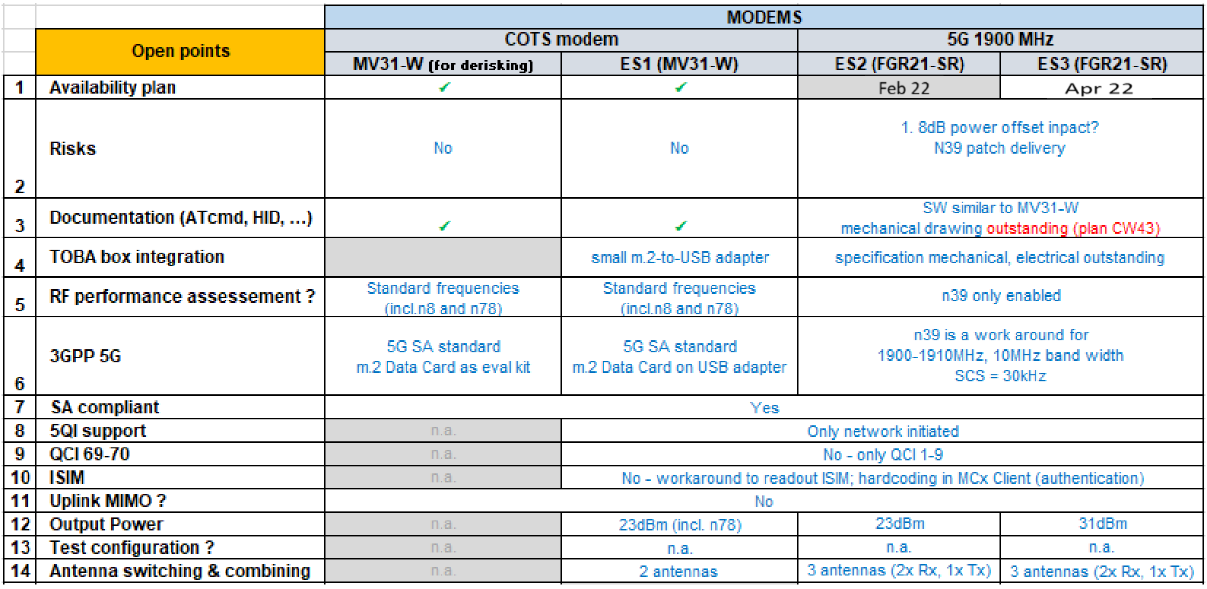
AT+CGTFT =[<cid>, [<packet filter identifier>, <evaluation precedence index> [,<source address and subnet mask> [,<protocol number (ipv4) / next header (ipv6)> [,<destination port range> [,<source port range> [,<ipsec security parameter index (spi)> [**,<type of service (tos) (ipv4**) and mask / traffic class (ipv6) and mask> [,<flow label (ipv6)>]]]]]]]]

It supports the dynamic QoS control.

4.4.3 GNSS

The reuse of the modems receive antennas for GNSS to save antenna connectors require the corresponding antenna design. The standard antennas are not suitable for this approach.
Therefore the use of modem’s GNSS with antennas not directed to the sky will prevent the expected accuracy, stability of the fix, etc. GNSS removed from the feature set.

4.4.4 Modem table



		MODEMS			
		COTS modem		5G 1900 MHz	
	Open points	MV31-W (for derisking)	ES1 (MV31-W)	ES2 (FGR21-SR)	ES3 (FGR21-SR)
1	Availability plan	✓	✓	Feb 22	Apr 22
2	Risks	No	No	1. 8dB power offset inpact? N39 patch delivery	
3	Documentation (ATcmd, HID, ...)	✓	✓	SW similar to MV31-W mechanical drawing outstanding (plan CW43)	
4	TOBA box integration		small m.2-to-USB adapter	specification mechanical, electrical outstanding	
5	RF performance assessement ?	Standard frequencies (incl.n8 and n78)	Standard frequencies (incl.n8 and n78)	n39 only enabled	
6	3GPP 5G	5G SA standard m.2 Data Card as eval kit	5G SA standard m.2 Data Card on USB adapter	n39 is a work around for 1900-1910MHz, 10MHz band width SCS = 30kHz	
7	SA compliant	Yes			
8	5QI support	n.a.	Only network initiated		
9	QCI 69-70	n.a.	No - only QCI 1-9		
10	ISIM	n.a.	No - workaround to readout ISIM; hardcoding in MCx Client (authentication)		
11	Uplink MIMO ?	No			
12	Output Power	n.a.	23dBm (incl. n78)	23dBm	31dBm
13	Test configuration ?	n.a.	n.a.	n.a.	n.a.
14	Antenna switching & combining	n.a.	2 antennas	3 antennas (2x Rx, 1x Tx)	3 antennas (2x Rx, 1x Tx)

Table 19: Modem ES summary

The following Engineering samples are/will be prepared for the 5G Rail project.

4.4.4.1 ES1 – Engineering sample 1

The ES1 is intended to support the TOBA hardware integration. It has no output booster and no frequency band adaptations, transmitting on standard frequencies according to the MV31 specification [1] and with 23dBm max output power. It is suitable to be used with the public networks for test purposes. It doesn't harm any network.
The power supply is separated, because the needed power supply (1.5A) is usually not available on a USB2.0 connector.

This modem supports the n78 band @23dBm (private network) requested for test by Nokia for DB.

The modem is designed on a small USB-2.0 adapter for use in the TOBA box.

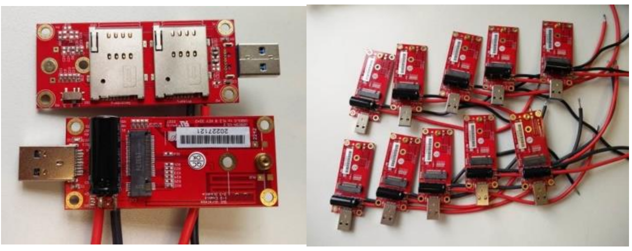


Figure 24: ES1 photos

4.4.4.2 ES2 – Engineering sample 2

The ES2 is intended for first integration with the core network in lab environment. It has no output booster but is already supporting the FRMCS-1900MHz band at 23dBm max output power.

It is intended to support the verification of the communication with the core network – system information reading, SIM configuration, registration, IP context setup, QoS concept, etc.

The modem type MR21-SR is built as a new module generation with the QCX315 baseband from Qualcomm. This QCX315 platform uses the same RF transceiver as SDX55 and provides nearly the same feature set for the IoT market.

The modem will be extended to support the n39 band. This band has the specification:
TDD 1880 - 1920 MHz (40MHz) @ 23dBm.
This band covers completely the FRMCS-1900MHz with the frequency specification
TDD 1890 – 1900 MHz (10MHz) @ 31dBm (CAB-RADIO),
but the output power.

The frequency band usage can be controlled by the network covering only the FRMCS-1900MHz portion of the band.

Delivery plan

Due to timeline constraint, finally the ES2 will not be delivered. ES3 will be the N39 modem candidate for the first integration in TOBA gateway.

4.4.4.3 ES3 – Engineering sample 3

The ES3 is intended for integration with the core network for verification of the test configuration for trials on the track. It will transmit on FRMCS-1900MHz @ 31dBm max output power according to the ECC specification.

It is highly recommended to verify at first the transmitting hardware for compliance with the regulatory, ECC and other standards' requirements before going on-air and on track.

For the increase of the output power up to 31dBm an external LDMOS power amplifier is designed. The Power Amplifier is matched, wideband 40-watt, 2-stage, LDMOS integrated amplifiers intended for use in all typical modulation formats from 1800 to 2000 MHz. These devices are offered in thermally-enhanced ceramic packages for cool and reliable operation.

This amplifier ensures high linearity for the 5G signal and low ACP.

The quiescent current is 500mA.
During operation the power consumption (92.5% duty cycle) raise to 1.5A@28V = 42W.
The power consumption for the MR21-SR module itself is 1.6A@3.3V = 5.2W
This requires a large heat sink capable to dissipate up to 42+5.2 ~ 50W in peak load cases, keeping the temperature of the radio module below 85°C – approx. 0.7°K/W.

Delivery plan

The ES3 will be delivered in the final form factor shown in 2.4.1 Mechanical dimensions.
Current planning shows delivery in April 2022.

4.4.4.4 ES4 – Engineering sample 4

This device was planned to verify FRMCS-900MHz. **It is not feasible yet and cannot be delivered as part of the 5G Rail project.**

1. The FRMCS-900MHz is partly occupied by GSM-R system. No guaranty can be given that there will be no distortion of the GSM-R system.

UL: 874.4-880.0MHz / DL: 919.4-925.0MHz, >23dBm and <31dBm (CAB-RADIO)

2. The FRMCS-900MHz is not specified by the 3GPP and cannot be used in conjunction with the 5G system yet. Major characteristics especially on the low layers logical levels are missing. Any change here is subject to firmware changes not possible today.

3. There are no components available for this frequency band and output power (FDD duplexer). Antenna isolation is required of 60dB. This is probably not reachable on the roof of the train.

Mitigation. If there is a need to verify **FRMCS-900MHz in the lab**, then n8@23dBm would be feasible, because it is part of the ES1.
It is “Lab only”, because n8 requires license for use in the field (on the track).

4.5 Modem integration in TOBA On Board gateway

4.5.1.1 Mechanical dimensions

The hardware integration assumes that the modem will have dimensions of 80x100mm:

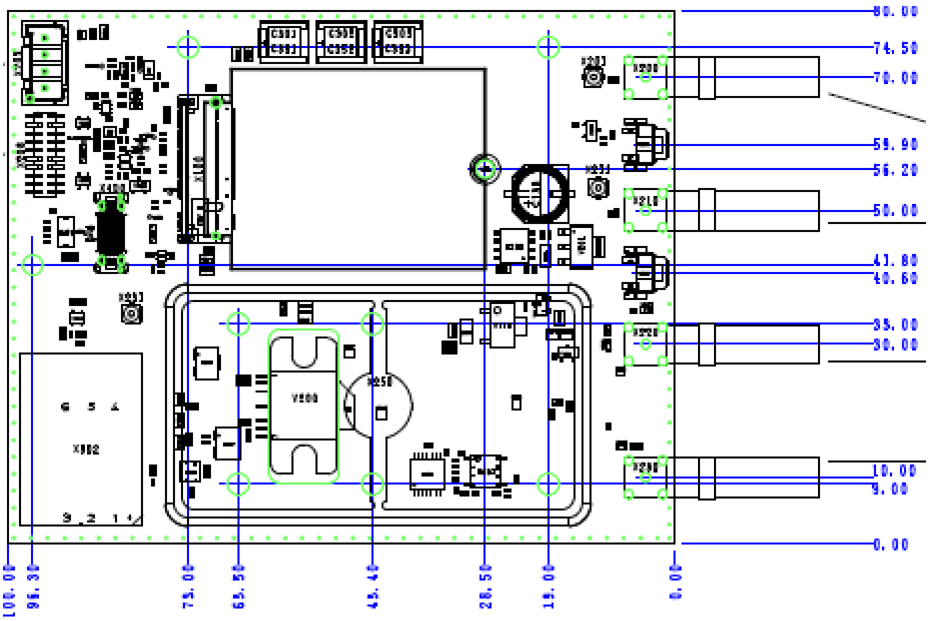


Figure 25: Modem mechanical dimensions

A first mechanical drawing out of the layout system is available in the attached document [6]

A more detailed mechanical drawing and 3D step-file will follow.

On the second page of the attached document there is the drawing of the heat spreader block for connection to the heat sink.

4.5.1.2 Sim card

Every modem needs a SIM card for the corresponding infrastructure. The first SIM slot can be mounted on the front panel for easy access. A second SIM slot is available on the modem Carrier PCB for use during standalone tests.

Substitute M.2 Data Card on the picture below with the System Connector.

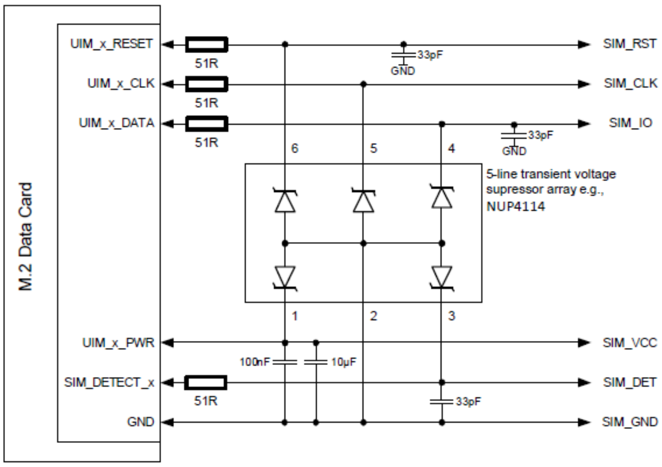


Figure 26: Modem SIM card

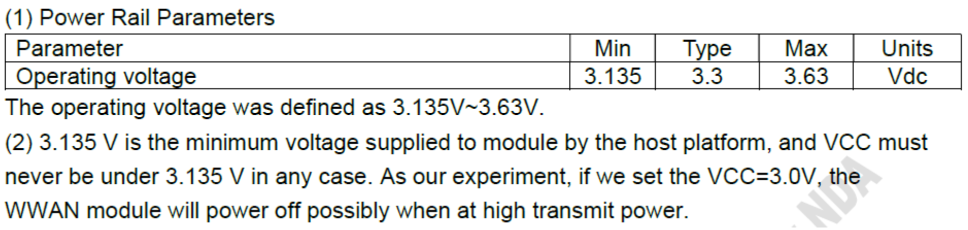
The SIM card is not accessible directly from the AT interface. Therefore optional ISIM fields e.g. for IMS authentication are not available on the AT interface.

4.5.1.3 USB

The USB-C connector offers a composite device with MBIM, AT, GNSS, Diag devices. The installation on Windows and Linux is described in the Linux integration [4] and Windows integration [5] documents. The AT command set for controlling the modem is described in AT-commands set [3].

4.5.1.4 The power supply interface

3.3V for the standard module. Max current is 1.5A@3V3



(1) Power Rail Parameters

Parameter	Min	Type	Max	Units
Operating voltage	3.135	3.3	3.63	Vdc

The operating voltage was defined as 3.135V~3.63V.

(2) 3.135 V is the minimum voltage supplied to module by the host platform, and VCC must never be under 3.135 V in any case. As our experiment, if we set the VCC=3.0V, the WWAN module will power off possibly when at high transmit power.

1. Power supply 28V max current 2A
2. Power supply 3.3V max current 2A

4.5.1.5 The system connector of the module offers pins for

1. SIM-1 interface

2. Ignition

3. Hardware Reset

4. LED interface for simple modem state indication.

5. Serial test interface

6. Antenna failure detection

4.5.1.6 Buttons and LED

On the carrier PCB there will be 2 Buttons with following functions

1. Hardware reset of the module
2. Reset the antenna monitoring circuit.

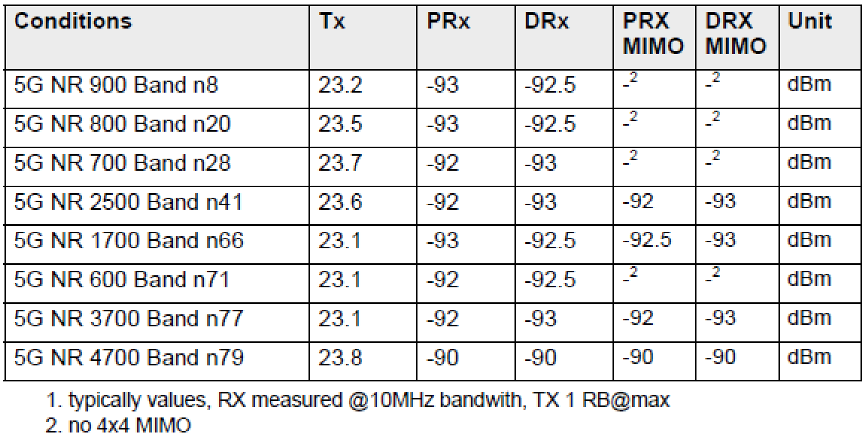
On the carrier board they will be 2 LEDs

1. LED for the connection status of the MR21-SR modem
2. LED in case of antenna problems (disconnected, not matched)

4.6 Modem antenna interface

The antenna isolation between the Tx antenna and any Rx antenna should be > 30dB. According to our measurements it translates to approx. 300mm distance between the antennas.

In the ES1 the antennas will have the following specification

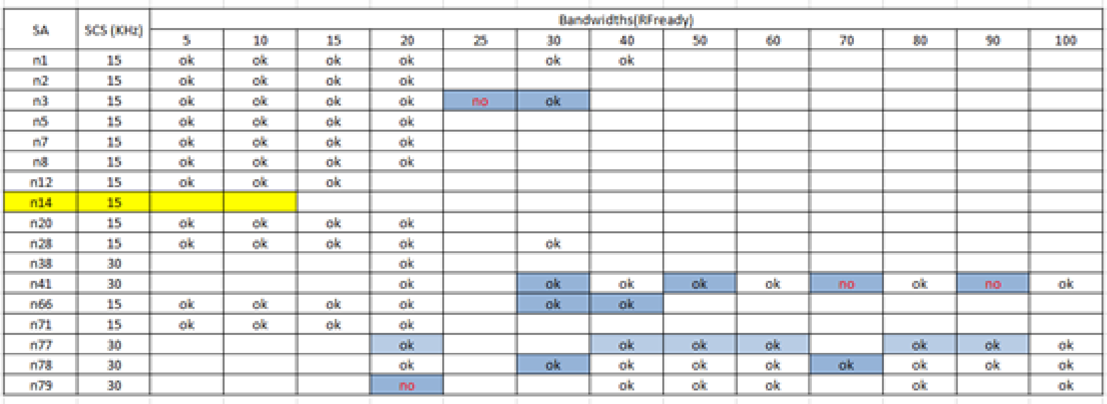


Conditions	Tx	PRx	DRx	PRX MIMO	DRX MIMO	Unit
5G NR 900 Band n8	23.2	-93	-92.5	-[2]	-[2]	dBm
5G NR 800 Band n20	23.5	-93	-92.5	-[2]	-[2]	dBm
5G NR 700 Band n28	23.7	-92	-93	-[2]	-[2]	dBm
5G NR 2500 Band n41	23.6	-92	-93	-92	-93	dBm
5G NR 1700 Band n66	23.1	-93	-92.5	-92.5	-93	dBm
5G NR 600 Band n71	23.1	-92	-92.5	-[2]	-[2]	dBm
5G NR 3700 Band n77	23.1	-92	-93	-92	-93	dBm
5G NR 4700 Band n79	23.8	-90	-90	-90	-90	dBm

1. typically values, RX measured @10MHz bandwith, TX 1 RB@max
2. no 4x4 MIMO

Table 20: Modem RF antenna interface

The available (tested) bandwidths on the different bands are summarized in the following table:



SA	SCS (KHz)	Bandwidths(RFready)												
		5	10	15	20	25	30	40	50	60	70	80	90	100
n1	15	ok	ok	ok	ok		ok	ok						
n2	15	ok	ok	ok	ok									
n3	15	ok	ok	ok	ok	no	ok							
n5	15	ok	ok	ok	ok									
n7	15	ok	ok	ok	ok									
n8	15	ok	ok	ok	ok									
n12	15	ok	ok	ok										
n14	15													
n20	15	ok	ok	ok	ok									
n28	15	ok	ok	ok	ok		ok							
n38	30				ok									
n41	30				ok		ok	ok	ok	ok	no	ok	no	ok
n66	15	ok	ok	ok	ok		ok	ok						
n71	15	ok	ok	ok	ok									
n77	30				ok			ok	ok	ok		ok	ok	ok
n78	30				ok		ok	ok	ok	ok	ok	ok	ok	ok
n79	30				no			ok	ok	ok		ok		ok

Table 21: Modem bandwidths

The antenna port specification for the FRMCS-1900MHz in ES2 and ES3 is to be defined.

There will be 4 antenna ports. The configuration will be as:

1. Tx transmit antenna port
2. Rx1 receive antenna port
3. Rx2 receive antenna port
4. GNSS antenna port

All antennas have an impedance of 50 Ohm. The design is for separate Tx and Rx antennas and antenna isolation of 30dB. The two receive antennas are needed for 2x2 MIMO configuration.

The Tx antenna has a monitoring circuit for antenna failures like disconnect, wrong impedance, broken or damaged cable, broken or damaged antenna.

4.7 Summary

The work on a modem for FRMCS frequencies is a very early try to verify the RF requirements. The component selection is hindered by the availability of RF components on the market as well as the needed firmware changes on the underlying platform.

Qualcomm is still working on the enabling of the n39 band in the platform using the QCX315 platform components on the cellular module.

The power amplification of the 5G signal in Band FRMCS-1900MHz is proven to be possible.

The development of a modem on the FRMCS-900MHz is not possible today. Beside limited availability of hardware components there is a significant change to the firmware of the platform. This is not feasible with the used platform before final standardization of the FRMCS frequencies.
As of today, ES4 cannot be delivered.
Possible workaround with n8 is limited to lab test only, because it is a public frequency and requires a license. The value of such lab tests is to be discussed and decided in the project.

First delivery of the evaluation kits (MV31) and first replay about installation and test is done.
The delivery of 28 pcs of ES1 is done as expected in July. They were built into the first TOBA devices.
In difference to the first planes, the ES1 were delivered on USB adapter.

The next deliveries are the ES2 and ES3 in form factor.
It is expected earliest in January and March 2022.
They are subject to the delivery of a n39 patch from Qualcomm.

4.8 Risks update (Modem status from 10th September 2021)

Risks, Impact and Mitigation

- Power dissipation of up to 50W needs a bigger heat sink (0.4°K/W) – very high

  Fact: For reaching needed linearity we need a PA of 40W instead 15W

  See 2.3.4.3. ES3 – Engineering sample 3

- External PA (40W) with shielding is too big to fit on 80x100 – medium

  Impact: Size extension 120 x 90mm

  No risk any more: Size kept to 80x100mm

- Antenna configuration needs module PCB change – medium

  Impact – more time for PCB design and production, new sample run

  Slip 4 weeks

  Resolution cw39

  No risk any more. Module PCB design finalized. No slip expected.

- QCX315 firmware not or partly not backwards compatible – medium

  Impact: More effort on the software development for merge or changes on the TOBA side

  Slip > 4 weeks

  Resolution CW46 or 2 weeks after Qualcomm’s first software delivery

  Still a risk @ CW43. n39 patch still not delivered. Issue escalated to Qualcomm.

- Delivered PA for external booster doesn't meet specification – low

  Slip >4 weeks, Mitigation: Use trustful supplier; Test of delivered samples in a test bed cw45

  No risk any more. 100 pcs delivered. One sample successfully tested. Parameters confirmed.

- 8dB output power offset disturbs and has side effects – low

  Slip >4 weeks, Mitigation: Consortium already informed months ago

  Still a risk. Proposal for the power loop ready for review

- Missing 5QI based QoS prevents use cases - low

  Slip >12 weeks, Mitigation: Consortium already informed months ago

  Still a risk. Several possibilities in evaluation.

4.9 Schedule

- Expected deliveries February and during March upon readiness

  Slip to original schedule -> 3 months

  Slip still available. No chance to pull back due to schedule slip in summer time frame.

- Higher development efforts
  - 3rd party NRE
  - Hardware changes expected
  - Additional prototyping run needed
  - Software efforts are expected

  The magnitude of the higher costs are subject to separate presentation.

5 FRMCS GATEWAY SERVICES IN THE SYSTEM VIEW

This chapter is a sub-part of the “TOBA Architecture report” prepared by WP2. Its objective is to describe the architecture, functions and interfaces of the two following FRMCS gateways:

- FRMCS On-Board gateway (FRMCS OB_GTW)
- FRMCS Trackside gateway (FRMCS TS_GTW)

Besides, it defines the corresponding prototypes deliverables for the execution of WP2.

The content of this document is based on input documents from UIC (at this stage: UIC FU-7100, UIC TOBA-7510 and MG-7904) and also on technical assumptions discussed within WP2 to complete the existing input documentation.

Reminder: In WP2 scope, two sets of FRMCS Gateways will be delivered:

- Kontron prototypes: FRMCS OB_GTW-K and FRMCS TS_GTW-K
- Alstom prototypes: FRMCS OB_GTW-A and FRMCS TS_GTW-A

These prototype deliveries will also include the O&M part described (at least one O&M client connected to the OB GTW) in the document. The RF combining & switching is also described even if not part of WP2 supplying.

5.1 FRMCS Gateway services – principles overview

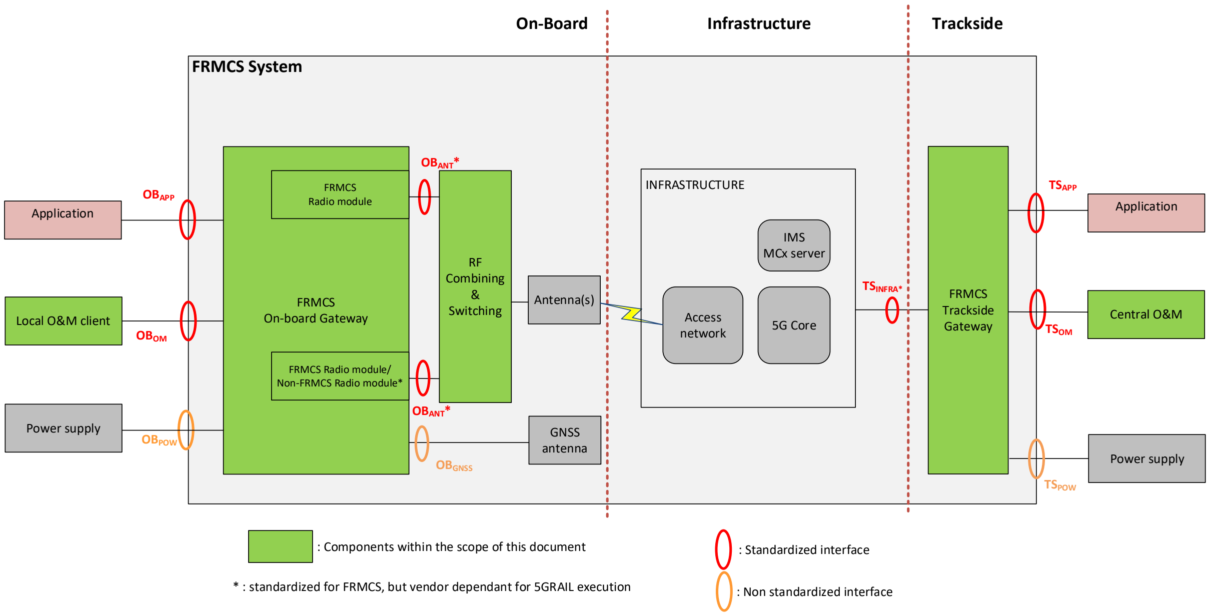


Figure 27: FRMCS Gateway services – Principles overview

The on-board part is the “FRMCS On-Board gateway”, which contains also FRMCS radio modems or non-FRMCS radio modems (such as Wi-Fi modem). It manages the interface with on-board applications on train side, and with radio networks on the other side. Besides, this document also describes two “on-board” components which are not part of OB_GTW but are in the WP2 scope: the O&M on-board client and the RF combining and switching function. These components are described in chapters **5.4.1** and **5.4.2**.

The trackside part is the “FRMCS Trackside Gateway” which manages the interface with the IMS/MCx server and the data network on one side, and with the trackside applications on the other side. Besides, this document also describes a “trackside” component which is not part of TS_GTW but is included in the WP2 scope: an O&M server which receives O&M data related to the FRMCS OB_GTW of the managed trains and O&M data related to the TS_GTW. This component is described in chapter **5.4.1.**

5.2 FRMCS On Board gateway

5.2.1 Architecture of OB_GTW

Proposal overview:

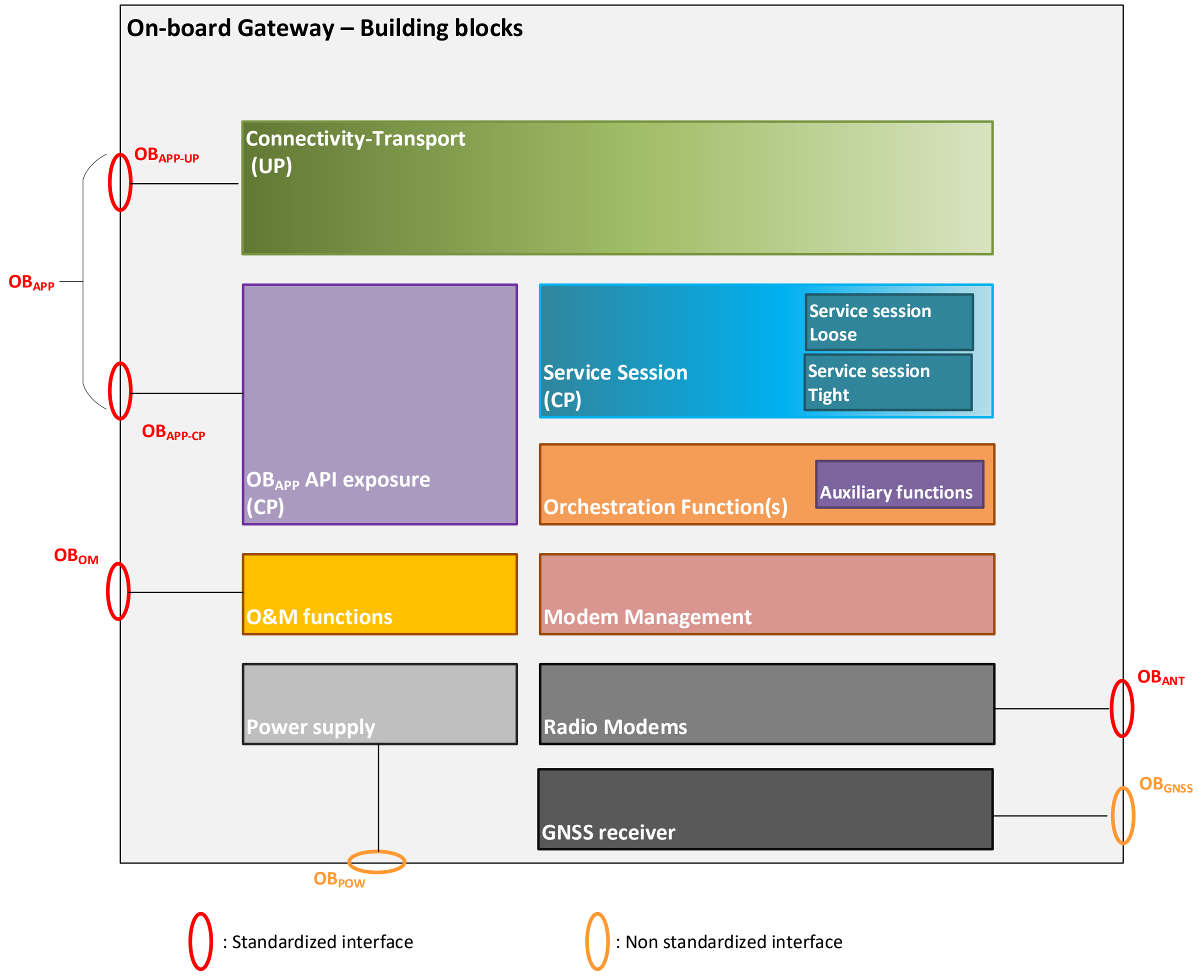


Figure 28: FRMCS on board gateway – Building blocks

Note: in this scheme, OB_{APP} interface is divided into 2 sub-interfaces. The details about these 2 sub-interfaces and the mapping regarding the coupling mode of the application are given in chapter **5.2.3.1**.

5.2.1.1 Connectivity Transport

"Connectivity Transport" building block consists in an IP interface presented to the on-board applications (IP gateway for the on-board applications to send data to trackside). This component is responsible for routing user plane data between on-board network and trackside network, using the available radio modems and through the established bearers.

It is a software/hardware component (considering the physical interface).

5.2.1.2 Service session

"Service session" building block is separated into two distinct parts:

- "Service session – Loose" is responsible for managing session for Loose-coupled applications (session establishment, session identification, …). This block contains also the MCx clients which can be used for Loose-coupled application which requires critical communication attributes.
- "Service session – Tight" is responsible for controlling session for tight-coupled applications. For tight coupling, the MCx client is embedded on the application side and the application is able to manage its own session, but the OB GTW must be aware of the session established by tight-coupled application.

It is a software component.

5.2.1.3 OB$_{APP}$ exposure

"OB$_{APP}$ exposure" building block is responsible for presenting to the application the necessary functions to interact with the OB_GTW to manage the control plane. This building block is mainly described in chapter 6.

It is a software/hardware component (considering the physical interface).

5.2.1.4 Orchestration function

"Orchestration function" building block oversees several functions:

- Control and monitor the relation between user plane and control plane (i.e. the established session)
- Ensure the correct communication attributes (QoS)
- Embed some "Auxiliary functions" required by some applications to OB_GTW, such as:
  - Link supervision: monitor and deliver to OB$_{APP}$ the quality/status of each link used by the established sessions
  - Positioning service: obtain the train localization from a GNSS receiver and provide it to the applications (this last functionality will not be implemented for 5GRAIL)

It is a software component.

Note: there is no external interface dedicated to orchestration/auxiliary function for the applications which needs these functions. The corresponding exchange will use OB$_{APP}$ interface. Hence, auxiliary function has an internal interface with OB$_{APP}$ exposure building block.

5.2.1.5 O&M functions

"O&M functions" building block is responsible for hosting the O&M functions:

- Providing information about events encountered by OB_GTW hardware and software components (supervision, monitoring, statistics, performance, …)
- Receiving instructions related to the operation of the system (configuration, software upgrade, …)

- Expose an interface to send/receive these data to/from a local O&M system.
- Expose an interface to send/receive these data to/from a central O&M system.

It is a software/hardware component (considering the physical interface).

5.2.1.6 Modem management

“Modem management” building block is responsible for managing the available radio modems, and interfacing radio modems with “connectivity transport” (for user plane) and “session management” (for control plane).

It is a software/hardware component (physical interface with the modems), assimilated with OBrad in the FRMCS TOBA FRS.

5.2.1.7 Radio modems

“Radio modems” building block is the set of available radio modems which can be used in OB_GTW.

It is a hardware component.

Modems for OB_GTW-A:

- Number of modems : up to 4 modems :
    - One or two 5G modem: Thales modem ES-n (based on COTS MV31-W); two modems are used for border-crossing test case, see 5.2.2.4.14
    - 4G modem: Quectel EC25
    - one Wi-Fi modem
- Possible interfaces for modems:
    - M.2 USB 3.0
    - USB3.0 on the front panel
- SIM card slot: up to 3 internal mini-SIM slots

Modems for OB_GTW-K:

- Number of internal modems: up to 4 internal modems
    - One or two Thales modem ES-n (based on COTS MV31-W)
    - One 4G modem
    - One Wi-Fi Modem
    - [one slot with n78 3.7 GHz for DB => Clarifications awaited]
- Internal interface for modems: mPCIe or/and USB 3
- SIM card slot: TBC

5.2.1.8 Power supply

“Power supply” building block is responsible for distributing power supply to the full OB_GTW. The implementation is different between Alstom and Kontron prototypes.

It is a hardware component.

Power supply for OB_GTW-A

- Input power: 24-110V DC
- Nominal consumption: 15-30W
- Physical connector: M12 code A male 4pins

Power supply for OB_GTW-K

- Input power: 24-110V DC (2.7 – 0.6 A)
- Nominal consumption (without modem part): ~15 W
- Physical connector: M12 male, 4 pins

5.2.1.9 GNSS receiver

There is one GNSS receiver embedded in FRMCS OB GTW. It acquires GNSS signal from GNSS antenna and distributes positioning and time information to the auxiliary function.

It is a hardware component.

Note: it is also possible to use the GNSS capabilities embedded in a 4G/5G modem. The choice between these two solutions (use GNSS capabilities embedded in the 4G/5G modem or use a dedicated GNSS receiver) is open to implementation.

For OB_GTW-A, a dedicated GNSS receiver will be used.

For OB_GTW-K, a dedicated GNSS receiver will be used

5.2.2 Functionalities

5.2.2.1 List of functions:

The list of functions related to FRMCS OB_GTW is extracted from chapter 1.4:

- OBGTW_F1: Provide transport services for on-board applications
    - OBGTW_F1.1: Expose an OB$_{APP}$ API to the applications for decoupling application and transport
    - OBGTW_F1.2: Multipath/BearerFlex
    - OBGTW_F1.3: Session management for loose-coupled applications
    - OBGTW_F1.4: Provide to the application the required communication attributes
    - OBGTW_F1.5: Local Binding

  - OBGTW_F1.6: Transport user plane data toward trackside
  - OBGTW_F1.7: Expose session supervision information to the applications which request it
  - OBGTW_F1.8: Session proxying for tight-coupled applications
- OBGTW_F2: Support multiple modems and radio technologies
- OBGTW_F3: *deleted*
- OBGTW_F4: Authenticate/authorize access to the FRMCS service level.
- OBGTW_F5: Ensure O&M functions:
  - OBGTW_F5.1: Fault management
  - OBGTW_F5.2: Performance & supervision management
  - OBGTW_F5.3: Configuration management
  - OBGTW_F5.4: Users or groups account/profile
  - OBGTW_F5.5: Expose O&M interface for local client
  - OBGTW_F5.6: Expose O&M interface for remote server
- OBGTW_F6: Support roaming capabilities
- OBGTW_F7: Positioning/Synchronization
  - OBGTW_F7.1: Obtain positioning and time information
  - OBGTW_F7.2: Provide positioning information to the applications (not implemented for 5GRAIL).

5.2.2.2 Traceability for each function

	TRACEABILITY	
FUNCTIONS	SOURCE FROM REQUIREMENTS	IMPLEMENTATION IN WP2 DOCUMENTS
OBGTW_F1.1: Provide transport services - Expose an OBAPP API to the applications for decoupling application and transport	Derived function from use case table (see 1.4.1	Chap. 5.2.2.4.1
OBGTW_F1.2: Provide transport services - Multipath (bearer flexibility, resilience, aggregation)	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.2
OBGTW_F1.3: Provide transport services - Session management for loose-coupled applications	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.3
OBGTW_F1.4: Provide transport services - Provide to the application the required communication attributes	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.4
OBGTW_F1.5: Provide transport services - Local binding	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.5
OBGTW_F1.6: Transport user plane data toward trackside	UIC TOBA FRS (TOBA-7510) Chap. 4.2.2	Chap. 5.2.2.4.6
OBGTW_F1.7: Expose session supervision to the application which request it	Derived function from use case table (see 1.4.1)	Chap. 05.2.2.4.7
OBGTW_F1.8: Session proxying for tight-coupled applications	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.8

OBGTW_F2: Support multiple modems and radio technologies	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.9
OBGTW_F4: Authenticate/authorize access to the FRMCS service level.	UIC MG-7904 Chap. 3.3.3	Chap. 5.2.2.4.10
OBGTW_F5.1: Ensure O&M functions - Fault management	UIC TOBA FRS (TOBA-7510) Chap. 7.6.4	Chap. 5.2.2.4.11
OBGTW_F5.2: Ensure O&M functions - Performance & supervision management	UIC TOBA FRS (TOBA-7510) Chaps. 7.6.2; 7.6.3; 7.6.6	Chap. 5.2.2.4.11
OBGTW_F5.3: Ensure O&M functions - Configuration management	UIC TOBA FRS (TOBA-7510) Chap. 7.6.5	Chap. 5.2.2.4.11
OBGTW_F5.4: Ensure O&M functions - Users or groups account/profile	UIC TOBA FRS (TOBA-7510) Chap. 7.8.2	Chap. 5.2.2.4.11
OBGTW_F5.5: Ensure O&M functions - Expose O&M interface for local client	UIC TOBA FRS (TOBA-7510) Chap. 7.8.2	Chap. 5.2.2.4.12
OBGTW_F5.6: Ensure O&M functions - Expose O&M interface for remote server	UIC TOBA FRS (TOBA-7510) Chap. 7.8.2	Chap. 5.2.2.4.13
OBGTW_F6: Support border-crossing capabilities	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.14
OBGTW_F7.1: Obtain positioning and time information	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.15
OBGTW_F7.2: Provide positioning information to the applications	Derived function from use case table (see 1.4.1)	Chap. 5.2.2.4.16

5.2.2.3 Allocation to building blocks

The table below presents the allocation of these functions to the building blocks described in chapter **5.2.1**.

Table 22: Allocation to building blocks

FUNCTIONS	ALLOCATED BUILDING BLOCK
OBGTW_F1.1 Expose an OB$_{APP}$ API to the applications for decoupling application and transport	OB$_{APP}$ exposure
OBGTW_F1.2 Multipath/BearerFlex	Connectivity Transport
OBGTW_F1.3 Session management for loose-coupled applications	Service session - Loose
OBGTW_F1.4 Provide to the application the required communication attributes	Orchestration function
OBGTW_F1.5: Local Binding	OB$_{APP}$ exposure
OBGTW_F1.6: Transport user plane data toward trackside	Connectivity Transport

OBGTW_F1.7: Expose session supervision to the applications which request it	Orchestration function
OBGTW_F1.8: Session proxying for tight-coupled applications	Service session - Tight
OBGTW_F2 Support multiple modems and radio technologies	Modem Management
OBGTW_F3 Connect to multiple radio networks	Radio Modems
OBGTW_F4 Authenticate/authorize access to the FRMCS service level.	Service session - Loose
OBGTW_F5.1 O&M functions- Fault management	O&M functions
OBGTW_F5.2 O&M functions- Performance & Supervision management	O&M functions
OBGTW_F5.3 O&M functions- Configuration management	O&M functions
OBGTW_F5.4 O&M functions- Users or groups account profile	O&M functions
OBGTW_F5.5 O&M functions- Expose O&M interface for local client	O&M functions
OBGTW_F5.6 O&M functions- Expose O&M interface for remote server	O&M functions
OBGTW_F6: Support border-crossing capabilities	Connectivity Transport
OBGTW_F7.1: Obtain positioning and time information	GNSS Receiver
OBGTW_F7.2: Provide positioning information to the applications	This function will not be implemented for 5GRAIL.

5.2.2.4 Details of functions

This chapter aims at explaining how OB_GTW will execute these functions.

5.2.2.4.1 F1.1: PROVIDE TRANSPORT SERVICES - EXPOSE AN OB$_{APP}$ API TO THE APPLICATIONS FOR DECOUPLING APPLICATION AND TRANSPORT

The OB_GTW embeds an OB$_{APP}$ API exposed to the application. All details about this API are in chapter 6.

5.2.2.4.2 F1.2: PROVIDE TRANSPORT SERVICES – MULTICONNECTIVITY/BEARERFLEX

The aim of this function is to provide multiconnectivity for user plane data between on-board and trackside.

For 5GRAIL execution, the BearerFlex function will not be standardized, and the solution will be vendor dependent.

Kontron implementation:

As shown in figure below, the BearerFlex function in Kontron solution is based on multi connectivity entities in OB_GTW and TS_GTW.

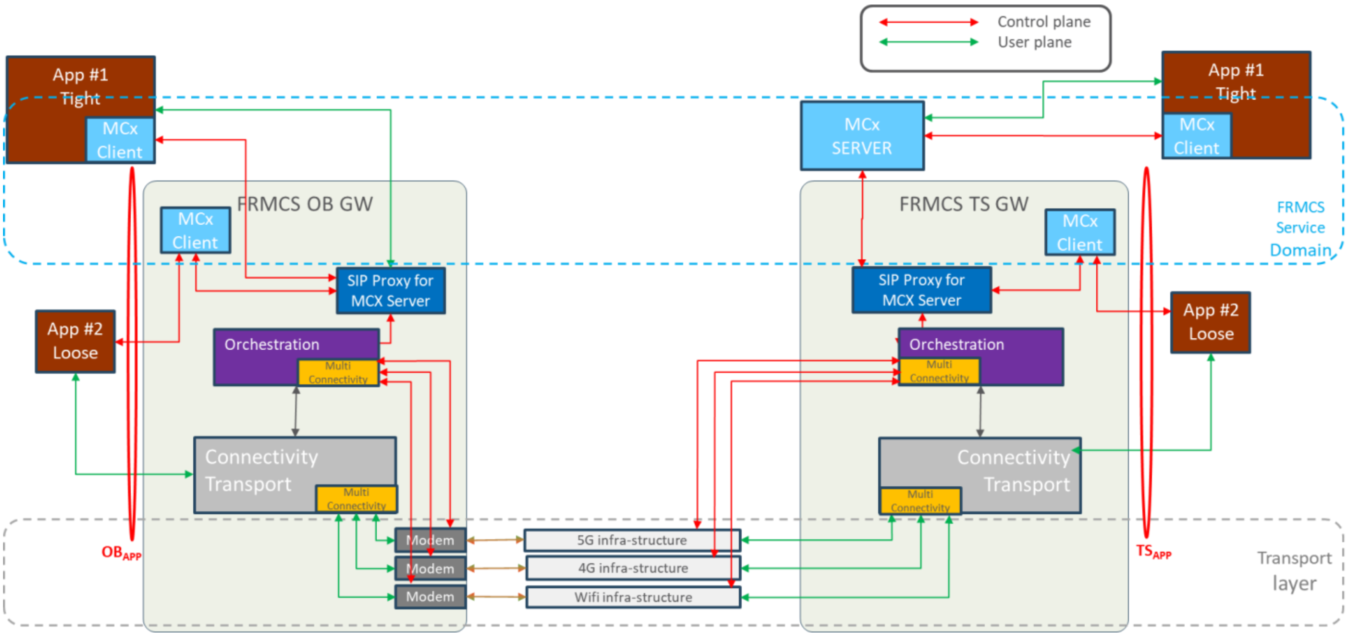


Figure 29: Kontron Multiconnectivity function

Those OB multi connectivity entities will manage the different radio bearers with their TS counterparts transparently for the applications.

On transport layer, the solution will be based on MPTCP as shown in the below figure.

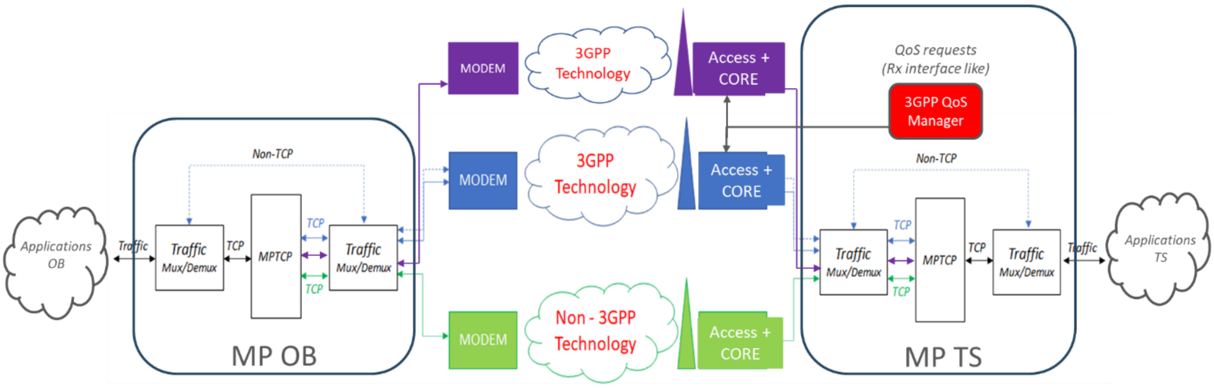


Figure 30: Kontron Multiconnectivity based on MPTCP

To make it transparent for the Service Layer, there will be an overlay with Tunnel mngt and local IP routing that will be reconfigured in case of bearer failure.

The remaining open points are:

- QoS propagation on all 3GPP Technology considered by MPTCP
- Application feedback if mapped on Non-3GPP (no QoS)

The open points are to be considered out of 5GRAIL and the QoS will be statically configured in 5GRAIL.

Alstom implementation:

In a first implementation, the multiconnectivity feature is achieved in a transparent way for Loose-coupled applications with a BearerFlex function embedded in OB_GTW-A and TS_GTW-A. Following one session establishment requested by an application, several MCData-IPconn session (i.e. GRE tunnel for the user plane) would be established in parallel and managed by the OB_GTW/TS_GTW BearerFlex functions.

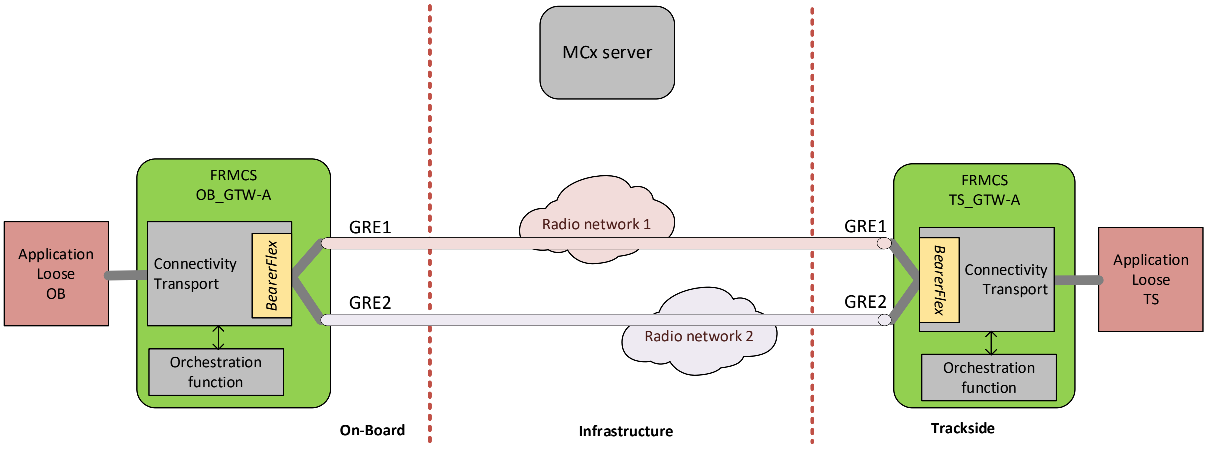


Figure 31: Alstom multiconnectivity - User Plane

Then, the User Plane will benefit from multiconnectivity. Several solutions are still under evaluation for the protocol behind the BearerFlex function.

For MCx Signalling Plane, the multiconnectivity feature will or will not be achieved depending on the capabilities of the MCx server to expose different databases for each radio network.

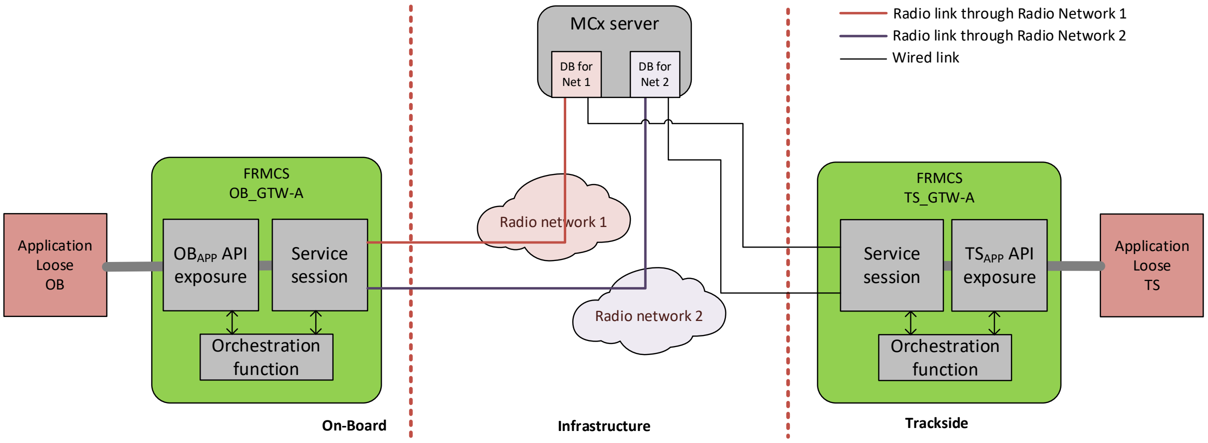


Figure 32: Alstom multiconnectivity - MCx signalling plane – possible implementation

Concerning tight-coupling, there is no multiconnectivity mechanism fully transparent for the application in OB_GTW-A and TS_GTW-A. A non-transparent mechanism could be proposed but will not be tested in 5GRAIL context since tight applications are not foreseen for WP4 lab tests (only lab tests to use OB_GTW-A and TS_GTW-A).

5.2.2.4.3 F1.3: PROVIDE TRANSPORT SERVICES - SESSION MANAGEMENT FOR LOOSE-COUPLED APPLICATIONS

This function is realized through MCx clients embedded in the OB_GTW.

When a loose-coupled application requests to establish a session to a trackside equipment through OB$_{APP}$ API, then the MCx client is responsible for opening a MCData-IP connectivity session with the relevant MCx client in TS_GTW.

The session establishment mechanism for a loose-coupled application is based on MCdata ID of the MCData client embedded in the OB_GTW. The basic use case of an applications registering and requesting a session establishment toward TS application is given in **Appendix 2 - End to end dataflows**.

Alstom view: there is also a possibility to manage “non-MCx session” for loose application, which is for non-critical ones such as Train Maintenance. In this case, there is no MCx client in OB_GTW for the ongoing session. It can be viewed as a deviation from the standards in which only MCx approach is targeted.

There are two important mechanisms which are managed by this function and detailed below:

- How the OB_GTW translates the ID provided by the application (in REGISTER or SESSION_START functions, see chapters **6.2.5.4.1** and **6.2.5.4.3**) into MCx ID
- How the OB_GTW provides the destination IP address to be used for UP data sent by the application.

Translation of application name into MCx ID:

- **Assumptions**:
    - Application name is recovered from OB/TSapp register with the parameter “originator_id”
    - Each application instance has a unique originator_id
    - Each MC DATA user must be provisioned in advance in MCX server
    - There will be 1 MC DATA user per loose coupled application instance
- **Translation rules:**
    - A standardized rule will be defined to associate originator_id and MC DATA user. This rule is used following REGISTER request (originator_id transmitted during REGISTER request)
    - A standardized rule will be defined to translate dest_id to MC DATA user to be contacted. This rule is used following SESSION_START request. Contrary to originator-id to be considered, the list of dest_id cannot be known in advance by the OB GTW.
- **Each OB and TS GTW will be provisioned with a table with two columns**:
    - 1st column : the list of originator_id for the local loose coupled applications that need to be supported for local binding
    - 2nd column; the list of the corresponding MC DATA users ID

Following discussions with WP3 and WP4, a table with the needed MCx clients was realized and is given in **Appendix 7 – ID to be used in WP3 and WP4**.

Provision of destination IP address for User Plane:

The proposed principle for a session initiated by on-board to trackside is the following:

- On-board: The OB_GTW has a pool of “virtual session IP addresses”. Following a SESSION_START request, the OB_GTW distributes one of these virtual addresses to the application. This will be linked to the established session (GRE tunnel if using MCData). The OB_GTW uses this IP address to filter and redirects UP data to the relevant tunnel.
- Trackside: The TS_GTW has a pool of “virtual session IP addresses”. Following an incoming session request, the TS_GTW uses one of these virtual addresses (as source IP address) to forward the future message to the concerned application. This will be linked to the established session (GRE tunnel if using MCData). The TS_GTW uses this IP address to filter and redirects UP data to the relevant tunnel.

NAT is performed on the side that did not “initiate” the session (e.g. TS_GTW for ETCS application).

For a session initiated by trackside to on-board, we only have to invert OB_GTW and TS_GTW in the previous explanations.

This solution using virtual session IP addresses allows to expand on the host2host addressing to have a full session establishment mechanism for Loose-coupled application through MCData.

An example of a session establishment from on-board to trackside with this approach is presented in **Appendix 6 – Example to illustrate the virtual session IP address**.

5.2.2.4.4 F1.4: PROVIDE TRANSPORT SERVICES - PROVIDE TO THE APPLICATION THE REQUIRED COMMUNICATION ATTRIBUTES

When requesting for a session establishment, a loose-coupled application asks for a needed communication attribute (see OB$_{APP}$ API definition). This function consists in ensuring that the relevant QoS parameter will be achieved on the radio link(s) to satisfy these requested communication attributes.

The communication attributes requested by the application must not be linked to 5QI (it would not be compliant with the decoupling between application and transport). It is proposed that the application requests for a “comm_profile” and a specific QoS treatment is applied by the infrastructure for each comm_profile.

For the first 5GRAIL implementation, it is not expected to have a dynamic QoS mechanism in the core Network (e.g. a MCx server which requests some communication attributes to the PCF, which would trigger dedicated QoS flows establishment in the network for the considered session). The QoS will be statically managed in the core network (please refer to WP3 and WP4 documents for more details). The network will be able to differentiate the flows for which a dedicated QoS flows must be used thanks to the DSCP value. Then, the OB_GTW is responsible for applying the relevant DSCP value in the UP data transmitted toward the network. For Loose-coupled application, the DSCP value will be inserted in the IP layer carrying the GRE tunnel (MCData-IPconn session). For tight applications, the DSCP value will be directly inserted in the UP data by the application itself.

A translation table between comm_profile and corresponding DSCP values is given in **Appendix 1 – Communication attributes to QoS**.

Note1: the QoS parameters for each comm_profile/DSCP value depends on infrastructure

Note 2: At this stage of the implementation, QoS is only managed for FRMCS modems (not for 4G, Wi-Fi, etc.); the framework for Quality of Service within the FRMCS System is used. Refer to assumption #49.

5.2.2.4.5 F1.5: PROVIDE TRANSPORT SERVICES - LOCAL BINDING

The local binding function covers a local identification, authentication and authorization of an on-board application. A specific function of OB$_{APP}$ API is dedicated to local binding: function FRMCS_GTW_REGISTER. The authentication part is based on TLS protocol used for WebSocket exchanges between application and OB_GTW. Authentication between client and server should use certificate exchange (it covers authentication need). Hence, as soon as an application opens a WebSocket with OB_GTW, it means that it is authenticated.

Finally, the local binding of an on-board application is divided into two steps:

- Establish a TLS connection with the OB_GTW, using mutual authentication (mTLS). During the TLS handshake, client (application) and server (OB_GTW) send their certificate and authenticate themselves.
- Open a websocket connection (over the previous TLS layer) and perform the FRMCS_GTW_REGISTER function (see chapter **6.2.5.4.1**). As a result, the application retrieve a unique ID, named app_uuid, which is to be used for every further request in OB$_{APP}$ API.

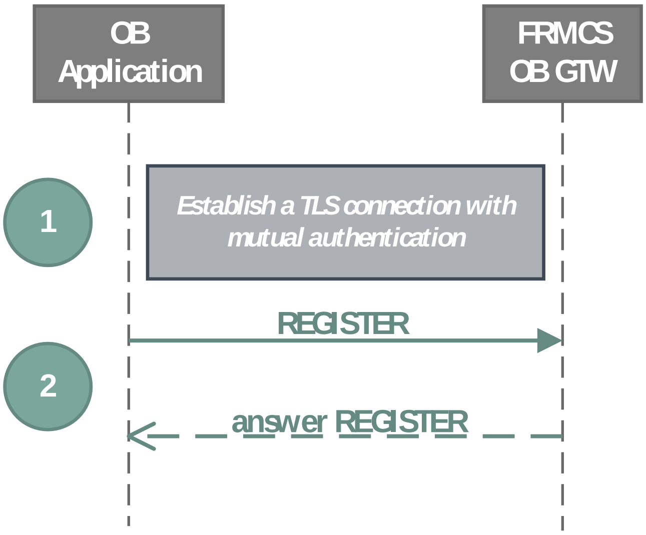


Figure 33: 2 steps in local binding

For 5GRAIL implementation, a PKI offline solution is used. This PKI embeds a CA which generates and provides signed certificated to clients (applications) and servers (OB_GTW-A and OB_GTW-K). More details about PKI and certificate management which is planned for 5GRAIL local binding are given in 9.7.

Note 1: The authentication is optional in WebSocket exchange and will be avoided for a first step of implementation.

Note 2: Local binding covers authentication for loose-coupled and tight-coupled application, which uses OB$_{APP}$ API. For flat-IP mode (used for phasing needs), a static authentication needs to be done (e.g. based on IP or MAC address).

5.2.2.4.6 F1.6: PROVIDE TRANSPORT SERVICES -TRANSPORT USER PLANE DATA TOWARD TRACKSIDE

The OB GTW shall expose to the application an IP interface with an IP gateway address that can be used by the application to send data to trackside.

The aim of this function is to redirect user plane data (IP flows) to the relevant bearer established within control plane.

The way to perform this function is open to implementation.

For OB_GTW-A, basically, the function F1.6 uses IP routing table to manage properly the user plane data flow to the correct tunnel (i.e. GRE tunnel if using MCData-IPconn). Control plane will result in modifying dynamically the IP routing rules of OB GTW and TS GTW to manage correctly the user plane.

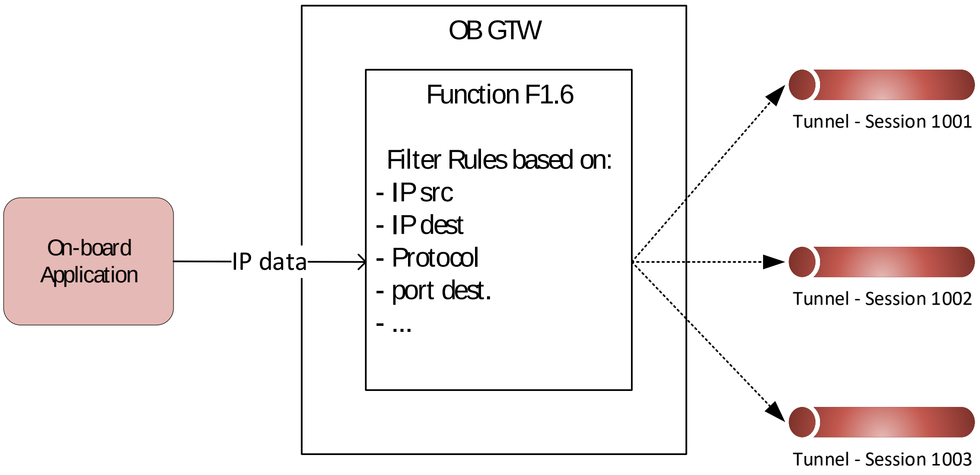


Figure 34: User plane management

For a session between on-board and trackside in case of a Loose-coupled application, the UP data will go through a **direct** GRE tunnel (between OB_GTW and TS_GTW) resulting from an MCdata-IPconn request. It is an MCData-IPconn implementation choice made for 5GRAIL. Hence, a requirement is that the TS_GTW must be able to reach the OB_GTW with the OB_GTW IP address. Indeed, the OB_GTW will insert its own IP address in the SIP INVITE message (in the SDP content) and the TS_GTW will use this IP address to mount its part of the underlying GRE tunnel. This requirement must be taken into account in WP3, 4, 5.

Important note: if the OB_GTW is not reachable with its own IP address, host to host GRE tunnel between OB_GTW and TS_GTW will not be available. In this solution a workaround solution must be found. This is an important constraint exported to WP 3, 4 and 5, strongly linked with the “host to host MCdata-IPconn” session.

5.2.2.4.7 F1.7: EXPOSE SESSION SUPERVISION TO THE APPLICATIONS WHICH REQUEST IT

For each established session, the OB GTW shall know :

- Which link is used,
- What is the status of each of these links,
- What are the communication attributes requested by the application,
- What is the current QoS available for this session.

This corresponds partly to the role of Auxiliary function.

Then, the corresponding status is sent to the function “F1.1 Expose an OB$_{APP}$ API” which is responsible for transmitting the relevant information to the application.

The content of the session status information sent to the application can be get by two ways:

- “session_status” field in the answer of SESSION_STATUS request. See chapter **6.2.4.4.5**
- "session_status”field in the SESSION_STATUS_CHANGED notification. See chapter **6.2.4.4.8**

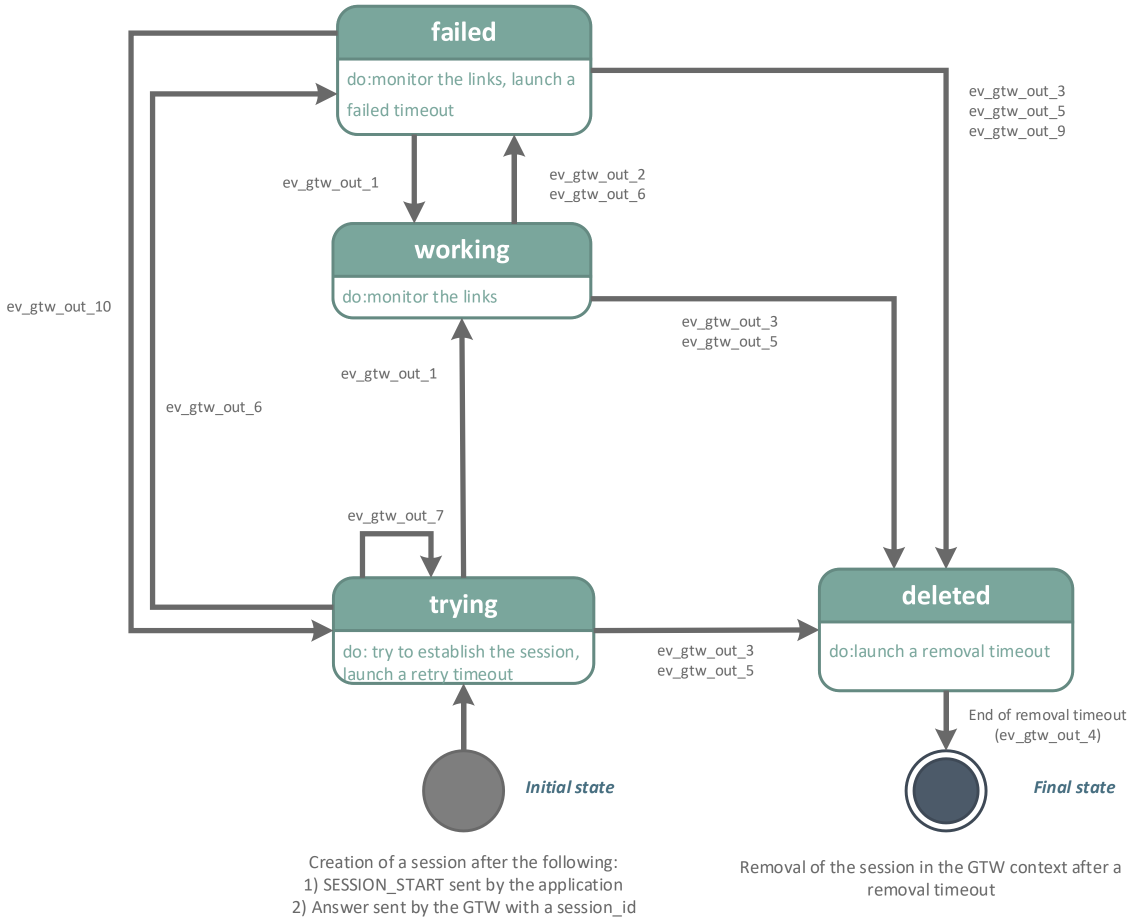
The status value is one of the 4 following states:

- “Trying”: when the OB_GTW is trying to establish the requested session, for example just after receiving a SESSION_START request.
- “Working”: once the session is established and at least one radio link is available (and satisfies the communication attributes requested by the application) for this session.
- “Failed”: the session is established but all the radio link used are failed, or do not guarantee the required QoS to satisfy the communication attributes requested by the application. The “failed” status must come with a “detail” content, containing the rationale of this state (examples: “no radio link available”; “radio link available but the communication profile cannot be satisfied”,…)
- “Deleted”: the session is deleted, for example after receiving a SESSION_END request from the application (on-board or trackside).

Each transition must be notified to the application through a SESSION_STATUS_CHANGED notification. See chapter **6.2.4.4.8**.

The state diagram of a session depends on the originator of the session. From the OB_GTW point of view, an outgoing session is a session initiated by an on-board application in the same train. An incoming session is a session initiated by an application outside the train (a trackside application, or in another train).

The state diagram for an outgoing session is the following:


failed
do:monitor the links, launch a failed timeout
working
do:monitor the links
trying
do: try to establish the session, launch a retry timeout
deleted
do:launch a removal timeout
ev_gtw_out_1
ev_gtw_out_2
ev_gtw_out_6
ev_gtw_out_3
ev_gtw_out_5
ev_gtw_out_9
ev_gtw_out_10
ev_gtw_out_6
ev_gtw_out_1
ev_gtw_out_3
ev_gtw_out_5
ev_gtw_out_7
ev_gtw_out_3
ev_gtw_out_5
End of removal timeout
(ev_gtw_out_4)
Initial state
Final state
Creation of a session after the following:
1) SESSION_START sent by the application
2) Answer sent by the GTW with a session_id
Removal of the session in the GTW context after a removal timeout

Note: the event "ev_gtw_out_8" triggers the immediate removal of the session context.

Figure 35: Session state diagram – outgoing session

The list of events used in this state diagram is the following :

Event ID	Description
ev_gtw_out_1	Monitoring signal becomes OK on one GRE tunnel used for this session
ev_gtw_out_2	Monitoring signal becomes NOK on the last GRE tunnel available for this session
ev_gtw_out_3	Request “frmcs_gtw_app_session_end” received from the local application AND the request is accepted by the OB_GTW/TS_GTW
ev_gtw_out_4	End of removal_timeout for this session
ev_gtw_out_5	Reception of a message from one service server requesting to delete the session (e.g. SIP BYE)
ev_gtw_out_6	Reception of a message from one service server saying that the session establishment has failed (e.g. SIP 4xx, 5xx or 6xx answer)
ev_gtw_out_7	End of session_retry_interval timeout
ev_gtw_out_8	Loss of the local WebSocket connection with the application OR deregistration of the local application
ev_gtw_out_9	End of failed_session timeout
ev_gtw_out_10	Recovery of one link which can be used for the application initiating the session.

These events are internal to the OB_GTW/TS_GTW, they are not to be known by the application and the application are not informed about the event which triggered the change of state. A monitoring mechanism is needed for each GRE tunnel.

Few timeouts are to be defined in the OB_GTW/TS_GTW

- removal_timeout : start when the session becomes « deleted ». If needed, the GTW may keep a deleted session in its memory to manage delayed request from the network.
- session_retry_interval : start when the session becomes « trying ». after this timeout, the GTW will try to transmit again the session establishment request (e.g. SIP INVITE).
- failed_session_timeout : start when the session becomes « failed ». To avoid that a session stays indefinitely in « failed » status (e.g. because the application forgets to delete it or do not have properly configure a timeout from their side), the session shall become "deleted" after this timeout.

The state diagram for an incoming session is the following:

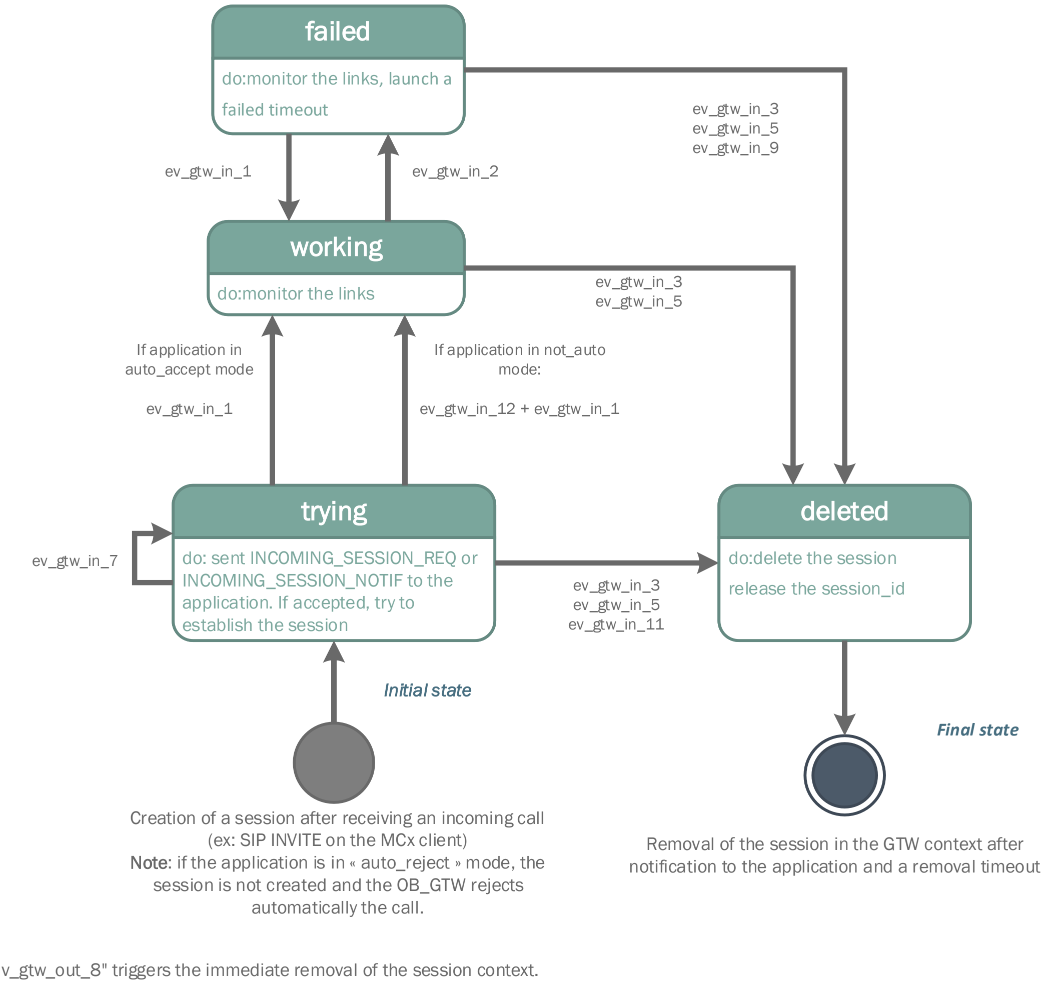

failed
do:monitor the links, launch a failed timeout
ev_gtw_in_1
ev_gtw_in_2
ev_gtw_in_3
ev_gtw_in_5
ev_gtw_in_9
working
do:monitor the links
ev_gtw_in_3
ev_gtw_in_5
If application in auto_accept mode
ev_gtw_in_1
If application in not_auto mode:
ev_gtw_in_12 + ev_gtw_in_1
trying
do: sent INCOMING_SESSION_REQ or INCOMING_SESSION_NOTIF to the application. If accepted, try to establish the session
ev_gtw_in_7
deleted
do:delete the session
release the session_id
ev_gtw_in_3
ev_gtw_in_5
ev_gtw_in_11
Initial state
Final state
Creation of a session after receiving an incoming call (ex: SIP INVITE on the MCx client)
Note: if the application is in « auto_reject » mode, the session is not created and the OB_GTW rejects automatically the call.
Removal of the session in the GTW context after notification to the application and a removal timeout
Note: the event "ev_gtw_out_8" triggers the immediate removal of the session context.

Figure 36: Session state diagram - Incoming session

The list of events used in this state diagram is the following:

Event ID	Description
ev_gtw_in_1	Monitoring signal becomes OK on a GRE tunnel for this session
ev_gtw_in_2	Monitoring signal becomes NOK on the last GRE tunnel available for this session
ev_gtw_in_3	Request “frmcs_gtw_app_session_end” received from the local application AND the request is accepted by the OB_GTW/TS_GTW
ev_gtw_in_4	End of removal_timeout for this session
ev_gtw_in_5	Reception of a message from one service server requesting to delete the session (e.g. SIP BYE)
ev_gtw_in_6	*deleted*
ev_gtw_in_7	End of session_retry_interval timeout
ev_gtw_in_8	Loss of the local WebSocket connection with the application or deregistration of the local application
ev_gtw_in_9	End of failed_session timeout
ev_gtw_in_10	*deleted*

ev_gtw_in_11	Answer from the application to the frmcs_app_incoming_session_req : call rejected
ev_gtw_in_12	Answer from the application to the frmcs_app_incoming_session_req : call accepted

Timeout definitions were given in the previous chapter for outgoing sessions.

Note: the termination of a session is always triggered by the application (SESSION_END). Thus, if a session is in “Failed” state due to inadequate quality of service provided by the network, the application will be able to continue the session anyway and try to send application data through the available link(s).

Once an application has requested a session establishment and has received a session_uuid from the OB_GTW (see function SESSION_START in OB$_{APP}$ API), it automatically subscribes to the notification for any session change.

5.2.2.4.8 F1.8: SESSION PROXYING FOR TIGHT COUPLED APPLICATION

The proxying function for the tight coupled application is needed to allow the BearerFlex function of the FRMCS OB/TS GTW.

This function allows also to keep the application and the transport strata independent.

Indeed, all the data exchanged between on-board and trackside applications should go through the FRMCS OB GTW and the FRMCS TS GTW to allow the GTW to be able to manage a change at transport level without impacting the applications.

This function is in charge of forwarding the control and the data planes of the tight coupled applications. It is also in charge of forwarding the control plane of the loose coupled applications (for OB_GTW-K only, see chapter **5.2.2.4.2**).

This proxying function is transparent for the applications.

The proxying function is based on a SIP Proxy (as defined in RFC 3261). This proxy is implemented as a stateless proxy.

This proxying function could also be used, in future version, to retrieve at least QoS information and to allow the orchestration part of the GTW to handle the different UP accordingly.

5.2.2.4.9 F2: SUPPORT MULTIPLE MODEMS AND RADIO TECHNOLOGIES

The OB GTW shall support multiple modem:

- At least one FRMCS modem
- At least one non-FRMCS modem (4G modem, Wi-Fi modem, …)

The OB GTW contains several interfaces with these modems. These interfaces, named OB$_{RAD}$, are internal to OB GTW, hence are not described in this document.

5.2.2.4.10 F4: AUTHENTICATE/AUTHORIZE ACCESS TO THE FRMCS SERVICE LEVEL

The aim of this function is to enable the access to the IMS/MCx server.

For loose-coupled applications, the corresponding MCData client embedded in the OB GTW must perform:

- MCX user authentication.
- SIP Registration and Authentication.
- MCX Service Authorization.

These 3 steps are performed following 3GPP TS 33.180 (version 16.5.0, chapter 5.1.1). The basic mechanism is shown in Figure 37.

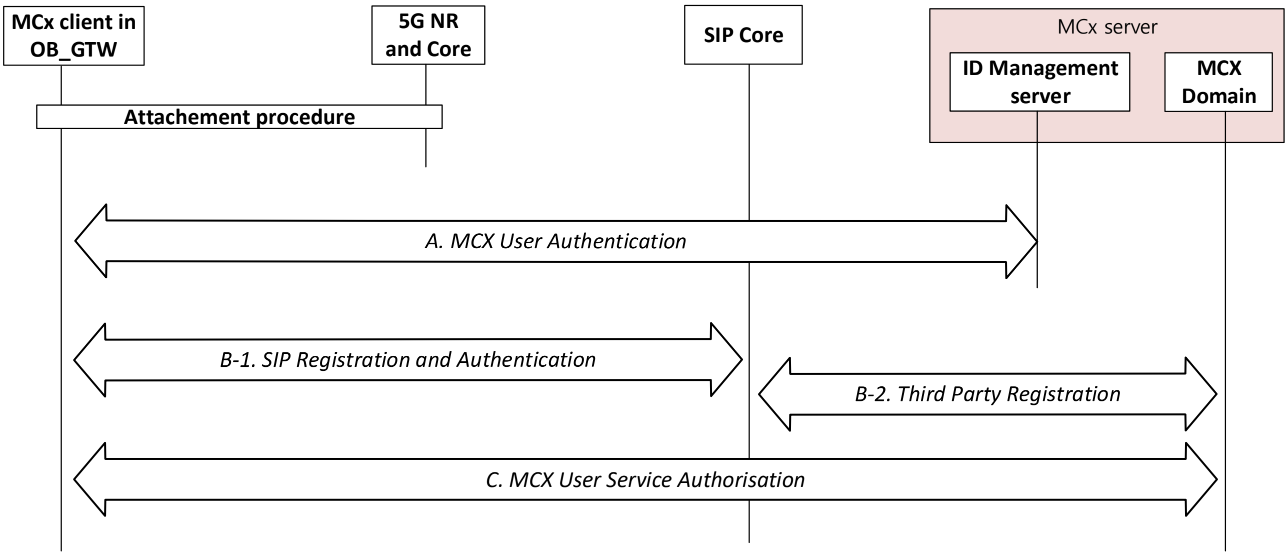

MCx client in OB_GTW
5G NR and Core
SIP Core
MCx server
ID Management server
MCX Domain
Attachement procedure
A. MCX User Authentication
B-1. SIP Registration and Authentication
B-2. Third Party Registration
C. MCX User Service Authorisation

Figure 37: MCx authentication and authorization

For tight-coupled applications, these 3 steps are performed by the application itself. However, the transparency of access to the FRMCS service level is still an open point since the proxying function (F1.8) may also affect the access to the IMS/MCx server by the on-board application.

5.2.2.4.11 F5.1 TO F5.4: O&M GENERAL FUNCTIONS

This chapter deals with function F5.1, F5.2, F5.3 and F5.4.

The OB_GTW shall embed an O&M function dedicated to:

- providing information about events encountered by its hardware and software components (supervision, monitoring, statistics, performance, etc.)

- receiving instructions related to the operation of the system (configuration, software upgrade, etc.)

Then, the OB_GTW includes a SW component responsible for the corresponding functionalities. It is divided into 4 categories:

- Fault management: the underlying requirements are described in chapter 7.6.4 of [S9].
- Performance & supervision management: the underlying requirements are described in chapters 7.6.2, 7.6.3 and 7.6.6 of [S9].
- Configuration management: the underlying requirements are described in chapter 7.6.5 [S9].
- Users or groups account/profile : the underlying requirements are described in chapter 7.8.2 of [S9].

5.2.2.4.12 F5.5: O&M FUNCTIONS - EXPOSE O&M INTERFACE FOR LOCAL CLIENT

This function depends on implementation (Kontron or Alstom)

Alstom implementation:

The OB_GTW exposes an http interface. The client connects to the OB_GTW O&M function with a web client. Hence, the OB_GTW includes a http server in order to expose the http interface for local clients.

Kontron implementation:

The OB_GTW exposes an SNMP (v2c) and REST API interface. The client connect to the OB_GTW O&M function through a client.

5.2.2.4.13 F5.6: O&M FUNCTIONS - EXPOSE O&M INTERFACE FOR REMOTE SERVER

This function depends on implementation (Kontron or Alstom)

The OB_GTW shall expose an interface for a central O&M server on trackside.

Alstom implementation:

The OB_GTW sends SNMP traps to a remote server. The addressing of the remote server is statically configured in the OB GTW.

The OB_GTW implements a SNMPv2c or a SNMP v3 agent.

The OB_GTW implements a MIB-II as defined by reference **[S2]**.

Kontron implementation:

The remote server will connect to the OB_GTW and collect the O&M information through SNMP (v2c) and /or REST API.

5.2.2.4.14 F6: SUPPORT BORDER-CROSSING CAPABILITIES

This function addresses the ability for the OB_GTW to maintain transport service for applications while crossing a border between two countries (or more generally between two radio networks).

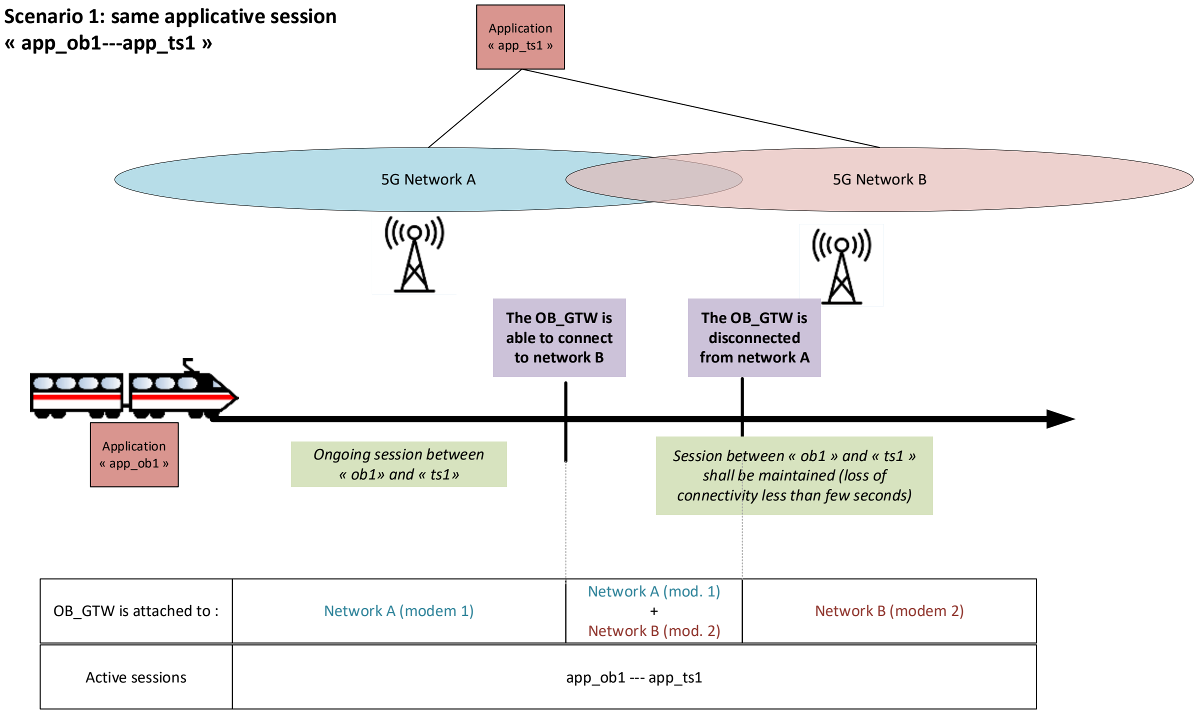
For example, it is essential for the operation of international trains, transporting passenger or freight across borders.

The border-crossing function implemented for 5GRAIL requires at least two modems (e.g. two 5G modems for a border-crossing between two 5G networks) and makes use of the multiconnectivity feature described in **5.2.2.4.2** to trigger the switching of user plane data from the first network to the second one.

NOTE: The use of two modems for border-crossing scenario is a 5GRAIL choice and other solutions could be explored in other projects. Initially, the use of one modem was envisaged but due to too long interruption of communication around the change of network, a solution using two modems was considered then.

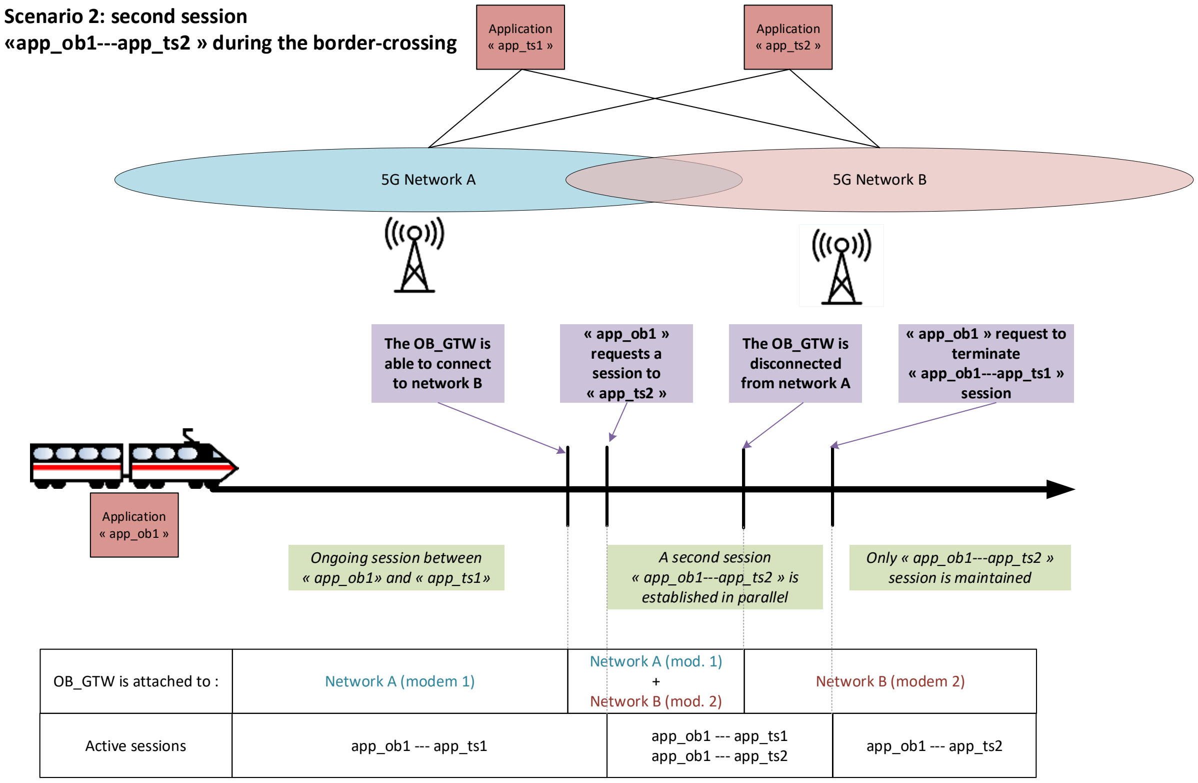
The corresponding test cases considered for 5GRAIL are represented in **Figure 38** and **Figure 39**. There are two scenarios:

- Scenario 1 (ATO-like) : initially, the train is connected to a 5G network A (country A) with its modem A, and the application “app_ob1” has an ongoing session to “app_ts1”. Arriving near country B, the train is able to connect to a 5G network B (country B) with a second modem B; then it will lose the connection to network A, but shall maintain the session between “app_ob1” and “app_ts1” using network B.
- Scenario 2 (ETCS-like) : Same than scenario 1, but “app_ob1” will request a second session to “app_ts2” just before or just after the connection to network B. The connection to the network B and the request for the second session to “app_ts2” from the application “app_ob1” are fully decorrelated events (the application does not have any knowledge about the networks used by the OB_GTW), even if, for ETCS, the second session request is triggered by a track beacon which is located in the overlapping area between Network A and B, following ETCS subset specifications.


Scenario 1: same applicative session
« app_ob1---app_ts1 »
Application
« app_ts1 »
5G Network A
5G Network B
The OB_GTW is able to connect to network B
The OB_GTW is disconnected from network A
Application
« app_ob1 »
Ongoing session between « ob1» and « ts1»
Session between « ob1 » and « ts1 » shall be maintained (loss of connectivity less than few seconds)

OB_GTW is attached to :	Network A (modem 1)	Network A (mod. 1) + Network B (mod. 2)	Network B (modem 2)
Active sessions	app_ob1 --- app_ts1		

Figure 38: Border-crossing “ATO-like”


Scenario 2: second session
«app_ob1---app_ts2 » during the border-crossing
Application
« app_ts1 »
Application
« app_ts2 »
5G Network A
5G Network B
The OB_GTW is able to connect to network B
« app_ob1 » requests a session to « app_ts2 »
The OB_GTW is disconnected from network A
« app_ob1 » request to terminate « app_ob1---app_ts1 » session
Application
« app_ob1 »
Ongoing session between « app_ob1» and « app_ts1»
A second session « app_ob1---app_ts2 » is established in parallel
Only « app_ob1---app_ts2 » session is maintained

<table>
<tr><td>OB_GTW is attached to :</td><td>Network A (modem 1)</td><td colspan="2">Network A (mod. 1)
+
Network B (mod. 2)</td><td colspan="2">Network B (modem 2)</td></tr>
<tr><td>Active sessions</td><td colspan="2">app_ob1 --- app_ts1</td><td colspan="2">app_ob1 --- app_ts1
app_ob1 --- app_ts2</td><td>app_ob1 --- app_ts2</td></tr>
</table>

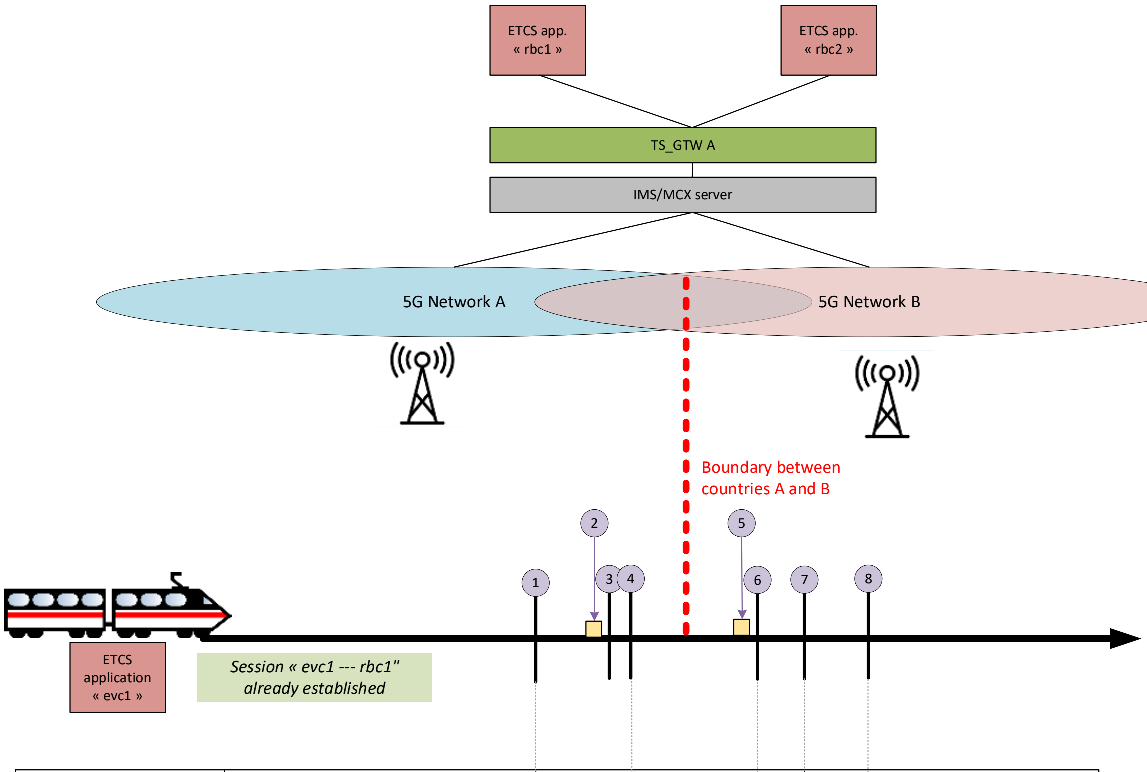
Figure 39: Border-crossing "ETCS-like"

There are several possible implementations for the infrastructure and trackside architectures related to the border-crossing scenario (e.g. same MCx server or two different servers and domains, same TS_GTW or two different TS_GTW, ….). This architecture is not specified yet in FRMCS specifications. In 5GRAIL, the border-crossing scenario makes use of one MCx server and one TS_GTW, as described in the ETCS example below.

Example : ETCS Border-crossing

The **Figure 40** provides a detailed example of border-crossing scenario applied to ETCS application, which is supported by 5GRAIL implementation of "*F6: Support border-crossing capabilities*".

It considers a scenario where the train goes from a country A (using a 5G network A) to a country B (using a 5G network B); ETCS on-board equipment (EVC) has to communicate with RBC1 in country A and RBC2 in country B. Initially, the session between EVC and RBC1 is already established using network A.



OB_GTW is attached to :	Network A (modem 1)	Network A (mod. 1) + Network B (mod. 2)			Network B (modem 2)	
Session evc1---rbc1	Active Using network A	Active Using Network A or Network B (*)	Active Using Network A or Network B (*)	Deleted		
Session evc1---rbc2	Not existing yet		Active Using Network A or Network B (*)	Active Using Network A or Network B (*)		Active Using network B

(*) the switching from Network A to Network B is triggered by BearerFlex feature of the OB GTW. It may occur in step 1 or step 6, depending on priority configuration.

Figure 40: Border-crossing details in 5GRAIL

The events identified in the figure are detailed in the table below:

Step	Description
1	The OB GW becomes attached to network B with its second modem (it is still attached to network A using the first modem). Depending on the priority level configured for each modem, the session between evc1 and rbc1 may directly switch on network B.
2	The ETCS On-Board detects a beacon requesting to reach rbc2. **Note 1** : in 5GRAIL, this step is triggered by beacon simulation (not real beacon). **Note 2**: Within FRMCS, Step 2 does not depend on Step 1 because applicative session requests are decorrelated from Network events. Thus, Step 1 may occur after steps 2, 3 and 4
3	The ETCS On-Board sends (through OB$_{APP}$ API) a session establishment request to reach rbc2
4	The session between evc1 and rbc2 has been established by OB_GTW and is ready to use (status=”working”¸see OB$_{APP}$ API specification). Depending on the priority level configured for each modem, the session between evc1 and rbc2 may use network A or network B.
5	The ETCS On-Board detects a beacon requesting to close connection to rbc1
6	The ETCS On-Board sends (through OB$_{APP}$ API) a request to terminate the session to rbc1
7	The train becomes out of coverage from network A
8	The OB_GTW detects the failure of links using network A. If session was still using network A, the OB_GTW switches to Network B.

5.2.2.4.15 F7.1: OBTAIN POSITIONING AND TIME INFORMATION

As described in chapter **5.2.1.9**, the OB_GTW includes a GNSS receiver (either a dedicated GNSS receiver, or the GNSS capabilities embedded in the 5G modem). The GNSS signal received is used by the OB_GTW to have:

- a GNSS positioning information
- a synchronized time information

The synchronized time information is for internal use of the OB_GTW (e.g. timestamping), but at this stage it is not expected to distribute time to the applications through NTP protocol.

5.2.2.4.16 F7.2: PROVIDE POSITIONING INFORMATION TO THE APPLICATION

The aim of this function is to distribute the GNSS positioning information to the applications which requests it.

This function will not be implemented in OB_GTW for 5GRAIL.

5.2.3 Interfaces

The external interfaces of OB_GTW are the following:

- OB_{APP} : interface with the application in tight mode, loose mode or flat-IP mode.
- OB_{OM} : interface with O&M client or O&M server.
- OB_{POW}: interface with the power supply
- OB_{ANT} :interface with RF combining & switching and the antennas
- OB_{GNSS}: interface with GNSS antenna

5.2.3.1 OB_{APP} interface (standard)

5.2.3.1.1 DESCRIPTION

OB_{APP} interface shall be able to support both the 2 coupling modes (tight and loose). It can be described by the following sub-components:

- OB_{APP-UP}: it is an IP interface for user plane which exposes the following to the applications:
  - a gateway IP address to join trackside from on-board
  - a DNS address
  - other optional IP services such as NTP server
- OB_{APP-CP}: interface to manage the control plane. It includes the local binding (authentication), and session management through the OBAPP API.

Note: the “flat-IP” applications will use only the OB_{APP-UP}.

For further details regarding OB$_{APP}$ interface, please refer to chapter **6.2**.

5.2.3.1.2 PHYSICAL INTERFACE

Whatever the coupling mode, the physical interface used for OB$_{APP}$ and related sub-interfaces is an M12 Ethernet port to face with vibration constraints.

OB_GTW-A:

Up to 4 ports can be configured to support OB$_{APP}$:

- 2 x Fast Ethernet 802.3 10/100 BASE-TX. Physical connector M12 female 4 pins D-Coding
- 2 x Giga Ethernet 802.3 10/100/1000 BASE-TX. Physical connector M12 female 8 pins X-Coding

OB_GTW-K:

- One Giga Ethernet port
- Physical connector: M12 female, 4 pins

5.2.3.1.3 FUNCTIONAL INTERFACE

See chapter **6.2**.

5.2.3.2 OB$_{OM}$ interface (not standard for 5GRAIL execution)

5.2.3.2.1 OB_GTW-A:

The physical interface is one of the 4 M12 Ethernet ports described in chapter **5.2.3.1**.

The functional interface is based on http protocol. The O&M client gains access to O&M information through a web interface exported by the OB_GTW. This web-interface shall present an authentication interface (login, password) to ensure that only authorized user can use this interface.

5.2.3.2.2 OB_GTW-K:

- One Giga Ethernet port
- Physical connector: M12 female, 4 pins

5.2.3.3 OB$_{ANT}$ interface (standard)

5.2.3.3.1 DESCRIPTION:

This is the standardized interface between the FRMCS Radio Modules (within FRMCS OB_GTW) and the antenna system.

5.2.3.3.2 PHYSICAL INTERFACE:

The RF connectors used for the physical interface will be SMA connectors or N-type connectors.

Per each internal FRMCS modem, there are at least 2 RF connectors in order to perform MIMO 2x1.

Per each internal non-FRMCS modem (4G or Wi-Fi), there are at least 2 RF connectors in order to perform MIMO 2x1.

The N-type connectors are front face female RF coaxial receptacles, of type N 50 Ohms, that fulfil the pinout illustrated in Table 23. They are compliant with standard **[S1]**.

Figure 41: N-type connector

Figure 42: SMA connector

Pin	Function
inner contact	Signal
outer contact	GND

Table 23: Pinout of the RF connectors

5.2.3.3.3 FUNCTIONAL INTERFACE:

Behind the physical OB_{ANT} interface described in **5.2.3.3.2**, the functional view of OB_{ANT} interface includes the following links:

- Logical link between the OB_GTW and the TS_GTW for the transmission of application data
- Logical link between the OB_GTW and the IMS/MCx server, to manage the service layer.

The first link enables to carry application data (IP based protocol) and is impacted by the BearerFlex functionalities provided by function F1.2. As explained in **5.2.2.4.2**, the BeareFlex function will not be standardized in a first 5GRAIL implementation, and the solution will be vendor-dependent. Hence, more descriptions about this logical interface will be provided in the next version of the document.

The second link relies on the standardized MCx exchanges between MCx client and MCx server, and covers the following:

- For loose-coupled applications:

- Authentication, registration and MCdata authorization procedures, for the MCdata clients embedded in the OB_GTW. See chapter **5.2.2.4.10** and 3GPP TS 33.180 (version 16.6.0).
- Management of MCData sessions: signalling control for the MCData client embedded in the OB_GTW: see 3GPP TS 24.282 (version 16.6..0, chapter 20 for MCData-IPcon)

- For tight-coupled applications: as explained in **5.2.2.4.8**, the OB_GTW will proxy the control plane messages of tight applications . Please refer to chapter **5.2.2.4.8**.

5.2.3.4 OB$_{POW}$ interface (not standard)

5.2.3.4.1 OB_GTW-A:

The features of the interface are given in**5.2.1.8.**

5.2.3.4.2 OB_GTW-K:

The features of the interface are given in **5.2.1.8.**

5.2.3.5 OB$_{GNSS}$ interface (not standard)

This is the interface with the GNSS external source (GNSS antenna) to receive a GNSS signal for positioning or synchronization.

5.2.3.5.1 OB_GTW-A:

The physical interface is an N-type connector female in the front panel of the OB_GTW.

As a dedicated GNSS receiver is used (see chapter **5.2.1.9**), this connector is internally linked to the GNSS receiver and not to the GNSS connector of the FRMCS modem.

5.2.3.5.2 OB_GTW-K:

The physical interface is a SMA female connector (with central hole on the box connector) in the front panel of the OB_GTW.

This connector is internally connected to the GNSS connector of the FRMCS modem.

5.2.4 Prototype deliverable

5.2.4.1 Hardware platform

5.2.4.1.1 OB_GTW-A:

In a first step, the hardware platform would be:

- A “box” compliant with main railways standards containing a Wi-Fi modem and a 4G modem.
- The 5G modem (MV-31W) will be “out of the box”, connected to the front panel of the box (USB3.0)

More details about hardware housing and standards are given below:

- Hardware housing:
  - Stainless aluminium « Box »
  - Form Factor (CEI 60297-3-101) : 3U x 21TE x 230mm
  - IP 20
  - Mass #2Kg
- Main standards
  - EN50155 (T3 Class for Base, TX Class for MPU/xPU, T1 Class for LTE DCS)
  - Certificates (CE, RED, FCC*,…)
  - Fire & Smoke (EN45545 HL3 Class)
  - RoHS, Reach

5.2.4.1.2 OB_GTW-K:

FRMCS On-Board Gateway hardware, including set of requested modems

TBC => Modems configuration can be different according to the Use Cases to demonstrate and the location (Labs vs Fields)

5.2.4.2 Software components

5.2.4.2.1 OB_GTW-A:

The OB_GTW-A is based on a Linux operating system, coming with an Alstom distribution. The software components are presented in chapter **5.2.1**.

5.2.4.2.2 OB_GTW-K:

The OB_GTW-K will be specific hardware box that will embed the software for the OB_GTW function.

5.2.4.3 Documentation

OB_GTW-A:

- FRMCS OB GTW User Manual

OB_GTW-K:

- FRMCS OB GTW User Manual
- TBC

5.3 FRMCS Track Side Gateway

5.3.1 Architecture

Proposal overview:

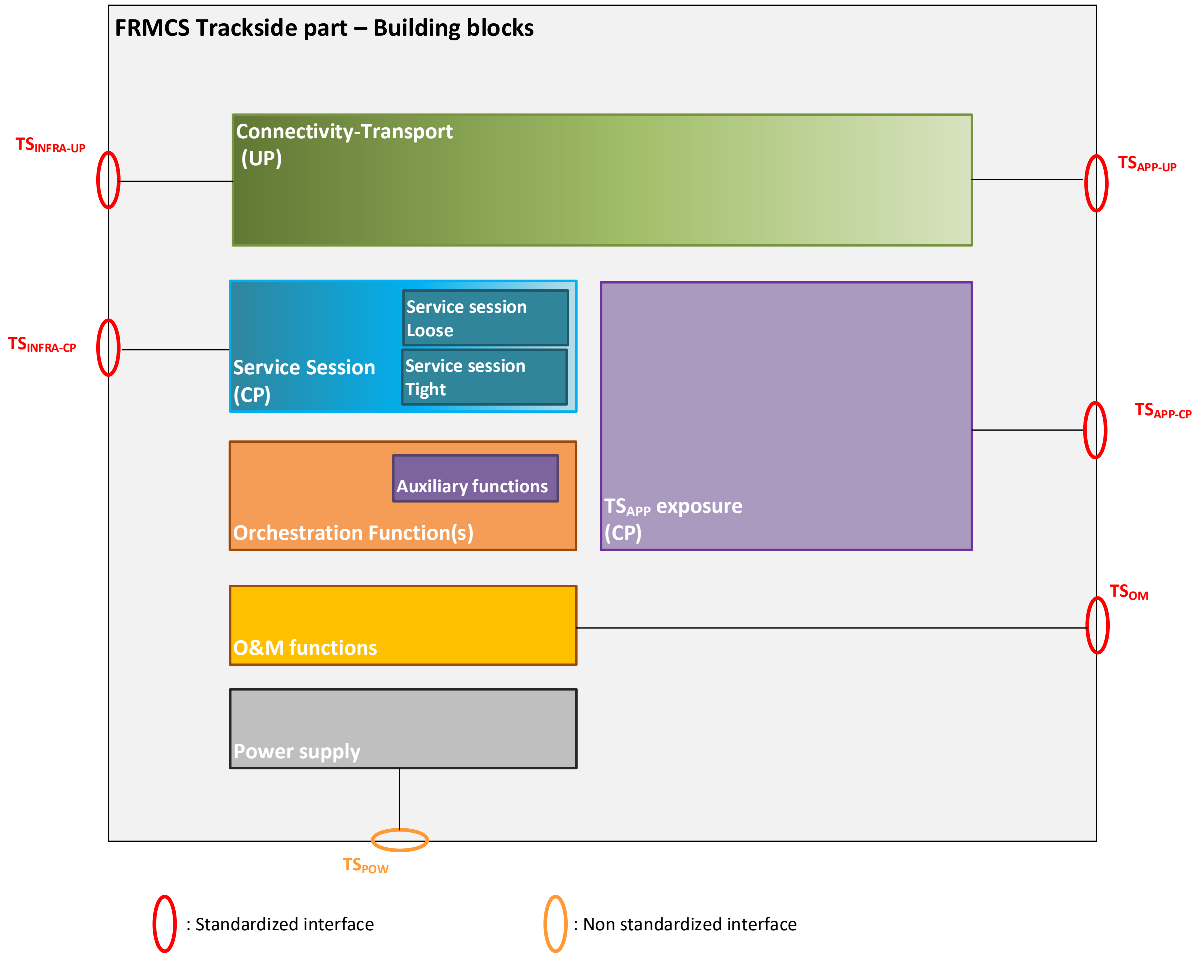


Figure 43: TOBA trackside gateway - Building blocks

5.3.1.1 Connectivity Transport

“Connectivity Transport” building block consists in an IP interface presented to the trackside applications (IP gateway for the trackside applications to send data to on-board). This component is responsible for routing user plane data between on-board networks to trackside network, using the available radio networks and through the established bearers.

It is a software/hardware component (considering the physical interface).

5.3.1.2 Service session

"Service session" building block is separated into two distinct parts:

- "Service session – Loose" is responsible for managing session for Loose-coupled applications (session establishment, session identification, …). This block contains also the MCx clients which can be used for Loose-coupled application which requires critical communication attributes.
- "Service session – Tight" is responsible for controlling session for tight-coupled applications. For tight coupling, the MCx client is embedded on the application side and the application is able to manage its own session, but the OB GTW must be aware of the session established by tight-coupled application.

It is a software component.

5.3.1.3 Orchestration function

"Orchestration function" building block oversees several functions:

- Control and monitor the relation between user plane and control plane (i.e. the established session)
- Ensure the correct communication attributes (QoS)
- Embed some "Auxiliary functions" required by some applications, such as:
  - Link supervision: monitor and deliver to TS_{APP} the quality/status of each link used by the established sessions

It is a software component.

5.3.1.4 TS_{APP} API exposure

"TS_{APP} exposure" building block is responsible for presenting to the application the necessary functions to interact with the applications to manage the control plane. This building block is mainly described in chapter **6.3**.

It is a software/hardware component (considering the physical interface).

5.3.1.5 O&M functions

"O&M functions" building block is responsible for hosting the O&M functions:

- Providing information about events encountered by TS_GTW hardware and software components (supervision, monitoring, statistics, performance, …)
- Receiving instructions related to the operation of the system (configuration, software upgrade, …)
- Expose an interface to send/receive these data to/from a central O&M system.

It is a software component.

5.3.1.6 Power supply

"Power supply" building block is responsible for distributing alimentation to the TS_GTW components. The implementation is different between Alstom and Kontron prototypes.

It is a hardware component.

Power supply for TS_GTW-A:

- Input power: 230V AC
- Redundant power supply (2 input connectors)
- Nominal consumption: 500W

Power supply for TS_GTW-K:

The TS_GTW-K will be a virtual machine to be hosted in any off the shelf X86 server with no specific hardware needs.

5.3.2 Functionalities

5.3.2.1 List of functions:

- TSGTW_F1: Provide transport services for trackside tight-coupled applications and loose-coupled applications
  - TSGTW_F1.1: Expose a TS$_{APP}$ API to the applications for decoupling application and transport
  - TSGTW_F1.2: Multipath/BearerFlex
  - TSGTW_F1.3: Session management for loose-coupled applications
  - TSGTW_F1.4: Provide to the application the required communication attributes
  - TSGTW_F1.5: Local Binding
  - TSGTW_F1.6: Transport user plane data toward on-board
  - TSGTW_F1.7: Expose session supervision information to the applications which request it
  - TSGTW_F1.8: Session proxying for tight-coupled applications
- TSGTW_F2: *deleted*
- TSGTW_F3: Connect to multiple networks
- TSGTW_F4: Authenticate/authorize access to the FRMCS service level.

5.3.2.2 Traceability for each function

Table 24: Function traceability

FUNCTIONS	TRACEABILITY	
	SOURCE FROM REQUIREMENTS	IMPLEMENTATION IN WP2 DOCUMENTS
TSGTW_F1.1: Provide transport services - Expose a TS APP API to the applications for decoupling application and transport	Derived function from use case table	Chap. 5.3.2.4.1
TSGTW_F1.2: Provide transport services - Multipath (bearer flexibility, resilience, aggregation)	Derived function from use case table	Chap. 5.3.2.4.2
TSGTW_F1.3: Provide transport services - Session management for loose-coupled applications	Derived function from use case table	Chap. 5.3.2.4.3
TSGTW_F1.4: Provide transport services - Provide to the application the required communication attributes	Derived function from use case table	Chap. 5.3.2.4.4
TSGTW_F1.5: Provide transport services - Local Binding	Derived function from use case table	Chap. 5.3.2.4.5
TSGTW_F1.6: Transport user plane data toward on-board	UIC TOBA FRS (TOBA-7510) Chap. 4.2.2	Chap. 5.3.2.4.6
TSGTW_F1.7: Expose session supervision to the application which request it	Derived function from use case table	Chap. 5.3.2.4.7
TSGTW_F1.8: Session proxying for tight-coupled applications	Derived function from use case table	Chap. 5.3.2.4.8
TSGTW_F3: Connect to multiple networks	Derived function from use case table	Chap. 5.3.2.4.9
TSGTW_F4: Authenticate/authorize access to the FRMCS service level.	UIC MG-7904 Chap. 3.3.3	Chap. 5.3.2.4.10

5.3.2.3 Allocation to building blocks

The table below presents the allocation of these functions to the building blocks described in chapter **5.2.1**.

Table 25: Allocation to building blocks

FUNCTIONS	ALLOCATED BUILDING BLOCK
TSGTW_F1.1 Provide Transport services – Expose a TSAPP API to the applications for decoupling application and transport	TS_{APP} exposure
TSGTW_F1.2 Provide Transport services – Multipath/BearerFlex	Connectivity Transport
TSGTW_F1.3 Provide transport services – Session management for loose-coupled applications	Service session - Loose
TSGTW_F1.4 Provide transport services – Provide to the application the required communication attributes	Orchestration function
TSGTW_F1.5: Local Binding	TS_{APP} exposure
TSGTW_F1.6: Transport user plane data toward on-board	Connectivity Transport
TSGTW_F1.7: Expose session supervision to the application which request it	Orchestration function
TSGTW_F1.8: Session proxying for tight-coupled applications	Service session - Tight
TSGTW_F3 Connect to multiple networks	Connectivity Transport
TSGTW_F4 Authenticate/authorize access to the FRMCS service level.	Service session -Loose

5.3.2.4 Details of functions

5.3.2.4.1 F1.1: EXPOSE A TS_{APP} API TO THE APPLICATIONS FOR DECOUPLING APPLICATION AND TRANSPORT

The TS_GTW embeds a Ts_{APP} API exposed to the applications. All details about this API are in chapter **6.3**.

5.3.2.4.2 F1.2: MULTIPATH/BEARERFLEX

Please refer to chapter **5.2.2.4.2** which is also applicable for Trackside.

5.3.2.4.3 F1.3: SESSION MANAGEMENT FOR LOOSE-COUPLED APPLICATIONS

Please refer to chapter **5.2.2.4.3** which is also applicable for Trackside.

5.3.2.4.4 F1.4: PROVIDE TO THE APPLICATION THE REQUIRED COMMUNICATION ATTRIBUTES

Please refer to chapter **5.2.2.4.4** which is also applicable for Trackside.

5.3.2.4.5 F1.5: LOCAL BINDING

The local binding function covers a local identification, authentication and authorization if an on-board application. A specific function of TS_{APP} API is dedicated to local binding: function FRMCS_GTW_REGISTER.

The authentication part performed through TS_{APP} is the same as OB_{APP} (WebSocket over TLS). Please refer to chapter **5.2.2.4.5**.

5.3.2.4.6 F1.6: TRANSPORT USER PLANE DATA TOWARD ON-BOARD

The TS_GTW shall expose to the application an IP interface with an IP gateway address that can be used by the Trackside application to send data to on-board after the corresponding session has been established.

The aim of this function is to redirect user plane data (IP flows) to the relevant bearer established within control plane.

The way to perform this function is open to implementation.

For TS_GTW-A, basically, the function F1.6 uses IP routing table to manage properly the user plane data flow to the correct tunnel (i.e. GRE tunnel if using MCData-IPconn). Control plane will result in modifying dynamically the IP routing rules of OB GTW and TS GTW to manage correctly the user plane.

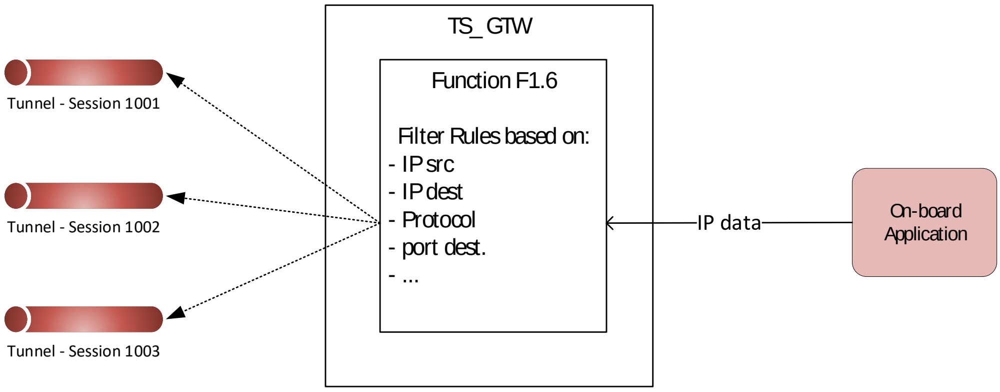


Figure 44: User plane management

A particular mechanism to face with NAT masquerading performed by the core network was explained in **5.2.2.4.6** and must be applied for TS_GTW.

5.3.2.4.7 F1.7: EXPOSE SESSION SUPERVISION INFORMATION TO THE APPLICATIONS WHICH REQUEST IT

Please refer to chapter **5.2.2.4.7** which is also applicable for Trackside.

5.3.2.4.8 F1.8: SESSION PROXYING FOR TIGHT-COUPLED APPLICATIONS

Please refer to **5.2.2.4.8** chapter which contains Proxying for tight coupled applications function for the OB and TS GTW.

5.3.2.4.9 F3: CONNECT TO MULTIPLE NETWORKS

In order to allow the BearerFlex function, the TS_GTW must be connected to several networks.

5.3.2.4.10 F4: AUTHENTICATE/AUTHORIZE ACCESS TO THE FRMCS SERVICE LEVEL.

Please refer to chapter **5.2.2.4.10** which is also applicable for Trackside.

5.3.3 Interfaces

Proposed list of interfaces:

- TS_{APP}
  - For loose-coupled applications
  - For tight-coupled applications
- TS_{OM} : interface with O&M server
- TS_{INFRA}: interface with infrastructure (core network, IMS, MCx server)
- TS_{POW}: interface with the power supply

5.3.3.1 TS_{app} interface (standard)

5.3.3.1.1 DESCRIPTION

TS_{APP} interface description may be different depending on the coupling mode of the application. It can be described by the following sub-components:

- TS_{APP-UP}: it is an IP interface for user plane which exposes the following to the applications a gateway IP address to join on-board equipment
- TS_{APP-CP}: interface to manage the control plane. It includes the local binding (authentication) if needed, and session management through the TS_{APP} API defined in chapter **6.3**.

Note: the “flat-IP” applications will use only the TS_{APP-UP}.

Note 2: “flat-IP” mode is considered for phasing approach of OB_{APP} but not considered as a target standardized mode.

For further details regarding TS_{APP} interface, please refer to chapter **6.3**.

5.3.3.1.2 PHYSICAL INTERFACE

The physical interface is constituted of one or several Ethernet ports (Fast Ethernet 802.3 10/100BASE-TX or Giga Ethernet 802.3 10/100/1000 BASE-TX). Contrary to OB_{APP} physical interface; the connector is not necessarily M12 as there is not the same vibration constraint than on-board.

5.3.3.1.3 FUNCTIONAL INTERFACE

The functional interface is described in chapter 6.

5.3.3.2 TS_{om} interface (not standard for 5GRAIL execution)

This interface enables the O&M server to be interfaced with O&M function of each available OB_GTW, in order to satisfy the requirements presented in **5.2.2.4.13**.

5.3.3.2.1 TS_GTW-A

One Ethernet port is dedicated for this interface. Same physical interface than $TS_{APP.}$

As described in **5.2.2.4.13**, the protocol used is SNMPv2c or SNMP v3.

5.3.3.2.2 TS_GTW-K

One Ethernet port is dedicated for this interface. Same physical interface than TS_{APP}.

5.3.3.3 TS_{infra} interface (not standard for 5GRAIL execution)

5.3.3.3.1 DESCRIPTION:

This interface enables the MCx client embedded in the TS_GTW (for loose-coupling) or in application (for tight-coupling) to communicate with the infrastructure.

It covers the control plane exchanges and the user plane exchanges (application data) with the infrastructure.

5.3.3.3.2 PHYSICAL INTERFACE:

The physical interface is constituted of one or several Ethernet ports (Fast Ethernet 802.3 10/100BASE-TX or Giga Ethernet 802.3 10/100/1000 BASE-TX).

5.3.3.3.3 FUNCTIONAL INTERFACE

For control plane, the functional interface relies on the standardized MCx exchanges between MCx client and MCx server, and covers the following:

- For loose-coupled applications:
  - Authentication, registration and MCdata authorization procedures, for the MCdata clients embedded in the OB_GTW. See chapter **5.2.2.4.10** and 3GPP TS 33.180 (version 16.6.0).
  - Management of MCData sessions: signalling control for the MCData client embedded in the OB_GTW: see 3GPP TS 24.282 (version 16.6.0, chapter 20 for MCData-IPcon)
- For tight-coupled applications: as explained in **5.2.2.4.8**,the OB_GTW will proxy the control plane messages of tight applications . Please refer to chapter **5.2.2.4.8**.

For user plane, the interface enables the transmission of application data. It allows to carry application data (IP based protocol) and is impacted by the BearerFlex functionalities provided by function F1.2. As explained in **5.2.2.4.2**, the BearerFlex function will not be standardized in a first 5GRAIL implementation, and the solution will be vendor-dependent. Hence, more descriptions about this functional interface will be provided in the future version of the document.

This IP interface must be duplicated for each network to which the TS_GTW is connected (5G, Wi-Fi, 4G, etc.).

5.3.3.4 TS$_{pow}$ interface (not standard)

5.3.3.4.1 TS_GTW_A

The features of the interface are given in **5.3.1.6**

5.3.3.4.2 TS_GTW_K

The features of the interface are given in **5.3.1.6.**

5.3.4 Prototype deliverable

5.3.4.1 Hardware platform

5.3.4.1.1 TS_GTW-A

TS_GTW-A consists in a 1U rackable server, for a 19’’ rack.

Model for first version: HPE Proliant DL20 GEN10

Dimension : 4.32 x 43.46 x 38.22 cm (H x l x p)

Figure 45: TS_GTW-A

It contains 4 Ethernet 1G ports.

5.3.4.1.2 TS_GTW-K

The TS_GTW-K will be a virtual machine to be hosted in any off the shelf X86 server with no specific hardware needs.

5.3.4.2 Software components

5.3.4.2.1 TS_GTW-A

The TS_GTW-A is based on a Linux operating system, with a CentOs distribution. The software components are presented in chapter **5.3.1.**

5.3.4.2.2 TS_GTW-K

The TS_GTW-K will be a virtual machine to be hosted in any off the shelf X86 server with no specific hardware needs.

5.3.4.3 Documentation

Similar to **5.2.4.3**.

5.4 Other On-board and Trackside components

5.4.1 O&M client and server

5.4.1.1 Alstom prototype

The O&M client is a laptop with a web browser to display the O&M application. It is connected to the OB_GTW through the dedicated Ethernet port (see .§5.2.3.2)

The O&M central is a server connected to the TS GTW.

5.4.1.2 Kontron prototype

OM client is connected to one FRMCS OB GTW through OB_{OM}. OM Server manages all OB GTW and is connected over the air to different OB GTW

For OB_{OM} (OB GTW):

- One Giga Ethernet port
- Physical connector: M12 female, 4 pins

5.4.2 RF combining & switching

As introduced in chapter 2.2.14, RF combining and switching might be needed to manage the different radio technologies and frequencies. This is described in the following paragraphs.

5.4.2.1 FRMCS 5G placing in GSM-R train

Taking into account:

1. Thales FRMCS Modem RF specifications:

and

2. The following antennas implementation on the roof of the train provided by SNCF:

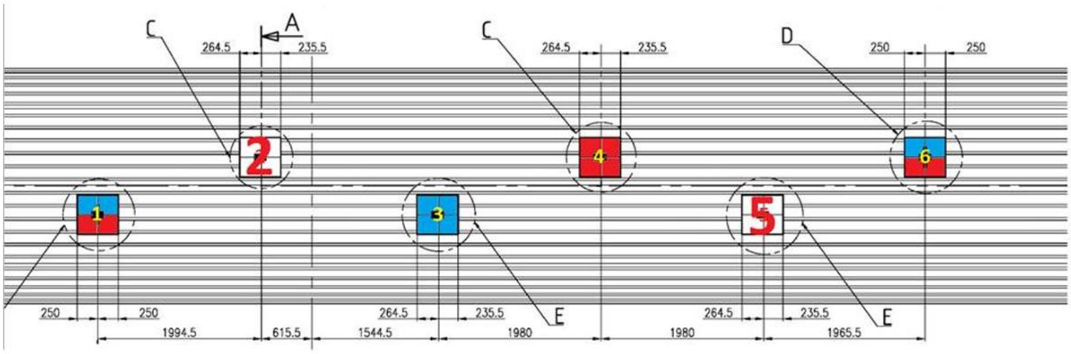


Figure 46: Antennas implementation

We recommend to connect the Thales FRMCS modem ports to the antenna’s as shown in the basic electrical schematic proposed here below.

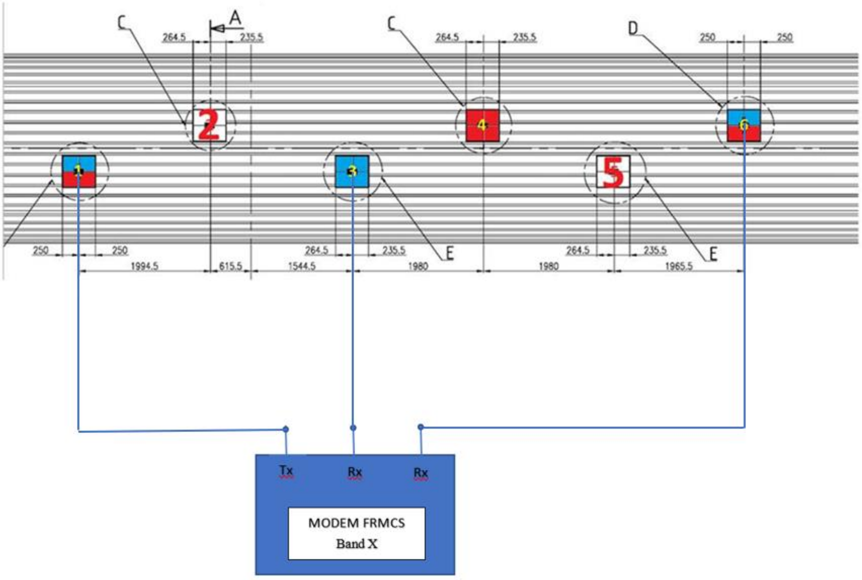


Figure 47: recommendation of connection

Special attentions shall be taken to:

1. Ensure a minimum distance separation of 3 meters between Tx antenna and Rx ones, as specified by the FRMCS modem supplier.
2. Secure a minimum 20 landa’s spacing between RX’s antenna to maximize the reception diversity gain.

This schematic is given as an example and does not constitute a definitive version.
Final position of FRMCS Tx and Rx antennas may vary in function of surrounding GSM-R antenna’s location on the roof of the train.

5.4.2.2 FRMCS Modem hardware redundancy

Two ways can be foreseen to implement the hardware redundancy of the FRMCS modem.

1. Using an RF switch?

Figure 48: RF switch

Or

2. Using a Power combiner?

Figure 49: Power combiner

Both of these two solutions has pros and cons that are detailed hereafter:

RF switching main benefit:

- Low added electrical losses => limited budget gain impact (cell coverage preserved).

RF switching drawbacks:

- As any active part:
  - A power supply is required
  - The Intermodulation products side-effects shall be considered.
- A control signal shall be provided.
- Hot redundancy is not feasible = service interruption.

Power combining main benefits:

- Hot redundancy implementable.
- Passive part:
  - No power supply nor control wire required.
  - Insignificant intermodulation products.

Power combining drawbacks:

- 3.2dB added electrical losses => cell coverage reduction.

To make the demonstration of the hot redundancy, we recommend to use a power combiner.

To compensate for the larger added loss, we propose to operate the two modems in parallel to double the data stream, every time throughput KPI shall be demonstrated instead of hardware redundancy.

For de-risking purpose, the power combiner isolation requirement shall be assessed during lab tests.

Previous proposed electrical schematic can be then updated as follow to introduce the hardware redundancy:

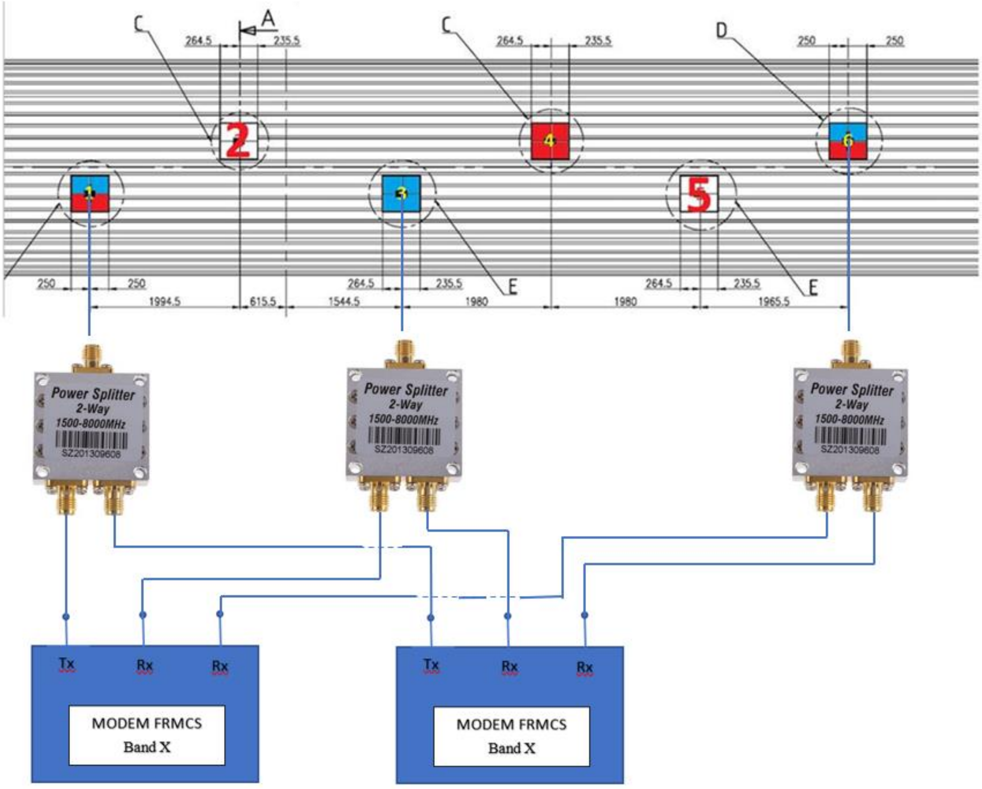


Figure 50: update of the electrical schematic to introduce the hardware redundancy

5.4.2.3 BearerFlex constraints

The bearer flex feature consists in operating multiple radio bearers simultaneously.

To make the demonstration of the bearer flex capabilities it is necessary to make sure that many different technologies (up to 3 in our application, i.e. GSM-R /LTE/5G) can be run simultaneously without interfering one another.

A minimum of 60dB isolation, between 2G, 5G or 4G standards, is required to guarantee the safe operation of the whole of them.

Antenna spacing and various antenna polarization arrangement (if realistic?) cannot provide such a large level of isolation.

Extra filtering is to be considered to provide the necessary 60 dB isolation.

The advanced electrical schematic proposed here below, is presenting a solution based on diplexer unit usage.

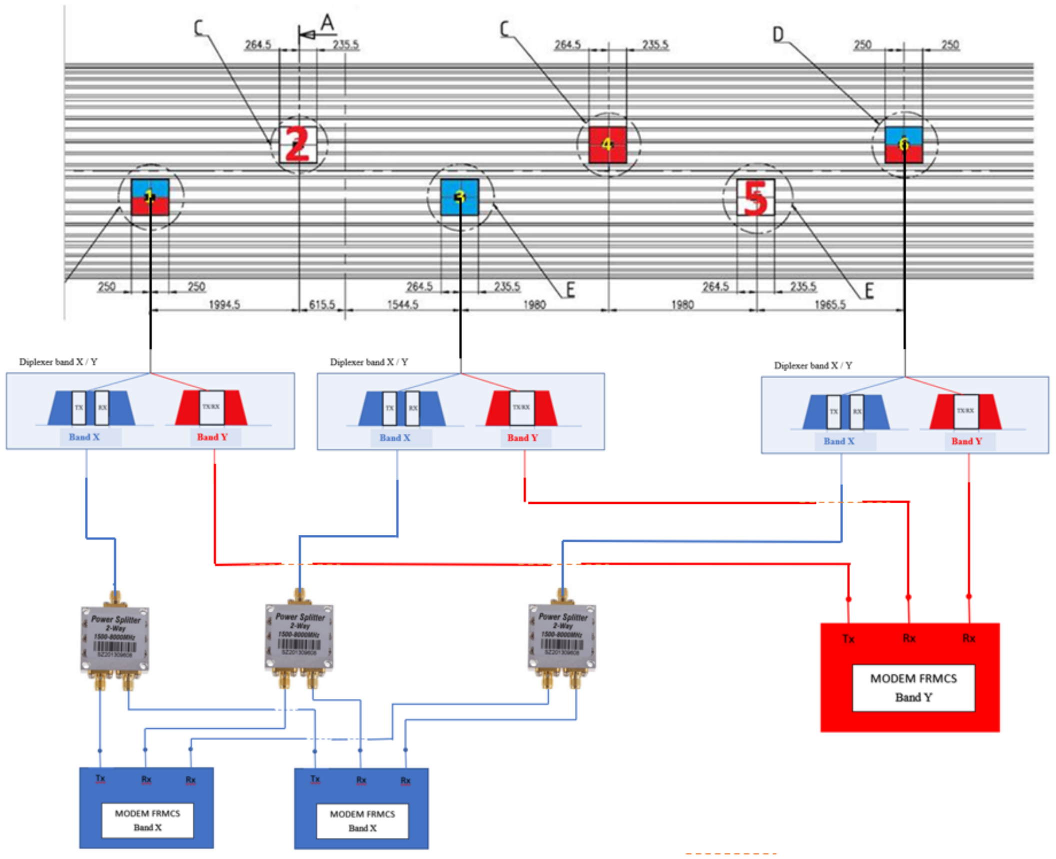


Figure 51: advanced electrical schematic

Remarks:

1. Filters shall be specified in accordance with the frequency bands X & Y selected for the trials.
2. A special attention shall be paid when selecting frequency bands X and Y to make sure that none of intermodulation products may affect the GSM-R network sensitivity.

6 APPLICATIONS & FRMCS GATEWAYS INTERFACES

This chapter describes the interfaces between the applications and the FRMCS gateways both for the on-board and the trackside domain meaning the OB_{APP} and the TS_{APP} interfaces.

The OB_{APP} interface stands between the on-board applications and the FRMCS Onboard Gateway.

The TS_{APP} interface stands between the ground applications and the FRMCS Trackside Gateway.

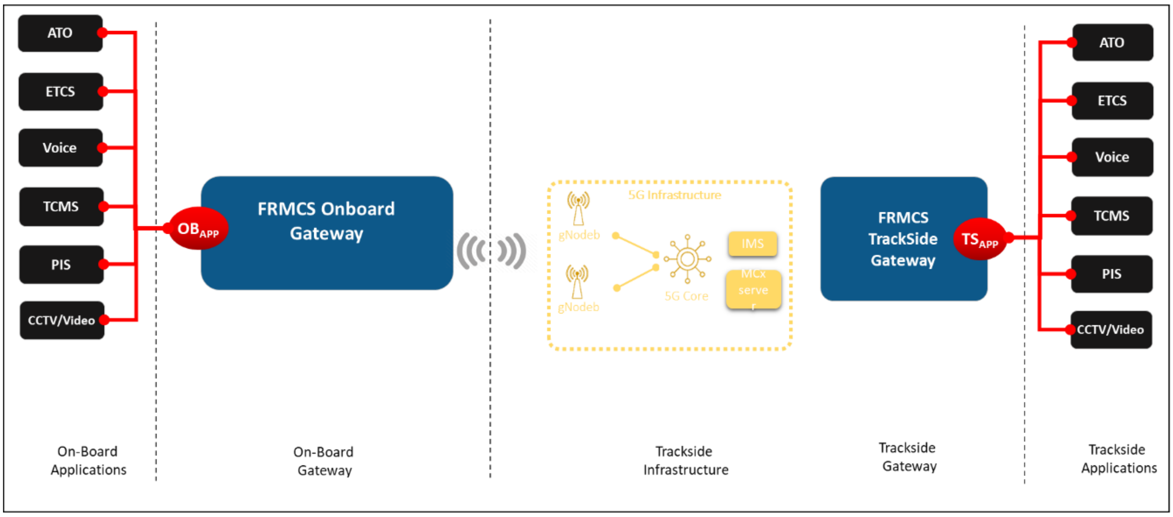


Figure 52: OB_{APP}/TS_{APP} location

The specifications of OB_{APP} and TS_{APP} interfaces are not yet available to support 5GRail execution. The goal is to define the minimal baseline for these interfaces to start the execution.

Those interfaces are divided into two sub-interfaces:

- One for the tight coupled applications: in that case, the MCx client is managed at application level.
- One for the loose coupled applications: in that case, the MCx client for the application is managed at the FRMCS Onboard Gateway level.

The two figures below represent the end to end communication for the tight coupled applications and for the loose coupled applications.

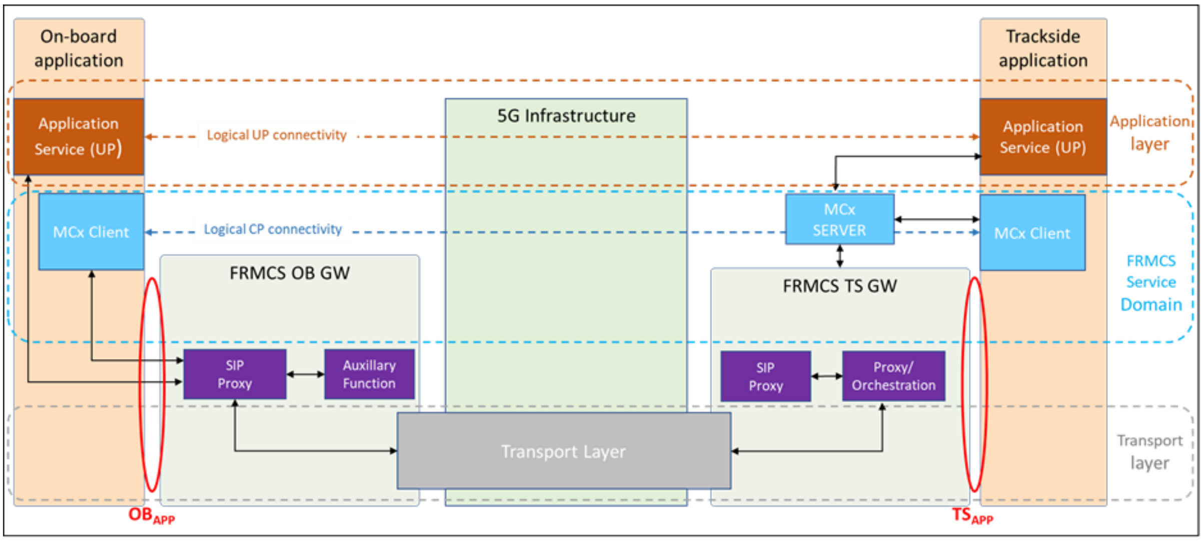


Figure 53: End to end communication for tight coupled applications

The SIP proxy box is in charge of forwarding the application SIP requests. It could also, in the future be in charge of screening the MCx control plane of the tight coupled applications in order to retrieve at least QoS information and to allow the orchestration part of the GTW to handle the different UPs accordingly.

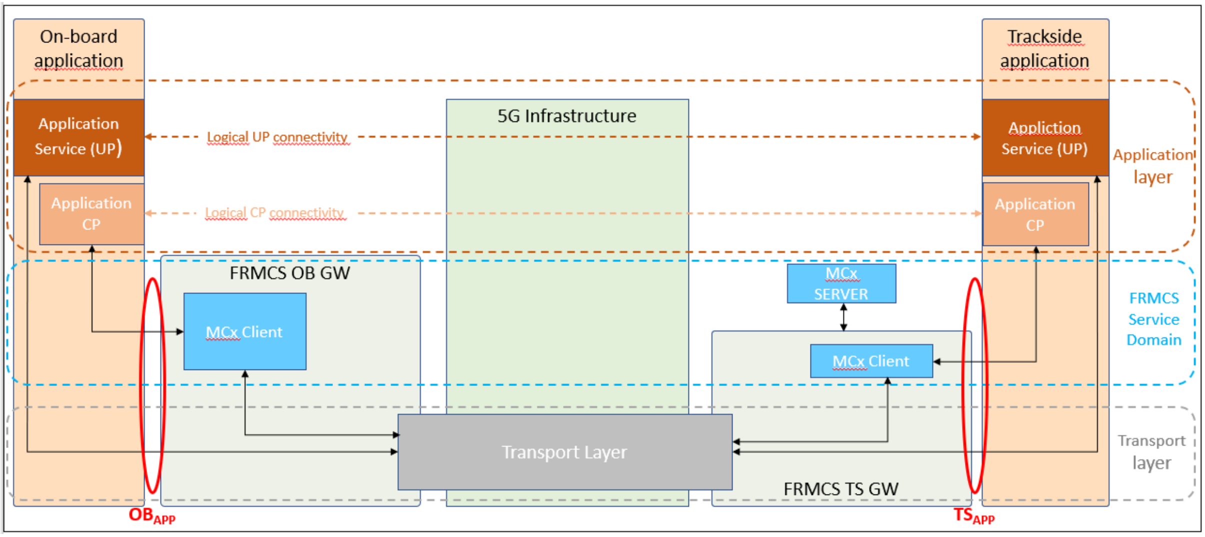


Figure 54: End to end communication for loose coupled applications

6.1 Application coupling mode

This paragraph shall contain the list of all the applications connected to the FRMCS gateways system through the OB_{APP} or the TS_{APP} interface.

For each application, this paragraph shall stand whether the application is a tight coupled application or a loose coupled one.

Table 26: Application coupling mode

APPLICATION	TS_{APP} AND OB_{APP} TIGHT COUPLING MODE	TS_{APP} AND OB_{APP} LOOSE COUPLING MODE
Voice	X	
ETCS		X
ATO		X
TCMS		X
PIS		X
CCTV/Video		X
SNCF Remote Vision		X on flat IP only approach

A flat IP only approach is introduced. It is defined as a sub-mode of the loose coupled in which the control plane is not managed by the application but done based on static configuration inside the gateways.

6.2 OB_{APP} interface

This paragraph shall contain the OB_{APP} interface description.

6.2.1 Functions

Table 27: OB_{APP} functions

FUNCTION	TIGHT	LOOSE	O/M[1]	FROM	TO	OUTCOME	API FUNCTIONS
OB application Identification and authentication Request	X	X	M	Application	Gateway	Waiting for FRMCS OB GTW response – local binding process	FRMCS_GTW_REGISTER
OB application Identification and	X	X	M	Gateway	Application	Allow session creation	FRMCS_GTW_REGISTER

authentication Response							
OB Initiating a communication service request		X	M	Application	Gateway	Waiting for FRMCS OB GTW response	FRMCS_GTW_SESSION_START
OB Accepting a communication service request from OB application		X	M	Gateway	Application	Allow data transfer	FRMCS_GTW_SESSION_START
OB Rejecting a communication service request from OB application		X	M	Gateway	Application	Close the requested communication session	FRMCS_GTW_SESSION_START
OB Ending an established communication service		X	M	Application	Gateway	Close the requested communication session	FRMCS_GTW_SESSION_END
OB Release association	X	X	M	Application	Gateway	Close the association	FRMCS_GTW_DEREGISTER
OB Communication service information on FRMCS availability		X	O	Gateway	Application	Application aware of the FRMCS service availability	FRMCS_APP_SESSION_STATUS_CHANGED
OB FRMCS Availability Request		X	O	Application	Gateway	Application request for the FRMCS availability	FRMCS_GTW_SESSION_STATUS
OB Providing Specific Service	X	X	O	Gateway	Application	Specific services provided to the application by the Auxiliary Function	FRMCS_APP_SERVICE_RESPONSE
OB asking for Specific Service Request	X	X	O	Application	Gateway	Application asking for specific service link to Auxiliary Function	FRMCS_GTW_SERVICE_REQUEST
OB Incoming communication Request		X	M	Gateway	Application	Waiting incoming communication response	FRMCS_APP_INCOMING_SESSION

OB Accepting incoming communication		X	M	Application	Gateway	Allow data transfer	FRMCS_APP_INCOMING_SESSION
OB Rejecting incoming communication		X	M	Application	Gateway	Close the requested communication session	FRMCS_APP_INCOMING_SESSION

Note 1: the O/M column has to be interpreted as Optional or Mandatory function from the application point of view. That means that the Gateway has to implement all the defined functions. Moreover, the Gateway sends the optional messages to all the application and it is up to the applications to ignore them if optional on their side.

6.2.2 Physical interface

This section shall contain description of the physical interface for the OB$_{APP}$ interface.

The OB$_{APP}$ interface is based on IPv4 connections, on standard ETH socket. The physical interface is fully described in chapter 5.

6.2.3 Protocol stack

This section shall contain the description of the protocol stack for the OB$_{APP}$ interface for control and user planes.

The interface between the onboard applications and the FRMCS Onboard Gateway is compliant with the following protocol stacks, for control plane and user plane:

- For the tight coupled applications:

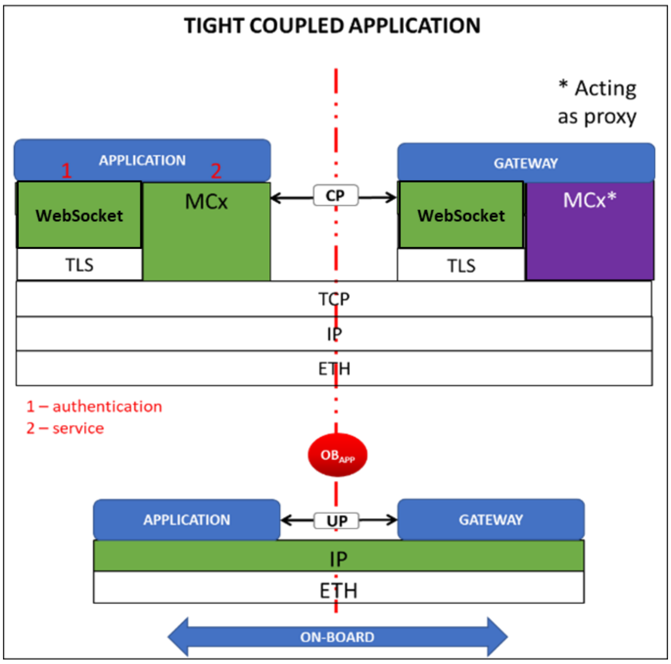


Figure 55: Tight coupled application OB$_{APP}$ protocol stack

The control plane for the tight coupled applications is based on the MCx framework as described in chapter 6.2.5.

- For the loose coupled applications:

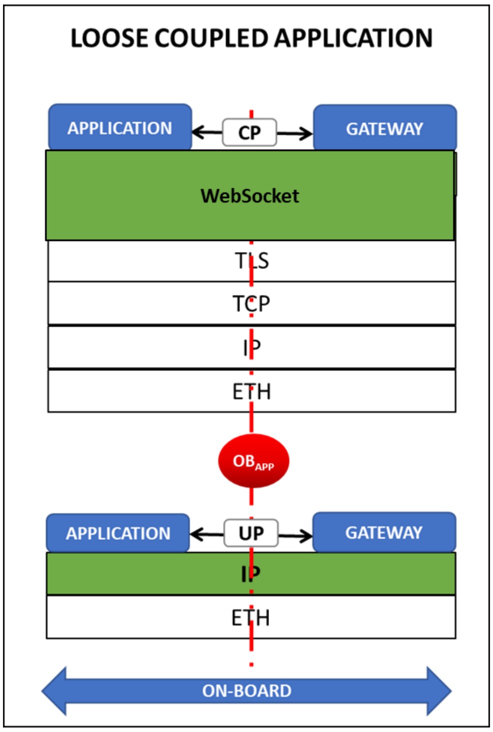


Figure 56: Loose coupled application OB$_{APP}$ protocol stack

An application interface (API), based on WebSocket, is provided to the application.

The proposed protocol for this API is WebSocket protocol for control plane. This is a standard IETF protocol (RFC 6455), which enables to have a full-duplex channel between client (i.e. the application) and server (i.e. FRMCS OB GTW). The use of this protocol is still compliant with RESTful architecture. As TCP session stays opened, optional authentication has been done one time.

More accurately, we propose to use “WebSocket over TLS”, that allows to authenticate and optionally encrypt the exchanges between client and server. Authentication between client and server should use certificate exchange (it covers local binding need).

The format of the data used will be JSON, the API could be realized following JSON-RPC v2.0 specifications (https://www.jsonrpc.org/specification).

On FRMCS On-board Gateway, one WebSocket is open per loose coupled application to be managed.

Based on this protocol, it is possible to define control plane part of the OB$_{APP}$ interface for loose coupled applications, as described in chapter 6.2.4.

6.2.4 API version and Websocket URI

In order to allow OB_{APP} client and server to exchange about their supported API version, the major URI version index shall be added at the end of the WebSocket URI.

Hence, the WebSocket URI to be used will have the following format:

- wss://myOBGTW-obapp:port/v0 for a secure Websocket (over TLS)
- ws://myOBGTW-obapp:port/v0 for a non-secure Websocket (first implementation without TLS)

where “myOBGTW-obapp” is the name or IP address of the OBapp interface of the OB_GTW (if a name is used, it shall be taken into account in the DNS used in the train network); and “port” is the listening port for OBapp API interface.

Note: the port to be used are to be confirmed in WP3/4 execution. If standard ports are used (e.g. 443 for WebSocket over TLS), it will not be necessary to indicates the port in WebSocket URI.

6.2.5 Loose coupled interface

This section shall describe the OB_{APP} interface for the loose coupled applications.

6.2.5.1 Functional needs for OB_{app} API in loose mode

In loose mode, OB_{APP} API shall meet to the following needs:

- Authenticate the on-board applications
- Register dynamically the on-board applications
- De-register a registered on-board application
- Establish a session between an on-board equipment (application side) and a trackside equipment (application side), considering the requested communication attributes.
- Find and share the destination IP address to be used to join a trackside equipment (application side).
- Notify the application for incoming communication request
- Notify the application for ending a session
- Provide an end of session service for the applications
- Notify the application about any change of the session status.
- Provide session status on demand
- Provide specific services (e.g. positioning services) on demand

To meet these functional needs, the client (on application side) sends requests to the server (FRMCS OB GTW) and receives answers from it. Besides, the server (FRMCS OB GTW) may send some notifications on its own to the client (application) without any request from the client.

6.2.5.2 Functions for OBapp API in Loose mode

6 functions (request) exposed by FRMCS OB GTW to the application:

- FRMCS_GTW_REGISTER : allow the application to register to the OB GTW.
- FRMCS_GTW_DEREGISTER : allow the application to deregister from the OB GTW
- FRMCS_GTW_SESSION_START : allow the application to request a session establishment to join a trackside equipment.
- FRMCS_GTW_SESSION_END : allow the application to close an established session.
- FRMCS_GTW_SESSION_STATUS : allow the application to ask for a status of a current session.
- FRMCS_GTW_SERVICE_REQUEST: allow the application to ask for some specific FRMCS services, such location services, or connectivity status.

3 functions or notifications are proposed from FRMCS OB GTW to Application:

- FRMCS_APP_INCOMING_SESSION_REQ: OB GTW informs the application that another FRMCS entity wants to establish a session and waits for an answer from the application to accept or reject the session. This is a request (answer needed).
- FRMCS_APP_INCOMING_SESSION_NOTIF : OB GTW informs the application that another FRMCS entity wants to establish a session; this session is accepted by the OB_GTW. This is a notification (no answer needed).
- FRMCS_APP_SESSION_STATUS_CHANGED: OB GTW informs the application that there are some changes on the session status (link failure, quality change, session closed from the other side, …). This is a notification (no answer needed).

Remark: the function FRMCS_APP_INCOMING_SESSION will not be implemented in ETCS FRMCS client, because the sessions are always initiated by the on-board side.

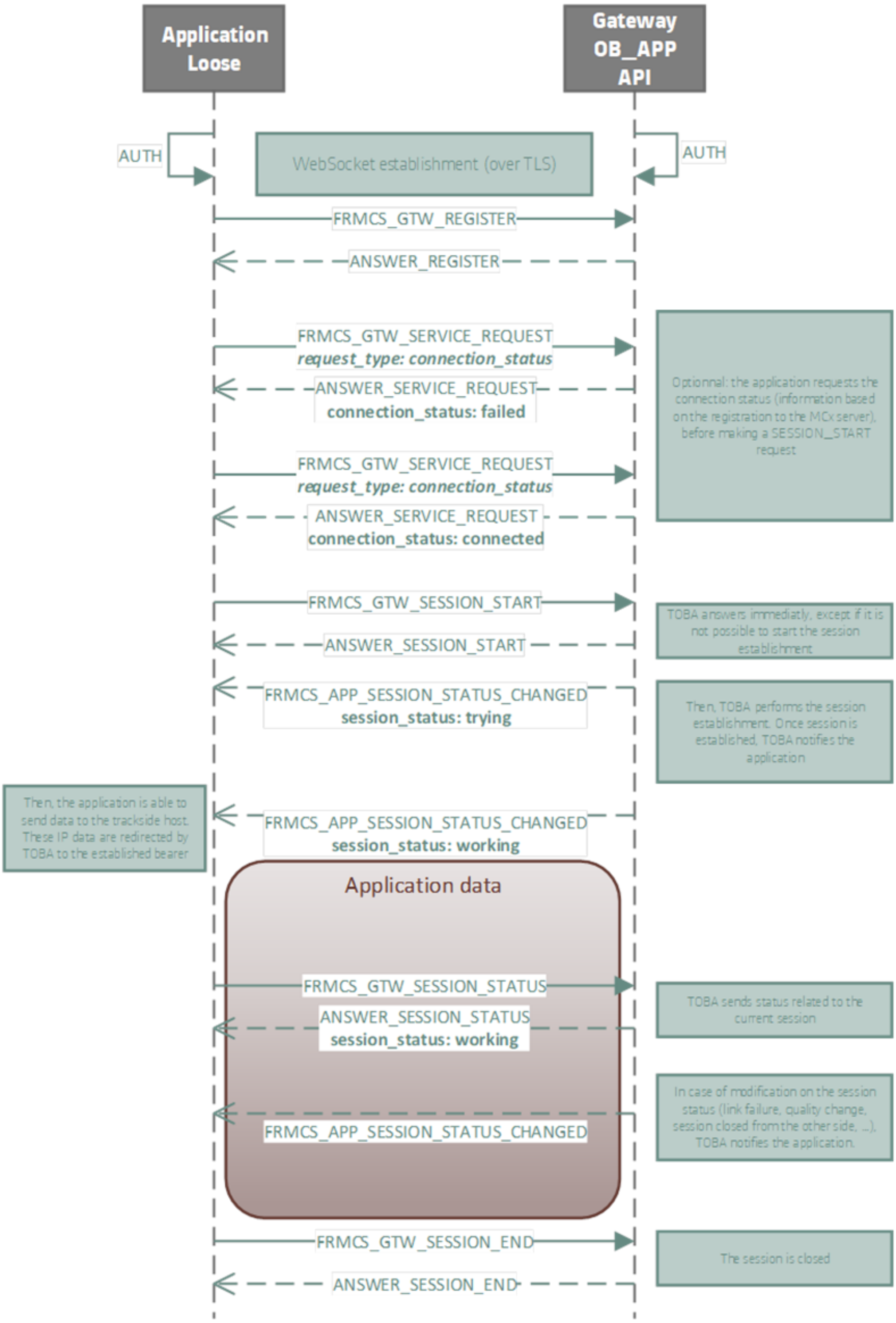

Application Loose
Gateway OB_APP API
AUTH
WebSocket establishment (over TLS)
AUTH
FRMCS_GTW_REGISTER
ANSWER_REGISTER
FRMCS_GTW_SERVICE_REQUEST
request_type: connection_status
ANSWER_SERVICE_REQUEST
connection_status: failed
FRMCS_GTW_SERVICE_REQUEST
request_type: connection_status
ANSWER_SERVICE_REQUEST
connection_status: connected
Optionnal: the application requests the connection status (information based on the registration to the MCx server), before making a SESSION_START request
FRMCS_GTW_SESSION_START
ANSWER_SESSION_START
TOBA answers immediatly, except if it is not possible to start the session establishment
FRMCS_APP_SESSION_STATUS_CHANGED
session_status: trying
Then, TOBA performs the session establishment. Once session is established, TOBA notifies the application
Then, the application is able to send data to the trackside host. These IP data are redirected by TOBA to the established bearer
FRMCS_APP_SESSION_STATUS_CHANGED
session_status: working
Application data
FRMCS_GTW_SESSION_STATUS
ANSWER_SESSION_STATUS
session_status: working
TOBA sends status related to the current session
FRMCS_APP_SESSION_STATUS_CHANGED
In case of modification on the session status (link failure, quality change, session closed from the other side, ...), TOBA notifies the application.
FRMCS_GTW_SESSION_END
ANSWER_SESSION_END
The session is closed

Figure 57: OBapp global exchanges

6.2.5.3 Notation for JSON-RPC protocol

A JSON-RPC request contains the following members:

- jsonrpc: protocol version. Must be equal to “2.0”
- method: name of the function used
- params: JSON object containing the parameters of the request
- id: an ID which allows to link request and answer

The answer of a request contains:

- jsonrpc: protocol version. Must be equal to “2.0”
- result: in case of success of the request, this member contains the results of the request
- error: in case of failed request, this is an object containing:
    - code: integer corresponding to the error code.
    - Message: description of the error
    - Data: additional data relative to the error

In the following chapters, we describe the member “params” for the request, and the members “result” or “error” for the answers.

6.2.5.4 Details of functions

6.2.5.4.1 FRMCS_GTW_REGISTER

Table 28: FRMCS_GTW_REGISTER parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	application_type	Int	Defines the application type Proposal to use an integer as defined in **Appendix 4 – Application type**
	originator_id	String	ID of the host For example with FQDN format: *Ex : <ETCS ID>.<ETCS ID type>*.etcs.frmcs
	mode	String : “loose” or “tight”	Defines the coupling type “loose” or “tight”
	incoming_auto	String: “auto_accept” “auto_reject” “not_auto”	« auto_accept » : the OB_GTW accepts automatically the incoming session without using FRMCS_APP_INCOMING_SESSION_REQ « auto_reject » : the OB_GTW rejects automatically the incoming session without using FRMCS_APP_INCOMING_SESSION_REQ « not_auto » : the OB_GTW uses the function

			FRMCS_APP_INCOMING_SESSION_REQ to ask to the application to accept or reject the incoming session.
ANSWER (success) result	app_uuid	String	The GTW must return a new local ID unique chosen by itself if the request is succeeded. Must be build following RFC4122
ANSWER (failed) error	code	-1	Error code. For error linked to the API OBapp, we will use always -1
	message	“API error”	Message code. For error linked to the API we will use always “API error”.
	data	String	details on the error reason. Example: • Coupling mode not supported for this application • originator_id unknown

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "register",
        "params": {     " originator_id": "host.consist.atc",
                        "application_type": 2,
                        "mode": "loose",
                        "incoming_auto" : auto_accept},
        "id": 1}

<-- {"jsonrpc": "2.0",
        "result": {     "app_uuid": “123e4567-e89b-12d3-a456-426614174000” }
        "id": 1}
Or
<-- {"jsonrpc": "2.0",
        "error": {      "code": -1,
                        “message”: “API error”,
                        "data": “Application already registered”}
        "id": 1}
Or
<-- {"jsonrpc": "2.0",
        "error": {      "code": -1,
                        “message”: “API error”,
                        "data": “Mode not supported for this application”}
        "id": 1}
…/…
```

6.2.5.4.2 FRMCS_GTW_DEREGISTER

Table 29: FRMCS_GTW_DEREGISTER parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	app_uuid	String	See 6.2.4.4.1
ANSWER (success) Result			void
ANSWER	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error. Example : ○ appUID unknown ○ impossible to contact the MCx server to perform the action ○ etc.

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "deregister",
        "params": {
                       "app_uuid": “123e4567-e89b-12d3-a456-426614174000”
        }
        "id": 2}

<-- {"jsonrpc": "2.0",
        "result": { }
        "id": 2}
Or
<-- {"jsonrpc": "2.0",
        "error": {     "code": -1,
                       “message”: “API error”,
                       "data": “app_uuid unknown”}
        "id": 2}
…/…
```

6.2.5.4.3 FRMCS_GTW_SESSION_START

Table 30: FRMCS_GTW_SESSION_START parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	app_uuid	String	See 6.2.4.4.1
	addr	String	ID of the trackside equipment that the application wants to join (FQDN or IP address).
	protocol	Int	Transport protocol used for the UP data of the requested session (TCP, UDP,

			SCTP; use of IP proto integer in the IP header)
	port_dest	Int	Destination port used for the UP data of the requested session
	comm_profile	Int	Communication attributes requested by the application. One of the value in the left column in **10.3**
ANSWER (success) result	session_uuid	String	ID of the session, must be built following RFC4122
	ip_dest	String	IP address to be used by the application as destination address for the user plane data
ANSWER (failed) error	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error. Example : ○ ID_dest impossible to reach ○ No answer from the destination ○ appUUID unknown ○ comm_profile incorrect

Example:

```
--> {   “jsonrpc”: “2.0”,
        “method”: “session_start”,
        “params”: {     “app_uuid”: “123e4567-e89b-12d3-a456-426614174000”,
                        “addr”: “id031123.ty01.etcs”,
                        “protocol”: 6,
                        “port”: 5678,
                        “comm_profile”: 10      }
        “id”: 3}

<-- {“jsonrpc”: “2.0”,
        “result”: {     “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”}
                        “ip_dest”: “172.16.1.20” }

        “id”: 3}
Or
<-- {“jsonrpc”: “2.0”,
        “error”: {      “code”: -1,
                        “message”: “API error”
                        “data”: “unknown app_uuid”
                }
        “id”: 3}
When the session in established, notification sent to the application:
<-- {“jsonrpc”: “2.0”,
        "method": "session_status_changed",
        "params": {     “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”,
                        “session_status”: “working”
                }
        }
…/…
```

6.2.5.4.4 FRMCS_GTW_SESSION_END

Table 31: FRMCS_GTW_SESSION_END parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	app_uuid	String	See 6.2.4.4.1. Get during REGISTER
	session_uuid	String	Session ID get during session establishment
ANSWER (success) result			void
ANSWER (failed) error	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error. Example : ○ session_uuid not known ○ app_uuid unknown

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "session_end",
        "params": {     "app_uuid": “123e4567-e89b-12d3-a456-426614174000”,
                        “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”   }
        "id": 4}

<-- {"jsonrpc": "2.0",
        "result": {     }
        "id": 4}
Or
<-- {“jsonrpc”: “2.0”,
        “error”: {      “code”: -1,
                        “message”: “API error”
                        “data”: “unknown app_uuid”
        “id”: 4}
…/…
```

6.2.5.4.5 FRMCS_GTW_SESSION_STATUS

Table 32: FRMCS_GTW_SESSION_STATUS parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	app_uuid	String	See 6.2.4.4.1. Get during REGISTER
	session_uuid	String	Session ID get during session establishment
ANSWER (success) result	status	String	See session state diagram in chapter 5.2.2.4.7.
	details	String	Additional details on the status.

ANSWER (failed) error	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error. Example : ○ session_uuid not known for this app_uuid ○ app_uuid unknown

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "session_status",
        "params": {     "app_uuid": “123e4567-e89b-12d3-a456-426614174000”,
                        “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”   }
        "id": 5}

<-- {"jsonrpc": "2.0",
        "result": {     "status": "working",
                        "details": “ras”}
        "id": 5}
Or
<-- {"jsonrpc": "2.0",
        “error”: {      “code”: -1,
                        “message”: “API error”
                        “data”: “unknown app_uuid”
                }

        "id": 5}
…/…
```

6.2.5.4.6 FRMCS_GTW_SERVICE_REQUEST

Table 33: FRMCS_GTW_SERVICE_REQUEST parameters

REQUEST/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
REQUEST params	app_uuid	String	See 6.2.4.4.1. Get during REGISTER
	request_type	String: “connection_status” “gnss”	Define the request: • “connection_status”: ask for a state of connection to FRMCS services • “gnss”: request for gnss positioning (not implemented for 5GRAIL)
ANSWER (success) result	connection_status	String	If request_type= connection_status State of the connection to the FRMCS service for the application: • « connected » : if MCx client connected to MCx services and MCx server is reachable • « failed » otherwise

	gnss_position	String	Not implemented for 5GRAIL
ANSWER (failed) error	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error. Example : ○ app_uuid unknown

```
Example :--> {   "jsonrpc": "2.0",
        "method": "service_request",
        "params": {     "app_uuid": "123e4567-e89b-12d3-a456-426614174000",
                        "request_type": "connection_status"    }
        "id": 6}

<-- {"jsonrpc": "2.0",
        "result": {     "connection_status": "connected" }
        "id": 6}
Or
<-- {"jsonrpc": "2.0",
        "error": {      "code": -1,
                        "message": "API error"
                        "data": "unknown app_uuid"}
        "id": 6}
…/…
```

The connection status returned by this function can have 2 different values : ”failed” and “connected”.

The “connected” status is reached once the radio is available, that means that at least one modem is available and the MCx service is also available, as described in figure below:

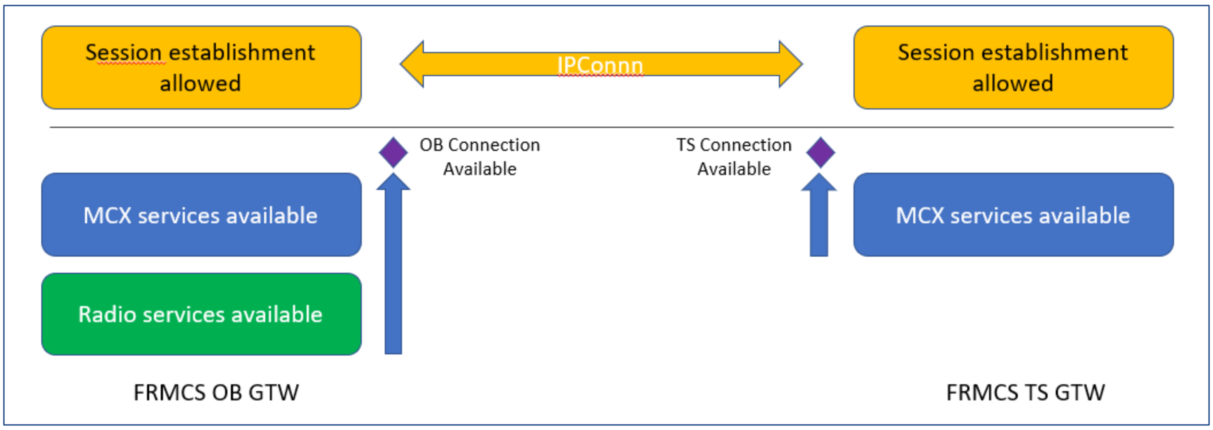


Figure 58: Connection Status management

6.2.5.4.7 FRMCS_APP_INCOMING_SESSION_REQ (OB_GTW --> APPLICATION)

Table 34: FRMCS_APP_INCOMING_SESSION parameters

NOTIFICATION/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
	session_uuid	String	Session ID for the incoming session

REQUEST params	source	String	ID of the caller. For example an FQDN Ex : id4572.ty01.etcs
	ip_src	String	IP address to be used for the user plane
ANSWER (success) result	return	String: “ok” “nok”	ok : the application accepts the session nok : the application rejects the session
ANSWER (failed) error	code	-1	code error
	message	“API error”	Message error
	data	String	details about the error

After a certain time without answer, the OB GTW shall consider that the session is rejected.

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "incoming_session_req",
        "params": {     “session_uuid”: “a458b45c5-a458b45c5”,
                        “source”: “id031123.ty01.etcs”,
                        “ip_src”: “172.16.20.1”
                        }
        "id": 1}

<-- {"jsonrpc": "2.0",
        "result": {     "return": "ok"  }
        "id": 1}

…/…
```

6.2.5.4.8 FRMCS_APP_INCOMING_SESSION_NOTIF (OB_GTW --> APPLICATION)

Table 35: FRMCS_APP_SESSION_STATUS_SESSION_NOTIF

NOTIFICATION/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
NOTIFICATION params	session_uuid	String	Session ID for the incoming session
	source	String	ID of the caller. For example an FQDN Ex : id4572.ty01.etcs
	ip_src	String	IP address to be used for the user plane
ANSWER	No answer (this is a notification)		

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "incoming_session_notif",
        "params":{      “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”,
                        “source”: “id031123.ty01.etcs”,
                        “ip_src”: “172.16.20.1”
                        }
}
```

```
…/…
```

6.2.5.4.9 FRMCS_APP_SESSION_STATUS_CHANGED (OB_GTW --> APPLICATION)

Table 36: FRMCS_APP_SESSION_STATUS_CHANGED parameters

NOTIFICATION/ ANSWER	NAME OF THE PARAMETER	TYPE AND POSSIBLE VALUES	COMMENTS
NOTIFICATION params	session_uuid	String	Session ID get during session establishment
	session_status	String	See session state diagram in **5.2.2.4.7**
	details	String	Additional details on the status.
ANSWER	No answer (this is a notification)		

Example:

```
--> {   "jsonrpc": "2.0",
        "method": "session_status_changed",
        "params":{      “session_uuid”: “9816177b-7447-415e-8de9-
78f5b19f091c”,
                        “session_status”: “failed”,
                        “details”: “radio link not available”}}
…/…
```

6.2.5.5 Additional proposal for the flat IP only approach

It is proposed to manage applications in flat IP only approach as an adapted part of loose mode described in this chapter.

Especially, the session for the flat IP only approach may be statically configured in FRMCS OB GTW. In other words, FRMCS OB GTW will establish and manage the session for this application as soon as FRMCS OB GTW is powered up. The application would not be able to use other session than the ones statically configured in FRMCS OB GTW. Thus, from the application view, it consists in IP routing to hosts (or LANs) statically configured.

Example:

Considering an on-board application which is in flat IP only approach (it is not able to call OB$_{APP-LOOSE}$ API functions).

In FRMCS OB GTW static configuration, we would have the information related to the camera itself ((identified by its IP, optionally its MAC address), and the information related to the trackside server to be joined (static IP address, or FQDN to be solved). Then, when FRMCS OB GTW is switched on, automatically it establishes a bearer (i.e. open a session) toward this trackside server and redirect IP flows from this (or these) camera(s) to this established bearer. It is like this application have triggered

FRMCS_GTW_REGISTER and FRMCS_SESSION_START functions, but the input parameters of these functions are statically configured in FRMCS OB GTW.

6.2.5.6 User plane management in loose coupled mode

To manage user plane interface with the loose-coupled application, the OB GTW should expose an IP interface with an IP gateway address that can be used by the application to send data to trackside.

One aim of the control plane functions defined in **6.2.4.4** is to dynamically configure the on-board gateway to redirect user plane data (coming from the application) to the relevant established tunnel.

More details about the user plane management by the on-board gateway are given in chapter 5.

6.2.6 Tight coupled interface

This section shall describe the OB_{APP} interface for the tight coupled applications.

6.2.6.1 Functional needs for OB_{APP} API in tight mode:

In the tight mode, OB_{APP} API shall meet to the following needs:

- Register an on-board application
- Deregister a registered on-board application
- Provide specific service (e.g. positioning services or connectivity status) on demand

6.2.6.2 Functions for OB_{APP} API in tight coupled mode

The following functions (request) shall be exposed by FRMCS OB GTW to the application:

- FRMCS_GTW_REGISTER : allows the application to register to the OB GTW.
- FRMCS_GTW_DEREGISTER : allows the application to deregister from the OB GTW
- FRMCS_GTW_SERVICE_REQUEST: allows the application to ask for some specific FRMCS services, such location services, or connectivity status.

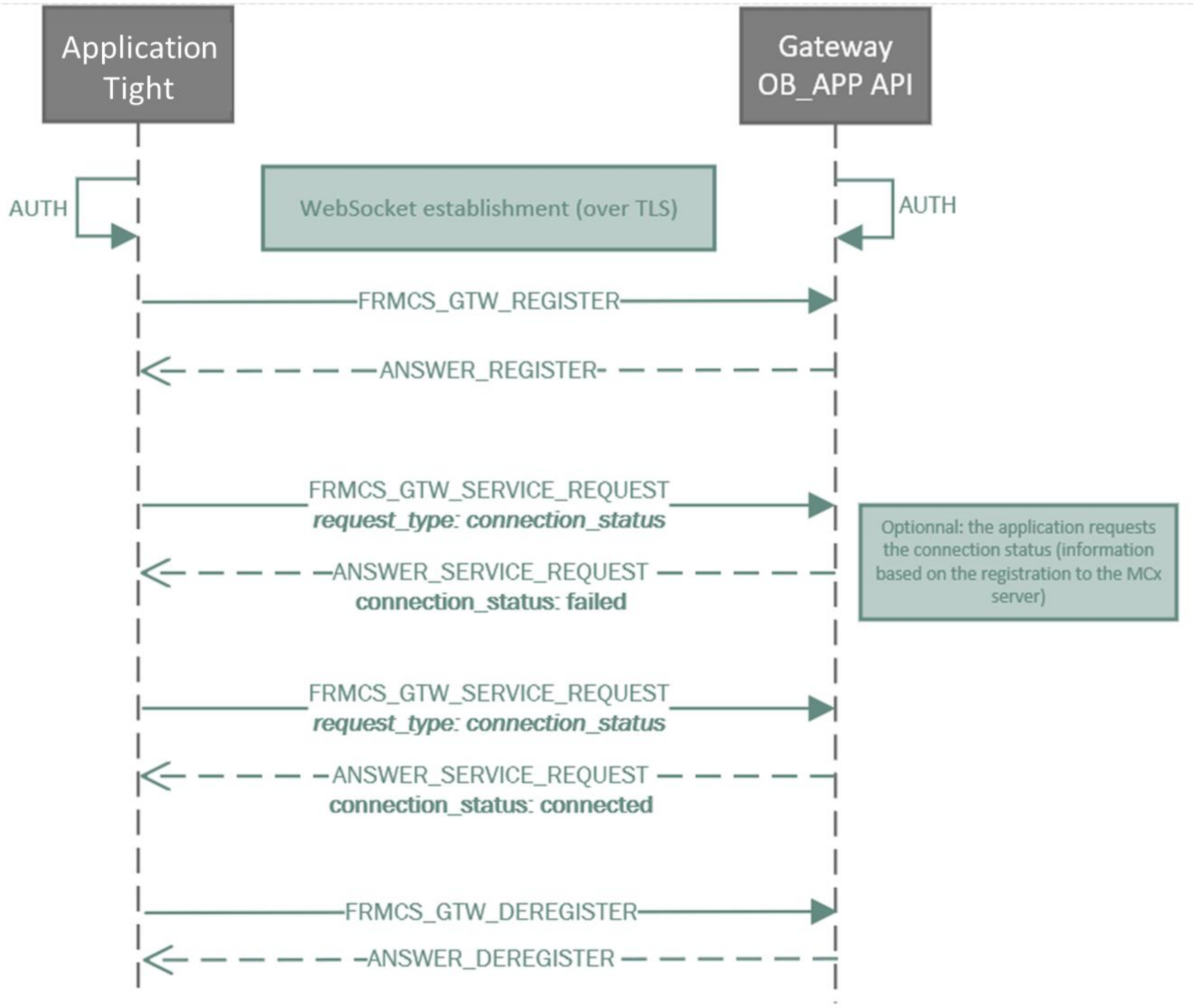

Application Tight
Gateway OB_APP API
AUTH
WebSocket establishment (over TLS)
AUTH
FRMCS_GTW_REGISTER
ANSWER_REGISTER
FRMCS_GTW_SERVICE_REQUEST
request_type: connection_status
ANSWER_SERVICE_REQUEST
connection_status: failed
Optionnal: the application requests the connection status (information based on the registration to the MCx server)
FRMCS_GTW_SERVICE_REQUEST
request_type: connection_status
ANSWER_SERVICE_REQUEST
connection_status: connected
FRMCS_GTW_DEREGISTER
ANSWER_DEREGISTER

Figure 59: OB$_{APP}$ global exchanges in tight coupled mode

6.2.6.3 Details of functions

6.2.6.3.1 FRMCS_GTW_REGISTER

Same API definition than for Loose coupling, see chapter **6.2.5.4.1**

6.2.6.3.2 FRMCS_GTW_DEREGISTER

Same API definition than for Loose coupling, see chapter **6.2.5.4.2**

6.2.6.3.3 FRMCS_GTW_SERVICE_REQUEST

Same API definition than for Loose coupling, see chapter **6.2.5.4.6**.

6.2.6.4 User plane management in tight coupled mode

The user plane in a tight coupled voice application is responsible for carrying audio network traffic between on-board and trackside clients. This is using the available radio modems and through the established bearers. It is based on the 3GPP MCx framework. This will be managed by the FRMCS On-Board System which will acts as a proxy. The proxying function is based on a SIP Proxy (as defined in RFC 3261). The proxy mode will be stateless.

6.3 TS$_{APP}$ interface

This paragraph shall contain the TS$_{APP}$ interface description.

6.3.1 Functions

Table 37: TS$_{APP}$ functions

FUNCTION	TIGHT	LOOSE	REQUESTER	PROVIDER	OUTCOME
TS Identification and authentication Request		X	Application	Gateway	Waiting for FRMCS OB GTW response
TS Identification and authentication Response		X	Gateway	Application	Allow session creation
TS Initiating a communication service request		X	Application	Gateway	Waiting for FRMCS OB GTW response
TS Accepting a communication service request from TS application		X	Gateway	Application	Allow data transfer
TS Rejecting a communication service request from TS application		X	Gateway	Application	Close the requested communication session
TS Ending an established communication service		X	Application	Gateway	Close the requested communication session

TS Release association (power down)		X	Application	Gateway	Close the association
TS Incoming communication Request		X	Gateway	Application	Waiting incoming communication response
TS Accepting incoming communication		X	Application	Gateway	Allow data transfer
TS Rejecting incoming communication		X	Application	Gateway	Close the requested communication session

6.3.2 Physical interface

This section shall contain description of the physical interface for the TS_{APP} interface.

Same as OB_{APP}, please see chapter 6.2.2

6.3.3 Protocol stack

This section shall contain the description of the protocol stack for the TS_{APP} interface for control and user planes.

- For the tight coupled applications:

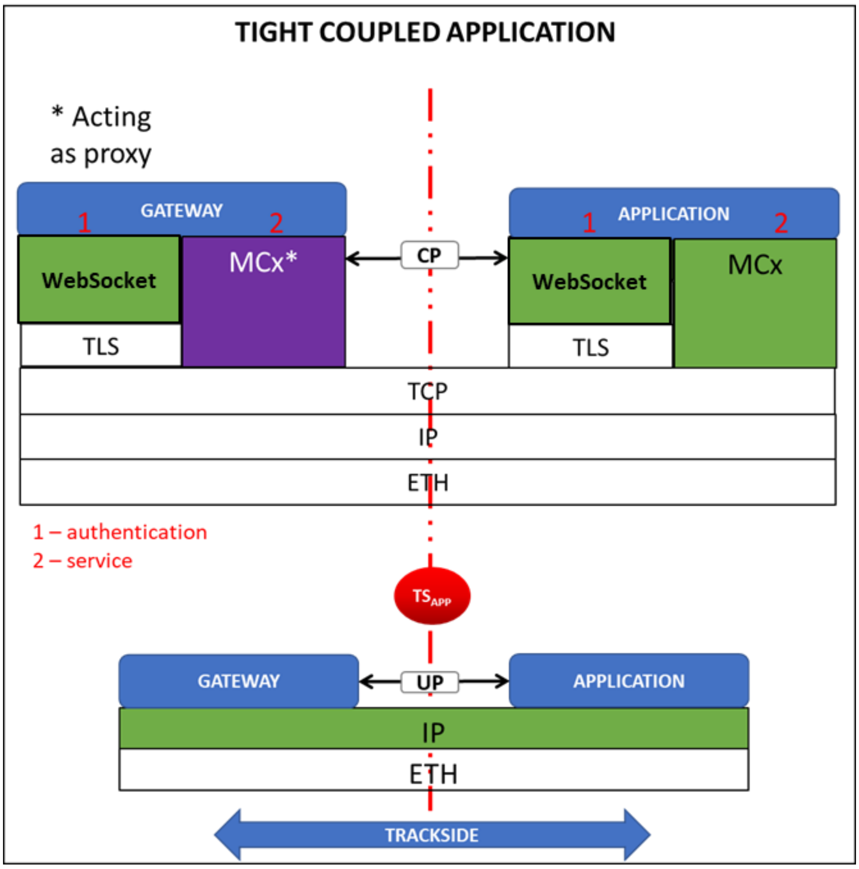


Figure 60: Tight coupled application TS$_{APP}$ protocol stack

The control plane for the tight coupled applications is based on the MCx framework as described in chapter 6.3.5.

As part of the 5GRail project, there is no connection between the Dispatcher (tight coupled application) and the FRMCS TS GW through the TS$_{APP}$.

- For the loose coupled applications:

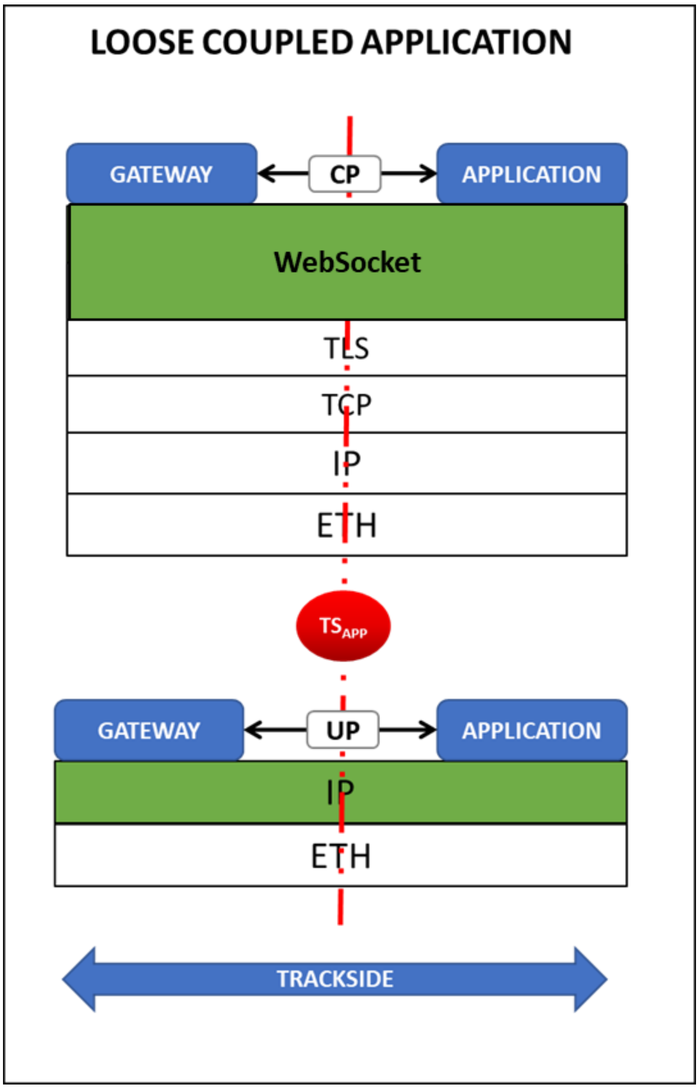


Figure 61: Loose coupled application TS$_{APP}$ protocol stack

Same functions as OB$_{APP}$, please see chapter 6.2.3.

6.3.4 Loose coupled interface

This section shall describe the TS$_{APP}$ interface for the loose coupled applications.

Same functions as OB$_{APP}$, please see chapter 6.2.4.

6.3.5 Tight coupled interface

The Dispatcher (thigh coupled application) is not connected to the GW through the TS$_{APP}$, but directly connected to the MCx Server.

7 Applications

7.1 ALSTOM ETCS

7.1.1 APPLICATION ARCHITECTURE PROPOSAL

7.1.1.1 Architecture Overview

Figure below gives an overview of on board and trackside ETCS applications.

Basically, the n board applications are:

- Safe application (position reports, etc.),
- Non-safe applications (KMC client for key management, RMR client for remote maintenance and PKI client for cyber security aspects).

These applications communicate with trackside equipment thanks to an internal software component called CFM (Communication Functional Module), which is interfaced with on board FRMCS GTW.

From point of view of OBapp interface, CFM is the only one ETCS application, forwarding safe or non-safe messages. Safe and non-safe messages may have a different priority on network (corresponding to a different QoS), which is specified during session opening. A session corresponds either to a safe or to a non-safe communication.

To summarize, there is one on-board ETCS application, called CFM, which is in charge to exchange safe and non-safe messages with different priorities.

On the other hand trackside applications are:

- RBC (movement authorities, etc.),
- KMC server (for key management),
- RMR server (for remote maintenance),
- PKI server (for cyber security aspects).

Note: RBCs are not reachable directly from network: NTG (Network Transmission Gateway) is interfaced with trackside FRMCS TS_GTW, and communicates with each RBC following RBC identifier present in application layer. NTG is an ALSTOM device which is equivalent to “CFM trackside” specified in Subset 037-2.

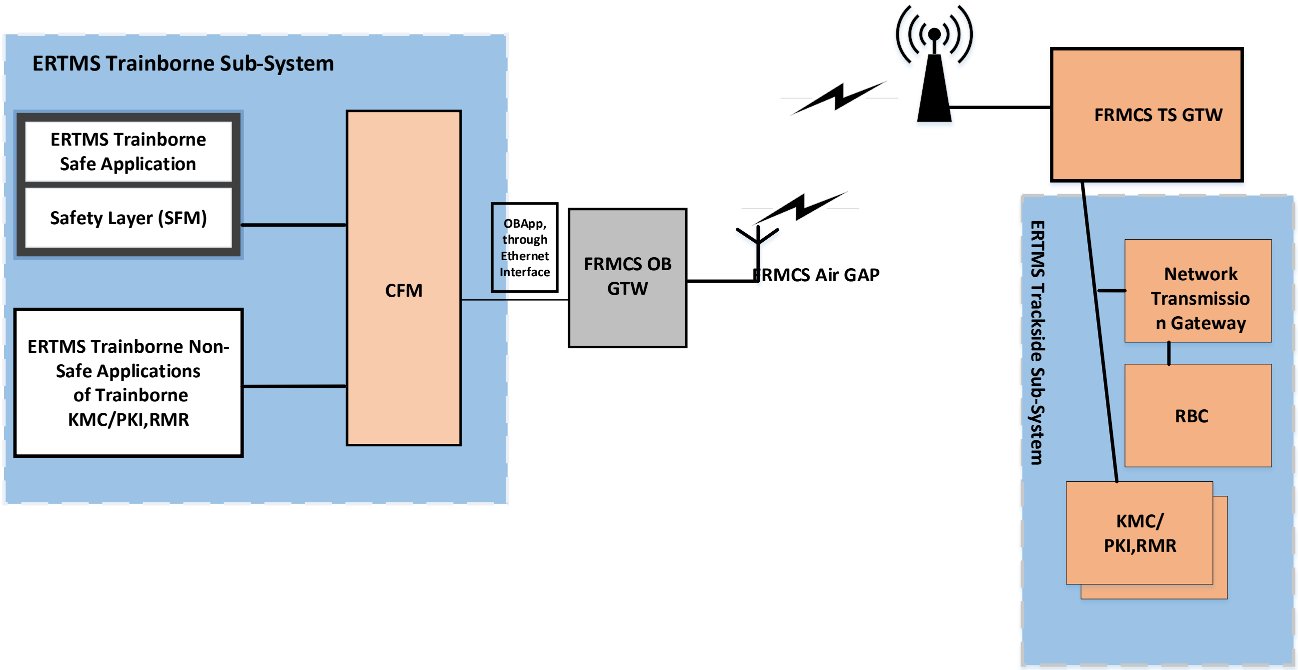

ERTMS Trainborne Sub-System
ERTMS Trainborne Safe Application
Safety Layer (SFM)
ERTMS Trainborne Non-Safe Applications of Trainborne KMC/PKI,RMR
CFM
OBApp, through Ethernet Interface
FRMCS OB GTW
FRMCS Air GAP
FRMCS TS GTW
ERTMS Trackside Sub-System
Network Transmission Gateway
RBC
KMC/ PKI,RMR

Figure 62: ETCS system architecture with both on board and track side parts

Only CFM component will communicate with FRMCS OB_GTW, and it will be considered as unique ETCS application (safe and non-safe applications are not visible for OB_GTW). Safe and non-safe may initiate communications with trackside, with different priorities, but in both cases, only interface with FRMCS OB GW managing OBapp is CFM. Moreover, for FRMCS use case, network is fully managed by FRMCS system (in opposite of GSM-R/GPRS use case).

FRMCS OB_GTW will take care of all the network-related aspects (transparent handling of different mobile radio/access technologies, transparent handover during border crossing events, etc.) that are necessary to guarantee the communication among the ETCS application endpoints. ETCS application is not MCx aware, therefore FRMCS service client is managed by FRMCS gateway (no need to implement either MCx or SIP client at ETCS level)

ETCS on-board and trackside interfaces to OB_GTW and TS_GTW shall be based on IPv4 communication.

On a complete architecture, there are 2 CFMs components which are redounded, but only one CFM communicates at a time with FRMS OB_GTW. On the other side, if FRMCS OB_GTW is redounded, it shall be transparent to ETCS application (through a virtual IP address for example). Bearer type and modem used by FRMCS OB_GTW shall also be transparent for ETCS application.

7.1.1.1.1 START-UP SEQUENCE

At start-up, following steps are executed by both CFM components which are redounded:

- An autotest is executed by each CFM (part of EVC which hosts ETCS application) to check that link between EVC and FRMCS OB_GTW is working properly. FRMCS OB_GTW shall be present on Ethernet link, and it shall answer to a request from ETCS application when it is ready to communicate through OBApp interface. Autotest are achieved sequentially on each CFM component (CFM1 executes its autotest, and when it is finished, CFM2 executes its one).

- When auto tests are finished on both CFM components, one CFM instance becomes MASTER, and the other one becomes SLAVE. This selection is achieved following the results of the autotests, and through an arbitrary criterium (alternance at each start-up) if results are identical on both CFM components.
- Then, only MASTER CFM will communicate with FRMS OB_GTW through OBApp interface.
- Right after the MASTER election, a periodic polling is executed by MASTER CFM (even out of any communication sessions) to ensure that:
  - Link between EVC and FRMCS OB_GTW link is still healthy,
  - Onboard trackside communication is possible (FMRCS OB_GTW registered to the FRMCS network and ready to handle any ETCS communication request).

7.1.1.1.2 COMMUNICATION ESTABLISHMENT

When a safe or non-safe application requests a connection to a trackside device, CFM forwards requests to FRMCS OB_GTW only if OB_GTW is able to communicate (i.e. attached to FRMCS network, following polling result). Else corresponding safe or non-safe application is informed, and request is refused. No communication requests is sent to OB_GTW.

Communication requests may have a different priority (or profile) following safe or non-safe source. On the assumption that all the ETCS communications can be multiplexed on any of the available FRMCS resources, there is no internal management of priority in CFM component (in opposite of GSM-R/GPRS use case). Only corresponding profile (to set priority) is sent to OB_GTW.

Concerning trackside devices, they are identified through:

- IP address: it may be identical for several devices (e.g. RBCs) or different.
- Port: it may be fixed for several devices (e.g. 7911 for all RBCs), or different.

Several simultaneous communications (safe and non-safe) may be established by ETCS application. For 5G Rail project, only safe communication with trackside RBC will be taken into account to simplify deployment (particularly to avoid use of TLS and PKI deployment for non-safe communications).

Concerning communication establishment, sequence is following one:

- Safe application requests a communication with an identifier of RBC (RBC id).
- CFM uses RBC id to get an IP address from FRMCS OB_GTW (e.g. by building a FQDN).
- IP address is used to open communication with trackside device.
- Communication is ended by ETCS application when it is no longer needed.

In nominal case, ETCS application needs to manage hand over of RBC:

- A communication is established with RBC A.
- Another communication is established with RBC B (at border crossing for example)

- Communication with RBC A is closed by ETCS application.
- RBC A and RBC B may be on same network, or on different networks but it is not visible by ETCS application (it is managed by FRMCS system).

A TCP connection is directly established between CFM component and trackside device. This TCP connection is monitored with a user timeout. So, use of proxy will impact this mechanism (a monitoring is necessary from end to end).

7.1.1.1.3 PERFORMANCES

This chapter will be completed later with expected performances concerning bandwidth, various, timeouts and so on.

At most, 6 simultaneous communications may be established by ETCS application.

7.1.1.2 Hardware Platform

In case of ETCS, hardware supporting on board applications has no impact on OBApp interface. Indeed, communication with on board FRMCS GTW is achieved through Ethernet link. Figure below describes the whole ETCS system using simulator.

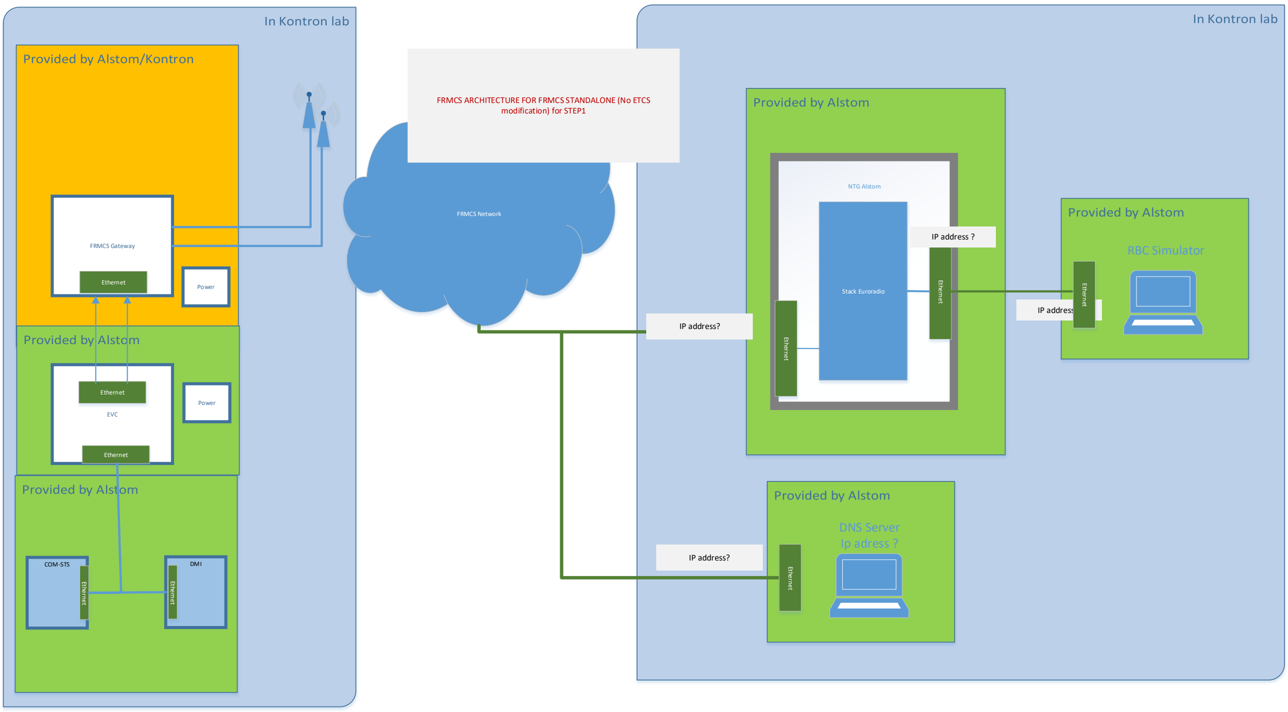


Figure 63: ETCS system using simulator

7.1.1.3 Software Platform

ETCS applications are split into different products with different languages and OS (Ada language, Linux…) but software architecture has no impact on OBApp interface because communication with on board FRMCS GTW is achieved through Ethernet link.

7.1.1.4 Simulators (if applicable)

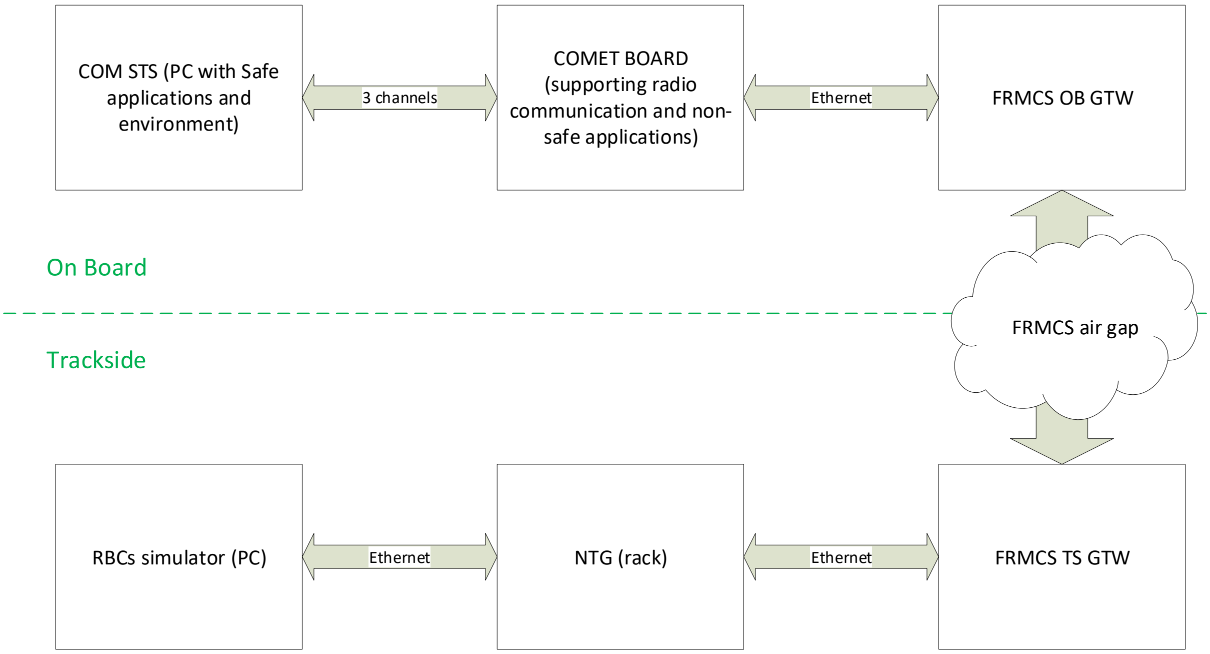

COM STS (PC with Safe applications and environment)
3 channels
COMET BOARD (supporting radio communication and non-safe applications)
Ethernet
FRMCS OB GTW
On Board
Trackside
FRMCS air gap
RBCs simulator (PC)
Ethernet
NTG (rack)
Ethernet
FRMCS TS GTW

Figure 64: Overview of simulators

7.1.1.4.1 ON BOARD SIMULATOR

COM STS (Single Train Simulator) simulates on board ETCS applications as well as trackside balises information (packets). It executes safe applications above COMET board which is hosted, either in EVC rack or in COMET Tool. COMET board is interfaced with FRMCS OB GTW through OBApp.

7.1.1.4.2 TRACKSIDE SIMULATOR

For trackside part, NTG (equivalent to CFM, i.e. in charge of IP, TCP and ALE layers) is interfaced with FRMCS TS GTW through IP addressing only (There is no implementation of TSapp in Loose or Tight mode for the trackside simulator). A PC, connected to NTG through Ethernet, allows simulating RBCs.

Note: if TLS is included in CFM as specified in Subset 037-3 (EuroRadio FIS - FRMCS Communication Functional Module), NTG shall be also modified. Impact is strong and it has not been planned.

7.1.2 INTERFACES

7.1.2.1 Interface to FRMCS OB_GTW via OB$_{APP}$

This subsection shall provide a full explanation of the interface to FRMCS OB_GTW via OB$_{APP}$ using the following coupling approaches:

- Loose approach

6functions (requests) exposed by FRMCS OB GTW to the application:

- FRMCS_GTW_REGISTER : allow the ETCS application to register to the FRMCS OB_GTW . This method is called only once (by CFM on board application, which manages both safe and non-safe messages).
- FRMCS_GTW_DEREGISTER : allow the ETCS application to deregister from the FRMCS OB_GTW
- FRMCS_GTW_SESSION_START : allow the ETCS application to request a session establishment to join a trackside equipment (RBC).
- FRMCS_GTW_SESSION_END : allow the ETCS application to close an established session.
- FRMCS_GTW_SESSION_STATUS : allow the ETCS application to ask for a status of a current session.
- FRMCS_GTW_SERVICE_REQUEST: allows the application to ask for some specific FRMCS services, such as connection status

One function (notification) is proposed from FRMCS OB GTW to ETCS application:

- FRMCS_APP_SESSION_STATUS_CHANGED: FRMCS OB_GTW informs the ETCS application that there are some changes on the session status (link failure, quality change, session closed from the other side, …) This notification is necessary and supported by CFM.

Note: notification may be optional and activated during register or session start for example.

Please refer to chapter concerning OBApp interface for more details.

- Tight approach is not applicable to ETCS application.

7.1.2.2 Interface to FRMS TS_GTW via TS$_{APP}$

This subsection shall provide a full explanation of the interface to FRMCS TS_GTW via TS$_{APP}$ using the following coupling approaches:

- Flat IP approach (Alstom proposal)

NTG equipment communicates only in IP mode with TS GTW.

Control plane is managed internally and autonomously by TS GTW (transparent for ETCS trackside applications) :

- Alias for RBC statically configured and translated into MC ID in FRMCS GTW (no registering by NTG). For example : id031123.ty01.etcs
- Authentication, registration, authorization to the IMS/MCx server with this MC ID
- Session is automatically accepted by TS GTW without any interaction with NTG.

ETCS trackside applications are directly connected in user plane mode.

- Loose approach is not applicable to ETCS trackside application.
- Tight approach is not applicable to ETCS application.

7.1.3 INTERWORKING WITH GSM-R

Implemented in later stage (step 3).

EDOR connected with ETCS application. Implemented during step 3 (interworking with GSM-R/GPRS).

When GSM-R/GPRS network Is used instead of FRMCS network, network management is achieved by ETCS application (network scan, network selection, and network registration). GSM-R/GPRS principle is completely different from FRMCS principle. Modem is also directly managed by ETCS application through AT commands.

7.2 CAF ETCS & TCMS

This chapter describes the TCMS and ETCS deliverables from CAF

7.2.1 ARCHITECTURE PROPOSAL

This section shall contain a description of the application architecture including the following subsections if applicable.

7.2.1.1 Architecture Overview

7.2.1.1.1 GENERAL TCMS AND ETCS

The overall architecture used in CAF for both TCMS and ETCS deployments can be seen in the Figure below:

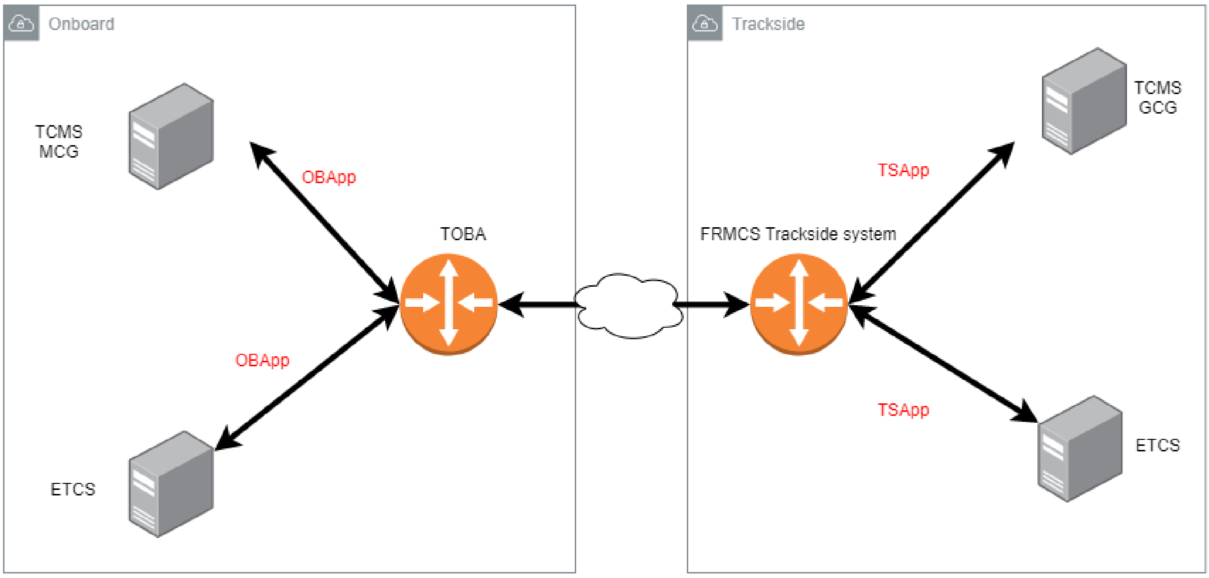


Figure 65: Overall TCMS and ETCS architecture

As it can be seen, the main focus is on the implementation of OBapp and its counterpart TSApp in the trackside for both TCMS and ETCS applications and its interaction with the FRMCS infrastructure.

For implementation purposes, and before the testing in the lab environment starts, CAF proposes to connect to the TOBA/Trackside counterpart prototype via VPN between KONTRON/NOKIA labs and the applications. This could provide some preliminary validations of both TCMS and ETCS applications prior to the lab testing.

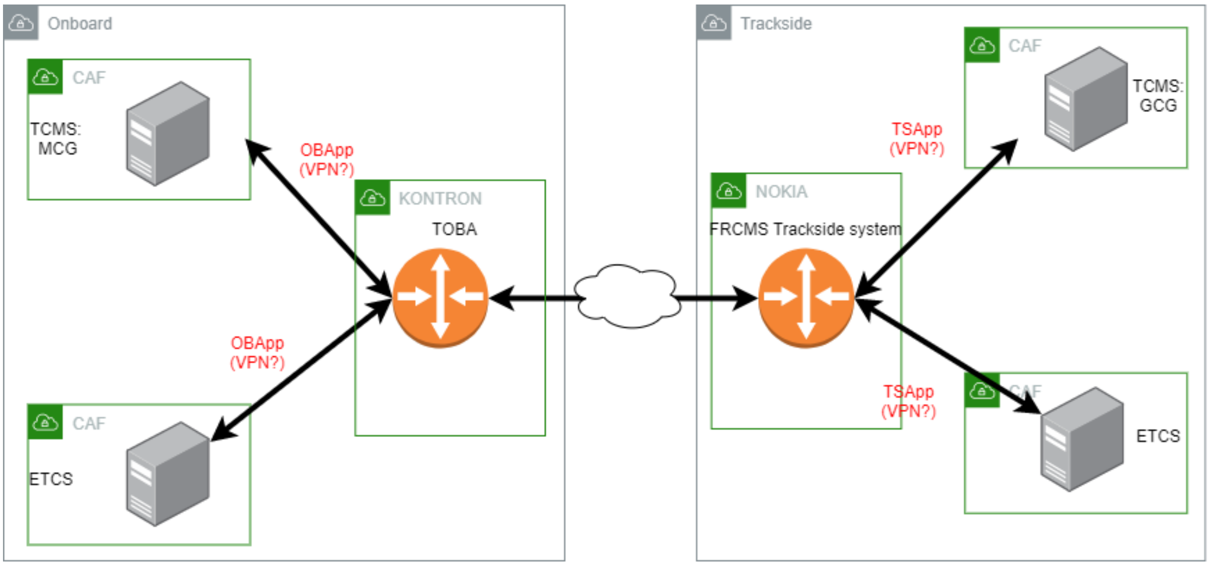


Figure 66: Proposed architecture for implementation testing environment

7.2.1.1.2 TCMS SPECIFIC ARCHITECTURE

For the TCMS case specifically the following architecture will be used to interact with the FRCMS system:

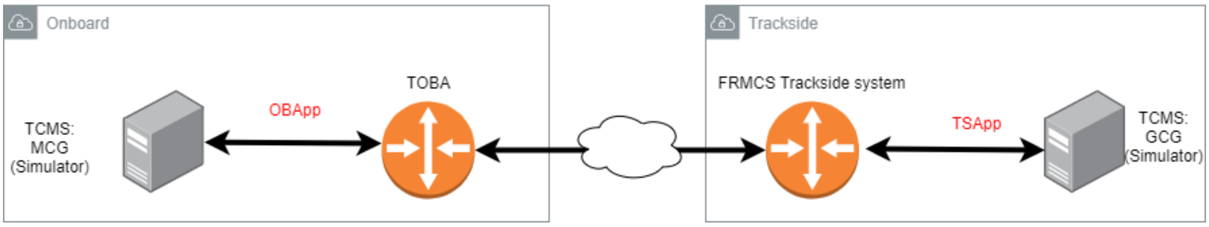


Figure 67: Overall TCMS architecture

As it can be seen, on the onboard side, the TCMS application consists of one simulated Hardware (potentially a laptop) with a software which simulates the TCMS Mobile Communication Service (MCG) according to IEC 61375-2-6 [01] standard. This MCG will interact with TOBA using the OBApp interface.

On the trackside side, the TCMS application has its counterpart with a similar setup which consists of a simulated Hardware (potentially a laptop) with a software which simulates the TCMS Ground Communication Service (GCG) according to IEC 61375-2-6 [01] standard. The Trackside will potentially contain additional supporting deployments such as a (s)FTP server and MQTT broker to fill with the use cases described in WP1 which will be based on the services described in the IEC 61375-2-6 [01] standard.

7.2.1.1.3 ETCS SPECIFIC ARCHITECTURE

For the ETCS case specifically the following architecture will be used to interact with the FRCMS system:

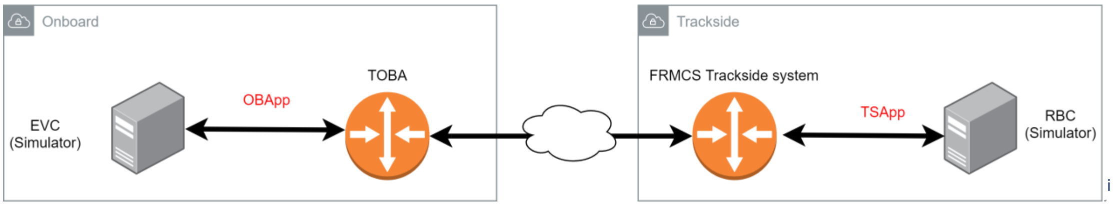


Figure 68: Overall ETCS architecture - detailed

As it is depicted in the diagram, the overall architecture could be separated in two. On one hand, the EVC simulator is located on the on-board part. This EVC simulator will contain the protocol stack defined in UNISIG SS037 [02] adapted to the OBApp interface, in order to be able to communicate with the TOBA. On the other side, the RBC simulator will be the trackside counterpart which will be symmetric to the EVC implementation (also implementing the protocol stack defined by UNISIG). Communication will be unidirectional from EVC to RBC as specified in SS026 [03].

7.2.1.2 Hardware Platform

7.2.1.2.1 TCMS AND ETCS APPLICATIONS

On the application side, the Hardware used on both applications is independent and are provided by CAF. This Hardware potentially will be an independent laptop which will simulate either TCMS or ETCS applications. Same will apply to its counterpart in the Trackside.

7.2.1.2.2 TCMS APPLICATION

For the TCMS specific case, both MCG and its counterpart in the Trackside, the GCG (simulated) are expected to run in a simulated HW (potentially a laptop) assuming that the objective of the tests is the validation of the interface of the application with the FRMCS and there is not much added value on having a real HW for the tests.

7.2.1.2.3 ETCS APPLICATION

With respect to the hardware, both entities (EVC and RBC simulator) are expected to run in a simulated HW (most probably a PC), assuming that the objective of the tests are the validation of the interface and End-To-End solution, and there is not much added value of using a real Safety HW.

7.2.1.3 Software Platform

7.2.1.3.1 TCMS APPLICATION

The SW will be a simulator for both onboard (MCG) and trackside (GCG) applications. In overall, the TCMS applications are divided in three groups (according to IEC 61375-2-6 [01]):

- On-train telemetry data streaming: Using Telemetry Service of the standard which is based on MQTT protocol to send the variables needed for various applications such as passenger count.
- Equipment control: Using the Train Wake-Up service of the standard based on HTTP(s) message interchange to initiate power-up sequences on the train.
- File data Transfer: Using the File Transfer service of the standard to upload a file from the train to ground (using (s)FTP or HTTP(s)) for data analytics of for example energy consumption via transferring energy metering files.

7.2.1.3.2 ETCS APPLICATION

As stated in 7.2.1.1.3, the EVC simulator will contain the protocol stack defined in UNISIG SS037 [02] adapted to the OBApp interface, in order to be able to communicate with the TOBA. On the other side, the RBC simulator will be the trackside counterpart which will be symmetric to the EVC implementation (also implementing the protocol stack defined by UNISIG). Communication will be unidirectional from EVC to RBC as specified in SS026 [03].

On top of both applications, CAF Signalling ETCS Simulators will contain a pattern-based traffic generator as well as a QoS parameter monitorization tool. This way, the simulators will be able to not only validate, but to demonstrate the performance of the End-To-End solution.

7.2.1.4 Simulators (if applicable)

This subsection shall provide an overview of the simulators.

7.2.1.4.1 TCMS SIMULATOR

As stated 7.2.1.2.2 and 7.2.1.3.1, both HW and SW will be simulated. The HW will potentially be a laptop or a PC with a Linux installed and the SW will be a MCG onboard and a counterpart GCG on the trackside according to IEC 61375-2-6 [01] specification.

7.2.1.4.2 ETCS SIMULATOR

As stated in 7.2.1.2.3 and 7.2.1.3.2, both HW and SW will be simulated. The HW will potentially be a laptop or a PC with a Linux installed and the SW will be an EVC onboard and counterpart RBC on the trackside.

7.2.2 INTERFACES

This section shall contain a description of the interfaces including the following subsections (if applicable) as well as including static and dynamic parts.

7.2.2.1 Interface to TOBA via OB$_{APP}$

This subsection shall provide a full explanation of the interface to TOBA via OB$_{APP}$ using the following coupling approaches:

- Loose approach

7.2.2.1.1 GENERAL

The applications communicate with TOBA and the FRMCS using the Loose coupled approach following the architecture presented in the Figure below:

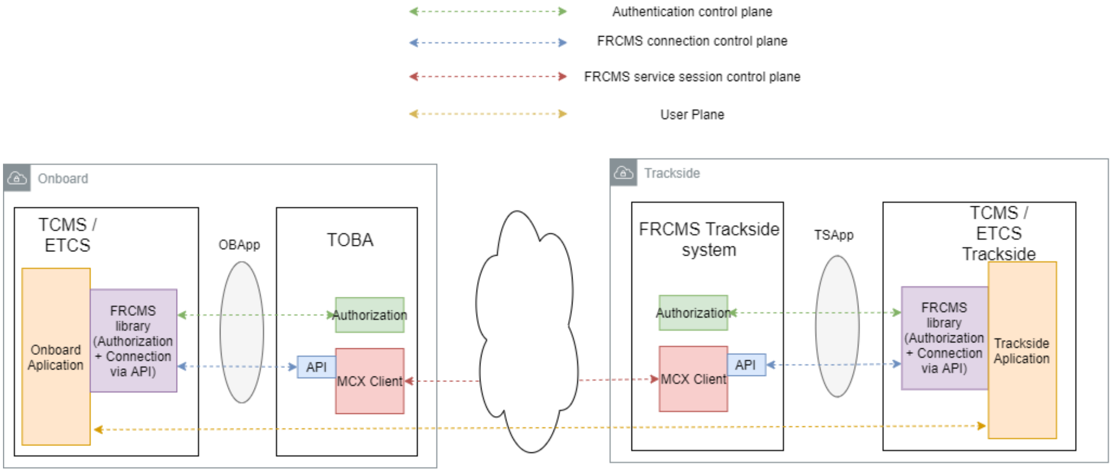

Authentication control plane
FRCMS connection control plane
FRCMS service session control plane
User Plane
Onboard
TCMS / ETCS
Onboard Aplication
FRCMS library (Authorization + Connection via API)
OBApp
TOBA
Authorization
API
MCX Client
Trackside
FRCMS Trackside system
Authorization
MCX Client
API
TSApp
TCMS / ETCS Trackside
FRCMS library (Authorization + Connection via API)
Trackside Aplication

Figure 69: Overall TCMS and ETCS architecture - detailed

As it can be seen, both applications share the same FRMCS library which is used to access the application to FRMCS onboard and trackside systems and to establish IP connectivity from the onboard client to the ground server. Once the connection is established, each application will use the user plane to fulfil the use cases described in WP1.

7.2.2.1.2 TCMS APPLICATION

The overall architecture and its interaction with TOBA and the FRMCS Trackside System for the TCMS application is described In the Figure below:

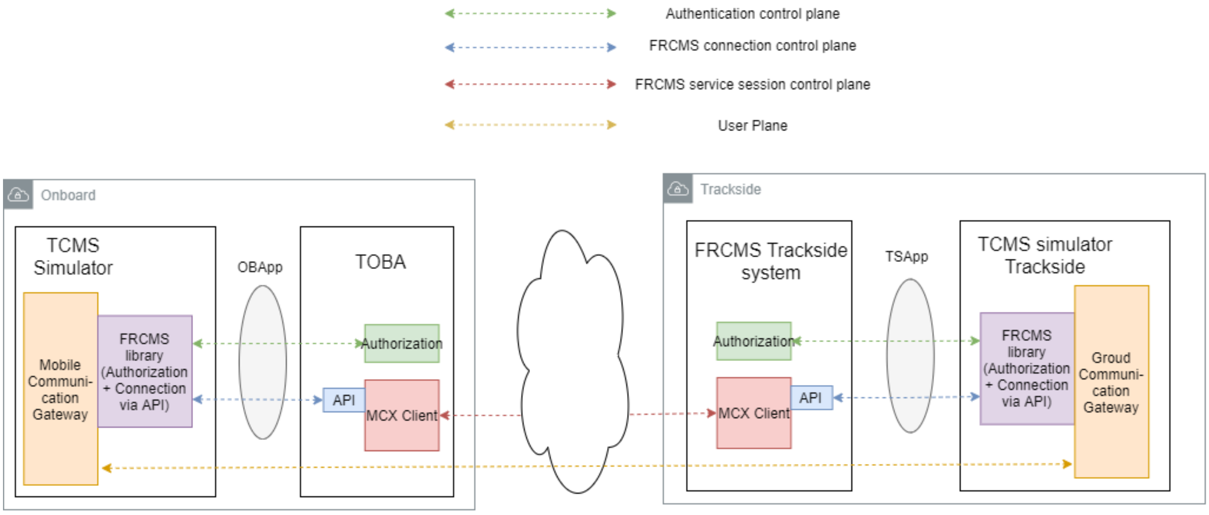

Authentication control plane
FRCMS connection control plane
FRCMS service session control plane
User Plane
Onboard
TCMS Simulator
Mobile Communi-cation Gateway
FRCMS library (Authorization + Connection via API)
OBApp
TOBA
Authorization
API
MCX Client
Trackside
FRCMS Trackside system
Authorization
MCX Client
API
TSApp
TCMS simulator Trackside
FRCMS library (Authorization + Connection via API)
Groud Communi-cation Gateway

Figure 70: Overall TCMS architecture - detailed

As it can be seen, the MCG will interact with the TOBA onboard using the OBApp interface using the FRMCS library which will be implemented. This library will fulfil the OBApp specification to authenticate the application with the FRMCS and establish the IP connectivity. Once the IP connectivity is established, the MCG will provide the services listed in IEC 61375-2-6 [01] according to the use cases defined in WP1.

It is expected that FRMCS network gateways on both onboard and trackside will provide IP connectivity and will abstract the used network interface, handling the network itself and providing the TCMS applications the ability to set QoS requirements.

7.2.2.1.3 ETCS APPLICATION

The overall architecture and its interaction with TOBA and the FRMCS Trackside System is described In the Figure below:

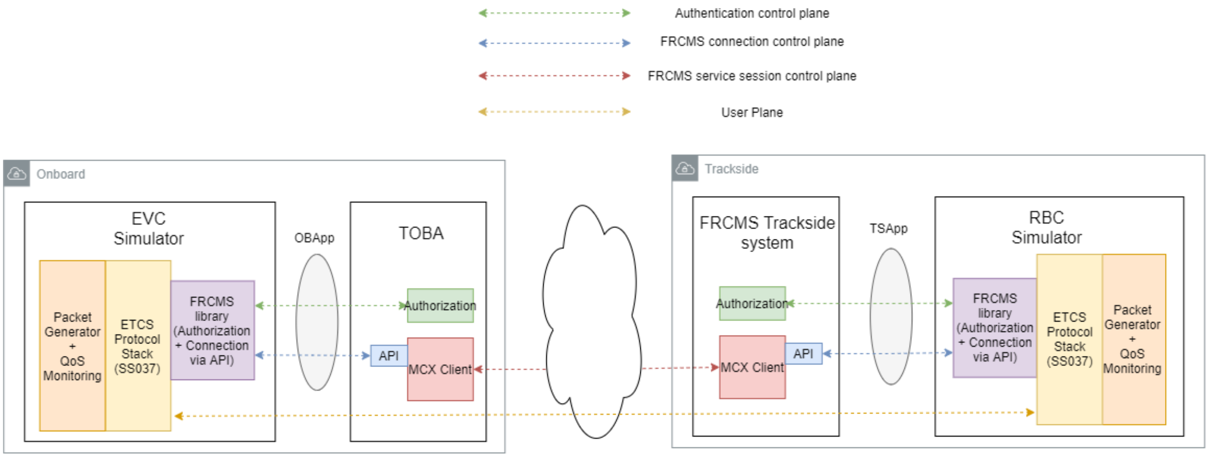

Authentication control plane
FRCMS connection control plane
FRCMS service session control plane
User Plane
Onboard
EVC Simulator
Packet Generator + QoS Monitoring
ETCS Protocol Stack (SS037)
FRCMS library (Authorization + Connection via API)
OBApp
TOBA
Authorization
API
MCX Client
Trackside
FRCMS Trackside system
Authorization
MCX Client
API
TSApp
RBC Simulator
FRCMS library (Authorization + Connection via API)
ETCS Protocol Stack (SS037)
Packet Generator + QoS Monitoring

Figure 71: Overall ETCS architecture - detailed

As it can be seen, the EVC Simulator will interact with the TOBA onboard using the OBApp interface using the FRMCS library which will be implemented. This library will fulfil the OBApp specification to authenticate the application with the FRMCS and establish the IP connectivity. Once the IP connectivity is established, the EVC simulator will request a connection to the trackside counterpart (RBC simulator) using the protocol stack defined in UNISIG SS037.

Once the safe connection is established, both entities will start the transmission of packets of different sizes with a determined periodicity, based on a configuration file which includes those parameters. Frames will be timestamped and sequence numbered in order to be able to measure the E2E latency as well as the throughput.

- Tight approach

7.2.2.1.4 INTERFACE TO TOBA VIA TS$_{APP}$

This subsection shall provide a full explanation of the interface to TOBA via TS$_{APP}$ using the following coupling approaches:

- Loose approach

7.2.2.1.5 TCMS APPLICATION

The MCG explained in chapter 7.2.2.1.2 will have a counterpart on the Trackside, called GCG and supporting deployments depending on the use case ((s)FTP server and MQTT broker). These GCG will interact with the FRMCS Trackside System using the FRMCS library which will implement the TSApp according to the specification provided.

As it was stated in 3.1, it is expected that FRMCS network gateways on both onboard and trackside will provide IP connectivity and will abstract the used network interface, handling the network itself and providing the TCMS applications the ability to set QoS requirements.

7.2.2.1.6 ETCS APPLICATION

As stated in chapter 7.2.2.1.4, there is a counterpart called RBC which will mirror the usage of the OBApp by the onboard EVC via TSApp in the trackside.

- Tight approach

7.2.3 INTERWORKING WITH GSM-R

There is no interworking with GSM-R expected from CAF's implementation (neither TCMS nor ETCS)

7.3 ATO

7.3.1 APPLICATION ARCHITECTURE PROPOSAL

7.3.1.1 Architecture Overview

This architecture provides an overview of the proposed application architecture, including the sub-assemblies that will be used to pass data between ATO-OB and ATO-TS under the FRMCS protocol.

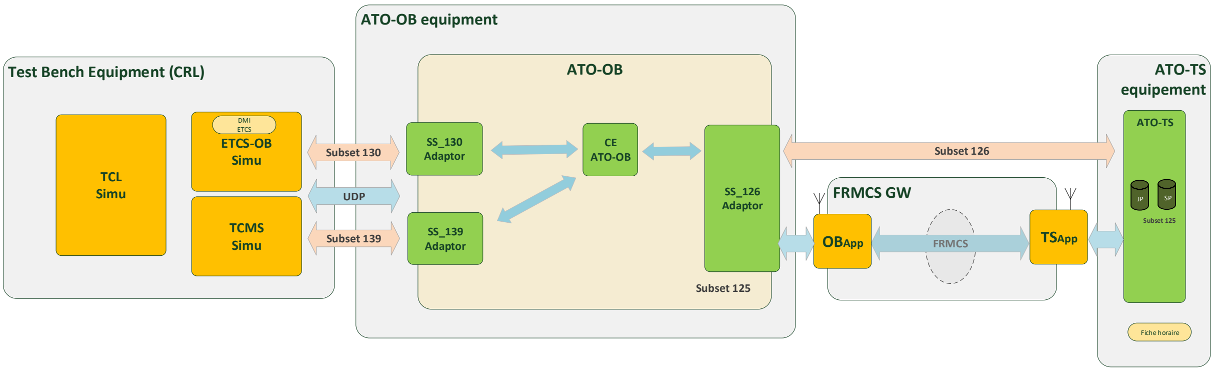


Figure 72: ATO over FRMCS

The figure above gives an overview of the different equipment to be put together during the test phase.

The TE shall provide an adapter to communicate remotely with ATO-OB through Subset 130 and 139 interfaces.

Note: The architecture and the functionalities of the Test Bench Equipment is in the responsibility of Alstom CRL.

1. Test Bench Equipment:

- TCL (Test control and Logging) simulator,

The TCL’s architecture shall be in scope of the test environment supplier.

The TCL shall be able to execute scripted test cases.

The TCL shall be able to log and analyze all data exchanged via the adapter interfaces.

- ETCS simulator,

ETCS simulator will allows to supervise the movement of the train on basis of trackside information as specified in [subset 026]

- TCMS simulator.

TCMS simulator simulates the data communication to other train borne systems and telecommunication to support systems operating remotely on the wayside.

2. ATO-OB Equipment:

- SS 130 Adaptor

The communication between ETCS-OB and ATO-OB shall be realized as specified in [Subset-130]. IP addresses of both communication partners shall be static for lab purposes. The lower levels of communication are given in [SS-130-App]. For the purpose of the test bench activities the communication will be based on payload data only without any security layers.

- SS 126 Adaptor

The SS 126 Adaptor allows the communication between the ATO-OB and the ATO-TS of mission data in the format SS126 format (Mission Profile, Journey Profile, Segment Profile).

NOTE: this component is also responsible for sending periodic status report from ATO-OB to ATO-TS. For some testing purposes (especially regarding border-crossing scenario), it is possible to configure the period between two successive status report messages in order to have regular applicative messages. A period of few seconds can be configured.

- SS 139 Adaptor

The SS 139 Adaptor will allow the ATO to communicate with the TCMS in order to control the train system in traction/braking.

3. ATO-TS Equipment:

- ATO -TS Server,

The ATO-TS Server is the server on which the different trains will connect to retrieve their routes, route updates, and feedback of their positions on the track.

The ATO-TS Server will also connect to the MPE to receive route updates and timetables.

- MPE (Mission Profile Editor),

The MPE will interface between the TMS and the ATO-TS, it will convert the timetables received from the TMS to modify the ATO-TS datastores and trigger the timetables and the route updates for the concerned trains.

7.3.1.2 AoE Subsets

The system requirements are defined in Subset-125. Based on this document several interfaces are going to be specified. Figure 72 gives an overview of the interfaces used by ATO and its standardized subset references.

The following interfaces might be in interest of a system test:

a) Subset-126 (ATO-TS <-> ATO-OB)
b) Subset-126 APP A (FRMCS): Current version of this document is only relative to GSM-R
c) Subset-130 (ETCS-OB <-> ATO-OB)
d) Subset-139 (ATO-OB <-> TCMS (Vehicle/Train)

7.3.1.3 Hardware Platform

the hardware platform, we are going to use here is an ITA platform from Advantech, model ITA 5231

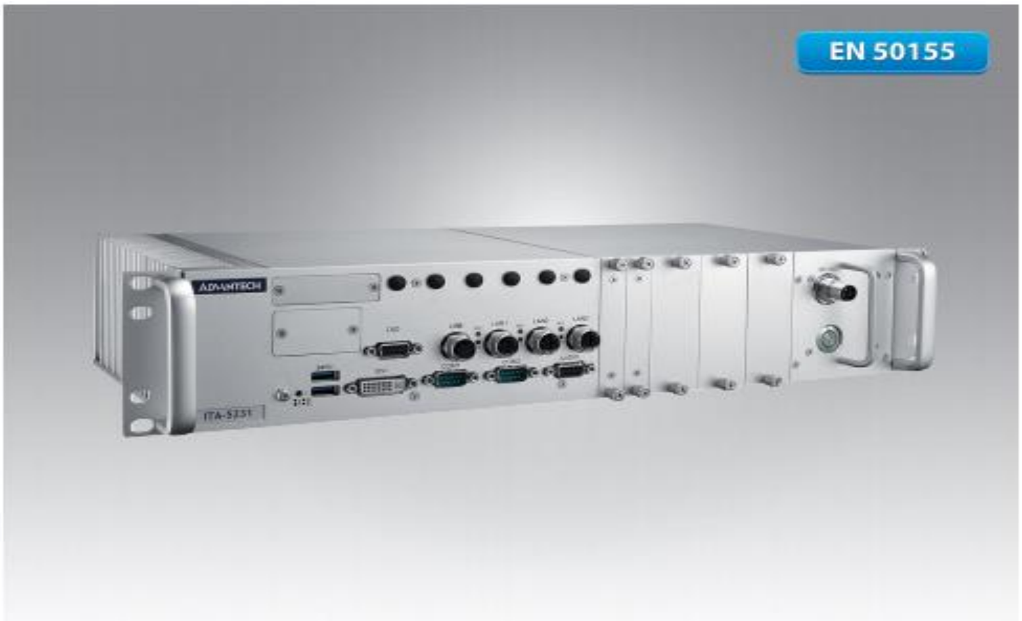


Figure 73: Hardware platform

ITA 5231 features:

- Fanless computer for railway vehicle applications, fully compliant with EN 50155
- Satisfies temp. standard: EN 50155 TX (-40 ~ 70 °C) and IEC 61373 body mount class B
- Compliant with EN 50121-3-2/ EN 50121-4 EMC test standard
- Ruggedized connectors (M12) used for communication and power ports
- Supports easy-swap storage module and I/O module
- No RED Certification

Front view

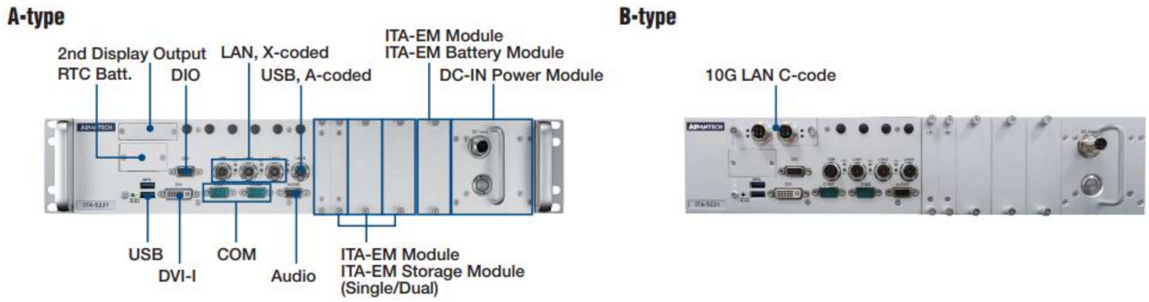


Figure 74 Front view of the ITA-5231

7.3.1.4 Software Platform

This subsection shall provide an overview of the software platform.

To be defined in further release.

7.3.1.5 Simulators (if applicable)

The simulator is composed of a test environment who communicates with ATO equipment through additional adaptors in order to Provide several data. The simulator is able to stimulate an ATO deliverable for test purposes and possess a track layout for simulation purposes.

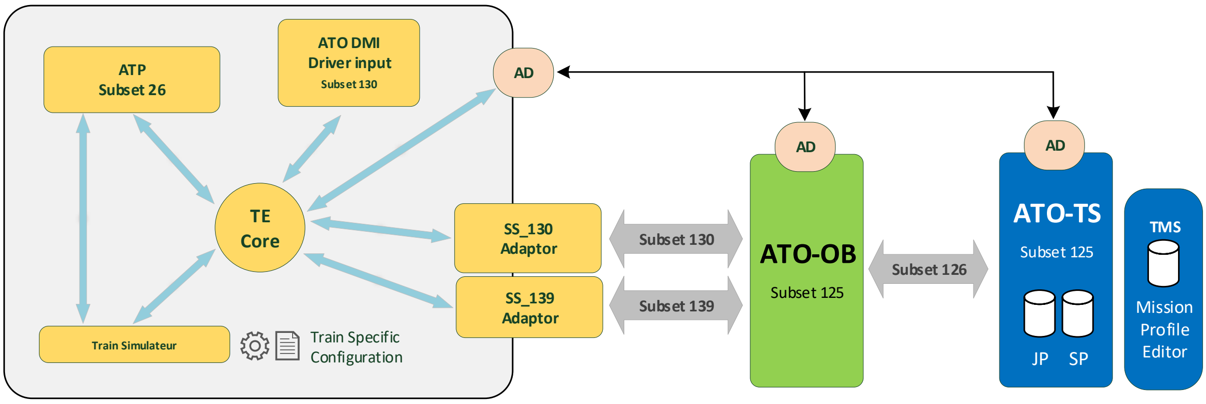


Figure 75: Simulator

7.3.2 INTERFACES

7.3.2.1 Interface to TOBA via OB_{APP}

This subsection shall provide a full explanation of the interface to TOBA via OB_{APP} using the following coupling approaches:

- Loose approach

There are 6 functions (requests) exposed by FRMCS OB GTW to the application:

- FRMCS_GTW_REGISTER: allow the ATO-OB application to register to the TOBA Gateway.
- FRMCS_GTW_DEREGISTER: allow the ATO-OB application to deregister from the TOBA Gateway
- FRMCS_GTW_SESSION_START: allow the ATO-OB application to request a session establishment to join a trackside equipment (ATO-TS).
- FRMCS_GTW_SESSION_END: allow the ATO-OB application to close an established session.
- FRMCS_GTW_SESSION_STATUS: allow the ATO-OB application to ask for a status of a current session.
- FRMCS_GTW_SERVICE_REQUEST: allow the ATO-OB application to request specific services FRMCS

Two functions (notification) are proposed from FRMCS OB GTW to ATO-OB application:

- FRMCS_APP_SESSION_STATUS_CHANGED: TOBA informs the ATO-OB application that there are some changes on the session status (link failure, quality change, session closed from the other side, …)

- FRMCS_APP_INCOMING_SESSION: TOBA informs the ATO-OB application that an incoming session request has been made. TOBA waits for a response from the ATO-OB application to establish the session.

7.3.2.2 Interface to TOBA via TS_{APP}

7.3.3 INTERWORKING WITH GSM-R

There is no interworking with GSM-R expected from ATO implementation.

7.4 VOICE

7.4.1 APPLICATION ARCHITECTURE PROPOSAL

The FRMCS voice application will provide the following functionalities:

- F1: Initiate a point-to-point voice communication between a train driver and a train controller and vice versa
- F2: Initiate a point-to-point voice communication between a GSM-R User and FRMCS Users
- F3: Join an on-going voice communication between a train driver and a train controller
- F4: Terminate a driver to controller(s) voice communication and vice versa
- F5: Initiate a multi-train voice communication for drivers including ground user(s)
- F6: Initiate a multi-train voice communication between GSM-R Users and FRMCS Users
- F7: Join an on-going multi-train voice communication
- F8: Terminate a multi-train voice communication
- F10: Initiate a Railway Emergency alert
- F11: Initiate a Railway Emergency voice communication
- F12: Provide a multiuser talker control
- F13: Interworking between GSM-R and FRMCS (manual network switch)
- F14: Registration and deregistration of a functional identity
- F15: Provide and request location information to/from GSM-R Users and FRMCS Users
- F16: Authorization of communication
    - Permit / Deny communication
- F17: Authorization of application
    - Enabling / Disabling applications
- F18: Arbitration
- F19: Call restriction service

7.4.1.1 Architecture Overview

Siemens Voice Radio 400+ series (SVR400+) is a dual mode onboard solution that provides voice communication between a train driver and a train controller as well as a train driver and drivers of other trains over the existing GSM-R Network and the new FRMCS system. Figure 76 illustrates the Dual Mode GSM-R/FRMCS voice application.

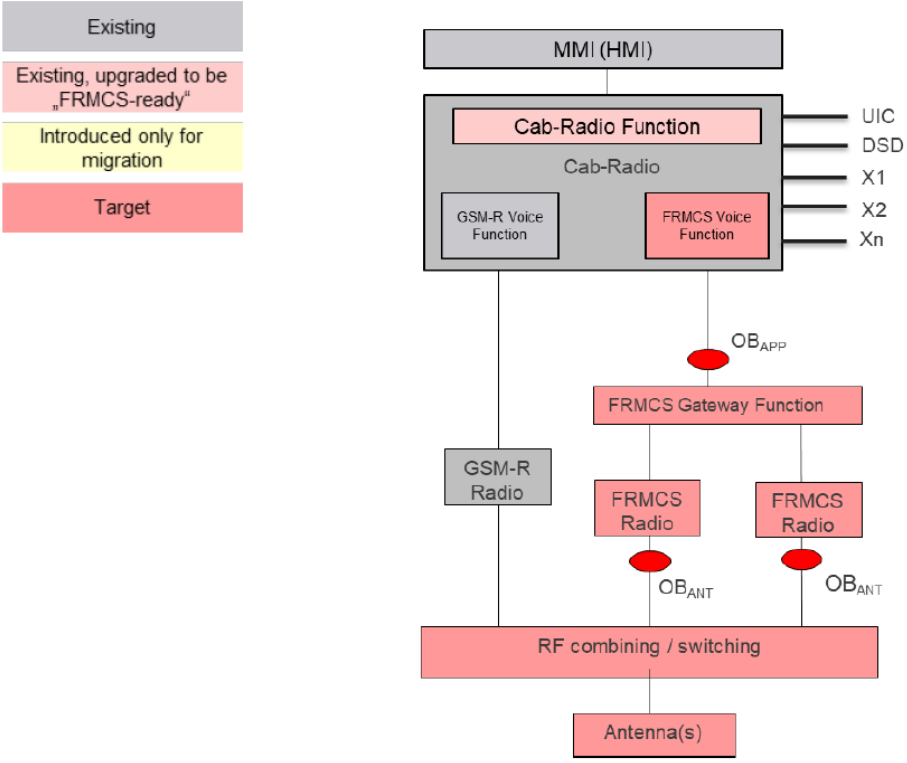


Figure 76: Dual Mode GSM-R/FRMCS Voice Application

7.4.1.2 Hardware Platform

7.4.1.2.1 ON-BOARD

SVR400+ is an EIRENE compliant GSM-R voice cab radio solution that includes an additional i.MX microprocessor card which runs the FRMCS voice application. The Siemens' dual mode onboard solution comprises four units as illustrated in Figure 77 and further described in the following subsections.

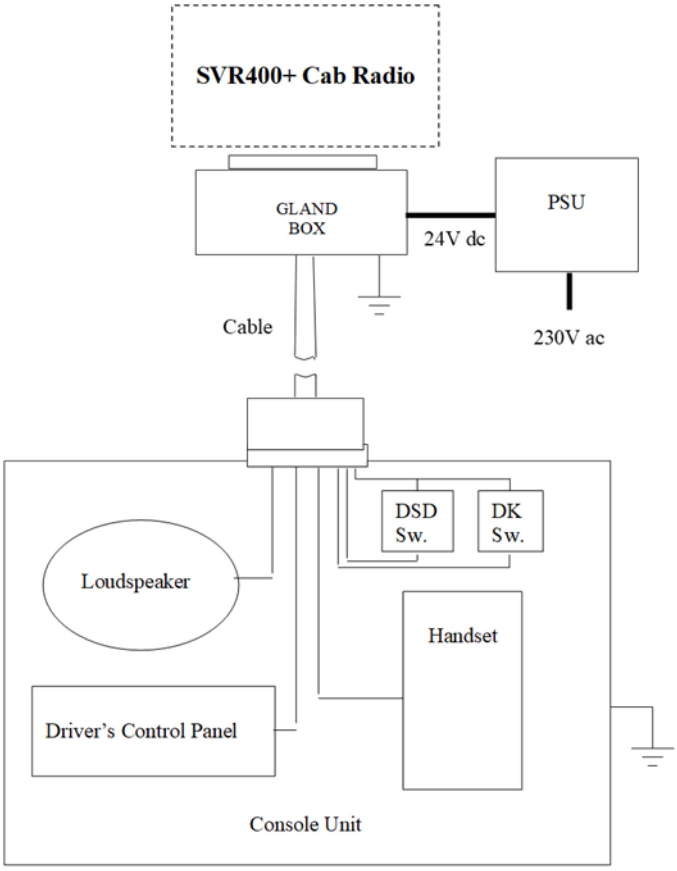


Figure 77: Siemens' hardware platform

7.4.1.2.1.1 VOICE CAB RADIO

The SVR400+ is sealed to IP54 and has a standard operating temperature range of -20ºC to +70ºC. This is achieved by the incorporation of an active cooling unit.

A photograph of the SVR400+ is shown in Figure 78:

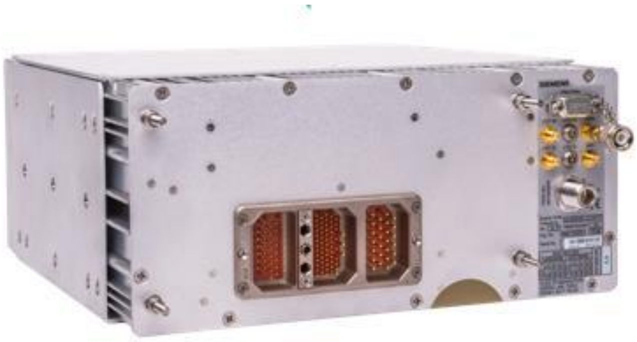


Figure 78: SVR400+ front panel

The Table below provides specification of the SVR400+ Voice Cab Radio solution:

Table 38: SVR400+ Specification

PHYSICAL SPECIFICATION	
Dimensions of the SVR400+ Voice Cab Radio unit	135.8mm (h), 299mm (w) and 241mm (d)
Dimensions of the gland box unit mounted on the rear face of the radio unit	120mm (h), 200mm (w) and 120mm (d)
Dimensions of the fan unit mounted on the front face of the radio unit.	133mm (h), 299mm (w) and 65mm (d) Plus, a minimum air gap of 20mm on the depth
Weight of the Voice Cab Radio	9kg
Weight of the gland box	0.5kg
Weight of the fan unit	0.5kg
INTERFACES	
Voice Cab Radio Unit	Interface to the Console Unit 1 off ARINC type 404, triple male connector
	Interface to the GSM-R Antenna 1 off N type female connector
	Interface to the GPS antenna TBC
	Interface to the Portable Maintenance Unit (PMU) 15 way D type (gender?)
Console Unit	Interface to the Voice Cab Radio 1 off N type male connector
	Power (?)
Gland Box	Interface to the Voice Cab Radio 1 off ARINC type 404, triple female connector
	Interface to the Console Unit Flying lead terminated with a D connector
	Interface to the PSU DIN connector
	OB$_{APP}$ interface connector 1 off M12 (gender?) Ethernet connector
	Interface to the PIS UIC 561 PA – we will need to make a cable with a connector
POWER	
Train Input Power Supply	24 - 110VDC (nominal)
Output power to control panels	13V +/- 5%
Power Consumption	60W max, ~36W Nominal <1.5A (assuming dual DCP) at 24V DC

7.4.1.2.1.2 CONSOLE UNIT

The Console Unit comprises a metal enclosure containing a Graphical Driver’s Control Panel, Driver’s Handset and Loudspeaker. Electrical connection to this unit is made via a D connector on the rear panel of the Console Unit.

Two switches are provided on the front panel of the Console Unit, which operate the Driver's Key and DSD Inputs on the Cab Radio for test purposes. Each of these switches provide 24V from the Power Supply Unit to the relevant digital inputs within the SVR400+ Voice Cab Radio.

Photographs of the Console Unit are shown in Figure 79 and Figure 80.

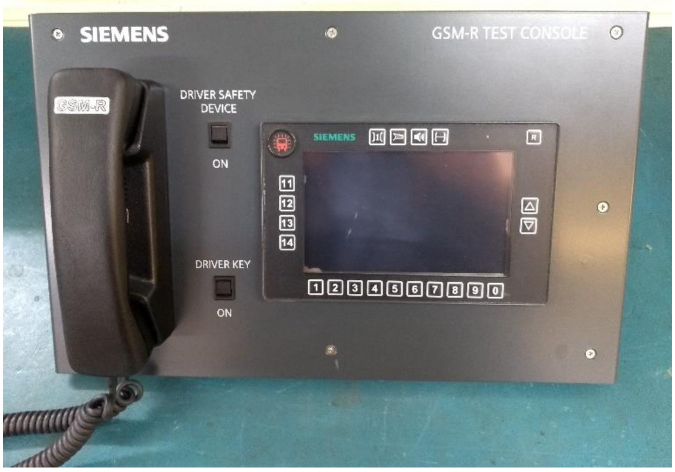


Figure 79: Console Unit front panel

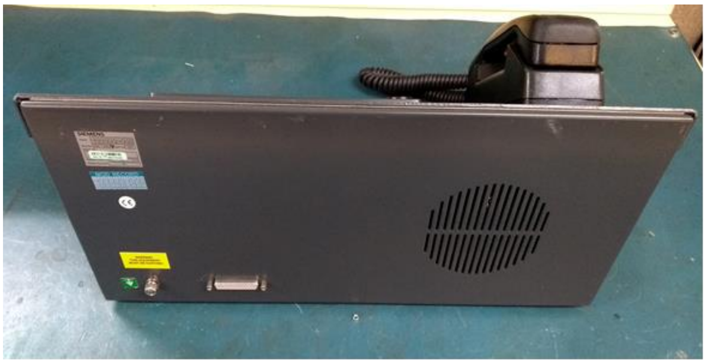


Figure 80: Console Unit rear panel

7.4.1.2.1.3 GLAND BOX

The Gland Box contains an ARINC connector for connection to the SVR400+ Voice Cab Radio, a flying lead terminated with a D connector for connection to the Console Unit and a DIN connector for connection of the PSU, ethernet M12 connector for connection to FRMCS Onboard Gateway and UIC

A photograph of the Gland Box is shown in Figure 81.

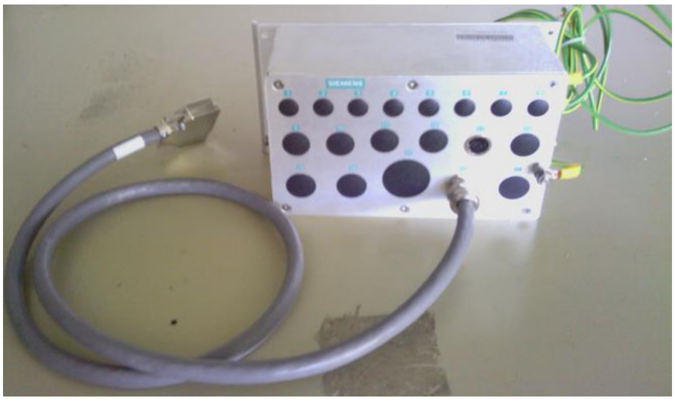


Figure 81: Gland Box

7.4.1.2.1.4 POWER SUPPLY UNIT

The PSU is an AC/DC External Unit, which operates from a 230V, 50Hz mains supply and provides a 24V dc supply to the Gland Box assembly. This is used to provide power to the connected SVR400+ Voice Cab Radio.

A photograph of the Gland Box is shown in Figure 82.

Figure 82: Power Supply Unit

7.4.1.2.2 TRACKSIDE

The SVR400+ Voice Cab Radio onboard solution communicates to MCx Server located between the FRMCS Onboard Gateway and the FRMCS Track Side Gateway which then communicates to the Dispatcher Server located on the trackside. The trackside solution is outside of Siemens' scope and will be provided by WP3, led by Nokia.

7.4.1.3 Simulators (if applicable)

Not Applicable

7.4.2 INTERFACES

7.4.2.1 Interface to TOBA via OBAPP

FRMCS Voice application is connected to the FRMCS Onboard Gateway via OB_{APP} interface using tight coupled approach i.e. the MCx client is embedded in the application.

The definition of the OB_{APP} tight coupled interface is given in chapter 6.2.5.

7.4.2.2 Interface to TOBA via TSAPP

Not applicable

7.4.2.3 External Interfaces (if applicable)

The SVR400+ Voice Cab Radio dual mode solution incorporates extensive external interfaces.

7.4.2.3.1 4G/5G MODEM

4G/5G modem is incorporated within the FRMCS Onboard Gateway. The SVR400+ interface to the TOBA is via a M12 Ethernet connector.

7.4.2.3.2 GSM-R ANTENNA

The SVR400+ interface to the GSM-R antenna is via a N type female connector on the cab radio side.

If required, a GSM-R antenna can be provided by Siemens.

7.4.2.3.3 GSM-R MODEM

A GSM-R modem will be incorporated within the SVR400+ Voice Cab Radio onboard solution.

7.4.2.3.4 GPS

N/A – Location service will be provided by the FRMCS Onboard Gateway

7.4.2.3.5 LTE ANTENNA

Not applicable

7.4.2.3.6 WI-FI

Not applicable

7.4.2.4 User Interfaces (if applicable)

The SVR400+ Voice Cab Radio interact with the following user interfaces

7.4.2.4.1 GRAPHICAL DRIVER'S CONTROL PANEL

See section 7.4.1.2.1.2

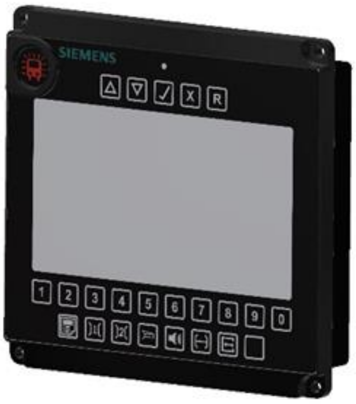


Figure 83: Graphical Driver's Control Panel

BUTTON LEGEND	RADIO FUNCTION	BUTTON LEGEND	RADIO FUNCTION	BUTTON LEGEND	RADIO FUNCTION	BUTTON LEGEND	RADIO FUNCTION
🚨	Emergency Call	☰	Menu	)1(	Call Primary Controller	)2(	Call Secondary Controller
📢	Call/Page Chief Conductor	🔊	Call to Public Address	(↔)	Train to Train Call	⇄	Register / Deregister
■	Network Switch	△	Direction Up	▽	Direction Down	✓	Enter Button
X	Cancel Button	R	Reset Radio				

Table 39: Graphical Driver's Control Panel hard keys legend

SOFTKEY LEGENDS				
0	1	2	3	4
5	6	7	8	9

Table 40: Graphical Driver's Control Panel soft keys legend

7.4.2.4.2 HANDSET

See section 7.4.1.2.1.2

7.4.2.4.3 LOUDSPEAKER

See section 7.4.1.2.1.2

7.4.3 INTERWORKING WITH GSM-R

The FRMCS Principle Architecture requires a dual mode coordination between the GSM-R & FRMCS Networks. Due to the FRMCS Onboard Gateway limitations, the GSM-R modem will be included within the Siemens' hardware platform. This will be interfaced as per the diagram in Figure 76.

This dual mode coordination will need to be developed with a minimal coordination function therefore, Siemens proposes a simple solution where a driver can manually switch between the two systems using a dedicated hard key on the GDCP.

7.4.4 CYBERSECURITY

The FRMCS voice application will be cyber security tested in accordance with Siemens' Product & Solution Security (PSS) process.

The Siemens' PSS process is based on the IEC 62443-2-4 standard – Security program requirements for Industrial Automation and Control Systems (IACS) service providers. It provides a systematic and practical approach to cybersecurity for industrial systems.

7.5 PIS

7.5.1 APPLICATION ARCHITECTURE PROPOSAL

This section contains a description of PIS application architecture.

7.5.1.1 Architecture Overview

PIS application consists of two parts, one installed into the train and the other one in trackside. The diagram represented in Figure 84: PIS application architecture overview.gives an overview of PIS architecture.

To enable passenger information managers to create, distribute and present integrated, synchronized real-time visual, audio announcements and time information in the trains, “Trackside” and “On-board” PIS components are interconnected with the FRMCS infrastructure via the interfaces TS_{APP} (Trackside) and OB_{APP} (On-Board).

The description and the definition of the FRMCS infrastructure in chapters 2 and 5. The description of the interfaces OB_{APP}/TS_{APP} are given in chapter 6.2 and 6.3.

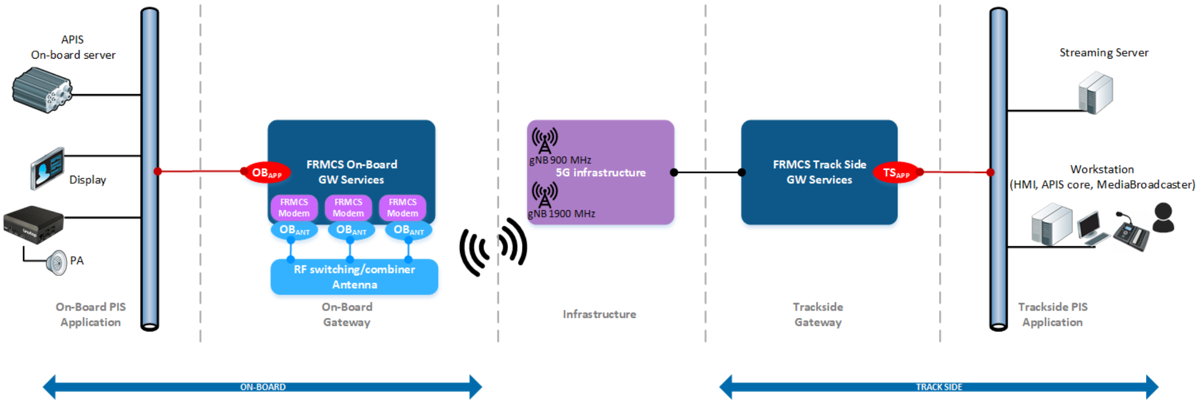


Figure 84: PIS application architecture overview.

7.5.1.2 Hardware Platform

7.5.1.2.1 ON-BOARD

7.5.1.2.1.1 APIS ON-BOARD SERVER

On-board railway certified server (EN 50155, EN 61373, EN 50121-3-2, EN45545-2) which hosts APIS on-board application and an on-board framework which manages APIS on-board & trackside communication.

.

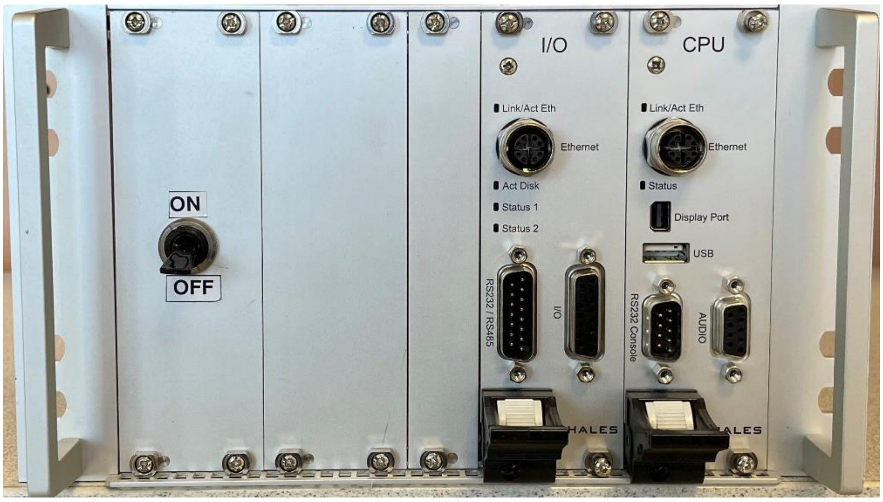


Figure 85: APIS on-board server (Front panel).

Table 41 gives the description of the APIS on-board server:

INTEL ATOM PROCESSOR QUADCORE RAM MEMORY 4GB DDR3L STORAGE 500GB (SSD)	
CPU board (front panel) • height: 3U (128 mm) • width: 8TE (40,64 mm)	Ethernet connector • 8 pins female M12 X-Coded • 10/100/1000Mbps interface
	Display port connector • 20 pins Mini Display port type
	USB port connector • USB Type A
	RS232 Console connector • 9 pins male D-Sub
	Audio connector • 9 pins female D-Sub
	Link/Act Eth LED • Green: 10/100Mbps Ethernet Link • Red: 1000Mbps Ethernet Link • Orange blinking: Ethernet activity
	Status LED • Applicative Status
I/O board (front panel)	Ethernet connector • 8 pins female M12 X-Coded 10/100/1000Mbps interface
	RS232 / RS485 connector • 15 pins male D-Sub • RS232 ○ Data rate: up to 1MBaud ○ RTS, CTS signals • RS485 ○ Half duplex

	○ Data rate: up to 1MBaud ○ Optional Bus termination resistor (120 Ohms)
	I/O connector • 15 pins female D-Sub
	Link/Act Eth LED • Green: 10/100Mbps Ethernet Link • Red: 1000Mbps Ethernet Link • Orange blinking: Ethernet activity
	Act Disk LED • Green: Board powered • Green/Orange blinking: Disk activity • No color : Board not powered
	Status 1 LED
	Status 2 LED

Table 41: Description of the front panel description of the APIS on-board server.

The APIS on-board server is connected to the FRMCS on-board gateway. It hosts the APIS on-board application which will be compatible with OBapp. This application handles messages sent by APIS trackside application and dispatches them to loudspeaker or display device.

7.5.1.2.1.2 ON-BOARD PAS SERVER

The on board PAS server is a fanless embedded system which controls the PA announcements.

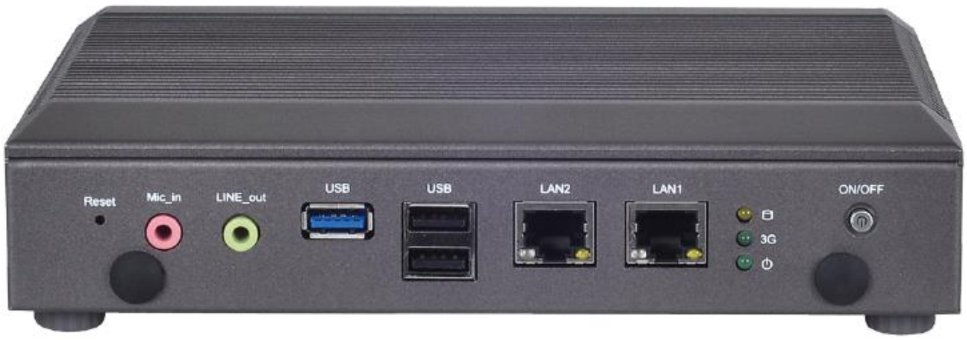


Figure 86: VIPA-HOST.

Via its Ethernet port, the On-board PAS server is connected to the same LAN as APIS on-board server and receives audio data from it. The audio data are sent to the loudspeaker which is connected to the on board PAS server via an audio jack cable.

Table 42 gives the hardware description of the on board PAS server:

Processor	Intel® Celeron® J1900 4 cores
Memory	8 GB DDR3L
Audio	Codec Realtek ALC662 High Definition 2 x Phone Jack for MIC-in and Line-out
Ethernet	2 x RJ45 10/100/1000 Mbps
I/O	Serial Port 2 x RS-232/422/485, DB9 male USB 2.0 2 x Type A USB 3.0 1 x Type A
Power	Power Type ATX Power Supply Voltage +12 VDC Connector DC Jack with Lock Power Consumption (Idle) 7.36W Power Consumption (Full Load) 11.43W Power Adaptor AC to DC, AC 90 to 240 VAC Input, DC 12V/5A 60W
Dimension (WxHxD)	198 x 42 x 145 mm
Certification	EMC CE/FCC, Class A

Table 42: Hardware description of the VIPA-HOST server.

7.5.1.2.1.3 LOUDSPEAKER

The loudspeaker broadcasts audio information sent by the passenger information manager to the passengers in the train.

It is a standard PC speaker directly connected to VIPA-HOST server via an audio Jack connector.

7.5.1.2.1.4 TFT DISPLAY DEVICE

The display device displays text information like train time tables sent by the passenger information manager to the passenger in the train.

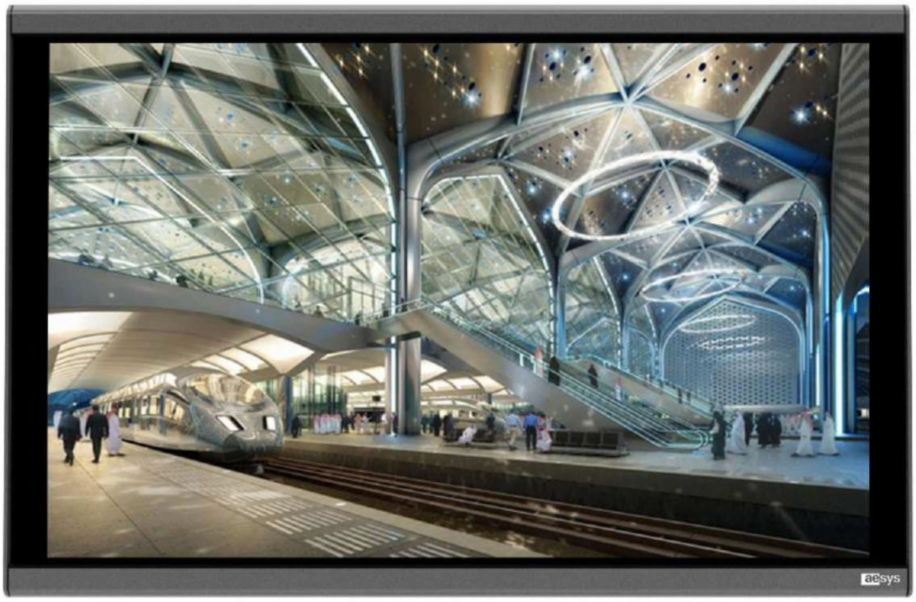


Figure 87: On-board TFT display device.

Table 43 gives the hardware description of the Display device:

Railway certifications	EN50155 – Railway applications – Electronic equipment used on rolling stock EN50121-3-2:2006 – Railway applications – Electromagnetic compatibility – Part 3-2: Rolling stock – Apparatus EN50122-1 – Railway applications – Fixed installations – Part 1: Protective provisions relating to electrical safety and earthing EN60529 – Degrees of protection provided by enclosures (IP Code) EN61373 – Railway applications – Rolling stock equipment – Shock and vibration tests EN60068-2-2-1998 – Dry heat test EN60068-2-1:2007 – Cold test EN60068-2-30:2005 – Damp heat, cyclic test EN45545-2:2010 – Railway applications — Fire protection on railway vehicles Part 2: Requirements for fire behavior of materials and components
Processor	Intel Celeron J1900 QuadCore
Memory	2 GB DDR3L
Display connection	VGA, LVDS, HDMI
Storage	1 x SSD 4GB

Input power supply voltage	Nominal voltage: 96Vdc According to EN50155 • Minimum voltage: (0,7 Un) 67,2 Vdc • Rated voltage: (1,15 Un) 110,4 Vdc • Maximum voltage: (1,25 Un) 120 Vdc • Between 0.6 ÷ 1.4 Un x 0.1S: no deviation of function • Between 1.25 ÷ 1.4 Un x 1S: no damage but equipment may not be fully functioning during these fluctuations
Dimensions Weight	580 (L) x 380 (H) x 55 (D) mm 11 Kg
Screen dimension	24” diagonal; format 16:10
Pixel format	1920 (H) x 1200 (V) px
USB	USB 3.0 USB 2.0 USB 2.0 on Internal I/O

Table 43: Hardware description of the on-board display device.

The display device embeds its own Operating System and via its Ethernet port is connected to the same LAN as the APIS on-board server and receives video data from it.

7.5.1.2.2 TRACKSIDE

7.5.1.2.2.1 STREAMING SERVER

7.5.1.2.2.2 MICROPHONE

The passenger information manager can make live audio messages using his microphone.

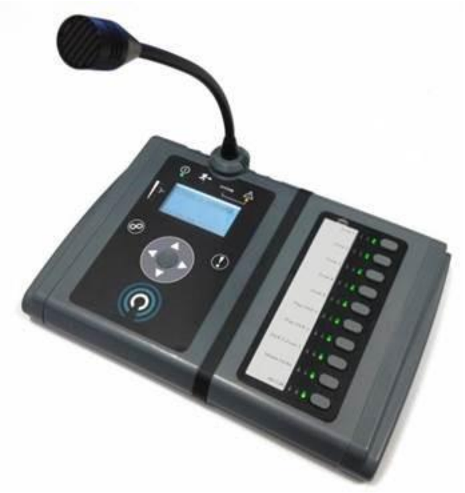


Figure 88: Trackside microphone.

Table 44 gives the hardware description of the microphone:

Input Voltage	18-40 V DC or PoE 42-57V DC
Connection	1 x 100BASE- T Ethernet (RJ45)
Dimensions (H x W x D mm)	58 x 175 x 200 (excluding gooseneck)

Table 44: Hardware description of the microphone.

The microphone is connected to the same LAN as the APIS trackside server via its Ethernet port and sends audio data to it.

7.5.1.2.2.3 APIS TRACKSIDE SERVER

From the APIS trackside server and a screen with a resolution of 1920 x 1080 pixels, the passenger information manager accesses to the APIS HMI via Chrome Web browser to dispatch information to passengers in the train.

Table 45 gives the hardware description of the APIS trackside server:

Processor	Intel® Xeon® E5-1650 v2
Memory	8 GB
Storage	400 GB
Ethernet	1 x RJ45 10/100/1000 Mbps

Table 45: Hardware of the APIS trackside server.

APIS trackside server hosts APIS trackside application. This application includes components responsible for interfacing with passenger information managers (HMI) and devices.

The APIS trackside server is connected to the FRMCS trackside gateway and the APIS trackside application will be compatible with TSapp.

7.5.1.3 Software Platform

Figure 89 describes the APIS software architecture.

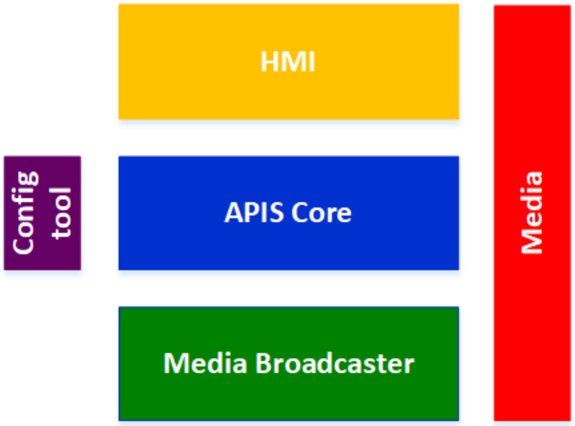


Figure 89: APIS software components.

7.5.1.3.1 APIS HMI

The APIS HMI is divided into two parts:

- HMI Frontend
- HMI Core

The HMI Frontend contains the Web Application which provides login, caching, reacting (refreshing) to APIS Core events and Windows navigation. The HMI Core connects to the APIS Core and serves as a mediator between the frontend and the core.

7.5.1.3.2 APIS CORE

The APIS Core is responsible for most of the business logic behind APIS. This component handles messages sent by the operator via the HMI then delivers them to the Media Broadcaster component.

7.5.1.3.3 APIS MEDIA BROADCASTER

The APIS Media Broadcaster is the component responsible for interfacing with and managing devices, broadcasting passenger information and managing message priorities.

7.5.1.3.4 MEDIA

The Media component is responsible for retrieving multimedia content from the database and making it available.

7.5.1.3.5 CONFIGURATION TOOL

APIS Configuration Tool is designed to simplify the task of configuring APIS. It takes information about the transport network, devices and operator roles contained in a configuration file and generates the appropriate XML configuration files.

7.5.1.4 Simulators (if applicable)

PIS application needs to know where the train is located in order to provide information to the passengers such as real-time train schedules and other operator service information. At this stage of the FRMCS specifications, available for 5GRAIL project, no FRMCS equipment has been specified to be responsible to provide location information to the applications that need it.

In that context, Thales in charge to deliver PIS prototype will provide a location simulator for PIS needs.

That simulator will be installed on-board.

Figure 90 describes PIS simulator architecture.

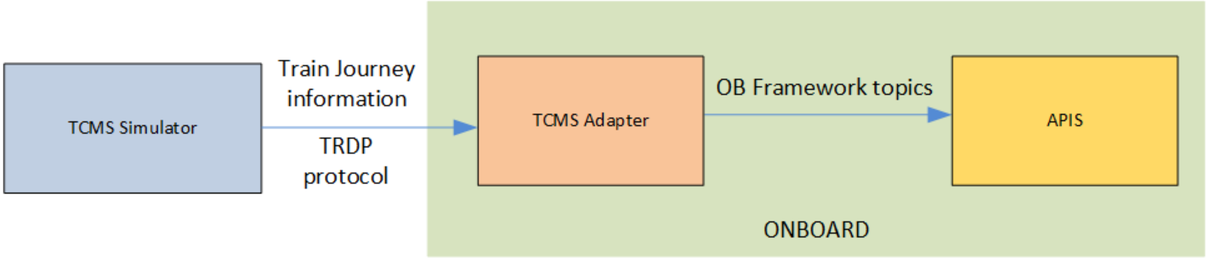


Figure 90: Location simulator for PIS.

The TCMS Simulator simulates the trip of train. It sends Train Journey information such as:

- Speed of the train,
- Distance from the next station,
- Name of the next station,
- Name of the current station,
- Beacons number installed along the track.

This information is sent to the TCMS adapter using TRDP protocol. The TCMS adapter adapts the format of the information received and publishes them to the applications, especially APIS that needs location information.

7.5.2 INTERFACES

7.5.2.1 Interface to TOBA via OB_{APP}

On-board PIS application embedded in the APIS on-board server is connected to the FRMCS on-board Gateway via OB_{APP} interface using loose coupled approach i.e. the MCx client is part of the FRMCS on-board Gateway.

The definition of OB_{APP} interface is given in chapter 6.2.

Trackside PIS application is connected to the FRMCS trackside Gateway via TS_{APP} interface using loose coupled approach i.e. the MCx client is part of the FRMCS trackside Gateway.

The definition of TS_{APP} interface is given in chapter 6.3.

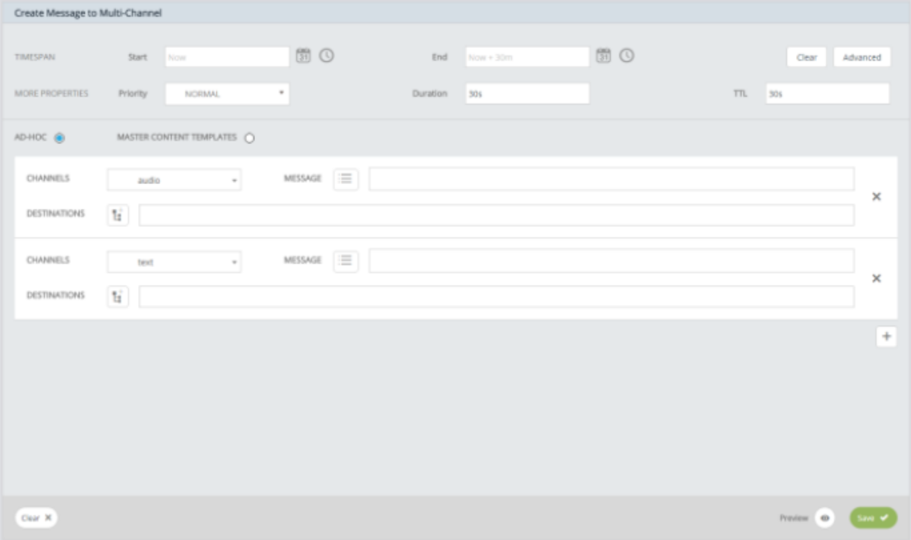
7.5.2.2 User Interfaces (if applicable)

7.5.2.2.1 PASSENGER INFORMATION SYSTEM

7.5.2.2.1.1 GENERAL INFORMATION MESSAGES

APIS allows a user to define the content of the messages. The content may be created using a new free content or by selecting content templates or master content templates that are already predefined and stored in the system. Message's mandatory and optional parameters are defined for each available channel. The maximum allowed size of the message for each channel is a configuration parameter: in the case of a free content message, APIS HMI shows the maximum number of characters permitted; otherwise, the message is truncated if the maximum size is surpassed.

Figure 91 shows the Multi-Channel message window: the operator is allowed to select several channels to send the message to using the scroll bar to navigate.



Create Message to Multi-Channel

TIMESPAN Start: Now End: Now + 30m

MORE PROPERTIES Priority: NORMAL Duration: 30s TTL: 30s

AD-HOC ● MASTER CONTENT TEMPLATES ○

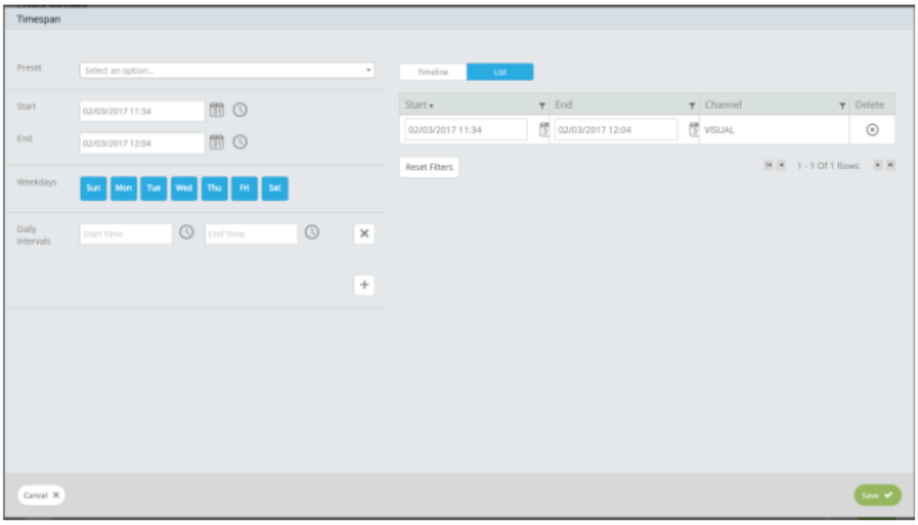
CHANNELS: audio MESSAGE:
DESTINATIONS:

CHANNELS: text MESSAGE:
DESTINATIONS:

Figure 91: Multi-Channel Message: selection of several channels.

7.5.2.2.1.2 MESSAGE SCHEDULING

When sending a message, the operator is able to schedule it to be broadcast or displayed with a specific duration and number of repetitions.



Timespan

Preset: Select an option...

Start: 02/03/2017 11:34

End: 02/03/2017 12:04

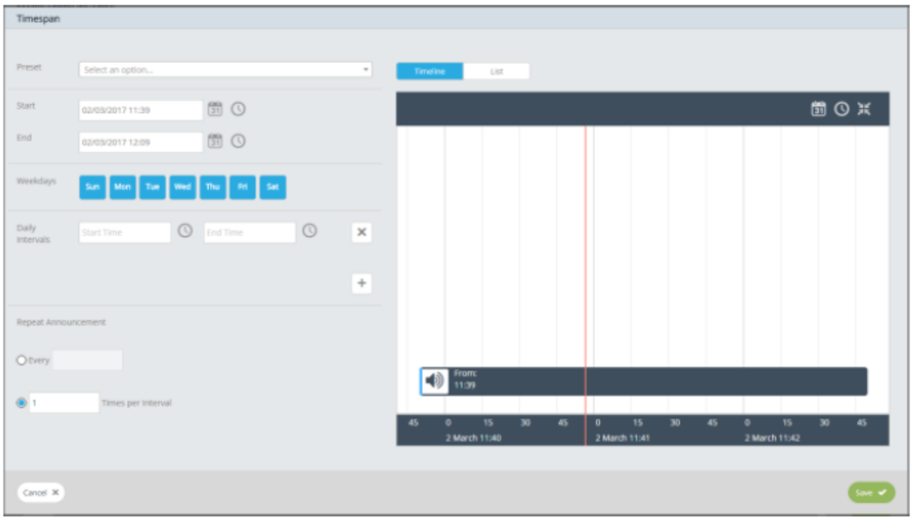
Weekdays: Sun Mon Tue Wed Thu Fri Sat

Daily Intervals: Start Time – End Time

Start	End	Channel	Delete
02/03/2017 11:34	02/03/2017 12:04	VISUAL	⊗

1 - 1 Of 1 Rows

Figure 92: Text message scheduling window.



Timespan

Preset: Select an option...

Start: 02/03/2017 11:39

End: 02/03/2017 12:09

Weekdays: Sun Mon Tue Wed Thu Fri Sat

Daily Intervals: Start Time – End Time

Repeat Announcement

○ Every

● 1 Times per interval

Figure 93: Audio message scheduling window.

7.5.3 INTERWORKING WITH GSM-R

Not applicable.

7.5.4 CYBERSECURITY

7.5.4.1 Hardening at all levels

7.5.4.1.1 BIOS

BIOS configuration follows ANSSI's requirements: https://www.ssi.gouv.fr/en/guide/hardware-security-requirements-for-x86-platforms/.

7.5.4.1.2 HYPERVISOR

On-board and trackside APIS applications are virtualized. In that context, the hypervisor used to manage these Virtual Machines is hardened based on ANSSI's recommendations: https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Virtualisation_NoteTech_v1-1.pdf.

7.5.4.1.3 OPERATING SYSTEM

APIS Operating System is based on Linux distribution.

APIS Operating System configuration is based on ANSSI's recommendations:
https://www.ssi.gouv.fr/en/guide/configuration-recommendations-of-a-gnulinux-system/.

7.5.4.1.4 APPLICATION

APIS application contains a Web server. This Web server is hardened based on OWASP recommendations.

7.5.4.2 Access control - Authentication and Authorization

Operations on APIS are permitted to the operator based on his/her user permissions and are derived from his/her roles, for example an operator with the role “Administrator” would be able to manage other users, whilst an individual with the role “Operator” would be able to send messages. These profiles are configurable through the HMI.

7.5.4.3 Network security and cryptography

APIS application embeds firewall to apply “point-to-point zero trust” policies (i.e. source-target IP/protocols filtering).

Data in motion exchanged between APIS components are encrypted mainly using preconized versions of TLS. Data at rest are encrypted (HD in on-board server have a native encryption).

7.5.4.4 PIS application Authentication and Authorization

Prior to send PIS information, on-board PIS application and trackside PIS application must authenticate respectively with the on-board FRMCS gateway using local binding features (see 6 5.2.2.4.5 and 5.3.2.4.5).

Then on-board and trackside FRMCS gateways will provide access to PIS application the access to the FRMCS service.

7.6 CCTV

CCTV system enables real-time view for onboard cameras and 24/7 recording of video. CCTV system is accessible from trackside OCC as well as by onboard crew members. CCTV offload allows the transfer of CCTV archives into the trackside servers, when train stops at the stations and/or depot.

7.6.1 APPLICATION ARCHITECTURE PROPOSAL

7.6.1.1 Architecture Overview

CCTV application consists of two parts, one installed into the train and the other one in trackside. The Figure 94 gives an overview of CCTV system architecture.

To enable end-to-end CCTV system implementation, “Trackside” and “On-board” CCTV components are interconnected with the FRMCS infrastructure via the interfaces TSAPP (Trackside) and OBAPP (On-Board).

The description and the definition of the FRMCS infrastructure and the interfaces OBAPP/TSAPP are given in chapters 5 and 6.

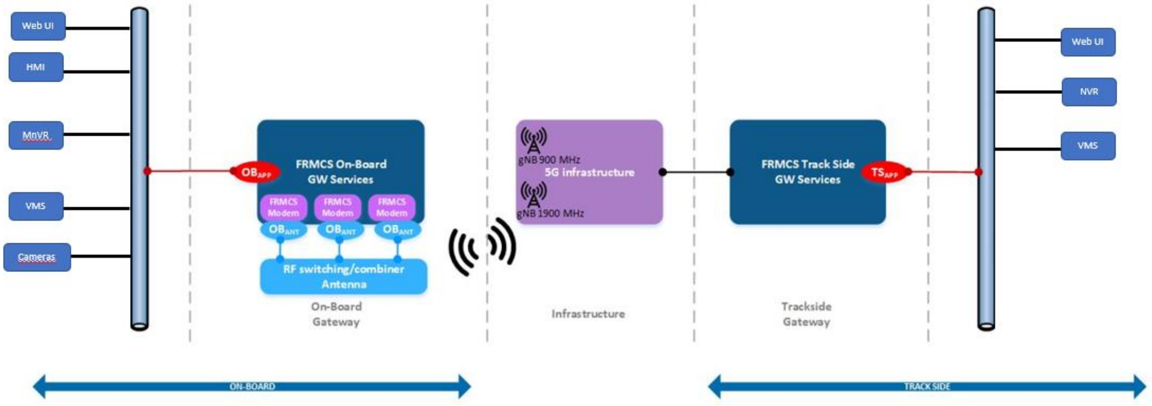


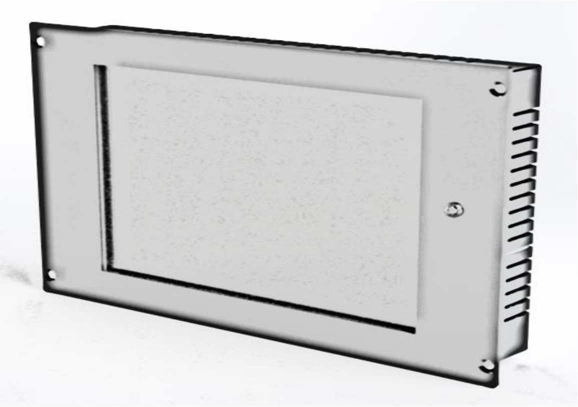
Figure 94: CCTV system architecture overview.

7.6.1.2 Hardware Platform

7.6.1.2.1 ON-BOARD

7.6.1.2.1.1 HUMAN MACHINE INTERFACE (HMI)

Figure 95: Human Machine Interface (HMI).



- Capacitive touchscreen for Human Machine Interface operation
- Easy installation and maintenance
- Fanless design and reliable TFT technology for low life cycle costs
- Light sensor for automatic brightness adjustment
- High brightness with bonded touchscreen for good visual performance
- H265 video

Table 46: Human Machine Interface Technical data

Usage	Rolling stock, indoor
Dimensions	420…430 x 270…280mm x ~60 (Not fixed, changes possible)
Weight	TBD
Housing	Aluminium/steel case
Protection class	IP54 front, IP30 back
Temperature range	Operational temperature -25°C to 60°C Storage temperature -40°C to 70°C
Operating voltage	110VDC, M12 connector
Power consumption	Approximately 34W at full brightness
Processor	Intel Atom E3940, 4GB RAM, 16GB eMMC Flash
Size and Format	15.6” / 16:9 aspect ratio
Active display area	344 x 194 mm
Resolution	1920 x 1080 pixels
Viewing angle	Wide viewing angle (170°). Symmetrical.
Brightness	850 cd/m², Backlight lifetime 50000h @ 25C
Contrast ratio	800:1
Interfaces	1 x Ethernet interface (10/100/1000BASE-TX, M12), Optional USB connection (TBD)
Standards	EN50155, EN50121-3-2, EN 45545-2

7.6.1.2.1.2 MOBILE NETWORK VIDEO RECORDER

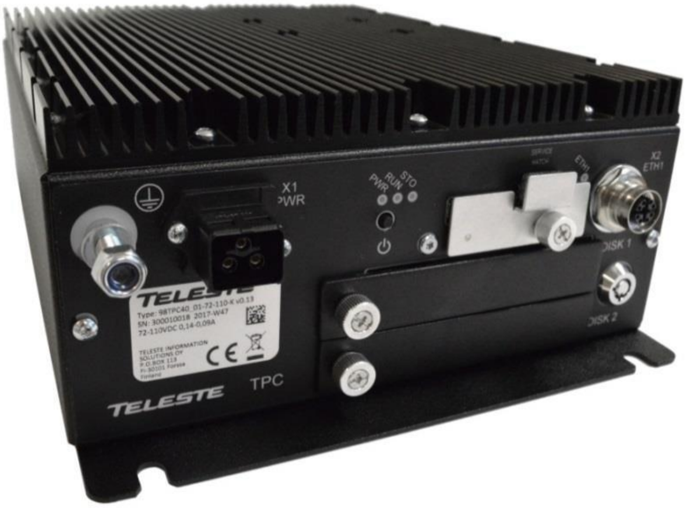


Figure 96: Mobile Network Video recorder.

- Standalone mass storage and video recording unit for rolling stock
- Alternative models for different operating voltages
- Two ejectable media trays with monitored lock for security (2 keys included)
- Media support for 2.5-inch SATA3 HDD or SSD drives, allowed thickness range 7…15 mm
- Passive cooling

Table 47: Mobile Network Video recorder Technical data

Usage	Rolling stock, indoor
Dimensions	190 x 89 x 278 mm (width x height x depth, including ground stud)
Weight	3.40 kg (without mass memories)
Housing	IP30, aluminium / steel sheet
Temperature range	Operational temperature -40 to +70 °C (EN 50155 class TX) Storage temperature -40 to +85 °C (both ranges may be limited by the installed disk drives)

Operating voltage	24 VDC (16.8 to 34.0 VDC) for model 98TPC40_01 72-110 VDC (50.4 to 137.5 VDC) for model 98TPC40_01-72-110
Power consumption	10 W (typical)
Processor	Intel® Atom™ E3845 Quad Core 1.91 GHz
Memory	4 GB DDR3L
Mass memory	16 GB eMMC for operating system and application software Media trays for 2.5-inch SATA mass memory HDD and/or SSD drives, SD card socket
Interface ports	10/100/1000 Mbps Ethernet (X-coded M12 Push-Pull), USB and DisplayPort for maintenance
Standards	EN 50155 (temperature range may be limited by selected disk drives), EN 50121-3-2, IEEE Std 1476, EN 45545-2, NFPA 130

7.6.1.2.1.3 CCTV CAMERA

CCTV camera

- Rugged network cameras for video surveillance in rolling stock
- H.264 with Zipstream technology and HD video resolutions
- WDR with forensic capturing and excellent light sensitivity with Lightfinder technology
- Power over Ethernet via M12 D-coded connector
- Various lens options available

Table 48: Technical data

	98VSC14	98VSC15	98VSC16
Usage	Rolling stock, indoor		
Dimensions	Height 49 mm, diameter 109 mm, without network cable (cable length is 300 mm).		
Weight	0.25 kg	0.25 kg	0.27 kg
Housing	IP66/67, IK08, aluminium / polycarbonate, light grey (NCS 1002-B)		
Temperature range	Operational temperature -40 to +60 °C, maximum intermittent +70 °C (EN 50155:2017 class OT2/ST2) Storage temperature -40 to +65 °C		
Power consumption	PoE class 2, max. 3.6 W		PoE class 2, max. 3.9 W
Maximum resolution	1280x720 to 160x90, HDTV 720p, max 25/30 fps	1920x1080 to 160x90, HDTV 1080p, max 25/30 fps	
Streaming	Multiple individually configurable streams in H.264 (with Zipstream) and MJPEG		
Angle of view	Angle of view 87° hor. & 47° ver. (on standard 3.6 mm F2.0 lens)		
Interfaces (on cable)	M12 D-coded 10/100BASE-TX port		M12 D-coded 10/100BASE-TX port, 3.5 mm audio input (mono), 4-pin terminal for digital I/O & 12 VDC output
Standards	EN 50155:2017 (vibration, mechanical shock, bump, temperature), EN 45545-2, EN 50121-3-2 (more data available upon request)		

7.6.1.2.2 TRACKSIDE

7.6.1.2.2.1 STREAMING SERVER

Figure 97: Streaming server.

VMS trackside Server is hosting multiple mandatory functionalities needed in video management system. These include system database, web access server, stream reflector, map server, device and telemetry controller. In more advanced systems these hosted services are available in stand-alone units. The VMS Server is responsible for user rights management including arbitration of priorities. It is managing log services, communication and handling system alarms. The configuration of system and component parameters is handled through configuration wizard application and stored into System Server’s database. The VMS Server is available in several pre-configured setups depending on the overall system parameters. The server can also take the role of back-up server within a system supporting redundancy.

7.6.1.3 Software Platform

Figure 98 below describes the CCTV VMS software components.

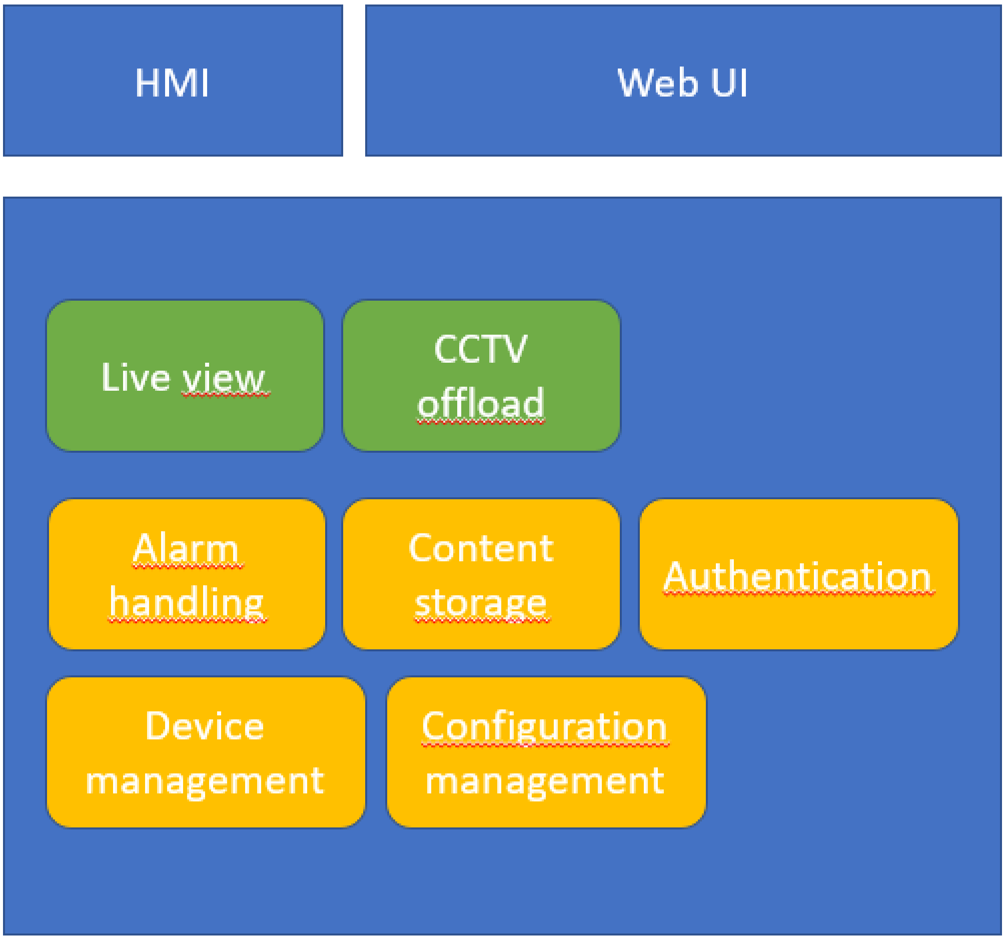


Figure 98: CCTV VMS software components.

7.6.1.3.1 HMI AND WEB USER INTERFACE

The Teleste VMS user interface can be is provided with HMI and as Web User Interface over PC.

- HMI
- Web User Interface

7.6.1.3.2 CCTV LIVE VIEW

Live View is an application, which allows live streaming of video from onboard cameras.

7.6.1.3.3 CCTV OFFLOAD

CCTV offload is an application, which allows the transfer of CCTV archives from onboard to the trackside.

7.6.1.3.4 ALARM HANDLING

Alarm handling monitors alarms and tags them with the events in the video. It also can create pre-configured actions and SOPs into other subsystems.

7.6.1.3.5 CONTENT STORAGE

Content storage module stores and manages recorded content and operates with CCTV offload application upon CCTV offload is triggered.

7.6.1.3.6 AUTHENTICATION

Authentication module is used to manage end user registrations.

7.6.1.3.7 DEVICE MANAGEMENT

Device management module maintains registrations of cameras and other sensors and devices.

7.6.1.3.8 CONFIGURATION MANAGEMENT

Configuration management is used to set-up different parameters of video streaming, e.g. resolution for cameras cyber security parameters and to configure interfaces with different systems.

7.6.1.4 Simulators (if applicable)

Not applicable.

7.6.2 INTERFACES

This section shall contain a description of the interfaces including the following subsections (if applicable) as well as including static and dynamic parts.

7.6.2.1 Interface to TOBA via OB$_{APP}$

On-board CCTV application is connected to the FRMCS on-board Gateway via OB$_{APP}$ interface using loose coupled approach i.e. the MCx client is part of the FRMCS on-board Gateway.

7.6.2.2 The definition of OB$_{APP}$ interface is given in chapter 6.

Trackside CCTV application is connected to the FRMCS trackside Gateway via TS$_{APP}$ interface using loose coupled approach i.e. the MCx client is part of the FRMCS trackside Gateway.

The definition of TS$_{APP}$ interface is given in chapter 6.3.

7.6.2.3 External Interfaces (if applicable)

Not applicable.

7.6.2.4 User Interfaces (if applicable)

7.6.2.4.1 CLOSED CIRCUIT TELEVISION (CCTV)

The web user interface can be tailored to the specific needs of operator. Standard templates or create user-specific layouts can be utilized based on individual needs. For example, third-party systemscan be integrated into the UI, or different content can be displayed from other systems. The web client is available through standard web browsers without OS or hardware dependencies

7.6.3 INTERWORKING WITH GSM-R

Not applicable.

7.6.4 CYBERSECURITY

7.6.4.1 Access control - Authentication and Authorization

Access and operations in the VMS are permitted to the operator based on his/her user permissions and are derived from his/her roles, for example an operator with the role “Administrator” would be able to manage other users, whilst an individual with the role “Operator” would be able to send messages. These profiles are configurable through the VMS webclient UI.

7.6.4.2 Network security and cryptography

Thoroughly taking care of personal data protection, VMS is compliant with state-of-the art cryptographic technologies will ensure that all your data stays safe and protected against cyber threats. You can encrypt internal communication between VMS applications, clients and servers connections, as well as between third party systems. In addition, the VMS enables functions such as watermarking, anti-tampering, video data encryption and digital video signature, which will harness your system with an extended level of cyber security.

7.7 REMOTE VISION

7.7.1 Remote Vision APPLICATION ARCHITECTURE PROPOSAL

7.7.1.1 Architecture Overview

Please note that the remote vision application is a sub system of the remote driving system. For integrity sake, we elaborate the details of the whole remote driving system which includes the remote vision application and to the remote driving desk.

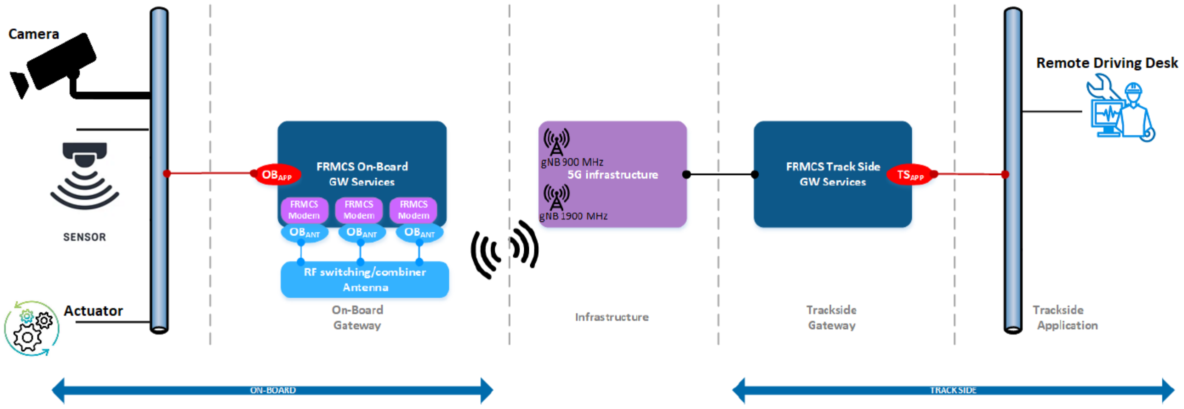


Figure 99: Global Architecture of the remote driving system in the FRMCS

The remote driving system has two parts: i) Onboard and ii) trackside one. The onboard part is depicted in Figure 100.

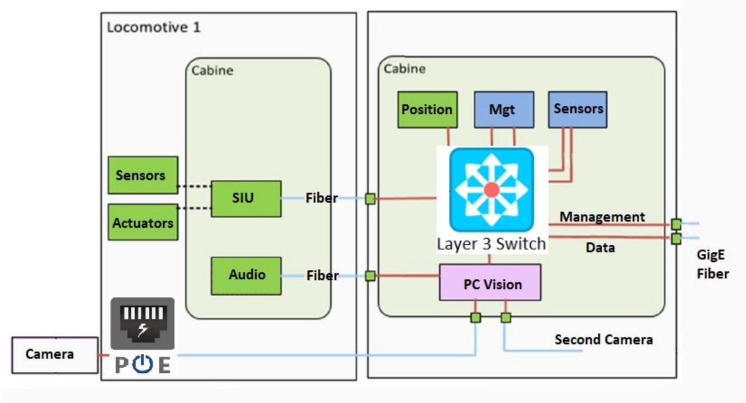


Figure 100: Onboard Logical Diagram

The onboard part includes a camera, a Power-over-Ethernet (PoE) module, a Specific Interface Unit (SIU) to concentrate sensors (Uplink: Moving Stock--Back-End) and actuators (Downlink: Back-End—Moving Stock), along to an audio input to provide a complete user-experience including video and voice.

Moreover, the SIU is connected through fiber optic cables to a Layer-3 (L3) switch, which also concentrates multiple blocks including: positioning input, bidirectional management, additional sensors, and most importantly, a PC vision block.

The PC vision block aggregates camera(s) inputs along to audio one and feed it to the L3 switch to transport the data and management streams using the transport stratum. This is where the remote vision application runs.

On the second hand, the trackside counter-part is depicted in Figure 101. It has a distributor to separate the FRMCS flow and synchronization data using NTP to a central authentication service (CAS), where another NTP source from a GPS antenna is fed, too. The data output from this CAS is fed into the remote driving desk for control and command.

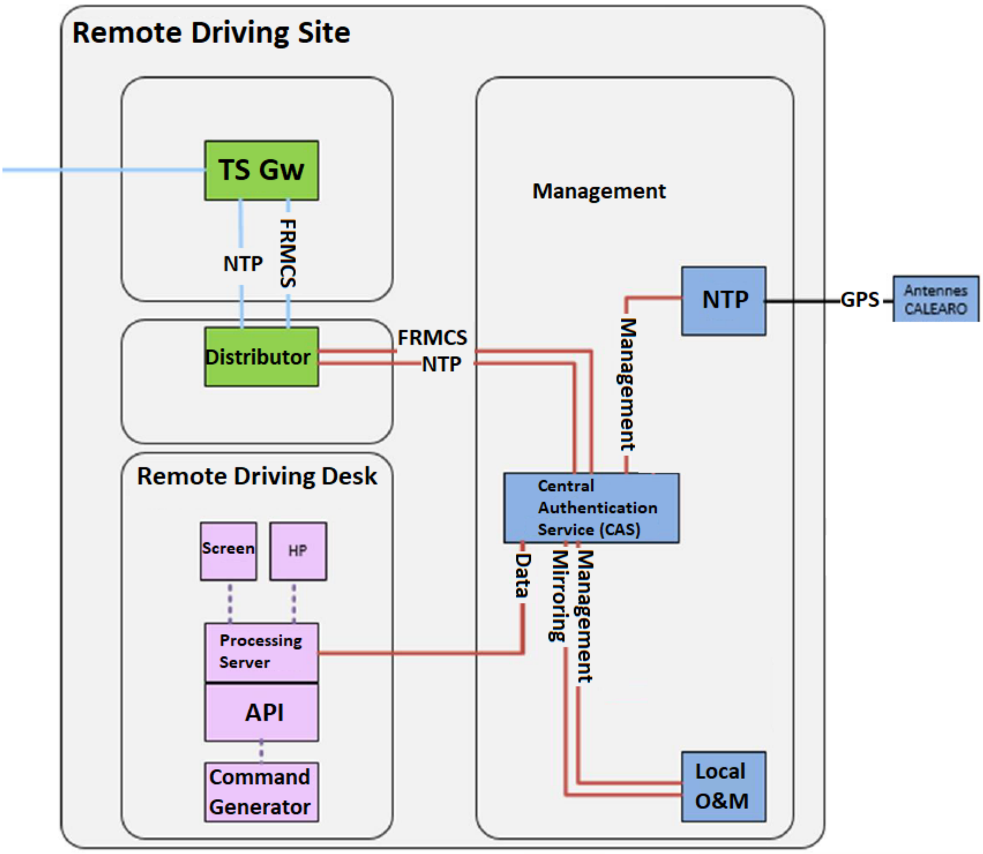


Figure 101: TrackSide Logical Diagram

7.7.1.2 Hardware Platform

Accordingly, we elaborate some technical details about the building blocks of the remote vision system.

7.7.1.2.1 CAMERA

The used camera is Prosilica GT1930 that is a 2.35 megapixel camera with a GigE Vision compliant Gigabit Ethernet port and Hirose I/O port. Prosilica GT1930 is available in both monochrome and color models.

This camera incorporates the high quality Sony IMX174 Exmor CMOS sensor with Pregius global shutter technology providing excellent monochrome and color image quality. At full resolution, this camera runs 50.8 frames per second. With a smaller region of interest, higher frame rates are possible.

This camera is a rugged camera designed to operate in extreme environments. It offers Precise iris lens control allowing users to fix the aperture size to optimize depth of field, exposure, and gain without the need for additional control elements.

7.7.1.2.2 LENS OBJECTIVE

This camera uses GigE Vision with 25 framerate/full HD/Global shutter by Stemmer with Cinegon 1.9/10-1901 lens objective. Such a wide angle 10 mm focal length C-Mount lens for 1" sensor with 5 mega-pixel resolution enables large field of views from short working distances.

The lens is equipped with a broadband Antireflection (AR) coating for 400 nm to 1000 nm suitable for use in visible and in NEAR-INFRARED (NIR) ranges.

Accordingly, the robust and compact design with lockable focus and iris setting guarantees reliable continuous images in production conditions.

7.7.1.2.3 POWER OVER ETHERNET INTERFACE

The Power Over Ethernet (PoE) assured by a Cudy POE300 60W Gigabit Ultra PoE+ Injector, consuming up to 60W Ultra Power Supply. This module features a 10/100/1000Mbps Shielded RJ-45, IEEE 802.3af/802.3at Compliant, Plug and Play, Metal housing 1 Gigabit Ethernet port input and 1 PoE+ Gigabit Ethernet port output that offers full duplex 2Gbps Ethernet speeds.

The PoE Injector is a single port PoE injector that offers a compact and cost-effective solution, it can convert standard 100-240V/AC power into low voltage DC that runs over existing LAN cable to power up IEEE802.3 BT/ AF/AT compliant network accessories.

7.7.1.2.4 REMOTE DRIVING DESK

The remote driving desk (RDD) subsystem exists in two flavors: heavy version and a light one. The difference is the number of screen and the complexity of the HMI. Note that the light version of the RDD consists of a screen and a PC only and it is already available off the shelf. It might be used during the tests as it is easier for transportation rather than the heavy one.

The RDD subsystem in its both flavors is configurable with adaptative algorithm according to network performances supporting Low-Definition/Medium-Definition/High-Definition. The heavy version of the RDD is depicted in Figure 102.

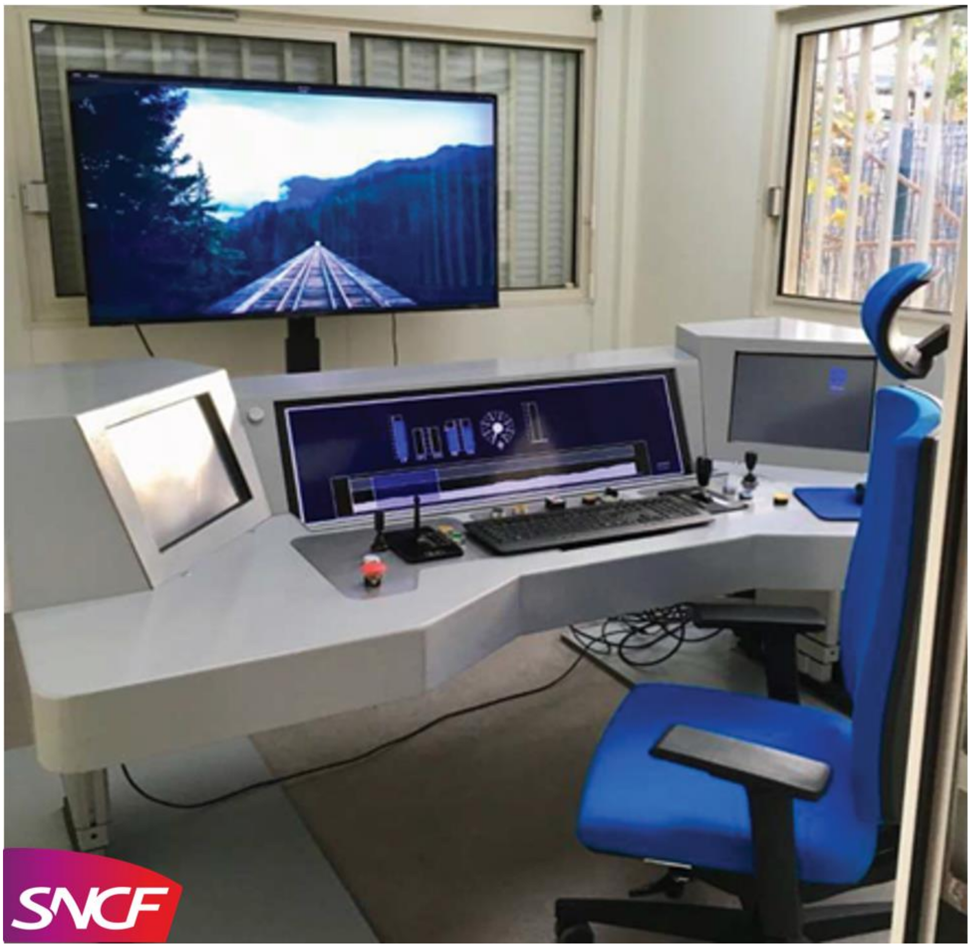


Figure 102: Photo of the Heavy version of the Remote Driving Desk

7.7.1.3 Software Platform

The PC vision provides low latency live image acquisition and video file transfer solution. It is optimized for remote IP links (satellite link, 4G, 3G, etc.).

Its software suite is made up of three components as depicted in Figure 103:

- An Encoder
- A Player
- and a Transcoder

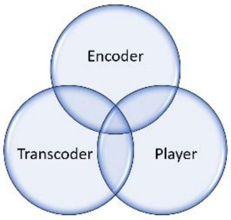


Figure 103: Software Platform of the PC Vision System

The Encoder captures an audio / video signal, compresses it in real time and broadcasts it to the Player. It adapts the bitrate according to the bandwidth of the IP link. The player decodes and displays the audio / video stream of the Encoder. The end-user can interact with an audio return voice that sends the sound back to the Encoder.

Finally, the Transcoder allows to transform a high bitrate format into a low bitrate one. The low-speed format is then transferred to a remote location via a low-speed link. Upon reception, the Transcoder transcodes back the low bit rate format to a high bit rate one that is usable in conventional video editing software.

The entire solution is based on the High Efficiency Video Coding (HEVC), also known as H. 265 and “MPEG-H Part 2” codec, allowing a significant gain in image quality.

7.7.2 INTERFACES

7.7.2.1 Interface to TOBA via OB_{APP}

On-board Remote vision application is connected to the FRMCS on-board Gateway via OB_{APP} interface using Flat-IP approach that is equivalent to “super-loose coupling”.

The definitions Flat-IP and the OB_{APP} interface are given in chapter 7.7.1.1.

7.7.2.2 Interface to TOBA via TS_{APP}

Trackside Remote driving desk is connected to the FRMCS trackside Gateway via TS_{APP} interface using Flat-IP approach that is equivalent to “super-loose coupling”.

The definitions Flat-IP and the TS_{APP} interface are given in chapter 7.7.1.1.

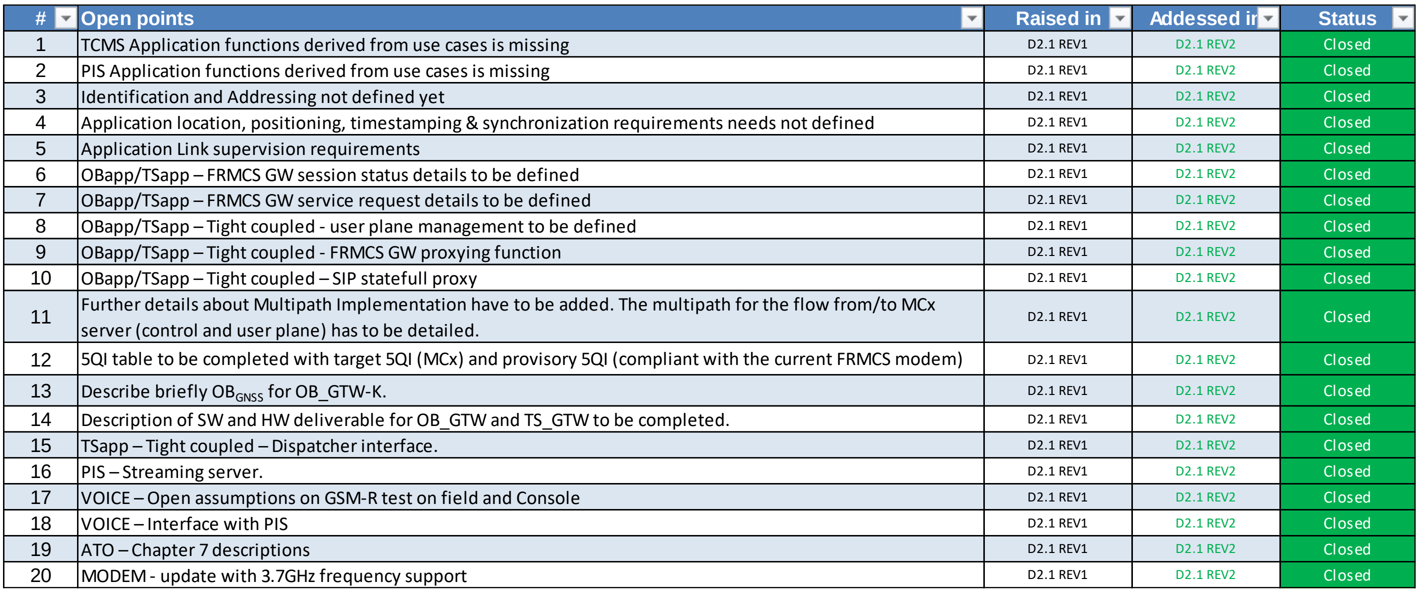
8 CONCLUSIONS

This document provides the architecture details to support the development of prototypes within WP2 that aims to be rolled out in Europe for a series of pilot tests (in labs & in the field) to demonstrate how these technical solutions can be integrated, to validate their feasibility and to evaluate their performance under a combination of environmental conditions in various test-sites (France, Hungary and Germany).

The main architecture challenge was the partial availability of specifications and to overcome that there is a set of assumptions listed in the chapter 3. This list linked to 5GRAIL context has been revisited in this release: based specification progress, some have been deleted, others have been updated or kept.

On top of that, several technical open points have emerged naturally during the architecture elaboration and were listed in revisions 1.0. These open points are in general due to FRMCS/5G specifications gaps. All these open points have been addressed in this revision, either by considering the specification work advance, or by agreeing within the Consortium assumptions.

Precisely, this D2.1 release 2.0 has addressed the below open points:



#	Open points	Raised in	Addessed ir	Status
1	TCMS Application functions derived from use cases is missing	D2.1 REV1	D2.1 REV2	Closed
2	PIS Application functions derived from use cases is missing	D2.1 REV1	D2.1 REV2	Closed
3	Identification and Addressing not defined yet	D2.1 REV1	D2.1 REV2	Closed
4	Application location, positioning, timestamping & synchronization requirements needs not defined	D2.1 REV1	D2.1 REV2	Closed
5	Application Link supervision requirements	D2.1 REV1	D2.1 REV2	Closed
6	OBapp/TSapp – FRMCS GW session status details to be defined	D2.1 REV1	D2.1 REV2	Closed
7	OBapp/TSapp – FRMCS GW service request details to be defined	D2.1 REV1	D2.1 REV2	Closed
8	OBapp/TSapp – Tight coupled - user plane management to be defined	D2.1 REV1	D2.1 REV2	Closed
9	OBapp/TSapp – Tight coupled - FRMCS GW proxying function	D2.1 REV1	D2.1 REV2	Closed
10	OBapp/TSapp – Tight coupled – SIP statefull proxy	D2.1 REV1	D2.1 REV2	Closed
11	Further details about Multipath Implementation have to be added. The multipath for the flow from/to MCx server (control and user plane) has to be detailed.	D2.1 REV1	D2.1 REV2	Closed
12	5QI table to be completed with target 5QI (MCx) and provisory 5QI (compliant with the current FRMCS modem)	D2.1 REV1	D2.1 REV2	Closed
13	Describe briefly OB_{GNSS} for OB_GTW-K.	D2.1 REV1	D2.1 REV2	Closed
14	Description of SW and HW deliverable for OB_GTW and TS_GTW to be completed.	D2.1 REV1	D2.1 REV2	Closed
15	TSapp – Tight coupled – Dispatcher interface.	D2.1 REV1	D2.1 REV2	Closed
16	PIS – Streaming server.	D2.1 REV1	D2.1 REV2	Closed
17	VOICE – Open assumptions on GSM-R test on field and Console	D2.1 REV1	D2.1 REV2	Closed
18	VOICE – Interface with PIS	D2.1 REV1	D2.1 REV2	Closed
19	ATO – Chapter 7 descriptions	D2.1 REV1	D2.1 REV2	Closed
20	MODEM - update with 3.7GHz frequency support	D2.1 REV1	D2.1 REV2	Closed

Thanks to these progresses, the prototype development activities can start, although they might be few system topics that will need further elaboration such as MCX domain management : in fact how the FRMCS gateways identifies the MCX origin domain and manage the migration to other MCX domains in use case such as cross-border scenario.

The objective is to clarify such points as we are progressing on the 5GRAIL project execution and this will be captured in the next deliverables. Meaning the very first integration test outcomes will be captured in D2.2 Integration Report and the findings from Lab and Field trial execution will be capitalized in D2.4 Test Report.

9 APPENDICES

9.1 Appendix 1 – Communication attributes to QoS

When requesting a session establishment, the application sends to the OB_GTW a requested comm_profile (see chapter **6.2.4.4.3**), which reflects its need for the session in terms of communication attributes. The OB_GTW must be able to bind it to QoS parameters relevant for 5G network (assuming that we provide QoS only on 5G in a first implementation, see assumption #49).

Then, we need a table to map the comm_profile (requested by the application) to QoS rules.

For the first 5GRAIL implementation, it is not expected to have a dynamic QoS mechanism in the core Network (e.g. a MCx server which requests some communication attributes to the PCF, which would trigger dedicated QoS flows establishment in the network for the considered session). The QoS will be statically managed in the core network (please refer to WP3 and WP4 documents for more details). The network will be able to differentiate the flows for which a dedicated QoS flows must be used thanks to the DSCP value. Then, the OB_GTW is responsible for applying the relevant DSCP value in the UP data transmitted toward the network.

The table below shows the correspondence between:

- 1st column: the comm_profile index requested by the application during the SESSION_START request
- 2nd and 3rd columns: the corresponding DSCP value to be applied by the OB_GTW on the UP data
- 4th column: the QoS parameters to be configured (statically) by the infrastructure for this DSCP value. Note: this column is given as an example only, but it will have to be completed with WP3 and WP4 to take into account the capabilities of the infrastructure and the modems.

Table 49: Translation table from comm_profile to QoS

Application	**OB_GTW**		**Infrastructure static configuration**
comm_profile transmitted by the application	**DSCP value (bit)**	**DSCP value (decimal)**	**QoS parameters on the FRMCS network**
1- Voice	101 101	43	*To be completed with WP3-4 following infrastructure and modem capabilities.* *See WP3-4 documentation*
2- Operational Voice	101 010	42	
3- Emergency voice	101 001	41	
4- Video	100 001	33	
5- Low latency Video	100 000	32	

6- Non harmonized Data	001 000	8	
7- Operational Data	010 011	19	
8- Emergency Data	010 111	23	
9- Low latency Data	010 110	22	
10 - ETCS	010 101	21	
11-ATO	010 100	20	

Note: This table has been elaborated following draft 0.2.2 of FRMCS SRS (which gives correspondence between applications and 5QI/ARP) and an IETF draft (https://tools.ietf.org/id/draft-henry-tsvwg-diffserv-to-qci-03.html) which gives some guidance for a mapping between DSCP values and 5QI following RFC4594 recommendations.

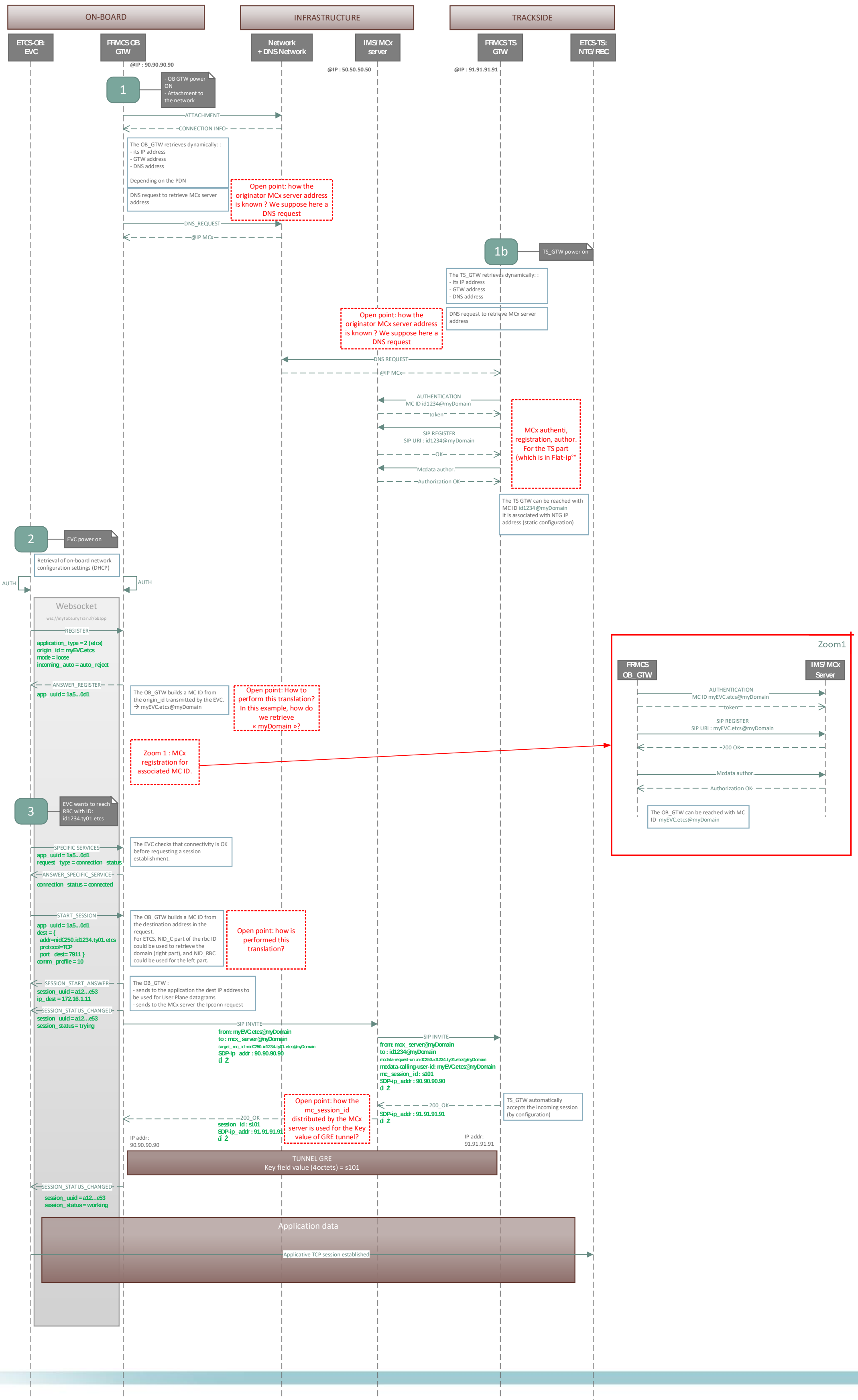
Note 2 : This is a provisory mechanism to ensure that a certain QoS will be applied. The target MCx mechanism (with MCx server performing dynamically a DIAMETER request to the PCF) cannot be undertaken due to the non-availability of PCF.

9.2 Appendix 2 - End to end dataflows

Example of dataflow diagrams for session establishment are given below:

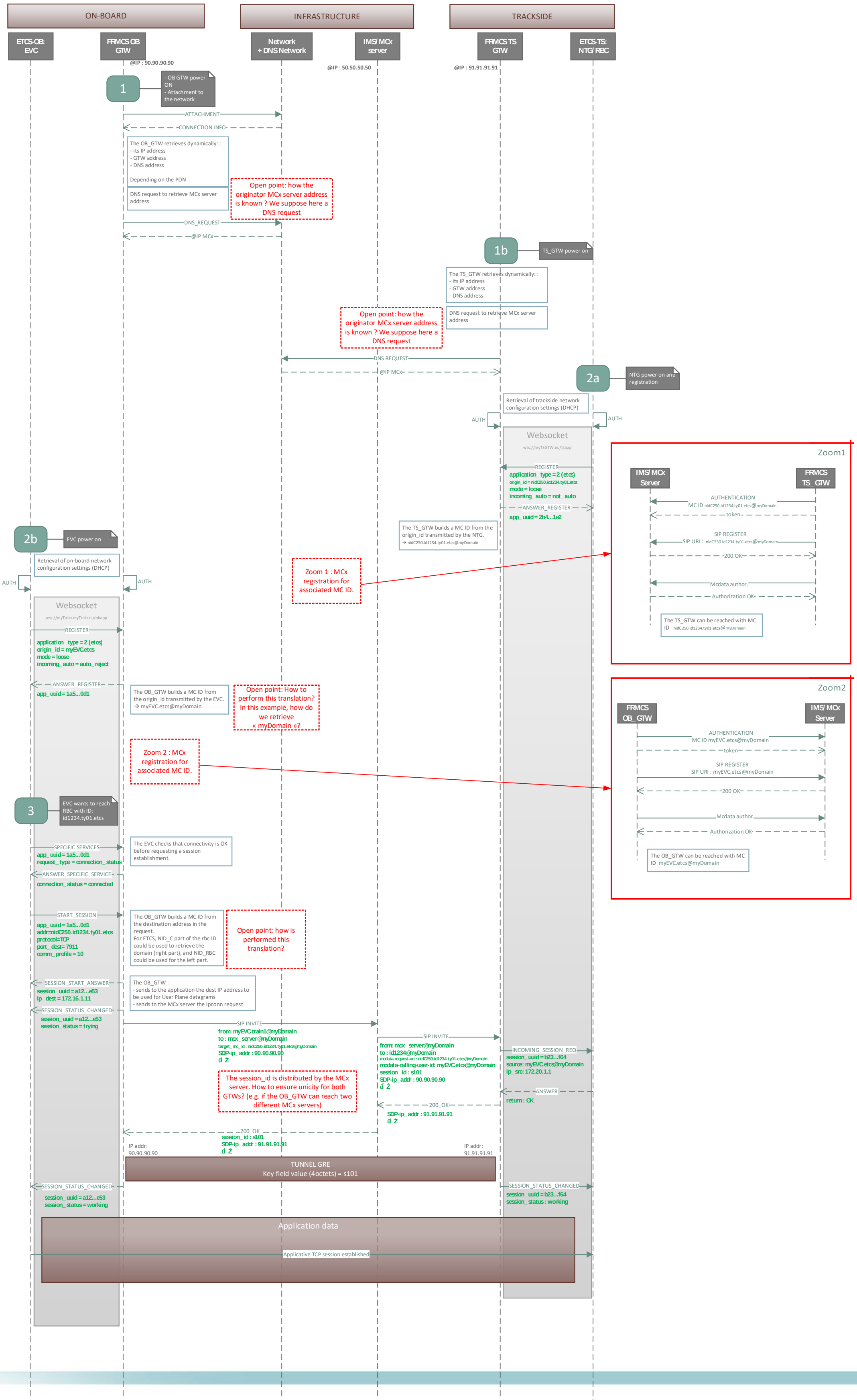
Session establishment for Loose-coupled application.

Example for ETCS-Alstom in Phase 2.2 (on-board in LC mode, trackside in Flat-IP mode).
FRMCS Session : Mcdata-IPcon
Scenario: one connection from the EVC to rbc with RBC ID id1234.ty01.etcs..


ON-BOARD
INFRASTRUCTURE
TRACKSIDE
ETCS-OB: EVC
FRMCS OB GTW
Network + DNS Network
IMS/ MCx server
FRMCS TS GTW
ETCS-TS: NTG/ RBC
@IP : 90.90.90.90
@IP : 50.50.50.50
@IP : 91.91.91.91
1
- OB GTW power ON
- Attachment to the network
ATTACHMENT
CONNECTION INFO
The OB_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address
Depending on the PDN
DNS request to retrieve MCx server address
Open point: how the originator MCx server address is known ? We suppose here a DNS request
DNS_REQUEST
@IP MCx
1b
TS_GTW power on
The TS_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address
DNS request to retrieve MCx server address
Open point: how the originator MCx server address is known ? We suppose here a DNS request
DNS REQUEST
@IP MCx
AUTHENTICATION
MC ID id1234@myDomain
token
SIP REGISTER
SIP URI : id1234@myDomain
OK
Mcdata author.
Authorization OK
MCx authenti, registration, author. For the TS part (which is in Flat-ip°°
The TS GTW can be reached with MC ID id1234@myDomain
It is associated with NTG IP address (static configuration)
2
EVC power on
Retrieval of on-board network configuration settings (DHCP)
AUTH
AUTH
Websocket
wss://myToba.myTrain.fr/obapp
REGISTER
application_type = 2 (etcs)
origin_id = myEVC.etcs
mode = loose
incoming_auto = auto_reject
ANSWER_REGISTER
app_uuid = 1a5...0d1
The OB_GTW builds a MC ID from the origin_id transmitted by the EVC.
→ myEVC.etcs@myDomain
Open point: How to perform this translation? In this example, how do we retrieve « myDomain »?
Zoom 1 : MCx registration for associated MC ID.
Zoom1
FRMCS OB_GTW
IMS/ MCx Server
AUTHENTICATION
MC ID myEVC.etcs@myDomain
token
SIP REGISTER
SIP URI : myEVC.etcs@myDomain
200 OK
Mcdata author.
Authorization OK
The OB_GTW can be reached with MC ID myEVC.etcs@myDomain
3
EVC wants to reach RBC with ID: id1234.ty01.etcs
SPECIFIC SERVICES
app_uuid = 1a5...0d1
request_type = connection_status
The EVC checks that connectivity is OK before requesting a session establishment.
ANSWER_SPECIFIC_SERVICE
connection_status = connected
START_SESSION
app_uuid = 1a5...0d1
dest = {
addr=nidC250.id1234.ty01.etcs
protocol=TCP
port_dest= 7911 }
comm_profile = 10
The OB_GTW builds a MC ID from the destination address in the request.
For ETCS, NID_C part of the rbc ID could be used to retrieve the domain (right part), and NID_RBC could be used for the left part.
Open point: how is performed this translation?
SESSION_START_ANSWER
session_uuid = a12...e53
ip_dest = 172.16.1.11
The OB_GTW :
- sends to the application the dest IP address to be used for User Plane datagrams
- sends to the MCx server the Ipconn request
SESSION_STATUS_CHANGED
session_uuid = a12...e53
session_status = trying
SIP INVITE
from: myEVC.etcs@myDomain
to : mcx_server@myDomain
target_mc_id :nidC250.id1234.ty01.etcs@myDomain
SDP-ip_addr : 90.90.90.90
ű Ź
SIP INVITE
from: mcx_server@myDomain
to : id1234@myDomain
mcdata-request-uri :nidC250.id1234.ty01.etcs@myDomain
mcdata-calling-user-id: myEVC.etcs@myDomain
mc_session_id : s101
SDP-ip_addr : 90.90.90.90
ű Ź
TS_GTW automatically accepts the incoming session (by configuration)
200_OK
SDP-ip_addr : 91.91.91.91
ű Ź
Open point: how the mc_session_id distributed by the MCx server is used for the Key value of GRE tunnel?
200_OK
session_id : s101
SDP-ip_addr : 91.91.91.91
ű Ź
IP addr: 90.90.90.90
IP addr: 91.91.91.91
TUNNEL GRE
Key field value (4octets) = s101
SESSION_STATUS_CHANGED
session_uuid = a12...e53
session_status = working
Application data
Applicative TCP session established

Session establishment for Loose-coupled application.

Example for ETCS with full OBapp/ TSapp (on-board in LC mode, trackside in LC mode).
FRMCS Session : Mcdata-IPcon
Scenario: one connection from the EVC to rbc with RBC ID id1234.ty01.etcs..



The OB_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address

Depending on the PDN

DNS request to retrieve MCx server address

Open point: how the originator MCx server address is known ? We suppose here a DNS request

The TS_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address

DNS request to retrieve MCx server address

Open point: how the originator MCx server address is known ? We suppose here a DNS request

Retrieval of trackside network configuration settings (DHCP)

The TS_GTW builds a MC ID from the origin_id transmitted by the NTG.
→ nidC250.id1234.ty01.etcs@myDomain

Zoom 1 : MCx registration for associated MC ID.

The TS_GTW can be reached with MC ID nidC250.id1234.ty01.etcs@myDomain

Retrieval of on-board network configuration settings (DHCP)

The OB_GTW builds a MC ID from the origin_id transmitted by the EVC.
→ myEVC.etcs@myDomain

Open point: How to perform this translation? In this example, how do we retrieve « myDomain »?

Zoom 2 : MCx registration for associated MC ID.

The OB_GTW can be reached with MC ID myEVC.etcs@myDomain

The EVC checks that connectivity is OK before requesting a session establishment.

The OB_GTW builds a MC ID from the destination address in the request.
For ETCS, NID_C part of the rbc ID could be used to retrieve the domain (right part), and NID_RBC could be used for the left part.

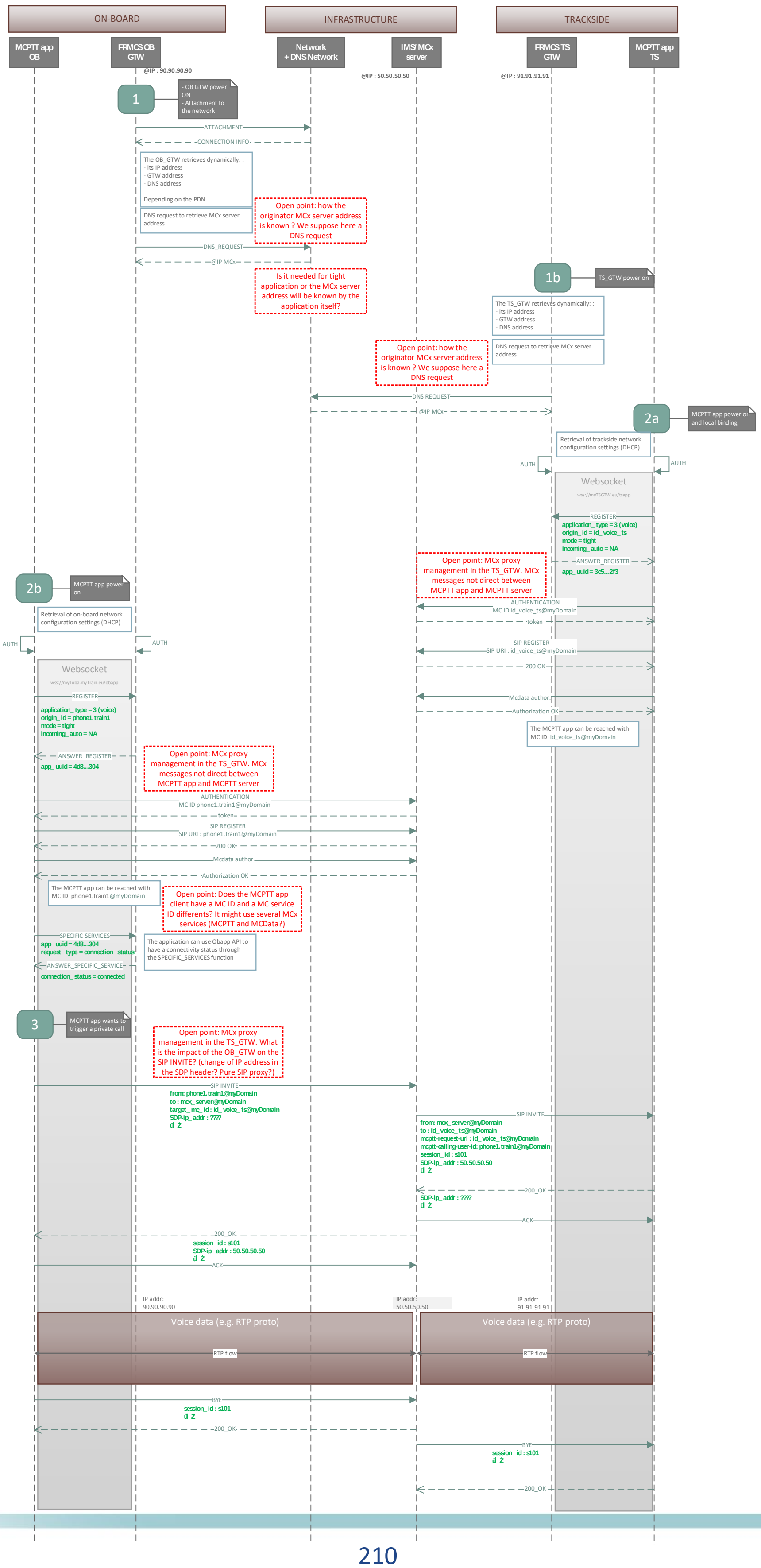
Open point: how is performed this translation?

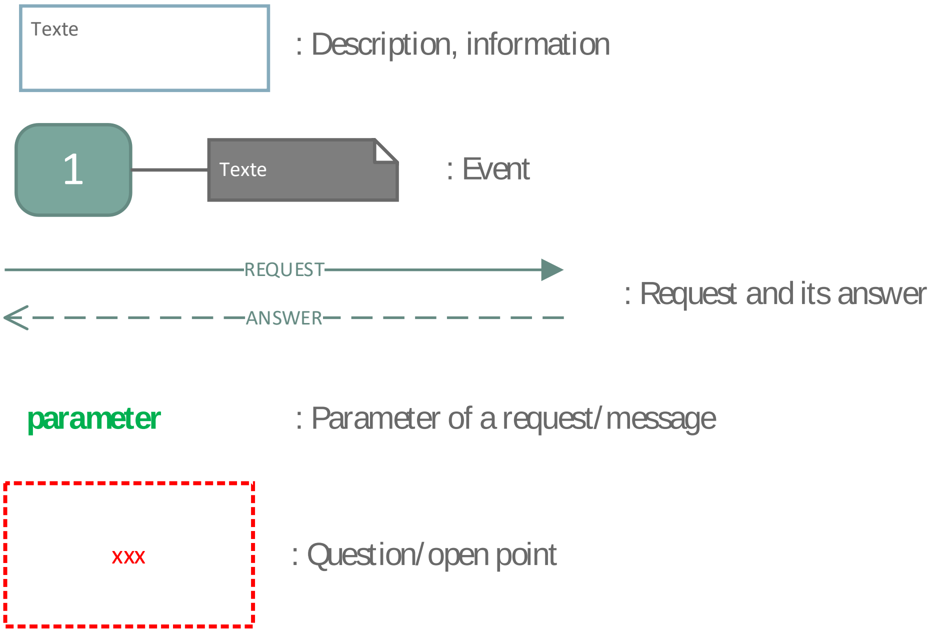
The OB_GTW :
- sends to the application the dest IP address to be used for User Plane datagrams
- sends to the MCx server the Ipconn request

The session_id is distributed by the MCx server. How to ensure unicity for both GTWs? (e.g. if the OB_GTW can reach two different MCx servers)

Session establishment for Tight-coupled application.

Example for voice application.
FRMCS Session : MCPTT
Scenario: one private call from train to ground.


ON-BOARD
INFRASTRUCTURE
TRACKSIDE
MCPTT app OB
FRMCS OB GTW
Network + DNS Network
IMS/ MCx server
FRMCS TS GTW
MCPTT app TS
@IP : 90.90.90.90
@IP : 50.50.50.50
@IP : 91.91.91.91
1
- OB GTW power ON
- Attachment to the network
ATTACHMENT
CONNECTION INFO
The OB_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address
Depending on the PDN
DNS request to retrieve MCx server address
Open point: how the originator MCx server address is known ? We suppose here a DNS request
DNS_REQUEST
@IP MCx
Is it needed for tight application or the MCx server address will be known by the application itself?
1b
TS_GTW power on
The TS_GTW retrieves dynamically: :
- its IP address
- GTW address
- DNS address
DNS request to retrieve MCx server address
Open point: how the originator MCx server address is known ? We suppose here a DNS request
DNS REQUEST
@IP MCx
2a
MCPTT app power on and local binding
Retrieval of trackside network configuration settings (DHCP)
AUTH
AUTH
Websocket
wss://myTSGTW.eu/tsapp
REGISTER
application_type = 3 (voice)
origin_id = id_voice_ts
mode = tight
incoming_auto = NA
ANSWER_REGISTER
app_uuid = 3c5...2f3
Open point: MCx proxy management in the TS_GTW. MCx messages not direct between MCPTT app and MCPTT server
AUTHENTICATION
MC ID id_voice_ts@myDomain
token
SIP REGISTER
SIP URI : id_voice_ts@myDomain
200 OK
Mcdata author.
Authorization OK
The MCPTT app can be reached with MC ID id_voice_ts@myDomain
2b
MCPTT app power on
Retrieval of on-board network configuration settings (DHCP)
AUTH
AUTH
Websocket
wss://myToba.myTrain.eu/obapp
REGISTER
application_type = 3 (voice)
origin_id = phone1.train1
mode = tight
incoming_auto = NA
ANSWER_REGISTER
app_uuid = 4d8...304
Open point: MCx proxy management in the TS_GTW. MCx messages not direct between MCPTT app and MCPTT server
AUTHENTICATION
MC ID phone1.train1@myDomain
token
SIP REGISTER
SIP URI : phone1.train1@myDomain
200 OK
Mcdata author.
Authorization OK
The MCPTT app can be reached with MC ID phone1.train1@myDomain
Open point: Does the MCPTT app client have a MC ID and a MC service ID differents? It might use several MCx services (MCPTT and MCData?)
SPECIFIC SERVICES
app_uuid = 4d8...304
request_type = connection_status
ANSWER_SPECIFIC_SERVICE
connection_status = connected
The application can use Obapp API to have a connectivity status through the SPECIFIC_SERVICES function
3
MCPTT app wants to trigger a private call
Open point: MCx proxy management in the TS_GTW. What is the impact of the OB_GTW on the SIP INVITE? (change of IP address in the SDP header? Pure SIP proxy?)
SIP INVITE
from: phone1.train1@myDomain
to : mcx_server@myDomain
target_mc_id : id_voice_ts@myDomain
SDP-ip_addr : ????
ú Ź
SIP INVITE
from: mcx_server@myDomain
to : id_voice_ts@myDomain
mcptt-request-uri : id_voice_ts@myDomain
mcptt-calling-user-id: phone1.train1@myDomain
session_id : s101
SDP-ip_addr : 50.50.50.50
ú Ź
200_OK
SDP-ip_addr : ????
ú Ź
ACK
200_OK
session_id : s101
SDP-ip_addr : 50.50.50.50
ú Ź
ACK
IP addr:
90.90.90.90
IP addr:
50.50.50.50
IP addr:
91.91.91.91
Voice data (e.g. RTP proto)
RTP flow
Voice data (e.g. RTP proto)
RTP flow
BYE
session_id : s101
ú Ź
200_OK
BYE
session_id : s101
ú Ź
200_OK



There are 3 diagrams:

- OB application in Loose-coupling; TS application in “flat-ip” coupling, MCdata session
- OB and TS applications in Loose-coupling, MCData session
- OB and TS applications in Tight coupling, MCPTT private call

9.3 Appendix 3 – Application type and application profile

The list of application_type (parameters given by the application during REGISTER function, see chapter **6.2.4.4.1**) has been reworked and simplified, it is given in the table below :

Table 50: Application type list

APPLICATION TYPE	TITLE
1	**ATO**
2	**ETCS**
3	**Voice**
4	**TCMS**
5	**PIS**

6	**CCTV offload**
7	**CCTV live view**
8	**Remote vision**

The mapping with 5GRAIL applications is obvious because is aligned with the list of applications for WP2.

During a REGISTER, the OB_GTW or TS_GTW must link an application_type to an application profile configured in the gateway. The definition of application profile is under discussion.

However, a proposal is presented below to define the format of an application_profile. The table below may evolve in the next versions following discussions on this open point.

Table 51: Example of application_profile

Profile	Allowed radio access and priority					Max number of connections	List of Allowed comm_profile index
	5G Modem 1	5G Modem 2	4G modem	Wi-Fi modem	Sat. modem		
1-ato	1	2	3	No	No	1	6; 7; 9; 11
2-etcs	1	2	3	No	No	1	6; 7; 9; 10
3-voice	1	2	No	No	No	10	Not applicable (tight-coupling)
4-tcms	1	2	3	No	No	1	6; 7; 9

9.4 Appendix 6 – Example to illustrate the virtual session IP address

This appendix provides an example of session establishment for a loose-coupled application with an illustration of the virtual session IP address principle.

This example is presented in the slides below presented during a 5GRAIL workshop addressing ETCS (October 2021):

1 Principles

Principles for a session initiated by the train side.

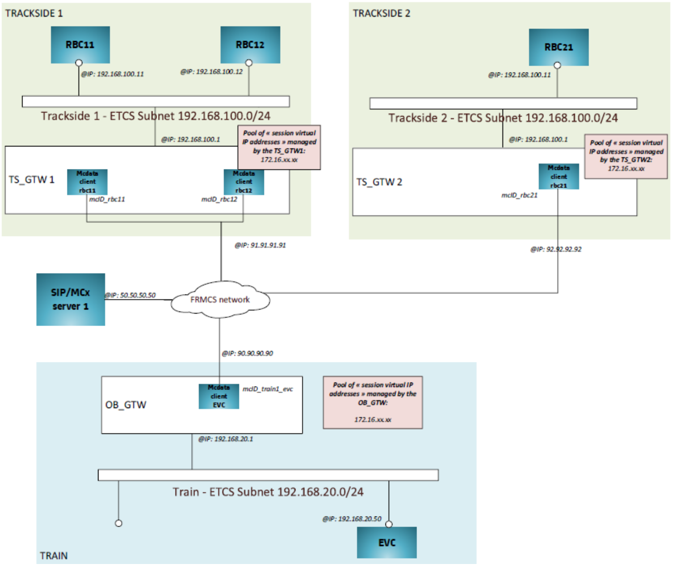
- On-board:
  - The OB_GTW has a pool of “virtual session IP addresses”. Following a SESSION_START request, the OB_GTW distributes one of these virtual addresses to the application. This will be linked to the established session (GRE tunnel if using MCData).
  - The OB_GTW uses this IP address to filter and redirects UP data to the relevant tunnel.
- Trackside:
  - The TS_GTW has a pool of “virtual session IP addresses”. Following an incoming session request, the TS_GTW uses one of these virtual addresses (as source IP address) to forward the future message to the concerned application. This will be linked to the established session (GRE tunnel if using MCData).
  - The TS_GTW uses this IP address to filter and redirects UP data to the relevant tunnel.
- NAT is performed on the side that did not “initiate” the session (TS_GTW for ETCS application).
- For a session initiated by trackside, we only have to invert OB_GTW and TS_GTW in the previous explanations.

2

Example 1

One EVC connected to two RBCs behind two TS_GTW, one MCx server

Initial situation



- After registrations to the MCx server from all the concerned clients, the MCx server has the following entrances:

MC ID	IP address
mcid_train1_evc	90.90.90.90
mcid_rbc11	91.91.91.91
mcid_rbc12	91.91.91.91
mcid_rbc21	92.92.92.92

- In this scenario, the pools of session virtual IP addresses are the same for all OB_GTW and TS_GTW (172.16.xx.xx), but it could be different.

SESSION_START performed by EVC to reach rbc11

- SESSION_START performed by the EVC to join rbc11 ; answer from the OB_GTW:

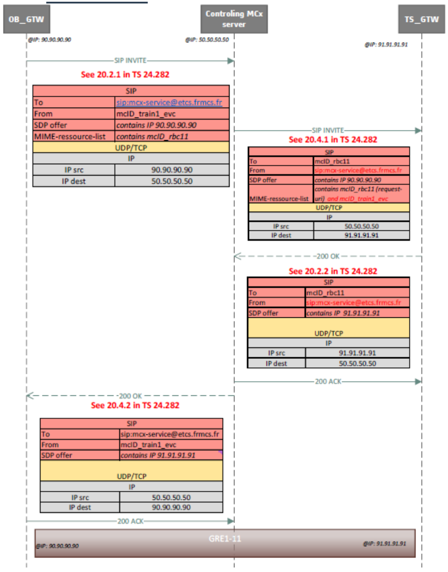
```
--> {  "jsonrpc": "2.0",
       "method": "session_start",
       "params": {    "app_uuid": "123e4567-e89b-12d3-a456-426614174000",
                      "destination": {
                              "addr": "rbc_id_11", #ETCS ID OF RBC 11
                              "protocol": 6,
                              "port": 7911
                              },
                      "comm_profile": 3     }
       "id": 3}

<-- {"jsonrpc": "2.0",
       "result": {    "session_uuid": "9816177b-7447-415e-8de9-78f5b19f091c"
                       "ip_dest": "172.16.1.11"   }
       "id": 3}
```

- The OB_GTW establishes the MCData session with TS_GTW1 (which contains the client answering to mcid_rbc11).
- This session is associated with dest IP address 172.16.1.11 (which is the so-called "virtual session IP address")

ALSTOM

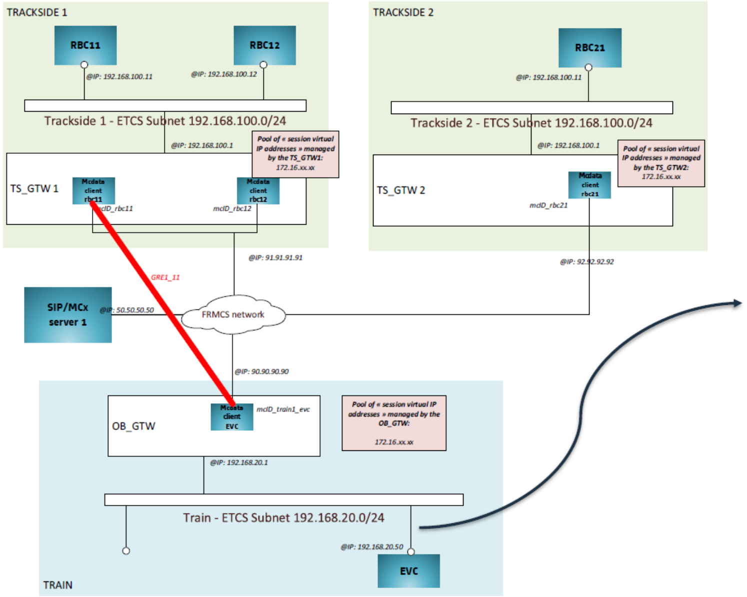
Tunnel establishment between OB_GTW and TS_GTW



- Mcdata session separated into two GRE tunnels or direct between both clients?
- For 5GRAIL, in a first approach, we consider a direct GRE tunnel between both OB_GTW and TS_GTW.
- The key used in the GRE layers must be aligned for both OB_GTW and TS_GTW (under responsibility of MCx server)

ALSTOM

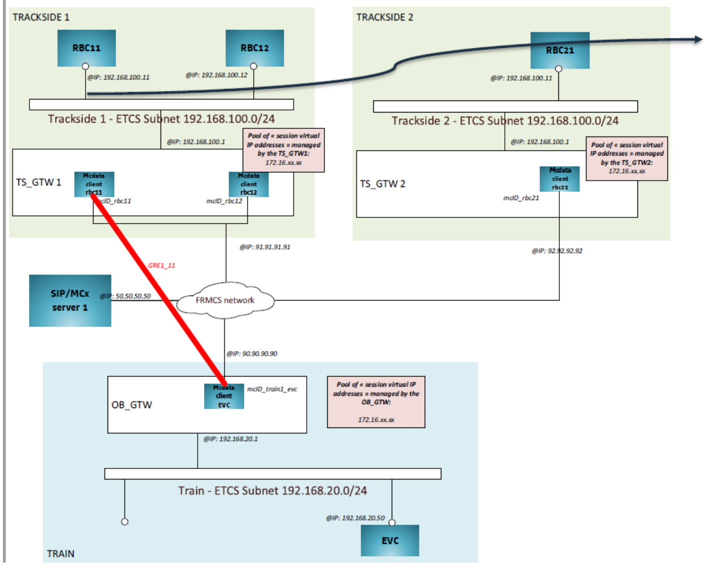
After session establishment - On-board side



- For the EVC, the RBC11 to join has the following IP address: 172.16.1.11
- The UP data will have the following features:
  - IP src: 192.168.20.50
  - IP dest: 172.16.1.11
  - Protocol: 6 (TCP)
  - Port dest: 7911

ALSTOM

After session establishment - Trackside



- When it receives the SIP INVITE, the TS_GTW knows that the session is directed to rbc11 (thanks to the dest MC ID) and knows that the local IP address of rbc11 is 192.168.100.11 (thanks to the REGISTER)
- It associates a “virtual session IP address” to the session : 172.16.1.50
- For the RBC11, the EVC has the following IP address: 172.16.1.50
- The incoming UP data arriving from the EVC have the following features:
  - IP src: 172.16.1.50
  - IP dest: 192.168.100.11
  - Protocol: 6 (TCP)
  - Port dest: 7911

ALSTOM

Second SESSION_START performed by EVC to reach rbc21

- SESSION_START performed by the EVC to join rbc21 ; answer from the OB_GTW:

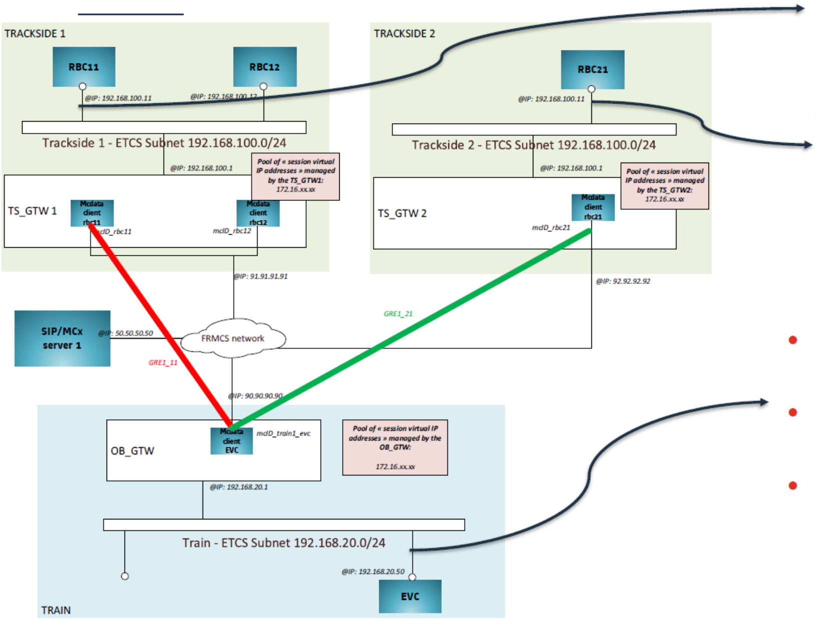
```
--> {  “jsonrpc”: “2.0”,
        “method”: “session_start”,
        “params”: {    “app_uuid”: “123e4567-e89b-12d3-a456-426614174000”,
                        “destination”: {
                                “addr”: “rbc_id_21”, #ETCS ID OF RBC 21
                                “protocol”: 6,
                                “port”: 5678
                                },
                        “comm_profile”: 3     }
        “id”: 3}

<-- {“jsonrpc”: “2.0”,
        “result”: {    “session_uuid”: “9816177b-7447-415e-8de9-78f5b19f091c”
                         "ip_dest": "172.16.1.21"  }
        “id”: 3}
```

- The OB_GTW establishes the MCData session with TS_GTW2 (which contains the client answering to mcid_rbc21). And builds the context of the session with filter rules, using the address 172.16.1.21.
- On TS_GTW2, let us assume that the virtual session IP address allocated for this session is 172.16.1.50 (it can be the same than the one allocated by TS_GTW1 for session with RBC11, since both pools are fully independent).

● ALSTOM ●

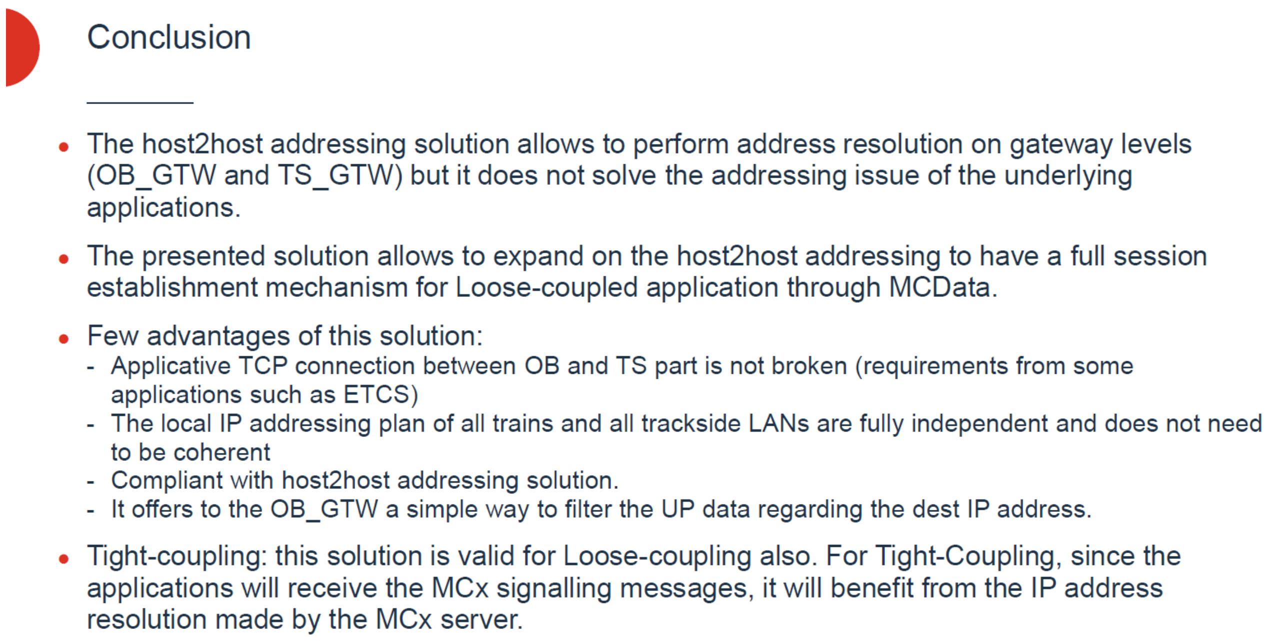
Session ready for rbc21 - User data plane sent to rbc21 (1/2)



- The RBC11 see the EVC of train 1 as it had the IP address 172.16.1.50
- The RBC21 see the EVC of train 1 as it had the IP address 172.16.1.50 (same than for RBC11 but it could be different)
- The EVC sends the data for rbc11 to the IP 172.16.1.11
- The EVC sends the data for rbc21 to the IP 172.16.1.21
- The OB_GTW uses this dest IP address to redirect to tunnel GRE1_11 or GRE1_21

● ALSTOM ● 11

3 Conclusion



Conclusion

- The host2host addressing solution allows to perform address resolution on gateway levels (OB_GTW and TS_GTW) but it does not solve the addressing issue of the underlying applications.
- The presented solution allows to expand on the host2host addressing to have a full session establishment mechanism for Loose-coupled application through MCData.
- Few advantages of this solution:
  - Applicative TCP connection between OB and TS part is not broken (requirements from some applications such as ETCS)
  - The local IP addressing plan of all trains and all trackside LANs are fully independent and does not need to be coherent
  - Compliant with host2host addressing solution.
  - It offers to the OB_GTW a simple way to filter the UP data regarding the dest IP address.
- Tight-coupling: this solution is valid for Loose-coupling also. For Tight-Coupling, since the applications will receive the MCx signalling messages, it will benefit from the IP address resolution made by the MCx server.

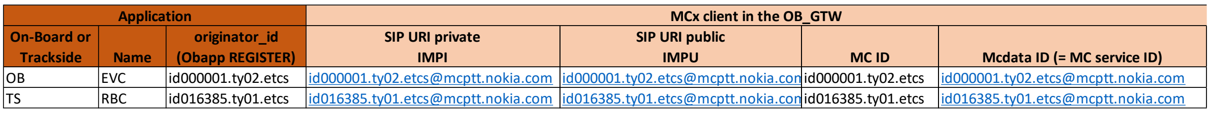
9.5 Appendix 7 – ID to be used in WP3 and WP4

The aim of these tables is to give a view of the OB_{APP}/TS_{APP} clients needed per each application, and the underlying SIP ID and MCx ID that must be configured in the infrastructure.

These tables were discussed during coordination meetings between Work packages 2, 3 and 4, it is a first pragmatic implementation of the SIP/MCx addressing to be used in 5GRAIL but not necessarily aligned with the standard addressing mechanism (which is to be further described in future version of FRMCS FIS). Especially, only one static domain part is used in each WP, and domain parts for SIP and MC IDs are the same.

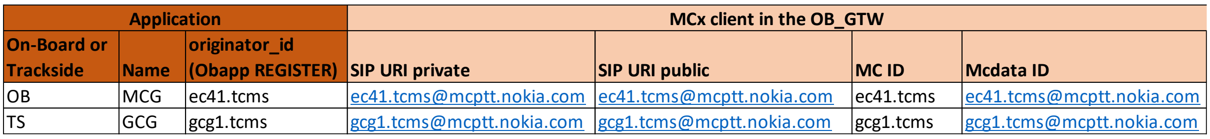
9.5.1 For WP3

ETCS (CAF):



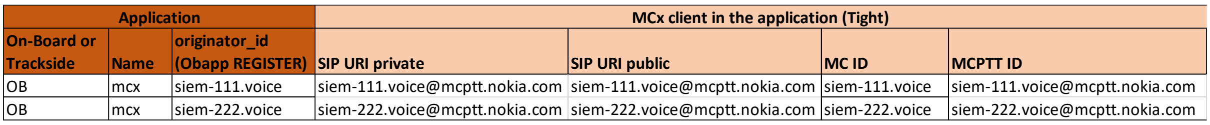
Application			MCx client in the OB_GTW			
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private IMPI	SIP URI public IMPU	MC ID	Mcdata ID (= MC service ID)
OB	EVC	id000001.ty02.etcs	id000001.ty02.etcs@mcptt.nokia.com	id000001.ty02.etcs@mcptt.nokia.con	id000001.ty02.etcs	id000001.ty02.etcs@mcptt.nokia.com
TS	RBC	id016385.ty01.etcs	id016385.ty01.etcs@mcptt.nokia.com	id016385.ty01.etcs@mcptt.nokia.con	id016385.ty01.etcs	id016385.ty01.etcs@mcptt.nokia.com

TCMS (CAF):



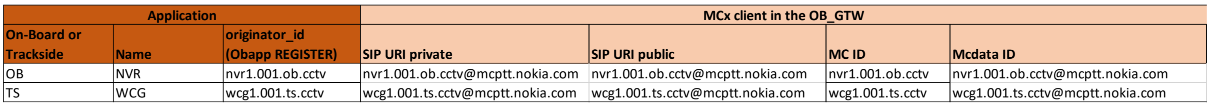
Application			MCx client in the OB_GTW			
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private	SIP URI public	MC ID	Mcdata ID
OB	MCG	ec41.tcms	ec41.tcms@mcptt.nokia.com	ec41.tcms@mcptt.nokia.com	ec41.tcms	ec41.tcms@mcptt.nokia.com
TS	GCG	gcg1.tcms	gcg1.tcms@mcptt.nokia.com	gcg1.tcms@mcptt.nokia.com	gcg1.tcms	gcg1.tcms@mcptt.nokia.com

Voice (Siemens):



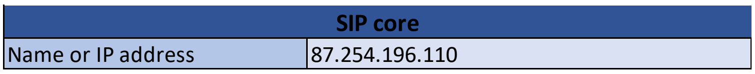
Application			MCx client in the application (Tight)			
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private	SIP URI public	MC ID	MCPTT ID
OB	mcx	siem-111.voice	siem-111.voice@mcptt.nokia.com	siem-111.voice@mcptt.nokia.com	siem-111.voice	siem-111.voice@mcptt.nokia.com
OB	mcx	siem-222.voice	siem-222.voice@mcptt.nokia.com	siem-222.voice@mcptt.nokia.com	siem-222.voice	siem-222.voice@mcptt.nokia.com

CCTV (Teleste):

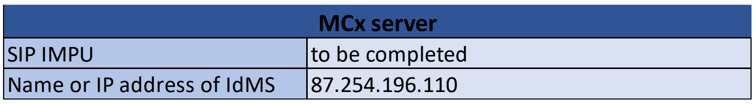


Application			MCx client in the OB_GTW			
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private	SIP URI public	MC ID	Mcdata ID
OB	NVR	nvr1.001.ob.cctv	nvr1.001.ob.cctv@mcptt.nokia.com	nvr1.001.ob.cctv@mcptt.nokia.com	nvr1.001.ob.cctv	nvr1.001.ob.cctv@mcptt.nokia.com
TS	WCG	wcg1.001.ts.cctv	wcg1.001.ts.cctv@mcptt.nokia.com	wcg1.001.ts.cctv@mcptt.nokia.com	wcg1.001.ts.cctv	wcg1.001.ts.cctv@mcptt.nokia.com

SIP core and MCx server related information:



SIP core	
Name or IP address	87.254.196.110



MCx server	
SIP IMPU	to be completed
Name or IP address of IdMS	87.254.196.110

9.5.2 For WP4:

ETCS (Alstom):

Application			MCx client in the OB_GTW				
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private IMPI	SIP URI public IMPU	MC ID	Call-list	Mcdata ID (= MC service ID)
OB	EVC	id000005.ty02.e	eoa.1@sv-lab.net	eoa.1@sv-lab.net	eoa.1	eoa.1; eta.1; eta.2	eoa.1@sv-lab.net
			eoa.2@sv-lab.net	eoa.2@sv-lab.net	eoa.2	eoa.2; eta.3; eta.4	eoa.2@sv-lab.net
			eok.1@sv-lab.net	eok.1@sv-lab.net	eok.1	eok.1; etk.1; etk.2	eok.1@sv-lab.net
			eok.2@sv-lab.net	eok.2@sv-lab.net	eok.2	eok.2; etk.3; etk.4	eok.2@sv-lab.net
TS	RBC1	id500033.ty01.e	eta.1@sv-lab.net	eta.1@sv-lab.net	eta.1	eoa.1; eta.1; eta.2	eta.1@sv-lab.net
			eta.3@sv-lab.net	eta.3@sv-lab.net	eta.3	eoa.2; eta.3; eta.4	eta.3@sv-lab.net
			etk.1@sv-lab.net	etk.1@sv-lab.net	etk.1	eok.1; etk.1; etk.2	etk.1@sv-lab.net
			etk.3@sv-lab.net	etk.3@sv-lab.net	etk.3	eok.2; etk.3; etk.4	etk.3@sv-lab.net
TS	RBC2	id500034.ty01.e	eta.2@sv-lab.net	eta.2@sv-lab.net	eta.2	eoa.1; eta.1; eta.2	eta.2@sv-lab.net
			eta.4@sv-lab.net	eta.4@sv-lab.net	eta.4	eoa.2; eta.3; eta.4	eta.4@sv-lab.net
			etk.2@sv-lab.net	etk.2@sv-lab.net	etk.2	eok.1; etk.1; etk.2	etk.2@sv-lab.net
			etk.4@sv-lab.net	etk.4@sv-lab.net	etk.4	eok.2; etk.3; etk.4	etk.4@sv-lab.net

ATO (Alstom):

Application			MCx client in the OB_GTW				
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private IMPI	SIP URI public IMPU	MC ID	Call-list	Mcdata ID (= MC service ID)
OB	ATO-OB	ato-ob.ato	aoa.1@sv-lab.net	aoa.1@sv-lab.net	aoa.1	aoa.1; ata.1	aoa.1@sv-lab.net
		ato-ob.ato	aoa.2@sv-lab.net	aoa.2@sv-lab.net	aoa.2	aoa.2; ata.2	aoa.2@sv-lab.net
		ato-ob.ato	aok.1@sv-lab.net	aok.1@sv-lab.net	aok.1	aok.1; atk.1	aok.1@sv-lab.net
		ato-ob.ato	aok.2@sv-lab.net	aok.2@sv-lab.net	aok.2	aok.2; atk.2	aok.2@sv-lab.net
TS	ATO-TS	ato-ts.ato	ata.1@sv-lab.net	ata.1@sv-lab.net	ata.1	aoa.1; ata.1	ata.1@sv-lab.net
		ato-ts.ato	ata.2@sv-lab.net	ata.2@sv-lab.net	ata.2	aoa.2; ata.2	ata.2@sv-lab.net
		ato-ts.ato	aok.3@sv-lab.net	aok.3@sv-lab.net	aok.3	aok.1; atk.1	aok.3@sv-lab.net
		ato-ts.ato	aok.4@sv-lab.net	aok.4@sv-lab.net	aok.4	aok.2; atk.2	aok.4@sv-lab.net

PIS (Thales):

Application			MCx client in the OB_GTW				
On-Board or Trackside	Name	originator_id (Obapp REGISTER)	SIP URI private IMPI	SIP URI public IMPU	MC ID	Call-list	Mcdata ID (= MC service ID)
OB	PIS-OB	msg.ob.pis	poa.1@sv-lab.net	poa.1@sv-lab.net	poa.1	poa.1; pta.1	poa.1@sv-lab.net
		msg.ob.pis	poa.2@sv-lab.net	poa.2@sv-lab.net	poa.2	poa.2; pta.2	poa.2@sv-lab.net
		msg.ob.pis	pok.1@sv-lab.net	pok.1@sv-lab.net	pok.1	pok.1; ptk.1	pok.1@sv-lab.net
		msg.ob.pis	pok.2@sv-lab.net	pok.2@sv-lab.net	pok.2	pok.2; ptk.2	pok.2@sv-lab.net
OB	PIS-OB	mgt.ob.pis	poa.3@sv-lab.net	poa.3@sv-lab.net	poa.3	poa.3; pta.3	poa.3@sv-lab.net
		mgt.ob.pis	poa.4@sv-lab.net	poa.4@sv-lab.net	poa.4	poa.4; pta.4	poa.4@sv-lab.net
		mgt.ob.pis	pok.3@sv-lab.net	pok.3@sv-lab.net	pok.3	pok.3; ptk.3	pok.3@sv-lab.net
		mgt.ob.pis	pok.4@sv-lab.net	pok.4@sv-lab.net	pok.4	pok.4; ptk.4	pok.4@sv-lab.net
OB	PIS-OB	log.ob.pis	poa.5@sv-lab.net	poa.5@sv-lab.net	poa.5	poa.5; pta.5	poa.5@sv-lab.net
		log.ob.pis	poa.6@sv-lab.net	poa.6@sv-lab.net	poa.6	poa.6; pta.6	poa.6@sv-lab.net
		log.ob.pis	pok.5@sv-lab.net	pok.5@sv-lab.net	pok.5	pok.5; ptk.5	pok.5@sv-lab.net
		log.ob.pis	pok.6@sv-lab.net	pok.6@sv-lab.net	pok.6	pok.6; ptk.6	pok.6@sv-lab.net
TS	PIS-TS	msg.ts.pis	pta.1@sv-lab.net	pta.1@sv-lab.net	pta.1	poa.1; pta.1	pta.1@sv-lab.net
		msg.ts.pis	pta.2@sv-lab.net	pta.2@sv-lab.net	pta.2	poa.2; pta.2	pta.2@sv-lab.net
		msg.ts.pis	ptk.1@sv-lab.net	ptk.1@sv-lab.net	ptk.1	pok.1; ptk.1	ptk.1@sv-lab.net
		msg.ts.pis	ptk.2@sv-lab.net	ptk.2@sv-lab.net	ptk.2	pok.2; ptk.2	ptk.2@sv-lab.net
TS	PIS-TS	mgt.ts.pis	pta.3@sv-lab.net	pta.3@sv-lab.net	pta.3	poa.3; pta.3	pta.3@sv-lab.net
		mgt.ts.pis	pta.4@sv-lab.net	pta.4@sv-lab.net	pta.4	poa.4; pta.4	pta.4@sv-lab.net
		mgt.ts.pis	ptk.3@sv-lab.net	ptk.3@sv-lab.net	ptk.3	pok.3; ptk.3	ptk.3@sv-lab.net
		mgt.ts.pis	ptk.4@sv-lab.net	ptk.4@sv-lab.net	ptk.4	pok.4; ptk.4	ptk.4@sv-lab.net
TS	PIS-TS	log.ts.pis	pta.5@sv-lab.net	pta.5@sv-lab.net	pta.5	poa.5; pta.5	pta.5@sv-lab.net
		log.ts.pis	pta.6@sv-lab.net	pta.6@sv-lab.net	pta.6	poa.6; pta.6	pta.6@sv-lab.net
		log.ts.pis	ptk.5@sv-lab.net	ptk.5@sv-lab.net	ptk.5	pok.5; ptk.5	ptk.5@sv-lab.net
		log.ts.pis	ptk.6@sv-lab.net	ptk.6@sv-lab.net	ptk.6	pok.6; ptk.6	ptk.6@sv-lab.net

SIP core and MCx server related information:

SIP core	
Name or IP address of the proxy CSCF	172.21.160.68:5060

MCx server	
SIP IMPU	sdp01@sv-lab.net
Name or IP address of IdMS	172.21.160.69:8450

Domain part of SIP URI	
domain part for SIP IMPU	sv-lab.net
domain part for MC service ID	sv-lab.net

9.6 Appendix 8 – Cybersecurity

The subject of this appendix is the FRMCS GW cyber security.

The study is written by THALES who has references in cyber security and whose cyber team has already conducted a risk analysis on the Automated Train for SNCF.

This document in addressed to all the members of the FRMCS consortium: UIC, NOKIA (DE, IT, HU), KONTRON, ALSTOM, DBN, SNCF, THALES, SBB, UNIFE, CAF, OEBB, SIEMENS, IP, IFSTTAR, TELESTE, DTU. The audience for this document includes the asset owner, system integrator, product supplier, service provider, and compliance authority. This document can respond to the cyber security threat only with the contribution of the stakeholders.

- It is asked to focus on FRMCS and its interfaces, in this version of the Architecture Report.

5Grail is a project funded by the European Commission. It is in the framework of the Call for proposal Information and Communication Technologies (H2020-ICT-2018-20), TOPIC ICT 53 (5G for Connected and Automated Mobility).

The aim of this document is to apply the necessary mitigations in a systematic, defensible manner (NF EN IEC 62443-3-3 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2019-04).

1. A first chapter identifies the System Under Consideration: FRMCS GW.
2. A cyber risk assessment is then written.
3. Some requirements are proposed.

9.6.1 ZCR 1: Identify the System Under Consideration

The following extract from IEC 62443-3-2 (security risk assessment for system design) specifies the ZCR 1 content: “The organization shall clearly identify the SUC (System Under Consideration), including clear demarcation of the security perimeter and identification of all access points to the SUC”.

This chapter focuses on the SUC FRMCS rather than an end-to-end SUC.

FRMCS figures and interfaces are first listed in order to have an overall view of FRMCS. The aim is to identify access points.

9.6.1.1 FRMCS GW

FRMCS Boundary representations:

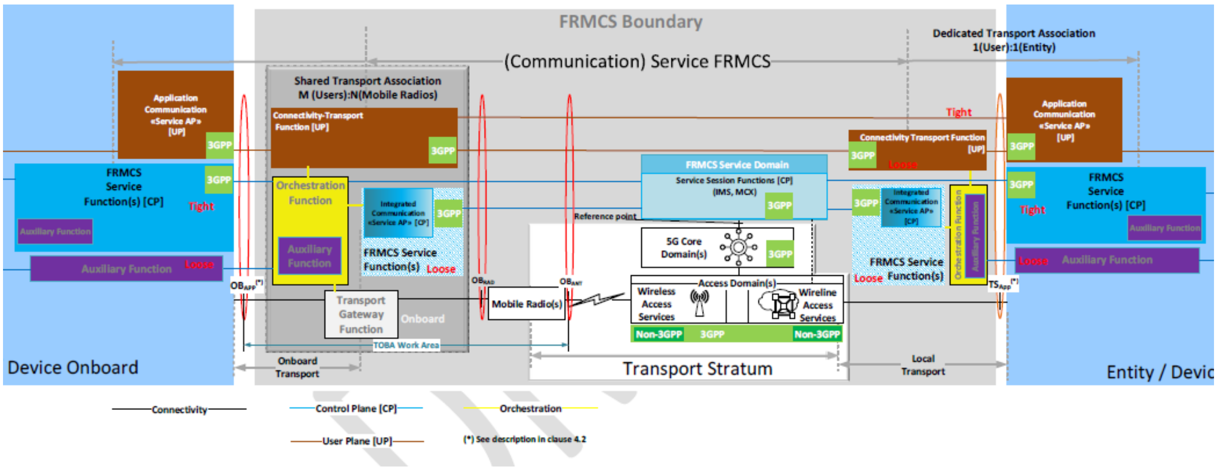


Figure 104: FRMCS principle architecture

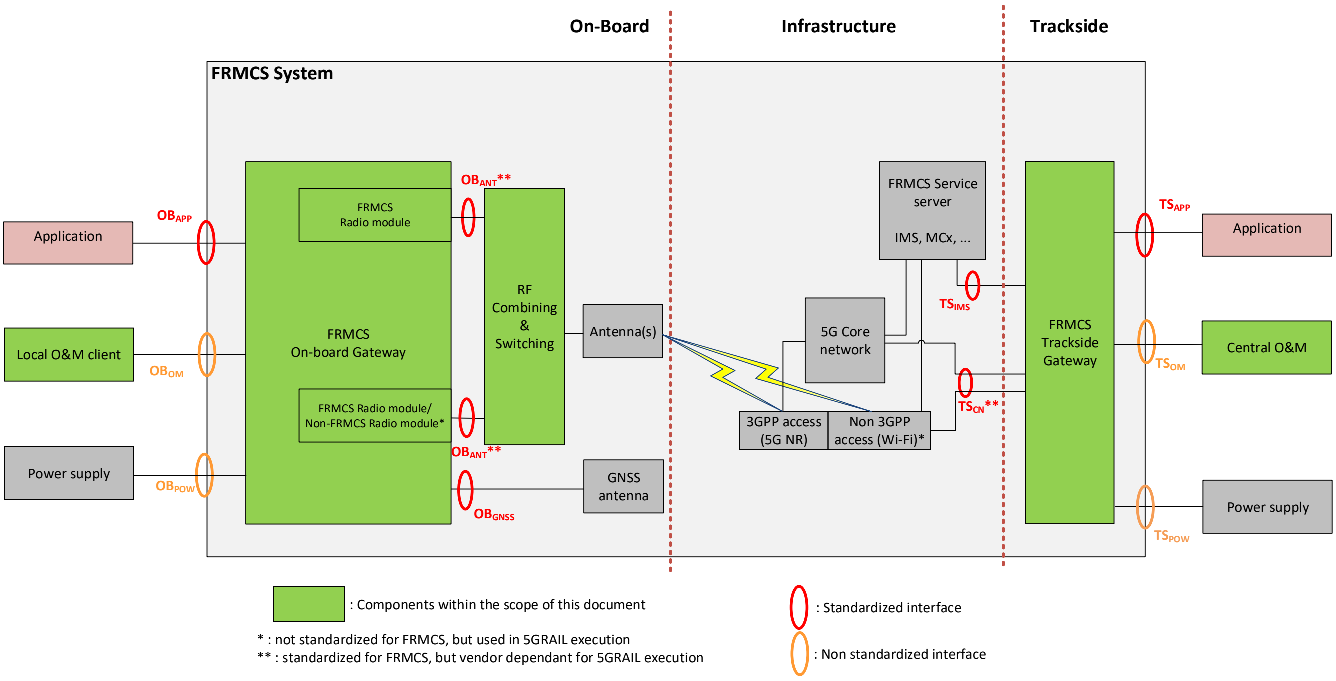


Figure 105: FRMCS Gateway services – Principle overview

9.6.1.2 FRMCS OB

FRMCS OB representation:

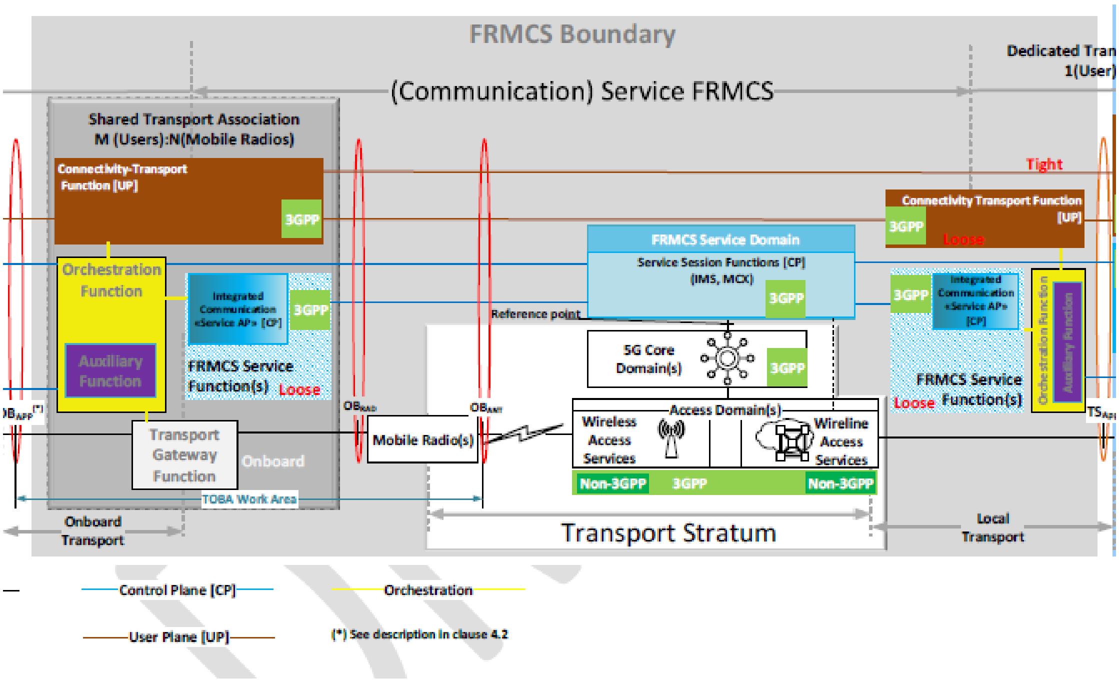


Figure 106: Focus on FRMCS OB

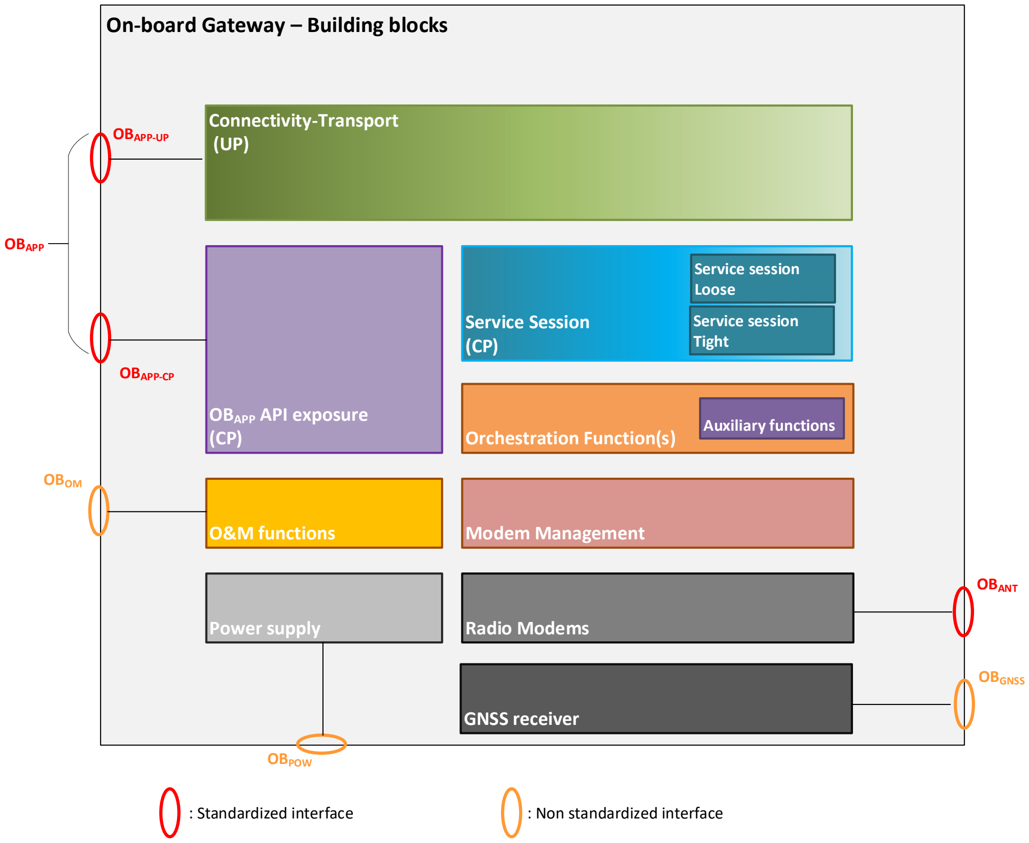


Figure 107: FRMCS on board gateway – Building blocks

Cyber security related functions:

FUNCTIONS	ALLOCATED BUILDING BLOCK
OBGTW_F1.5: Local Binding	OB_{APP} exposure
OBGTW_F4 Authenticate/authorize access to the FRMCS service level.	Service session - Loose
OBGTW_F5.2: Performance & supervision management Logs to O&M contain security logs are, see [7501, § 7.7.2.4, version 1.0.12]	O&M functions
OBGTW_F5.4 O&M functions- Users or groups account profile	O&M functions

9.6.1.3 FRMCS TS

FRMCS TS representation:

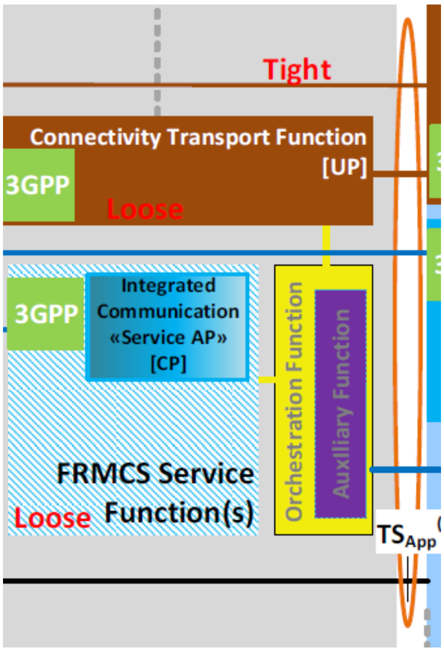


Figure 108 : FRMCS TS architecture principle

Entities who deliver On-board & Trackside Gateways:

- Kontron prototypes: FRMCS OB_GTW-K and FRMCS TS_GTW-K
- Alstom prototypes: FRMCS OB_GTW-A and FRMCS TS_GTW-A

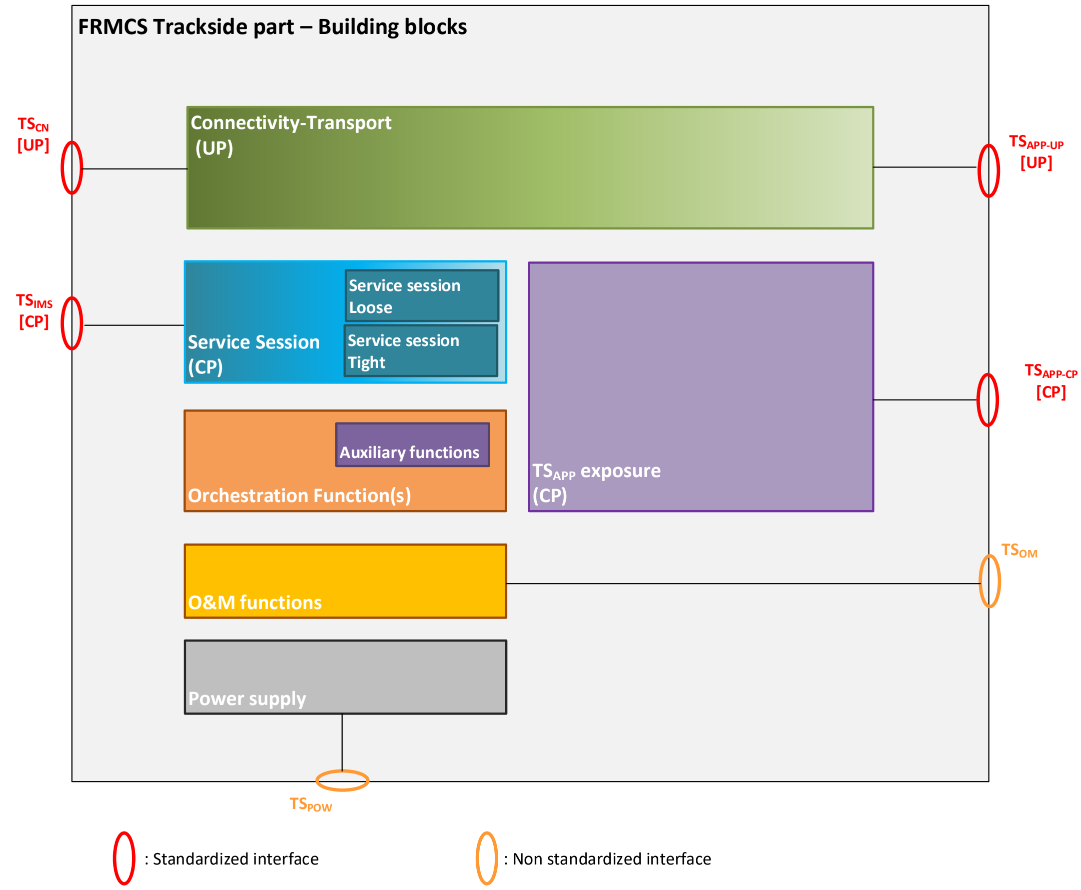


Figure 109: TOBA trackside gateway - Building blocks

Cyber security related functions:

FUNCTIONS	ALLOCATED BUILDING BLOCK
TSGTW_F1.5: Local Binding	TS_{APP} exposure
TSGTW_F4 Authenticate/authorize access to the FRMCS service level.	Service session -Loose

9.6.1.4 Interfaces

List of interfaces:

9.6.1.4.1 OB INTERFACES

The external interfaces of OB_GTW are the following:

- OB_{APP} : interface with the application in tight mode, loose mode or super-loose mode.
- OB_{OM} : interface with O&M client or O&M server.
- OB_{POW}: interface with the power supply
- OB_{ANT} :interface with RF combining & switching and the antennas
- OB_{GNSS}: interface with GNSS antenna

For the loose coupled applications section 6.2.3 from this document proposes the WebSocket protocol for control plane. This is a standard IETF protocol (RFC 6455), which enables to have a full-duplex channel between client (i.e. the application) and server (i.e. FRMCS OB GTW). As TCP session stays opened, optional authentication has been done one time.

More accurately, 6.2.3 proposes to use "WebSocket over TLS", that allows to authenticate and optionally encrypt the exchanges between client and server. Authentication between client and server should use certificate exchange (it covers local binding need).

OB_{AUTH} will not be implemented for the 1st prototype, see Table 15: Assumption table.

OB_{AUTH} is a local authentication between TOBA and on-board applications, it does not rely on a trackside server.

Behind the physical OB_{ANT} interface, the functional view of OB_{ANT} interface includes the following links:

- Logical link between the OB_GTW and the TS_GTW for the transmission of application data
- Logical link between the OB_GTW and the IMS/MCx server, to manage the service layer.

On the Figure 105: FRMCS Gateway services – Principle overview, two components are in green next to FRMCS OB GTW :

- Local O&M client
- RF Combining & Switching

However, they are on the other side of OB_{OM} and OB_{ANT}. In this way, these two components are outside of the SUC_{FRMCS}.

9.6.1.4.2 TS INTERFACES

- TS_{APP}
  - For loose-coupled applications
  - For tight-coupled applications
- TS_{OM} : interface with O&M (Operation & Maintenance)
- TS_{INFRA}: interface with infrastructure (core network, IMS, MCx server)
- TS_{POW}: interface with the power supply

- TS_{APP}
  - TS_{APP-UP}: it is an IP interface for user plane
  - TS_{APP-CP}: interface to manage the control plane.
    - It includes the local binding (authentication) if needed, and session management through the TS_{APP} API.

- TS_{OM} : interface with O&M server
  - TS_GTW-A
    - Same physical interface than TS_{APP}.
    - As described in **5.2.2.4.13**, the protocol used is SNMPv2c or SNMP v3.
    - The OB_GTW implements a MIB-II as defined by reference [S2].
  - TS_GTW-K
    - The remote server will connect to the OB_GTW and collect the O&M information through SNMP and /or REST API.

In SNMPv2c, the community password is in clear on the network on each request .There are neither authentication nor integrity. SNMPv3 has been developed in order to improve the security.

- TS_{INFRA}: interface with infrastructure : core networks and IMS/MCx server for control plane
  - This interface enables the MCx client embedded in the TS_GTW (for loose-coupling) or in application (for tight-coupling) to communicate with the IMS/MCx server.
  - For loose-coupled applications:
    - Authentication, registration and MCdata authorization procedures, for the MCdata clients embedded in the OB_GTW. See chapter **5.2.2.4.10** and 3GPP TS 33.180.
    - Management of MCData sessions: signaling control for the MCData client embedded in the OB_GTW: see 3GPP TS 24.282.
  - For tight-coupled applications: as explained in **5.2.2.4.8**,the OB_GTW will proxy the control plane messages of tight applications.

- TS_{POW}: interface with the power supply

9.6.1.5 Access Points

The identified access points are:

- 5G carrier between OB_{ANT} and TS
- Physical access to FRMCS OB

9.6.2 ZCR 2: Initial cyber security risk assessment

Requirement from the IEC 62443-3-2 about ZCR 2:

“The organization shall perform a cyber security risk assessment of the SUC or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the

- interference with critical IACS operations (French: résulte de l'interférence avec des opérations critiques de l'IACS),
- breach or disruption of IACS (fr.: d’infractions ou de perturbations de l'IACS) or
- disablement (fr.: désactivation) of mission critical IACS operations.”

A brief risk analysis is conducted here after. It follows the EBIOS RM method and vocabulary.

9.6.2.1 Scope and security baseline

Business Assets:

- Critical Communication Applications flow
- Performance Communication Applications flow

Supporting Assets:

- FRMCS OB GW
- FRMCS TS GW
- Are they in the scope ?
    - Local O&M client, Central O&M ?
    - RF combining & switching ?

Feared Event

BUSINESS ASSET	FEARED EVENT	IMPACTS	SEVERITY
Critical Communication Applications flow in FRMCS OB and TS	Loss of service Alteration of the flow	Loss of lives	4
Performance Communication Applications flow in FRMCS OB and TS	Loss of service	Loss of money, of image	3

The security baselines

The security baseline consists of the list of applicable requirements, and their implementation status..

Applicable requirements	Allocated building block	Implementation status
OBGTW_F1.5: Local Binding	OB$_{APP}$ exposure OB$_{APP}$ API function FRMCS_GTW_REGISTER over TLS flat-IP mode for phasing approach of OB$_{APP}$	For A-ETCS and A-ATO, no TLS for the 1st prototype.
OBGTW_F4: Authenticate/authorize access to the FRMCS service level	Service session – Loose	
OBGTW_F5.4: Users or groups account/profile	O&M functions	This function refers to [S9].
TSGTW_F1.5: Authenticate the on-board applications	TS$_{APP}$ exposure	See OB status
TSGTW_F4 Authenticate/authorize access to the FRMCS service level. The aim of this function is to enable the access to the IMS/MCx server.	Service session – Loose	See OB status

The following table is an extract from the FRMCS System Security Framework from 7900 FRMCS Use Case:

Applicable requirements	Implementation status
[R-12.15.2-001] The FRMCS System security framework shall enable the use of unique identities.	
[R-12.15.2-002] The FRMCS System security framework shall allow the grouping of identities.	
[R-12.15.2-003] The FRMCS System security framework shall provide mechanisms to authenticate a unique identity.	TLS But no local authentication for the 1st ETCS and ATO prototype [Alstom]
[R-12.15.2-004] The FRMCS System security framework shall provide authentication mechanisms required for the secured interaction between FRMCS network functions.	
[R-12.15.2-005] The FRMCS System security framework shall provide mechanisms to authorize communications and the use of applications.	OBGTW_F1.5: Local Binding OBGTW_F4: Authenticate/authorize access to the FRMCS service level
[R-12.15.2-006] The FRMCS System security framework shall provide a management of identities, passwords and keys required for the protection of FRMCS User communication, the interaction between FRMCS network functions as well as subscribers and service-related data.	OB_{AUTH} is a local authentication between TOBA and on-board applications, it does not rely on a trackside server.
[R-12.15.2-007] The FRMCS System security framework shall be able to block the use of any FRMCS Equipment when it is detected as being stolen or lost.	Not yet specified
[R-12.15.2-008] The FRMCS System security framework shall be able to unblock the use any recovered stolen or lost FRMCS Equipment.	Not yet specified

[R-12.15.2-009] "The FRMCS System security framework shall **protect** - the services provided by the FRMCS System; - bearer flexible access including 3GPP as well as non-3GPP access; - interaction between the FRMCS end user devices and FRMCS network; - interaction between FRMCS network functions; - stored data within the FRMCS System; - interworking between a FRMCS System and another FRMCS System; - Interworking between a FRMCS System and a legacy system."	OBGTW_F1.5: Local Binding OBGTW_F4: Authenticate/authorize access to the FRMCS service level OBGTW_F5.4: Users or groups account/profile
[R-12.15.2-010] "The FRMCS System security framework shall **prevent** software-based attacks which have an impact on any of the following security attributes: - data confidentiality; - information privacy; - data integrity; - non-repudiation of data; - FRMCS System availability."	Not yet specified .
[R-12.15.2-011] "The FRMCS System security framework shall be able to **detect** software-based attacks which have an impact on any of the following security attributes: - data confidentiality; - information privacy; - data integrity; - non-repudiation of data transfer; - FRMCS System availability."	OBGTW_F5.2: Performance & supervision management

[R-12.15.2-012] "The FRMCS System security framework shall be able to **react** on detected software-based attacks which have an impact on any of the following security attributes: - data confidentiality; - information privacy; - data integrity; - non-repudiation of data transfer; - FRMCS System availability."	Not yet specified
[R-12.15.2-013] The FRMCS System security framework shall provide procedures and mechanisms for management of FRMCS System security.	Not yet specified
[R-12.15.2-014] "The FRMCS System security framework shall be able to track users' actions such as usage of - communication services, - management operations, - configuration changes etc."	OBGTW_F5.2: Performance & supervision management OBGTW_F5.3: Configuration management
[R-12.15.2-015] The FRMCS System security framework shall be able to store security related data for post analysis, e.g. forensic.	Not yet specified

9.6.2.2 Risk origins

Source of Risk

- Hacktivist
- Cyber-terrorist
- Cyber criminal
- State

Targeted Objectives

This table lists the target objectives of each Source of risk in term of sought effect.

Source of Risk	Targeted Objectives	Motivation	Resource	Activity	Pertinence
State	Stop railway traffic in order to impress the citizens and to slow the national economy.	+++	+++	+++	High
State	Lead a reconnaissance campaign in order to be able to build an APT.	+++	+++	+++	High
Cyber criminal	Inject a ransomware in order to have more money.	++	++	+++	Moderate
Cyber terrorist	Tamper 5G flows in order to frighten the citizens.	++	+	+	Low

Cyber terrorists have other means to stop a train. They can drop curved iron bars on the catenary or on the wiring that transfer power to the train.

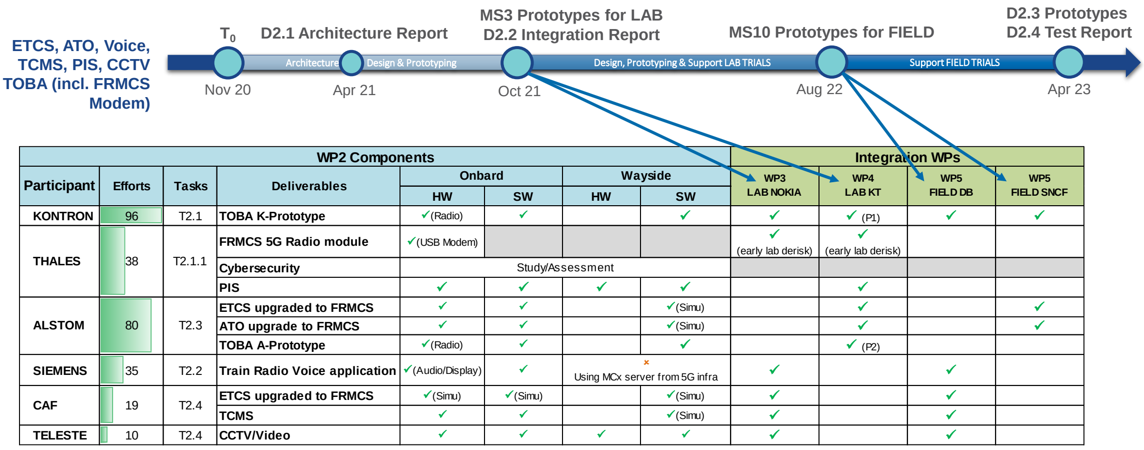
After, only Risk Origin with High or Moderate pertinence will be treated.

Stakeholders

Stakeholders are partners, subcontractors, subsidiaries. More and more cyberattack modus operandi leverages the most vulnerable links among stakeholders.

Stakeholders are IM, RU, suppliers.

The figure below shows the efforts from main participants and stakeholders in WP2.



WP2 Components								Integration WPs			
Participant	Efforts	Tasks	Deliverables	Onbard		Wayside		WP3 LAB NOKIA	WP4 LAB KT	WP5 FIELD DB	WP5 FIELD SNCF
				HW	SW	HW	SW				
KONTRON	96	T2.1	TOBA K-Prototype	✓(Radio)	✓		✓	✓	✓ (P1)	✓	✓
THALES	38	T2.1.1	FRMCS 5G Radio module	✓(USB Modem)				✓ (early lab derisk)	✓ (early lab derisk)		
			Cybersecurity	Study/Assessment							
			PIS	✓	✓	✓	✓		✓		
ALSTOM	80	T2.3	ETCS upgraded to FRMCS	✓	✓		✓(Simu)		✓		✓
			ATO upgrade to FRMCS	✓	✓		✓(Simu)		✓		✓
			TOBA A-Prototype	✓(Radio)	✓		✓		✓ (P2)		
SIEMENS	35	T2.2	Train Radio Voice application	✓(Audio/Display)	✓	× Using MCx server from 5G infra		✓		✓	
CAF	19	T2.4	ETCS upgraded to FRMCS	✓(Simu)	✓(Simu)		✓(Simu)	✓		✓	
			TCMS	✓	✓		✓(Simu)	✓		✓	
TELESTE	10	T2.4	CCTV/Video	✓	✓	✓	✓	✓		✓	

Figure 110: WP2 Prototype/component deliveries and targeted LAB and FIELD WPs

In WP2, the figure shows six main participants in WP2.

Stakeholders	Members of the consortium
Railway Undertaking Infrastructure Manager	DB, SNCF SBB (Schweizerische Bundesbahnen) OEBB (Österreichische Bundesbahnen) IP (Infrastruturas de Portugal)
Supplier	KONTRON ALSTOM THALES SIEMENS CAF TELESTE

Stakeholders	Members of the consortium
	NOKIA-DE, NOKIA-IT, NOKIA-HU
Specification	UIC UNIFE
Research	IFSTTAR DTU

9.6.2.3 Strategic Scenarios

DoS attack. A hostile state can carry a large scale coordinated DDOS (Distributed Deny Of Service) attack with the help of Advanced Persistent Threats (APT)

- on the FRMCS OB GW, on the FRMCS TS GW,
- on their interface
  - OB_{ANT} or OB_{GNSS}
    - Ill-intended people can exploit flows in 5G IoTs in order to decrease the available 5G bandwidth for OB_{ANT}.
  - On a rogue OB internet wireless (4G/5G/wifi) interface added in the FRMCS OB GW
  - TS_{CN} or TS_{IMS}
- With the strategic attack paths
  - Direct interaction with FRMCS products
  - Pressure on a stakeholder to tamper FRMCS products

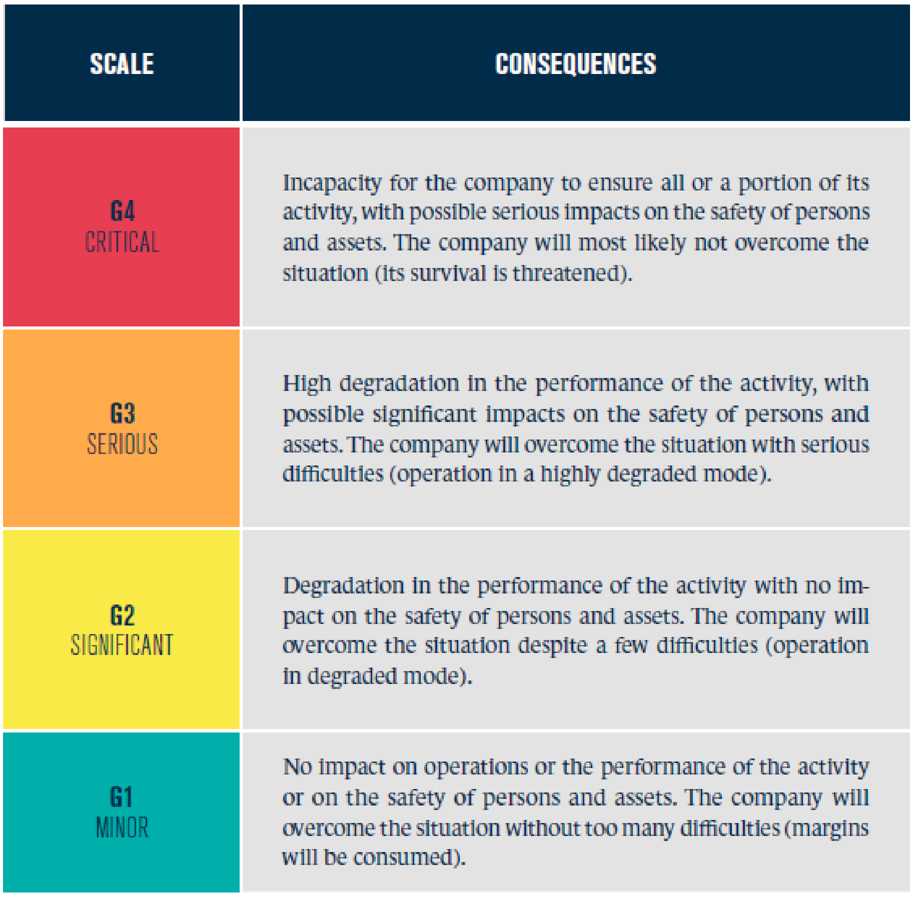
in order to paralyse the critical applications ETCS, TCMS, ATO, VOICE and PIS, CCTV.

Risk origin: State

Targeted Objectives: Stop railway traffic in order to impress the citizens and to slow the national economy.

Severity: 4

The scale for severity is:



SCALE	CONSEQUENCES
G4 CRITICAL	Incapacity for the company to ensure all or a portion of its activity, with possible serious impacts on the safety of persons and assets. The company will most likely not overcome the situation (its survival is threatened).
G3 SERIOUS	High degradation in the performance of the activity, with possible significant impacts on the safety of persons and assets. The company will overcome the situation with serious difficulties (operation in a highly degraded mode).
G2 SIGNIFICANT	Degradation in the performance of the activity with no impact on the safety of persons and assets. The company will overcome the situation despite a few difficulties (operation in degraded mode).
G1 MINOR	No impact on operations or the performance of the activity or on the safety of persons and assets. The company will overcome the situation without too many difficulties (margins will be consumed).

Intrusion. A Source of Risk can begin a reconnaissance operation

- on the mobile FRMCS OB GW, on the FRMCS TS GW,
- on their interfaces
    - ○ $\mathrm{OB}_{\mathrm{ANT,}}$ $\mathrm{OB}_{\mathrm{GNSS}}$, $\mathrm{OB}_{\mathrm{APP}}$

  - Try to install a rogue OB internet wireless (4G/5G/wifi) interface added in the FRMCS OB GW
  - TS_{CN}, TS_{IMS}
- with a focus on,
  - interconnection with other systems,
  - removable supports,
  - remote accesses by nomad users,
  - maintenance and exploitation operation done by external providers.
- With the strategic attack paths
  - Gaining access to specification documentations or
  - Pressure on participant of FRMCS or their suppliers

in order to prepare an APT attack.

Risk origin: State

Targeted Objectives: Lead a reconnaissance campaign in order to be able to build an APT.

Severity: 3

Ransomware. A Source of Risk can introduce a Ransomware in some FRMCS OB GW in order to

- impact the passenger service with for instance modification of information shown to passengers,
- enter in the Rail Undertaking or Infrastructure Manager IT system, exfiltrate RU or IM sensitive data, be ready to expose these data on Internet
- With the strategic attack paths
  - Direct interaction with FRMCS products

in order to have more money.

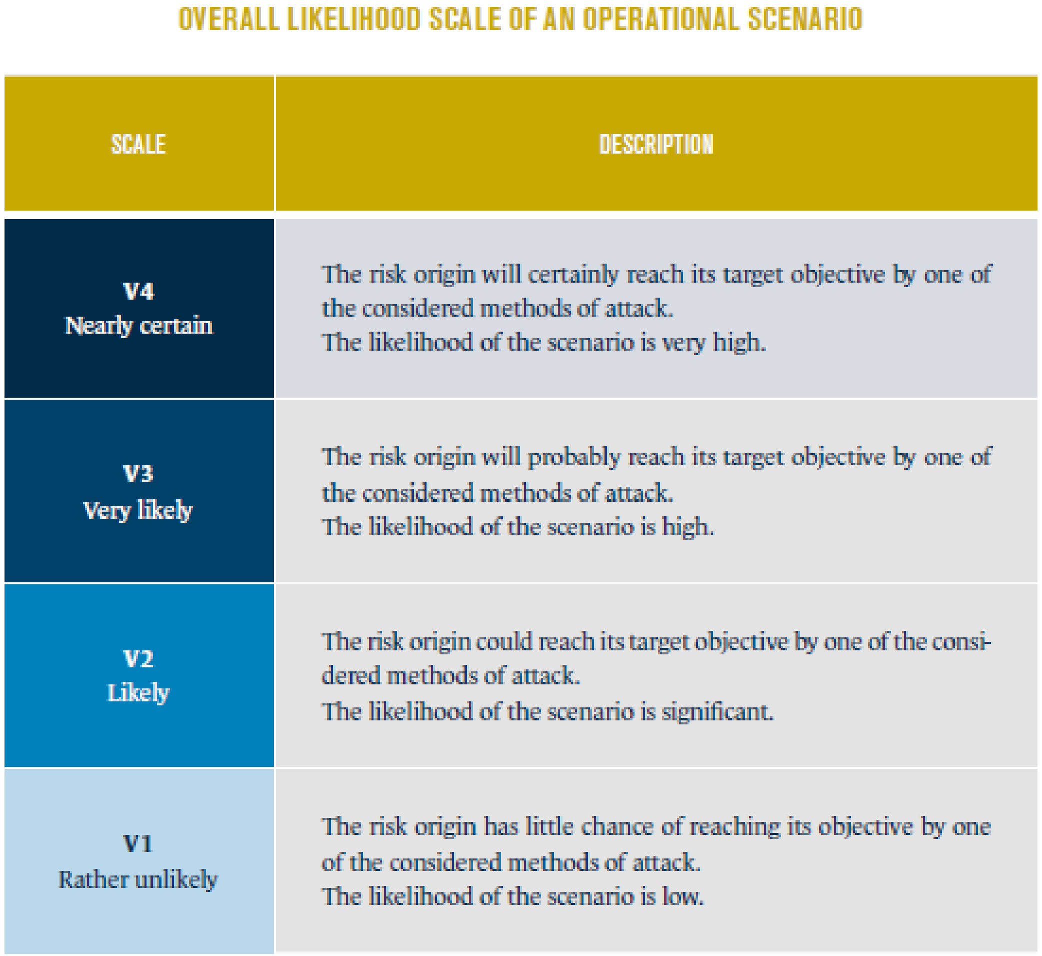
Risk origin: Cyber criminal

Targeted Objectives: Inject a ransomware in order to have more money

Severity: 4

9.6.2.4 Operational Scenarios

L means Likelihood on a scale from 1 to 4.



OVERALL LIKELIHOOD SCALE OF AN OPERATIONAL SCENARIO

SCALE	DESCRIPTION
V4 Nearly certain	The risk origin will certainly reach its target objective by one of the considered methods of attack. The likelihood of the scenario is very high.
V3 Very likely	The risk origin will probably reach its target objective by one of the considered methods of attack. The likelihood of the scenario is high.
V2 Likely	The risk origin could reach its target objective by one of the considered methods of attack. The likelihood of the scenario is significant.
V1 Rather unlikely	The risk origin has little chance of reaching its objective by one of the considered methods of attack. The likelihood of the scenario is low.

DDOS attack

KNOWING	ENTERING	FINDING	EXPLOITING	Overall Likelihood
Open-source external reconnaissance Read about app_uuid, RFC4122 and its security section.	Access to a train and a FRMCS OB GW in the targeted country. Likelihood 3 Connection to the modem USB port. L2.	Install a malware. L2 Find how to command the send of the FRMCS_GTW_DEREGISTER command. L2) Install a communication implant. L1	Order to the implant to stop the FRMCS OB GW service. L2. OR Send the jsonrpc FRMCS_GTW_DEREGISTER command with multiple app_uuid from OB to TS. L1.	L1
Advanced external reconnaissance Identification of the interface between internet and FRMCS TS GW. L2	Enter in systems in interface with Internet and FRMCS TS. L2 AND localization of FRMCS TS GW in the network. L1	Identification of flaws on the FRMCS TS interface. L2	Exploitation of FRMCS TS flows in order to change its configuration and stop mission critical flows. L2	L1
	Access to the private 5G network. No more detailed because it is outside FRMCS.			
	Access to the IMS, MCx servers. L2. Out of scope of FRMCS.			

Intrusion

KNOWING	ENTERING	FINDING	EXPLOITING	Overall Likelihood
Open-source external reconnaissance	Locate FRMCS OB GW in trains, on top of their roof. Likelihood 3 Connect to the FRMCS OB modem USB port. L2.	Identify flaws in the software or firmware. L2	Connect to the FRMCS TS GW and scan it. L2.	L2
	The same as the upper cell.	Install a rogue OB Internet wireless (4G/5G/wifi) interface added in the FRMCS OB GW, with its own SIM. L1	Initiate a Communication with its wireless implant. L1.	L1
	Connect to the Ethernet LAN in the train. L2 Out of FRMCS scope	Exploit possible lack of TLS between an OB Application and FRMCS OB. L2 OR exploit flows in TLS implementation. L2		Out of scope

Ransomware

KNOWING	ENTERING	FINDING	EXPLOITING	Overall Likelihood
Open-source external reconnaissance	Connect to the Ethernet LAN in the train. L2	Identify ports on FRMCS with low authentication mechanism. Identify flaws (vulnerabilities) in the software or firmware. L2	Inject a Ransomware that will operate after some delay. L2.	L2

9.6.2.5 Risk treatment

Strategic scenario has given the Severity.

Operational Scenario has given the likelihood.

The Risk Matrix can then be built.

SEVERITY					
4	DoS attack via FRMCS	Ransomware			
3		Intrusion			
2					
1					
	1	2	3	4	LIKELIHOOD

Table 52: Initial FRMCS risk matrix

The worst case is a Ransomware.

Initial requirements

SECURITY MEASURE	ASSOCIATED RISK SCENARIOS
The OB FRMCS GTW access should be physically protected.	DDOS Intrusion Ransomware
The access to the cabinet where the FRMCS OB GTW is located, should raise an alarm.	DDOS Intrusion Ransomware
Unused usb port should be locked by usb blocker key.	DDOS Intrusion Ransomware
The cyber security logs provided by the components of the FRMCS on-board system to the O&M Function should be listed.	DDOS Intrusion Ransomware
Cyber security Log flow should be isolated from the other flows. The FRMCS system should provide the capability to logically isolate log control system networks from non-critical control system networks.	Intrusion
The log flow should be treated with the same safety level as Telemetry flows.	Intrusion
The log flow status should be verified. The keep alive from log flow should be checked frequently.	Intrusion
The OB_GTW should implement a SNMP v3 agent and not a SNMPv2c agent if the connection between FRMCS OB GTW and FRMCS TS GTW is not ciphered (protected in confidentiality and integrity).	DDOS Intrusion Ransomware

9.6.3 ZCR 3: Partition the SUC into zones and conduits

9.6.3.1 ZCR 3.1: Establish zones and conduits

Zones :

- FRMCS OB GW zone
    - It contains following blocks :
        - Connectivity-Transport (UP)
        - OB$_{APP}$ API exposure
        - Service Session (CP)
        - Orchestration Functions(s)
            - Auxiliary functions
        - O&M Functions
        - Modem Management
        - Power supply
        - Radio Modems
        - GNSS receiver
    - It doesn’t contain
        - the RF Combining & Switching,
        - Local O&M client.
            - The interfaces from 8.1.1.4 delimit the SUC$_{FRMCS}$ especially OB$_{ANT}$ and OB$_{OM}$.

- FRMCS TS GW zone
    - It contains following blocks :
        - Connectivity-Transport (UP)
        - Service Session (CP)
        - Orchestration Functions(s)
            - Auxiliary function
        - TS$_{APP}$ exposure (CP)
        - O&M Functions
        - Power supply

The Auxiliary function is used to enable the ETCS application (loose-coupled) to receive necessary information about the link between train and trackside and the link between gateway and EVC.

The identified conduit is from OB$_{ANT}$ to TS$_{CN}$.

9.6.3.2 ZCR 3.3: Separate safety related assets

Mission Communication, Performance Communication and Business Communication Applications use the same building blocks. Thereby, the two zones are safety related zone.

9.6.3.3 ZCR 3.4: Separate temporarily connected devices

Devices that are permitted to make temporary connections to the FRMCS OB are Maintenance devices.

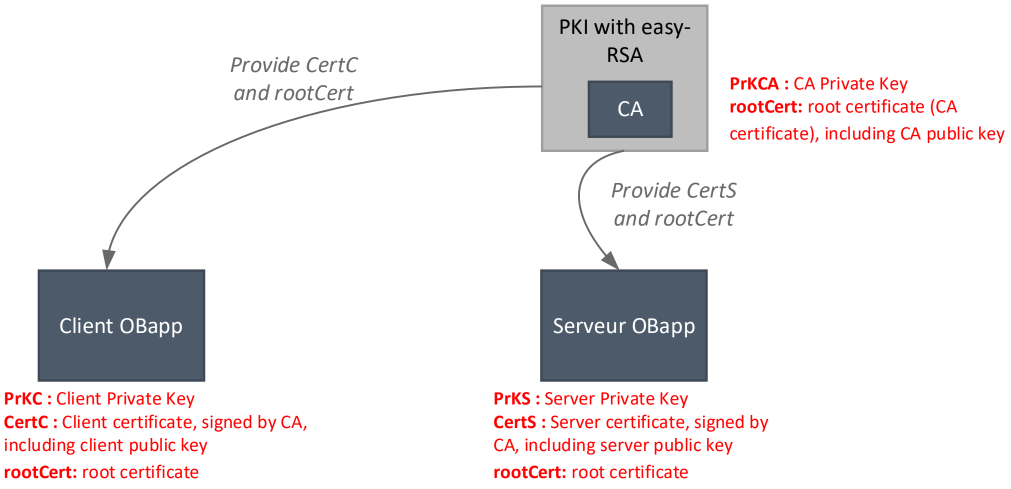
9.7 Appendix 9 – PKI and certificate management for local binding

As explained in chapter **5.2.2.4.5**, an offline PKI will be used for 5GRAIL local binding.

It is proposed to use de device with easy-rsa (open-source tool) as a light offline PKI, in order to create a certificate authority (CA) and manage certificates. See https://easy-rsa.readthedocs.io/en/latest/#easy-rsa-3

To manage the TLS connection, OB$_{APP}$ clients and servers shall have :

- A private key
- A certificate signed by CA, including public key
- A root certificate to check the validity of received certificate.



PrKCA : CA Private Key
rootCert: root certificate (CA certificate), including CA public key

PrKC : Client Private Key
CertC : Client certificate, signed by CA, including client public key
rootCert: root certificate

PrKS : Server Private Key
CertS : Server certificate, signed by CA, including server public key
rootCert: root certificate

Figure 111: Needs for TLS connection

Signed certificates are provided by the PKI.

There are two ways to process certificate generation:

- the client/server generates its own private key and generate a certificate request (csr file) to the CA, derived from this private key. Then, the CA generate the signed certificate from this csr file and provide it to the client/server. See **Figure 112**. This way is the preferred one.
- if the client/server is not able to generate its own private key, the CA can generate it and then derive a signed certificate from this private key. See **Figure 113**.

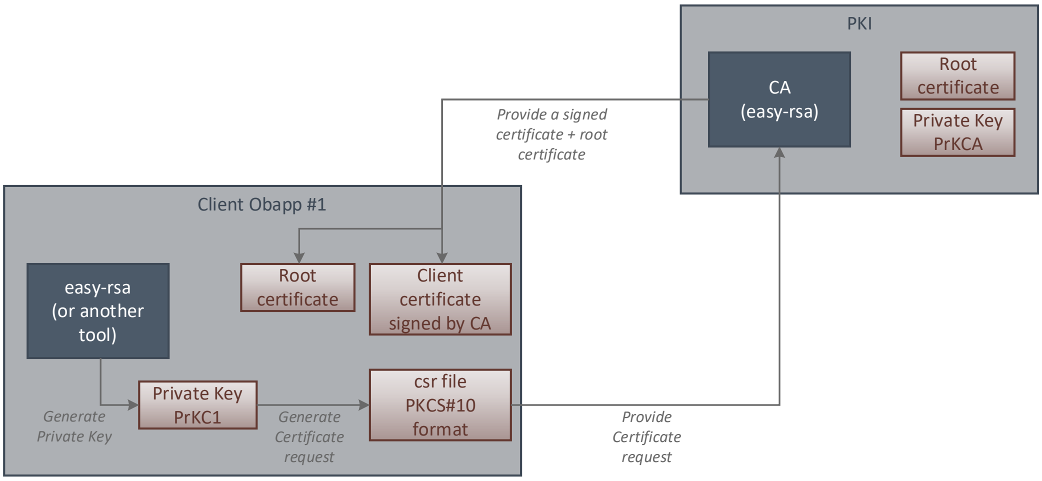

PKI
CA (easy-rsa)
Root certificate
Private Key PrKCA
Provide a signed certificate + root certificate
Client Obapp #1
easy-rsa (or another tool)
Root certificate
Client certificate signed by CA
Generate Private Key
Private Key PrKC1
Generate Certificate request
csr file PKCS#10 format
Provide Certificate request

Figure 112: certificate generation with client generating its private key

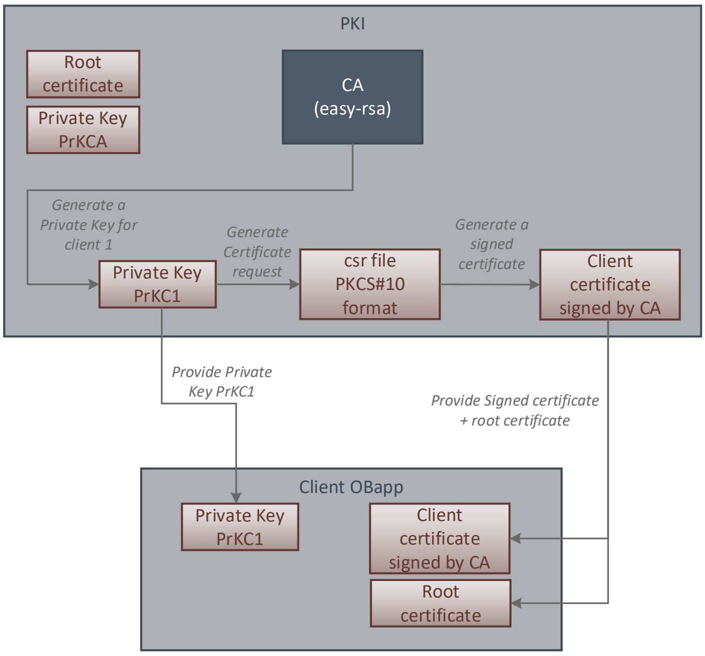

PKI
Root certificate
Private Key PrKCA
CA (easy-rsa)
Generate a Private Key for client 1
Private Key PrKC1
Generate Certificate request
csr file PKCS#10 format
Generate a signed certificate
Client certificate signed by CA
Provide Private Key PrKC1
Provide Signed certificate + root certificate
Client OBapp
Private Key PrKC1
Client certificate signed by CA
Root certificate

Figure 113: Certificate generation with CA generating the private key for the client

10 STANDARDS DOCUMENTS

[R1] Document Title	**[R2]** Reference, version
[S1] Radio-frequency connectors –Part 16: Sectional specification – RF coaxial connectors with inner diameter of outer conductor 7 mm (0,276 in) with screw coupling – Characteristics impedance 50 Ω (75 Ω) (type N)	IEC 61169-16
[S2] Management Information Base for Network Management of TCP/IP-based internet: MIB-II	RFC 1213
[S3] MC Services Security aspects (useful to understand MCx authentication and authorization)	3GPP TS 33.180
[S4] Mission Critical Data (MCData) signalling control; Protocol specification	3GPP TS 24.282
[S5] Mission Critical Data (MCData) media plane control; Protocol specification	3GPP TS 24.582
[S6] UIC - FRMCS Use cases	UIC MG-7900, Version 2.0.0
[S7] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Future Railway Mobile Communication System	3GPP TR 22.889
[S8] UIC - FRMCS Principle Architecture	UIC MG-7904 Version 0.3.0 (Draft)
[S9] UIC – FRMCS – Telecom On-board system – Functional Requirement Specification	UIC TOBA FRS-7510 Version 0.2.0 New version 1.0.12

[S10] Common functional architecture and information flows to support mission critical communication services	3GPP TS 23.280 Stage 2
[S11] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support Mission Critical Data (MCData)	3GPP TS 23.282 V17.6.0, Stage 2 (Release 17) - 04/2021
[S12] Rail Telecommunications (RT); Future Rail Mobile Communication System (FRMCS); Study on system architecture	ETSI TR 103.459 V1.2.1, 08/2020

11 REFERENCES DOCUMENTS

[R3] Document Title	**[R4]** Reference, version
UIC FRMCS – User Requirements Specification	FU-7100 Version 5.0.0
ETSI Future Rail Mobile Communication System (FRMCS) – Study on system architecture	ETSI TR 103 459 Version 0.2.2
UIC FRMCS – Functional Requirements Specification	FU-7120 Version 0.3.0
UIC FRMCS On-Board System Requirements Specification (TOBA SRS)	TOBA-7530
UIC FRMCS Functional Interface Specification (FRMCS FIS)	
UIC FRMCS Form-Fit Functional Interfaces (FRMCS FFFIS)	
UIC FRMCS System Requirements Specification (FRMCS SRS)	FW-AT-3404
THALES MV31-W Data Sheet https://m2m-communication.gemalto.com/Thales_MV31_Datasheet THALES MV31-W HID https://m2m-communication.gemalto.com/Thales_MV31_HID THALES MV31 AT Commands set https://m2m-communication.gemalto.com/Thales_MV31_ATC THALES MV31 Linux developer guide https://developer.gemalto.com/showcase/openwrt-raspberry-pi-networking-qmi https://developer.gemalto.com/showcase/openwrt-raspberry-pi-networking-mbim https://developer.gemalto.com/showcase/openwrt-raspberry-pi-networking-wwan https://developer.gemalto.com/showcase/openwrt-raspberry-pi-networking-pppd	

12 CYBERSECURITY STANDARDS AND REFERENCES DOCUMENTS

(n.d.). *04_5GRAIL_WP2_Application_Architecture_v2_CCTV.*

(n.d.). *05_5GRAIL_WP2_ArchiReport_-_Applications_TOBA_Interfaces_3.*

(n.d.). *3GPP TS 24.379 V17.2.0.*

(2021-03). *3GPP TS 24.380 V17.2.0 MCPTT media plane control; Protocol specification.*

(2021-04 (Release 16)). *3GPP TS 26.346 V16.9.0; Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs .*

CHAUMETTE, C. (10/12/2020). *Le contrôle/commande ferroviaire - TRP 3 075.* Techniques de l'Ingénieur.

(31/03/2021 version 0F). *data applications over FRMCS.* réf. 20E136.

(16/04/2021). *Deliverable D2.1 - Architecture Report (Work Package 2) – Applications & TOBA interfaces - 5GRAIL.*

(26/04/2021 - draft). *Deliverable D2.1 - Architecture Report (Work Package 2) - PIS Application.*

(16/04/2021). *Deliverable D2.1 Architecture Report (Work Package 2) – Applications & TOBA interfaces.* draft.

(15/04/2021 - draft). *Deliverable D2.1 Architecture Report (Work Package 2) – FRMCS Gateway Services.*

DINSIC, A. e. (version 1). *AGILITÉ ET SÉCURITÉ NUMÉRIQUES : MÉTHODE ET OUTILS À L'USAGE DES ÉQUIPES PROJET.*

EEIG ERTMS Users Group. (31/03/2021). *ERTMS data applications over FRMCS - Version: 0F.*

EFORT. (n.d.). *Introduction à la 5G.* http://www.efort.com. Retrieved from http://www.efort.com

ENISA. (FEBRUARY 2021). *SECURITY IN 5G SPECIFICATIONS - Controls in 3GPP Security Specifications (5G SA).*

ENISA. (NOVEMBER 2020). *RAILWAY CYBERSECURITY - Security measures in the Railway Transport Sector.*

(n.d.). *IEC 62443-4-1.*

IEC. (n.d.). *NF EN IEC 62443-3-2:2020-08 - Security for industrial automation and control systems - Part 3-2 : security risk assessment for system design.*

Inventory of Risk Management / Risk Assessment Methods. (n.d.). Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

IP Multimedia Subsystem. (n.d.). Retrieved mai 4, 2021, from https://en.wikipedia.org/wiki/IP_Multimedia_Subsystem

KTT_RAIL_SMO_TD_DB_SNCF-RES. (02-12-2020). *Deliverable 8.3 - Protection profile for Adaptable Communication System (ACS) components.*

MANAI, W. (15/04/2021 - Draft). *Deliverable D2.1 - Architecture Report (Work Package 2) - PIS Application.*

(27 March 2013). *NF EN 15380-4 - Railway applications — Classification system for railway vehicles — Part 4: Function groups.*

(n.d.). *NF EN IEC 62443-3-2:2020-08.*

(2019-04). *NF EN IEC 62443-3-3 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.*

(2019-04). *NF EN IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2 : technical security requirements for IACS components.*

UIC. (2020). *Future Railway Mobile Communication System - User Requirements Specification v5.0.0.* Retrieved 09 29, 2020, from https://uic.org/IMG/pdf/frmcs_user_requirements_specification-fu_7100-v5.0.0.pdf

UIC Ingo Wendler, Dan Mandoc. (14.12.2020 0.3.0). *FRMCS Principle Architecture Document No. MG-7904.*

X2Rail-3 Deliverable D8.3. (2020). *Definition of generic protection profiles - Shared Security Services.*

Grant agreement
No 951725