Deliverable D1.2

Test report conclusion from simulated/lab environments

Grant agreement
No 951725

5GRAIL

5G for future RAILway mobile communication system

D1.2 Test report conclusion from simulated/lab environment

Due date of deliverable: 30/06/2023

Actual submission date: 22/12/2023

Leader/Responsible of this Deliverable: UIC

Reviewed: Y

Document status		
Revision	**Date**	**Description**
1.0	28/08/2023	Consolidation of observations, outcomes from lab testing environment of WP3 and WP4
2.0	22/12/2023	1. §3.2.1.2 Improvement of readability for tables presenting IDs for tight-coupled applications in WP3 lab 2. §3.8.2 Update of figure 15 to focus only on MCPTT (KPI1&KPI2) which are measured during our tests. KPI3 presented only for information. 3. Performance measurements with MCPPT KPI2 for WP3 lab added in §3.8.3.1 4. §3.8.4.1 RTT delay as a performance KPI for ETCS application in combined scenario with ETCS and remote vision in nominal and degraded radio conditions in WP4 lab. 5. §3.8.4.2 RTT delay of ATO status report, as a performance KPI to evaluate the network impact to the application. 6. §3.9.2.1 RTT delay as a performance KPI in bearer-flex testing with TOBA-A. 7. §3.9.3.1Performances of CCTV offload with bearer-flex feature in WP3 lab

		9. §3.10.2.1.1RTT delay as a KPI for evaluation of cross-border 10. §9.3.1Additional explanations for inter-PLMN handover cross-border

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	x
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 (extended to 38 months)

Executive Summary

Test report conclusion from simulated/lab environment (D1.2) is the second deliverable of work package 1 (WP1) within 5GRAIL Project. This document is focused on the conclusions, observations and outcomes of tests achieved in the simulated/lab environments of work package 3 (WP3) in Budapest/Hungary (led by Nokia) and work package 4 in Montigny/France (led by Kontron). The document will bring the details of implementation and performance evaluation of each test scenario, which were not known even when the final version of D1.1 was published.

One of the main achievements of 5GRAIL was the development of the first FRMCS prototypes: On-board FRMCS (Telecom On-Board Architecture, TOBA box), Trackside FRMCS Gateway and Railway Applications, all tested in a 5G SA environment to validate the FRMCS v1 specifications. One of the challenges was that these specifications were developed and finalized in parallel with the project. The document will identify the technical constraints, reveal the implementation issues and explain the solutions provided which have influenced not only the FRMCS specifications but also the ETSI TC-RT and 3GPP specifications.

Finally, this deliverable will present to which extend both labs' observations have safely prepared the success of field activities.

Abbreviations and Acronyms

Abbreviation	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core
5G NSA	5G Non-Stand Alone
5G SA	5G StandAlone
aka	Also Known As
AMF	Access and Mobility Management Function
API	Application Programmable Interface
APN	Access Point Name
ATO	Automatic Train Operation
ATSSS	Access Traffic Steering, Switching & Splitting
CCTV	Closed Circuit TeleVision
COTS	Commercial Off The Shelf
CP	Control Plane
CSCF	Call/Session Control Functions
CU	Centralized Unit
DMI	Driver Machine Interface
DN	Domain Name
DSCP	Differentiated Services Code Point
DU	Distributed Unit
ES3	Engineering Sample 3 (reference to the Thales n39 band chipset)
ETCS	European Train Control System
EU	European Union
FDD	Frequency Division Duplexing
FFFIS	Form Fit Functional Interface Specification
FIS	Functional Interface Specification
FRMCS	Future Railway Mobile Communication System

FRS	Functional Requirements Specification
GA	Grant Agreement
GBR	Garanteed Bit Rate
GoA	Grade of Automation
GRE	Generic Routing Encapsulation (RFC8086) -> Tunnel GRE
GTW or GW	GaTeWay or GateWay
H2020	Horizon 2020 framework program
HMI	Human Machine Interface
HSS	Home Subscriber System
IMS	IP Multimedia Subsystem
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IP	Internet Protocol
IWF	Inter Working Function
JSON	JavaScript Object Notation
KPI	Key Performance Indicators
MCX	Mission Critical, with X=PTT (Push-To-Talk forVoice) or X=Video or X=Data
MM	Mobility Management
N3IWF	Non-3GPP Inter Working Function
NR	New Radio
OB	On Board
OB_GTW	On-Board Gateway
OBA	On-Board Application (e.g. ETCS on-board, ATO on-board)
OBU	On-Board Unit
O&M	Operation & Maintenance
OTA	Over The Air
OTT	Over The Top
PCC	Policy and Charging Control

PCRF	Policy and Charging Rules Function
P-CSCF	Proxy - Call Session Control Function
PPDR	Public Protection and Disaster Relief
PER	Packet Error Rate
PIS	Passenger Information System
PKI	Public Key Infrastructure
QCI	QoS Class Identifier
5QI	5G QoS Identifier
QoS	Quality Of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RBC	Remote Block Centre
REC	Railway Emergency Communication
RF	Radio Frequency
RTP	Real Time Transport Protocol
RTCP	Real-Time Transport Control Protocol
S-CSCF	Servicing-Call Session Control Function (Correspondence IMPU - @ IP)
SSC	Service and Session Continuity
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMF	Session Management Function
SSH	Secure Shell
SRS	System Requirements Specification
TDD	Time Division Duplex
TE	Test Environment
TFT	Traffic Flow Template
TLS	Transport Layer Security
TC	Test case

TCMS	Train Control Management System
TCP	Transmission Control Protocol
TOBA	Telecom On-Board Architecture
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
URS	User Requirements Specification
VMS	Video Management System
VoNR	Voice over New Radio
VoLTE	Voice over LTE
VPN	Virtual Private Network
WP	Work Package (e.g. WP1, WP2, WP3, WP4, WP5)

Definitions

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.
Application Service	Application part responsible of the UP management
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.
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).
End-to-End	Including all FRMCS ecosystem elements
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.
“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.
GoA2	**Grade of Automation 2**: Starting and stopping are automated, but a driver operates the doors, drives the train if needed and handles emergencies.
Interworking	Interworking is the function that enables two different networks to communicate with each other, enabling services to be delivered across them
iPerf	Open source tool used to evaluate network performances in a client-server architecture, available in different operating systems.

NG interface	The NG interface is a logical interface between an NG-RAN and 5GC. There are two interfaces under NG interface: NG-C for control plane and NG-U for user plane.
Priority service	A service that requires priority treatment based on operator policies.
PIS controller	She/he is the individual responsible for managing passenger information.
QCI (or 5QI)	A scalar that is used as a reference to a specific packet forwarding behaviour (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.
Super-loose mode	As considered by the application, can be characterized as a “flat IP”. An ‘agent’ is located between the application and the On-board Gateway, to make this mode OBapp compatible.
Transport Domain	A Transport Domain is the administrative realm of the Transport Stratum. The Transport Stratum comprises one or more access technologies controlled by a core network. A Transport Domain is uniquely identified by the PLMN-ID.
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.

CONTENTS

Table of figures

List of tables

1 INTRODUCTION

5GRAIL, as part of the FRMCS readiness activities is focused on:

- the development of the Telecom On-board Prototype (TOBA box),
- the validation of the first set of specifications by developing and testing the FRMCS On-Board and application prototypes, in lab and field environments, and
- providing feedback and lessons-learned to standardization organizations for consideration in updates of the specifications.

The content of D1.2 is mainly the analysis of results and observations of both labs, also emphasizing the impact on the specifications improvement.
It is important to note that the UIC FRMCS v1 specifications, currently part of the European CCS TSI 2023 (Control Command System Technical Specifications for Interoperability) and compatible with 3GPP R18 and early R19 specifications amendments, which were developed in parallel with this project.

To understand the orchestration position of WP1, as interacting with all the other 5GRAIL work packages, the following figure depicts how the inputs of the other work packages are processed by WP1 to create the D1.2:

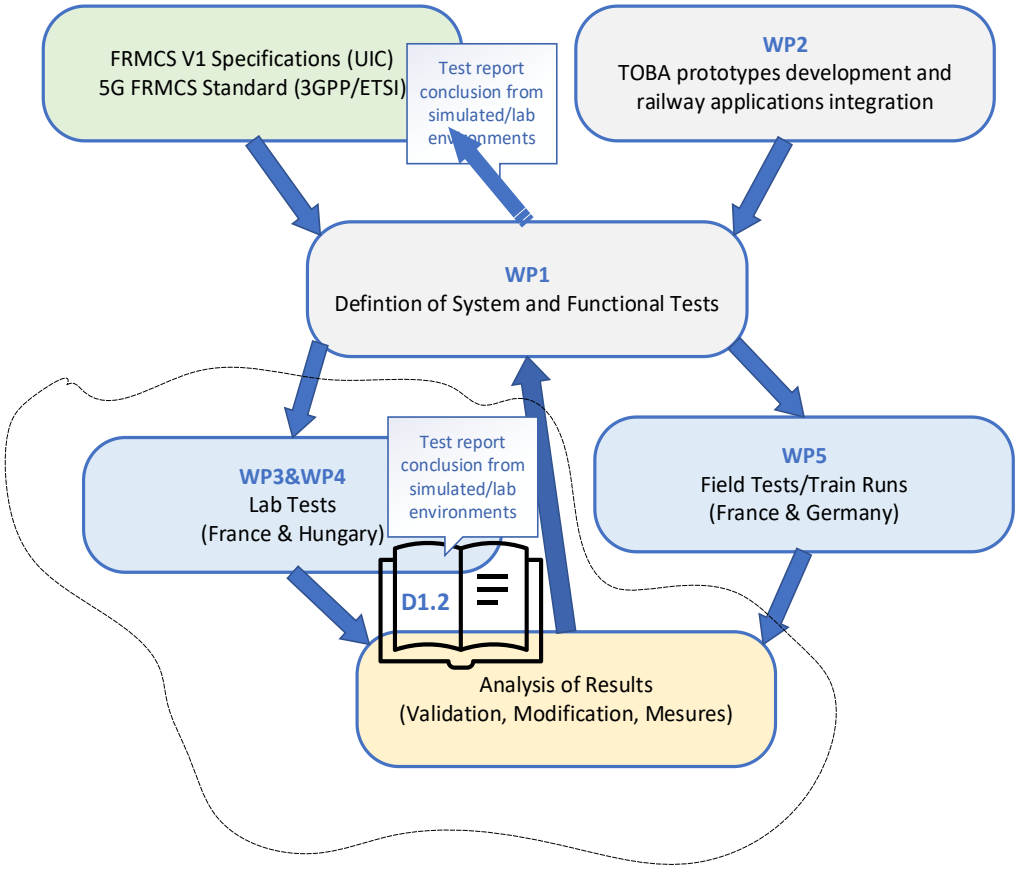


Figure 1: WP3 and WP4 outcome defines the content of D1.2 (loop-back to the FRMCS specification)

The main part of this document is organized around the FRMCS principles and features, considering also the global end-to-end architecture, the set-up and testing priorities of each lab.

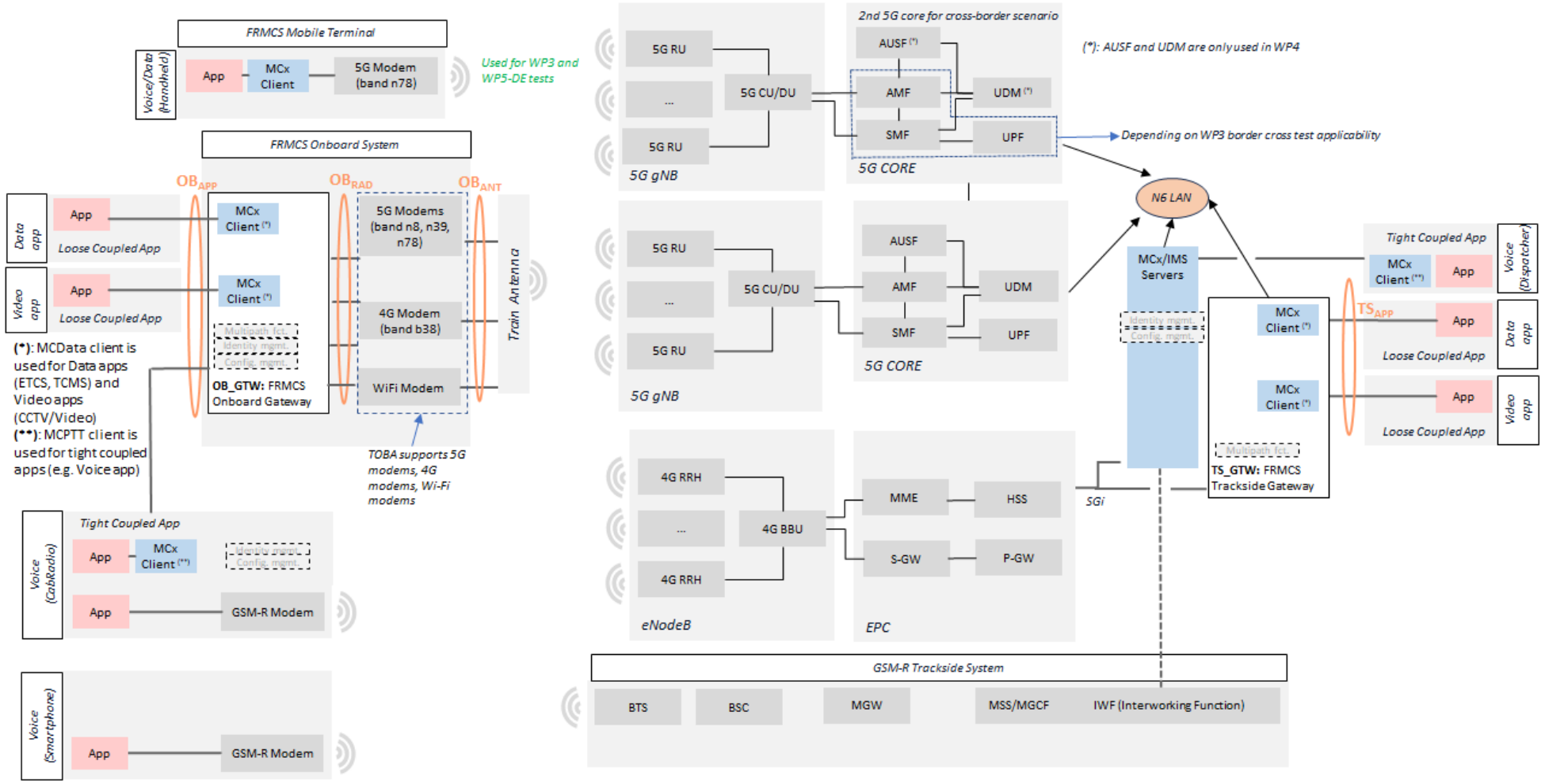
The structure is summarized in the following:

- Reminder of the global end-to-end architecture.
- WP3 environment and supported applications.
- WP4 environment and supported applications.
- Observations and conclusions derived from validation of FRMCS principles.
- Recommendations on radio configurations and observations due to the bands used.
- Lab experience, as a facilitator of field activities in WP5.
- Testing outcomes
- Impact on specifications (FRMCS v1 and 3GPP release 18 and beyond)

2 REMINDER OF THE GLOBAL END-TO-END ARCHITECTURE

FRMCS, is being specified and implemented as a standardized system, combining 5G SA transport means with Mission Critical (MC) features. To support such mission-critical rail applications, FRMCS relies on underlying telecom building blocks. These are the transport services provided by wireless networks based primarily on 3rd Generation Partnership Project (3GPP) technology, 5G Core and Access networks supporting at least Railway Mobile Radio (RMR) - harmonized spectrum for Europe (as per Electronic Communications Committee (ECC) (20)02 decision), ensuring the relevant performance requirements per railway application and the service layer leveraging the functionalities of the 3GPP Mission Critical Services (MCX).

These main components of the FRMCS ecosystem are represented in the following figure summarizing the end-to-end architecture, used in 5GRAIL project:



5GRail Generic e2e Test Architecture

The above overall architecture, explaining the building blocks of the FRMCS ecosystem (also including the elements of the GSM-R system) needs to be considered in close relation with the D2.1 view, introducing the two important constituents to be validated, the Gateways and the railway operational applications, FRMCS v1 compliant:

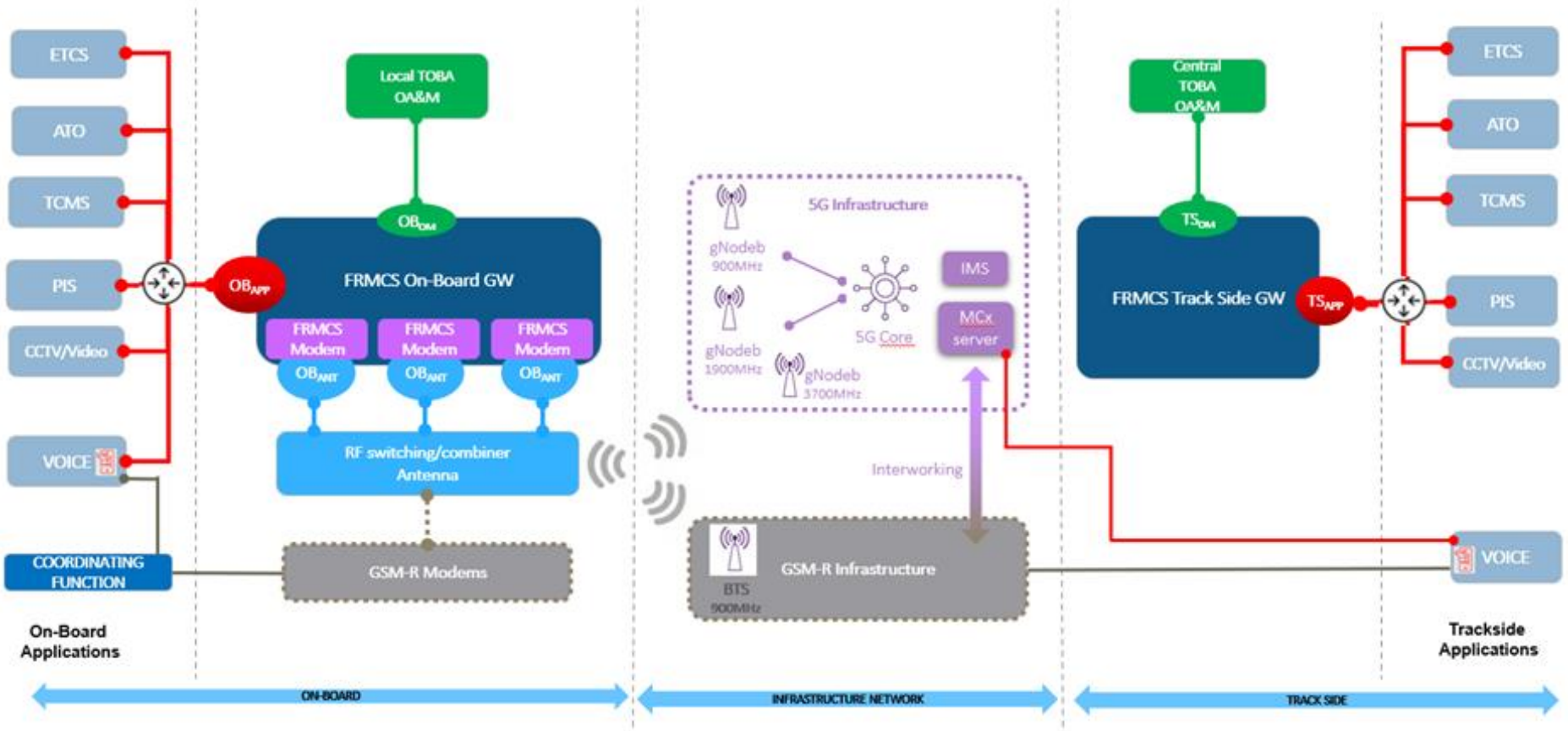


Figure 2: Architecture overview (Ref. D2.1)

The above figure is a complementary view of the global end-to-end architecture, adding the key elements that are used to validate the design concept and features:

- The two FRMCS Gateways for On-board and for Trackside, which are completely new prototypes specifically developed for FRMCS;
- The Applications, similar with the ones rolled out in GSM-R, such as ETCS, ATO and Voice, which were however ported over the new FRMCS system, being designed in compliance with the new FRMCS standardized reference points, On-board Application Interface (OB_{APP}) for the On-board part and Trackside Application Interface (TS_{APP}) for the trackside part, the underlying 5G infrastructure and inclusion of the MCX elements.;
- A set of new applications (ATO, TCMS, PIS, Video,..) have also been modified and tested to use FRMCS via the same OBapp and TSapp interfaces.

The key design principles expected to be fulfilled by the FRMCS gateways prototypes are:

- Decoupling of Applications and Communication Services/Transport strata.
- Ensuring improved performance and service availability (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, with individual QoS requirements for the applications and priorities among applications).

2.1 WP3 ENVIRONMENT AND SUPPORTED APPLICATIONS

WP3 lab hosted in Nokia's premises in Budapest – Hungary was focused on the integration and validation of the Voice applications over FRMCS, consider also interworking with GSM-R.
Also, some other data railway applications have been integrated and validated in this lab, as listed in the following:

Voice:

- 5G/FRMCS-based MCPTT point-to-point and group voice communication provided by Siemens,
- 5G/FRMCS-based Railway Emergency Call (REC) provided by Siemens,

Data:

- European Train Control System (ETCS) provided by CAF,
- Train Control and Monitoring System (TCMS) provided by CAF,
- Non-critical video application and CCTV archive transfer provided by Teleste.
- Voice application on COTS/Smartphone and Dispatcher provided by Nokia.

The following figure is a high-level presentation of WP3 lab in Hungary:

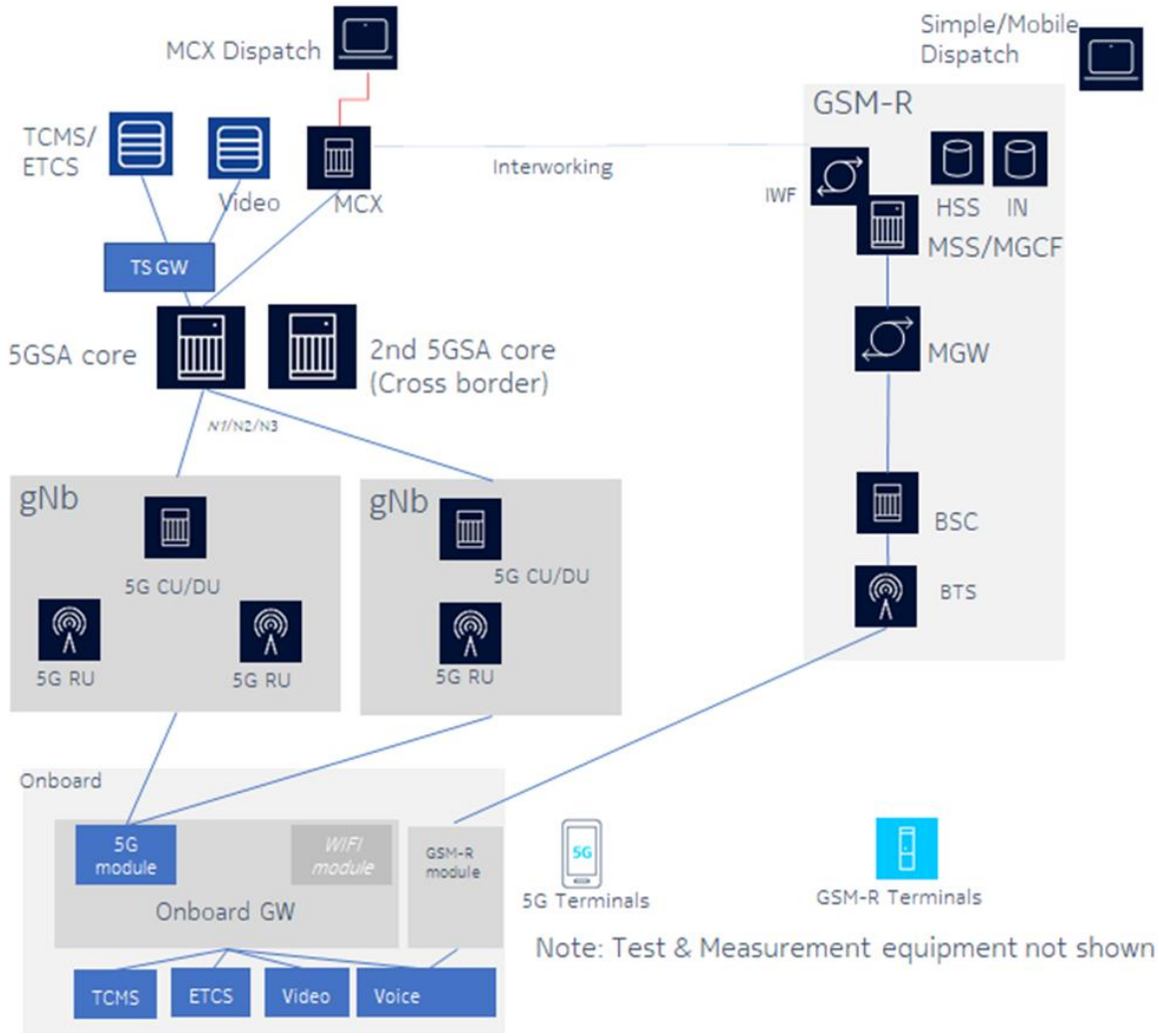


Figure 3: Overview of WP3 lab in Hungary (Ref. D3.1)

The spectrum used in this lab environment, aligned with WP5 field activities (in Germany) are 5G n78 (20 MHz in 3.7-3.8 GHz TDD enterprise band) for lab and field, and 5G n8 (5MHz in 900MHz) - for the lab test only. The observations and outcomes related to the usage of n78 band are considered to be interesting for later deployment of FRMCS.

The table below presents the features, FRMCS principles and MCX building blocks that are validated through the test cases defined and described in D1.1 in the framework of WP3:

	FRMCS principles												
Application	MCPTT client/ server communication	OBapp/TSapp	MCData IPConn	Functional Alias	Authorisation of communication	Authorisation of application [3]	QoS	Multi-user talker control	Arbitration	Interworking	Location services	Bearer flex	Inter-technology FRMCS/GSM-R cross-border
Voice [1]	✓	✓(OBapp only) [2]		✓	✓	✓	✓	✓	✓	✓			
REC	✓	✓(OBapp only) [2]		✓		✓	✓		✓	✓	✓		✓
ETCS - CAF		✓	✓			✓	✓						
TCMS		✓	✓			✓	✓						
CCTV		✓	✓			✓	✓					✓	
Video		✓	✓			✓	✓						

Table 1: FRMCS principles validated in WP3 lab

Notes: [1] Other voice communications except REC are considered. [2]: TSapp is not applied for Voice applications, [3]: Authorization of application is implicitly tested for all applications. However, for voice, there is a dedicated test case, Voice_004

2.2 WP4 ENVIRONMENT AND SUPPORTED APPLICATIONS

WP4 lab hosted in Kontron's premises in Montigny-le-Bretonneux in the suburban of Paris-France, was focused on the integration and validation of railway data applications. We have also performed some optional voice test cases in this lab, as listed in the following.

Data:

- European Train Control System (ETCS) provided by Alstom,
- Automatic Train Operation (ATO) provided by Alstom,
- Passenger Information System (PIS) provided by Thales,
- Remote Vision (RV) provided by SNCF and which aims at providing real time video from a camera installed in the front of the train engine,

Voice:

- Voice application based on Kontron's solution for optional operational tests.

The following figure is a high-level presentation of WP4 lab in Montigny-le-Bretonneux:

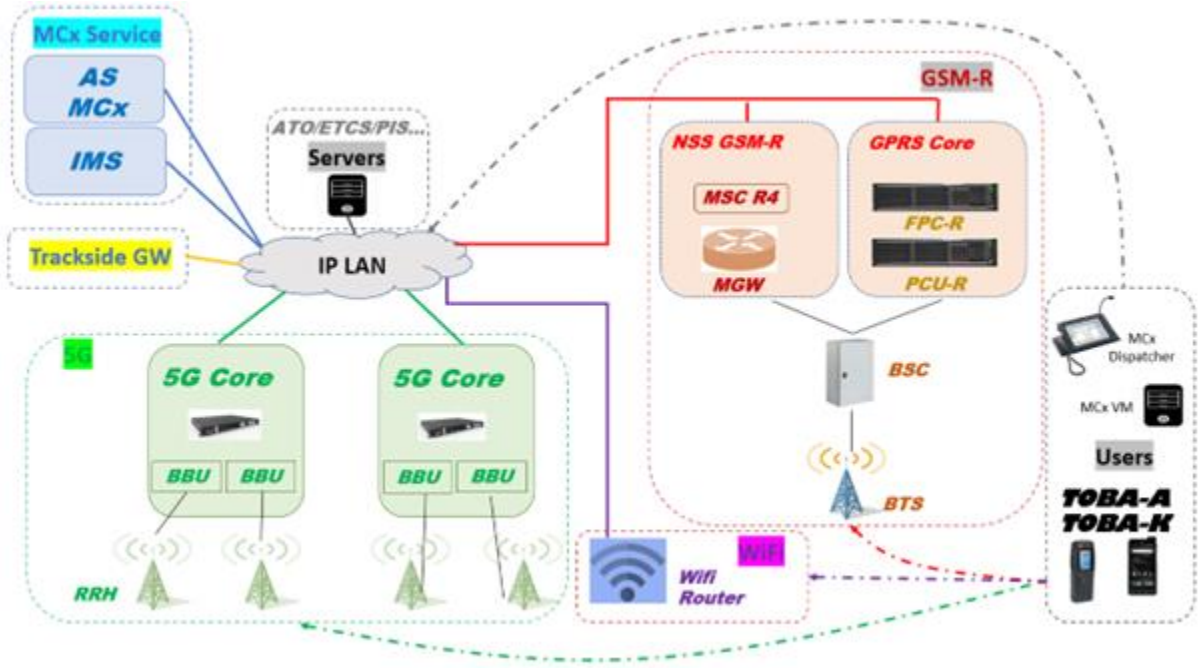


Figure 4: Overview of WP4 lab in France (Ref. D4.1)

WP4 had the possibility to test On-Board Gateways from two providers Kontron and Alstom, known as TOBA-K and TOBA-A respectively and their trackside counterpart. As spectrum used, this was 5G RU n8, n39 and n78 and in 4G RU in b38; Wi-Fi was also available in this lab, allowing combination of testing scenarios and interesting observations.
Related to 5G n39 – we have managed to obtain dedicated chipsets, that have been prepared to comply with FRMCS 1900 MHz band (1900 – 1910 MHz TDD, as per ECC (20) 02), which can be seen also as a subset of n39. These chipsets, that have been delivered at standard handheld power class 3,

have used a power booster, that brought them to Power Class 1 level, which is the FRMCS requirement for On Board Radio used in field tests. The chipsets have been provided by Qualcomm, and the radio module that have incorporated these chipsets and the power booster have been provided by Thales.

The table below presents the features, FRMCS principles and MCX building blocks that are validated through the test cases defined and described in D1.1 in the framework of WP4.

	MCDataIPConn	OBapp/TSapp	Access to FRMCS transport level	Access to FRMCS service level	QoS	Bearer flex	Cybersecurity Local binding/e2e TLS	Cross-border with 1UE	Cross-border with 2UE	
									TOBA-A with 2x5GUE(WP4)	TOBA-K with 1x5GUE&1x4GUE
ETCS - Alstom	✓	✓	✓	✓	✓	✓			✓	✓
ATO	✓	✓	✓	✓	✓	✓	✓			
PIS	✓	✓	✓	✓	✓					
Remote Vision (RV)	✓		✓	✓	✓			✓		

Table 2: FRMCS principles validated in WP4 lab

3 OBSERVATIONS AND CONCLUSIONS DERIVED FROM VALIDATION OF FRMCS PRINCIPLES

The purpose of this chapter is to present the implementations of FRMCS specifications using Gateways and application prototypes within 5GRAIL.

As the 5GRail prototypes have been designed and built in parallel with the finalization for the FRMCS specifications now part of 2023 CCS TSI, we had to consider assumptions based on the knowledge at that time, the available products, and the project timeline. Therefore, some of the features have been what we call workaround – they are explained in this document. This allowed to progress the project and provided valuable feedback to specification work in UIC and 3GPP work frames.

In the following, in case it is relevant due to the observations, the validation of the main FRMCS principles and MCX building blocks will be referenced to specific test cases in the lab.

3.1 Interfaces (OBapp/TSapp)

As presented in Figure 2, there are two interfaces between applications and FRMCS gateways:

- OBapp interface stands between the on-board applications and the FRMCS Onboard Gateway.
- TSapp interface stands between the ground applications and the FRMCS Trackside Gateway.

Those interfaces are applicable in both MCx coupling modes:

- the tight coupled applications where the MCx client is embedded in the application.
- the loose coupled applications where the MCx client for the application is hosted and managed at the FRMCS Onboard Gateway level.

In the following, each sub-chapter corresponds to a topic that have raised observation/comment related to OBapp/TSapp specification.

3.1.1 OBapp/TSapp interface – reminder

The OB_{APP} ensures access to the communication services allowing the authentication, authorization and quality of service profile management requested by the applications.

The OBapp Control Plane exposes three main functions, as presented in the below figure:

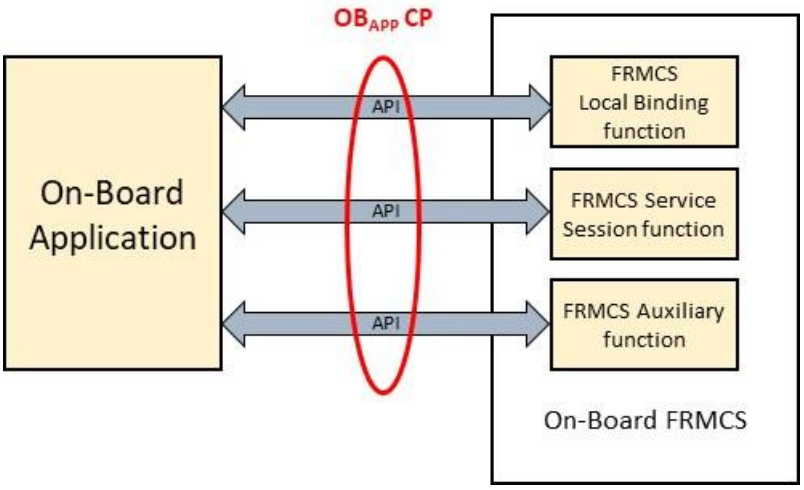


Figure 5: API features exposed by the OBapp Control Plane interface. (Ref. FRMCS FFFIS v1_7950)

Note: TSapp is not yet defined in FRMCS specifications. The assumption for 5GRAIL was that the API is the same for both OBapp and TSapp.

3.1.2 Protocol and structure used for the OBapp/TSapp API

There was a project decision to use the WebSocket protocol for accessing the OBapp and the TSapp, known for its ability to natively manage full-duplex transaction (client to server and server to client), and JSON-RPC structure for requests, responses and notifications.

All the requests, responses and notifications defined in D2.1 were correctly implemented by both clients and servers' providers.

There were some issues on the API syntax, but it was mainly due to uncertainties in the first versions of D2.1, which were clarified afterward in the next versions of D2.1. For example, case sensitivity issue occurs with some application using the mode "not_auto" (i.e., for incoming sessions, the FRMCS GTW sends a request to the application to know if it wants to accept or reject the session). The application answered with a parameter "return: ok", whereas the GTW expected a "return: OK". It was then decided to not use at all capital letters in the JSON-RPC request params, and answer result. Hence, WebSocket protocol is well adapted to OBapp/TSapp API and the use of notification.

WebSocket also brings the ability to monitor the OBapp/TSapp connection in a more flexible way that keep-alive TCP monitoring for example. The application (client) can monitor the WebSocket connection with the FRMCS gateway (server) following its need, and in the opposite the server can monitor the WebSocket connection with the applications. This mechanism (named WebSocket ping-pong mechanism) was widely used by the application providers. An important constraint is that the answer to a WebSocket ping request (and also the answer to any API request) shall be sent in less time than a specified value to allow applications and gateways implementation to consider a relevant timer before closing a WebSocket connection for failure reason (see more details in D2.4 where a related issue was raised).

- **Recommendations related to the WebSocket usage:**

  - A maximum time to answer to WebSocket ping request, or more generally to an API request, shall be specified in the interface definition.
  - In the opposite way, the OB GTW can use the native ping/pong mechanism to detect an application failure (application not responding to a ping, to differentiate inactivity and failure) and then delete the associated resources and close the related sessions.

Note: FRMCS V1 have considered at that time both the usage of WebSocket or of HTTP2 as OBapp and TSapp protocols.

Above the WebSocket layer, some improvements on the API could be done and these improvements are listed in the next chapter.

3.1.3 API improvements

This topic will be detailed in D2.4:

Few minor improvements could be performed in the API definition, such as:

- In the REGISTER method, the parameter **application_type should be a string** (ETCS, ATO, ..) instead of an integer, for a better readability.
- In the REGISTER method, we could add a parameter to say if the **originator_id** is absolute or relative, depending on the ability of the application to have a globally unique originator_id or if the OB_GTW has to add a part to make it unique. An absolute originator_id could be used directly by the OB_GTW to build the FRMCS identifiers (e.g., MCX/SIP identities); whereas relative originator_id could be completed with a suffix (such as identification of the train) before building FRMCS identifiers (e.g., MCX/SIP identities).

NOTE: This point depends on the addressing requirements which are FFS in the UIC FIS §8[22] specification.

- In case an application performs multiple registrations, e.g., PIS application which is registered with three originator_Ids at the same time, a minimum timer is needed between REGISTER messages to avoid issue on FRMCS gateway SIP registration. It was confirmed that the On-board gateway supports this multiple registration, but this was not correctly supported by the SIP core/MCX server. Sequential registrations (every 1 second) solved the issue, but it implies a loss of time and **a better improvement would be that the SIP core/MCX server support multiple registrations in a short time.**
- **SESSION_END processing**: Following a nominal session_end request, an application receives firstly a session_status_changed notification (with session_status=deleted), then a positive answer to the request. Some applications were expecting to receive firstly the answer, and secondly the notification with session_status deleted. The dynamic for a session_end was clarified in D2.1 document but was still questioned by few partners. **The order of responses and notifications shall be clearly defined for each use case.**

3.1.4 State diagram and independency between OBapp/TSapp requests and the MCX events.

This topic will also be detailed in D2.4:

The OBapp/TSapp API in D2.1 was designed to provide local and direct answers to the application requests, i.e., the FRMCS gateway is able to answer to a request quite immediately, without waiting for an answer from the network (e.g., from the IMS/MCx server). The results from updates/answer by the network (e.g., a SIP 200 OK message received from the IMS server) are then managed through notifications. For example, when an application sends a SESSION_START request, the FRMCS gateway is able to answer quite immediately, then send the corresponding SIP request to the IMS/MCX servers, and finally when it receives the answer (e.g., SIP 200 OK), it sends a SESSION_STATUS_CHANGED notification to the client to notify that the session is ready for use. The FRMCS gateway shall maintain a session status for each session (and a connection status for each registered application), in order to be able to answer directly to a status request at any time.

This allows to get very good reaction times for the answer to the different requests, and not get stuck by a non-availability of the network.

But this point should have been more explicitly required, because in some implementations the answer to a request was waiting for a reaction from the network. Then, the time to answer to the corresponding request was too long. **This feedback is also related to the specification of a maximum time to answer to an API request (see 3.1.2).**

Also, it enables the application to start API exchanges independently from the cellular connection of the OB_GTW and from the MCX client's registration. One issue encountered with a previous version of the OB_GTW used for the field test, for example, was the following: the ETCS application from WP4 was switched on under a non-coverage area. Then, the OB_GTW was not able to register the corresponding MCX client, and it was not performing neither when the coverage becomes OK. When the ETCS application was requesting a connection_status request, it never turn to "connected" status. This was corrected later on the OB_GTW.
Same kind of issue with ETCS application from WP3 when performing a session_start request when the OB_GTW was out of coverage. The OB_GTW was expected to receive the request only after a "connected" status. A mitigation was to add a timer in the ETCS (CAF) after the OBapp register request and before session_start request, to let time to the OB_GTW to register the MCX client to the MCX server. **In future version, it would be preferable that the OB_GTW supports session_start request under a non-coverage area, when the MCX clients is not registered yet.**

3.2 Addressing (MCX, SIP, IP)

This chapter presents the feedback related to addressing topic, divided into two categories:

- IMS/MCX identities
- IP addressing and especially end to end IP routing.

3.2.1 MCX/SIP addressing

The following figure presents the dependencies and location of the different service identities using the stratum model of FRMCS. It shows in which stratum and on-board and trackside the different identities are located.

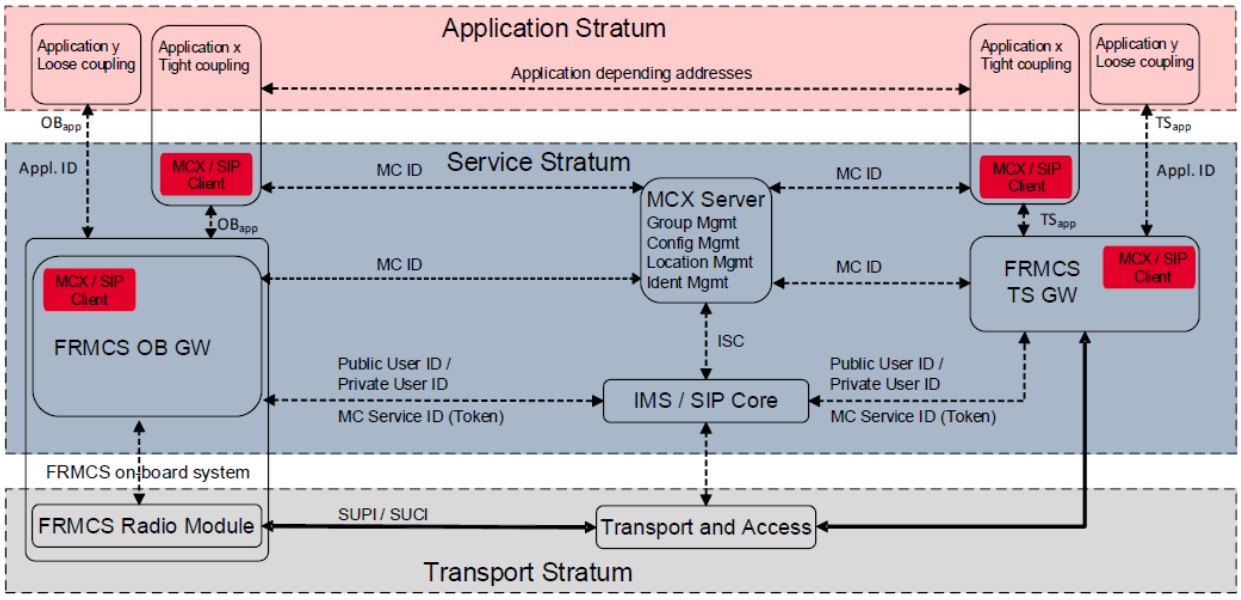


Figure 6: Identities and their location (Ref. UIC SRS FW-AT 7800)

3.2.1.1 MCX/SIP addressing for LC applications

In the framework of 5GRAIL, the Host -to-Host (H2H) addressing scheme is applied for loose coupled applications, as presented in the figure below:

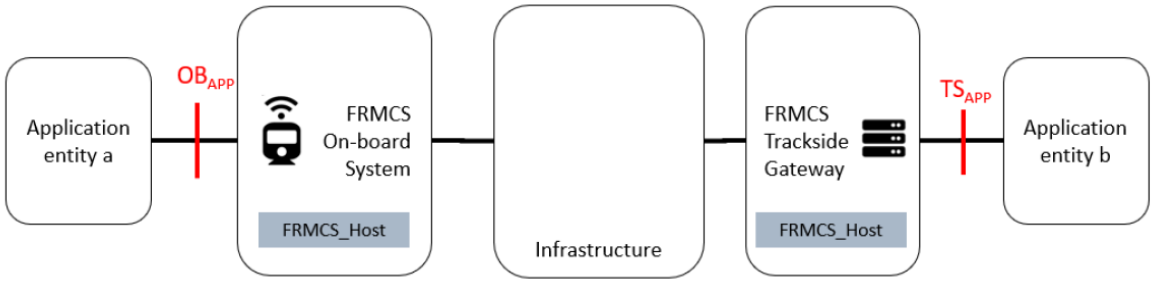


Figure 7: Host-to-Host (H2H) addressing principle in loose-coupled example (Ref. SRS FW-AT 7800)

In the H2H addressing scheme, an FRMCS "Host" represents a single application entity within the FRMCS system.

The MCX/SIP identities of LC application were configured in the FRMCS gateway. The FRMCS gateway has a mapping between the originator-id (parameter used in the local binding to locally identify the application) and the MCX/SIP identities (used to register the MCX client to the FRMCS service servers).

Only MCdata service was used for LC application, and MCdata-IPconn function was used to establish the session.
A dedicated MCdata user is provisioned per loose coupled application instance and all MCdata users are provisioned in advance in the MCX server.

NOTE: the multipath function of Alstom gateway was done at service level. For that, one MCdata user per link and per application was used.

In order to properly configure the MCdata users in FRMCS gateway and MCX/SIP servers, two mapping tables were used for WP3 and WP4 configurations. These mapping tables are given below, also presented in D1.1 §16.2.1 IDs used in WP3 and §16.2.2 IDs used in WP4 per application:

- **IDs used in WP3 for loose coupled applications:**
  - ETCS (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	EVC / ETCS	00100100010	+820100000031@mcptt.nokia.com	+820100000031@mcptt.nokia.com	00100100010	00100100010@mcptt.nokia.com
TS	RBC / ETCS	00100100011	+820100000032@mcptt.nokia.com	+820100000032@mcptt.nokia.com	00100100011	00100100011@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	MCPTT ID
OB	MCG / TCMS	00100100012	+820100000033@mcptt.nokia.com	+820100000033@mcptt.nokia.com	00100100012	00100100012@mcptt.nokia.com
TS	GCG / TCMS	00100100013	+820100000034@mcptt.nokia.com	+820100000034@mcptt.nokia.com	00100100013	00100100013@mcptt.nokia.com

  - CCTV/Video (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	MCPTT ID
OB	NVR / Video	00100100014	+820100000035@mcptt.nokia.com	+820100000035@mcptt.nokia.com	00100100014	00100100014@mcptt.nokia.com
TS	WCG / video	00100100015	+820100000036@mcptt.nokia.com	+820100000036@mcptt.nokia.com	00100100015	00100100015@mcptt.nokia.com
TS	WCG2 / video	00100100016	+820100000042@mcptt.nokia.com	+820100000042@mcptt.nokia.com	00100100016	00100100016@mcptt.nokia.com

- **IDs used in WP4 for loose coupled applications:**

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)
ETCS						
OB	EVC	id000005.ty02.etcs	id000005.ty02.etcs@sv-lab.net	id000005.ty02.etcs@sv-lab.net	id000005.ty02.etcs	id000005.ty02.etcs@sv-lab.net
TS	RBC1	id500033.ty01.etcs	id500033.ty01.etcs@sv-lab.net	id500033.ty01.etcs@sv-lab.net	id500033.ty01.etcs	id500033.ty01.etcs@sv-lab.net
TS	RBC2	id500034.ty01.etcs	id500034.ty01.etcs@sv-lab.net	id500034.ty01.etcs@sv-lab.net	id500034.ty01.etcs	id500034.ty01.etcs@sv-lab.net
TS	RBC3	id500035.ty01.etcs	id500035.ty01.etcs@sv-lab.net	id500035.ty01.etcs@sv-lab.net	id500035.ty01.etcs	id500035.ty01.etcs@sv-lab.net
TS	RBC4	id500036.ty01.etcs	id500036.ty01.etcs@sv-lab.net	id500036.ty01.etcs@sv-lab.net	id500036.ty01.etcs	id500036.ty01.etcs@sv-lab.net
ATO						
OB	ATO-OB	ato-ob.ato	ato-ob.ato@sv-lab.net	ato-ob.ato@sv-lab.net	ato-ob.ato	ato-ob.ato@sv-lab.net
TS	ATO-TS	ato-ts.ato	ato-ts.ato@sv-lab.net	ato-ts.ato@sv-lab.net	ato-ts.ato	ato-ts.ato@sv-lab.net
PIS						
OB	PIS-OB	msg.ob.pis	msg.ob.pis@sv-lab.net	msg.ob.pis@sv-lab.net	msg.ob.pis	msg.ob.pis@sv-lab.net
OB	PIS-OB	mgt.ob.pis	mgt.ob.pis@sv-lab.net	mgt.ob.pis@sv-lab.net	mgt.ob.pis	mgt.ob.pis@sv-lab.net
OB	PIS-OB	log.ob.pis	log.ob.pis@sv-lab.net	log.ob.pis@sv-lab.net	log.ob.pis	log.ob.pis@sv-lab.net
TS	PIS-TS	msg.ts.pis	msg.ts.pis@sv-lab.net	msg.ts.pis@sv-lab.net	msg.ts.pis	msg.ts.pis@sv-lab.net
TS	PIS-TS	mgt.ts.pis	mgt.ts.pis@sv-lab.net	mgt.ts.pis@sv-lab.net	mgt.ts.pis	mgt.ts.pis@sv-lab.net
TS	PIS-TS	log.ts.pis	log.ts.pis@sv-lab.net	log.ts.pis@sv-lab.net	log.ts.pis	log.ts.pis@sv-lab.net

Domain part of the destination of a session:
One difficult part of FRMCS session establishment for LC application is to translate the destination identity provided by the application in the session_start API request into a MCdata service identity, and also to know the SIP IMPU of the MCX server to be used. In 5GRAIL, a shortcut was used, since there was only one MCX/SIP server per lab test installation, so only one SIP domain and one MCX domain known by configuration in the FRMCS gateways.

Conclusion on 5GRAIL MCX/SIP addressing for LC application:
The MCX/SIP credentials used for LC applications were not dependent from SIM/ISIM parameters at all and rely on gateway configuration. This principle works well and allows to establish the MCdata-IPconn session needed without any issue.

The topic of saving MCX/IMS credentials in a secure way was not tackled in 5GRAIL and will have to be specified in FRMCS specifications.
Following the solution for multipath management (at service level or at transport level), the MCX/SIP addressing may be slightly different.

The way of providing FRMCS OB-GW with MCx credentials seems an important and complex topic. In 5GRAIL, all these logins, passwords and identifiers were stored in a common configuration file that could be easily updated according to the needs. But thinking of an efficient way to store these credentials in a mature FRMCS system, several questions are raised:

- How many MCx Ids should be configured per OB-GW? Can MCx Id be derived from information contained in the ISIM using a standardized method?
- Can some credentials be downloaded/updated OTA (Over The Air) an if so, is this a secured way?
- If some credentials have to be configured directly on the OB-GW, would it be interesting to do that with a data plug?

Besides, a global naming rule for the identifiers may be useful too and should be discussed.

In addition to these provisioning thoughts, the way one MCx client knows about the MCx Id it should communicate with, is also to be analysed, this part being also hardcoded in FRMCS gateways, used in WP4 lab.

3.2.1.2 MCX/SIP addressing for tight-coupled applications

The MCX/SIP identities of TC applications were configured in the application itself and provisioned in advance in the MCX/SIP servers.

For MCX/SIP identities used in WP3 are presented in the table below:

- IDs used in tight coupled applications.
  - Voice (Siemens)

Application			MCx client in the application (Tight)	
On-Board or Trackside	**Name**	**originator_id (Obapp REGISTER)**	**SIP URI private**	**SIP URI public**
	Smartphone1	00100100005	+820100000006@mcptt.nokia.com	+820100000006@mcptt.nokia.com
	Smartphone2	00100100006	+820100000007@mcptt.nokia.com	+820100000007@mcptt.nokia.com
TS	Controller (Nokia/dispatcher)	00100100003	+820100000001@mcptt.nokia.com	+820100000001@mcptt.nokia.com
OB	CAB2/voice	00100100008	+820100000025@mcptt.nokia.com	+820100000025@mcptt.nokia.com
OB	CAB1/voice	00100100009	+820100000041@mcptt.nokia.com	+820100000041@mcptt.nokia.com

Application			MCx client in the application (Tight)		
On-Board or Trackside	**Name**	**originator_id (Obapp REGISTER)**	**MC ID**	**MCPTT ID**	**Functional Alias**
	Smartphone1	00100100005	00100100005	00100100005@mcptt.nokia.com	dispatcher-111.voice@mcptt.nokia.com
	Smartphone2	00100100006	00100100006	00100100006@mcptt.nokia.com	dispatcher-222.voice@mcptt.nokia.com
TS	Controller (Nokia/dispatcher)	00100100003	00100100003	00100100003@mcptt.nokia.com	not supported
OB	CAB2/voice	00100100008	00100100008	00100100008@mcptt.nokia.com	driver-111.voice@mcptt.nokia.com
OB	CAB1/voice	00100100009	00100100009	00100100009@mcptt.nokia.com	driver-222.voice@mcptt.nokia.com

NOTE: Flexible MC ID needed based on URL, but 11 digits were agreed.

3.2.2 IP addressing and end-to-end IP routing.

3.2.2.1 IP addressing for LC applications – use of virtual session IP address.

To establish sessions between two LC applications, MCData-IPconn function was used. The purpose of this function is to establish an IP tunnel (GRE tunnel) between the two MC clients, in order to carry and encapsulate the applicative data, as illustrated below:

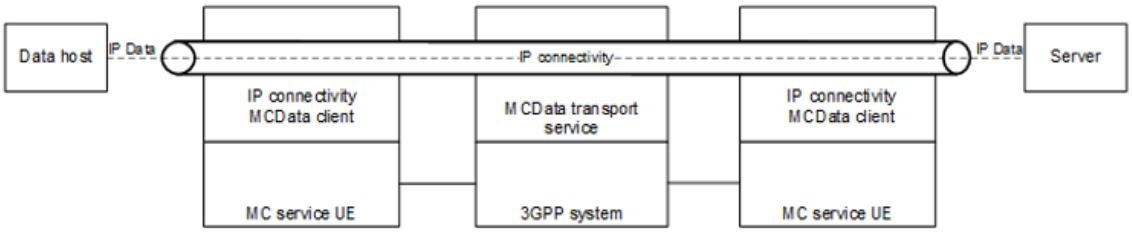


Figure 8: IP connectivity model (Ref. D2.1)

The IP addresses used by the applications for the applicative data encapsulated in the GRE tunnel rely on a virtual session IP address explained in D2.1 document, that allows to keep independency between trains and ground addressing plans.

Only IPv4 addresses were used.

Conclusion related to IP addressing for LC application.

The outcome of this addressing method is good, and the applicative sessions (mainly TCP) were correctly implemented, with both kinds of gateway (Kontron or Alstom). No issue was encountered with IP addressing.

Nevertheless, it was requested by some application providers to know in advance the pool of virtual IP addresses that is used by the local FRMCS gateway, in order to properly configure firewall or routing rules. This was not a difficult task, but since there was no alignment between Alstom and Kontron gateway on the pool of addresses, the applications in WP4 had to consider two different pools.

3.2.2.2 IP addressing for TC applications

Due to the non-not availability of SIP proxy functionality for TC / Voice application, a „route through" workaround solution was proposed. This approach needs to be adjusted as with simple IP forwarding of the OB-GW; the floor control did not work towards CAB radio since the RTCP packets did not reach the CAB radio. Therefore, a GRE tunnel (Generic Routing Encapsulation (GRE) which is a protocol for encapsulating data packets that use one routing protocol inside the packets of another protocol) was realized for voice applications, setup between the Thales modem in the OB-GW and the MCX server. This solution however had some drawbacks on the test execution when using dynamic assignment of IP addresses, as follows:

- IP address of n39 Thales modem in the OB-GW is dynamically allocated from 5G user IP pool during PDU session establishment, and the GRE tunnel is set to a fix IP address.
- when the IP of Thales modem is changing, a new GRE tunnel needs to be specified or the original one needs to be modified on both sides (OB-GW of Kontron and MCX Server of Nokia), according to the new IP of the Thales modem.

As a solution, WP3 decided to use static IP address allocation instead of dynamic one.

NOTE: For Loose-Coupled applications, a pool of virtual IP addresses is also used in the framework of WP3 lab.

Observations – Feedback to the FRMCS specifications:

The impact on end-to-end messages like MCX floor control needs to be considered when defining OB/TS-GW IP addressing schemes for FRMCS. Without SIP Proxy no scalable solution seems to be possible.

3.3 Functional alias

The functional alias is a user selectable alias that is linked to the assignment or task of the user. An MCPTT User can activate one or multiple functional aliases at the same time. The activation of the functional alias(es) will take place after the user has signed in to the MCPTT Server using the MC User ID. The same functional alias can be assigned for use to multiple users depending on MC Service Administrator settings.
A functional alias can be used to identify for example the driver(s) of a particular train, identified by train number and the role of the user on that train.
Each functional alias that is active on the MC system is unique for addressing purposes.

3.3.1 Feedback from functional alias testing

There is an ongoing analysis in the FRMCS specifications WGs about the method to use for the authentication/authorization by the FRMCS system, either user dependent credentials or preconfigured ones. There is a need for a dynamic assignment of functional alias because the current situation is that all the possible functional alias are preconfigured in the MCX server which is not suitable for a big railway network. There is any flexibility since the user is not able to manually introduce the functional alias but only to activate it.

In the framework of WP3, the functional alias registration is implemented using a predetermined list of functional aliases stored in the cab radio configuration file. However, in the future, users will register a functional alias by either manually entering their user ID and password, utilising a PKI card, or retrieving the list of functional aliases from the MCX Server.

Current limitations of MCX server allow the cab radio to register only a single functional alias. However, in the future, there will be an enhanced capability to register multiple functional aliases on a single cab radio, expanding its functionality.

3.4 Authorization of communication

The purpose of this test as described in the D1.1 Test plan was to demonstrate that the FRMCS System can be configured by the network operator to restrict voice communication between FRMCS Users. In the scope of 5GRAIL, a communication allowlist was configured using MCServiceID to control and regulate voice communications.

Thanks to this test, 3GPP specifications were amended because the existing call restriction was only based on source and destination MCX User identities (including functional alias(es)). It was not allowed to deny/permit calls based on subpart/elements of functional alias(es) of MCX Users. The CR which was an outcome of 5GRAIL testing included the denial/permission based on subparts of functional alias(es).

Another limitation discovered is that the current implementation at MCX server level configures denial/permission to the called party (e.g., dispatcher). There is no denial/permission based on the calling party.

3.5 Access to FRMCS service level

3.5.1 Reminder

The access to FRMCS service level mainly covers the following features that are necessary to use FRMCS services:

- SIP registration (to the IMS)
- MCX authentication (to the identity management of the MCX server)
- MCX service authorization (to the MCX server, through IMS)
- Session establishment (to the MCX server, through IMS)

For LC applications, all of these features are performed by the FRMCS gateway. For the TC applications, all are performed by the applications, through the FRMCS gateway which routes the underlying messages to the IMS/MCX server.

In the following chapters, the implementation will be presented for the two coupling modes.

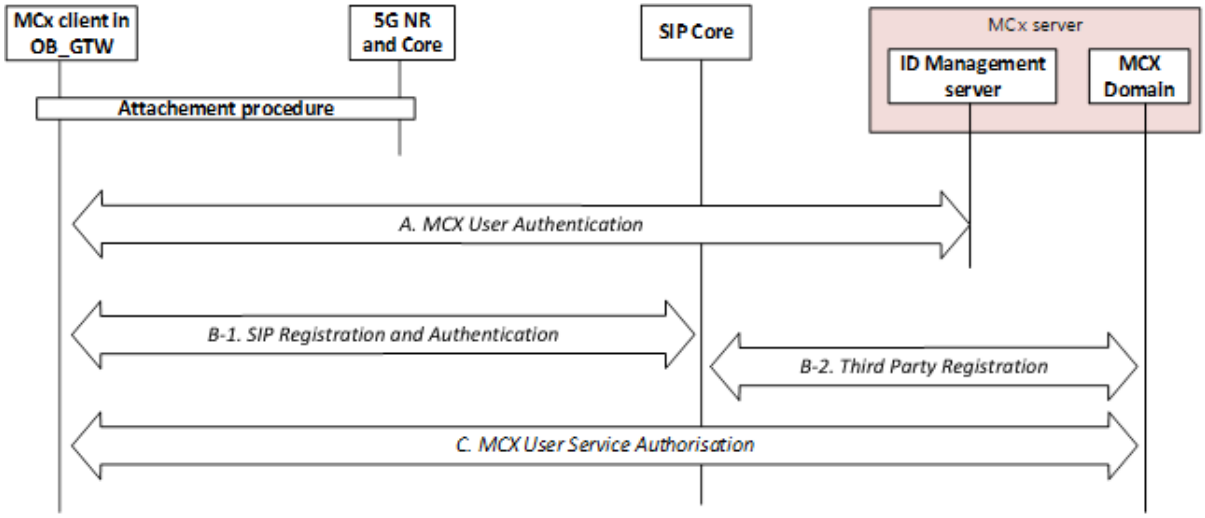


Figure 9: SIP registration, MCX authentication and MCX service authorization for LC application (ref. based on 3GPP 33.180 §5.1.1)

3.5.2 Loose-coupled applications

There is a one-to-one relationship between SIP identities (IMPI/IMPU) and MC ID used in 5GRAIL. The FRMCS gateway does not rely on any SIM/ISIM configuration related to SIP users.

3.5.2.1 SIP registration

SIP Registration is achieved using the REGISTER method in 5GRAIL. SIP Client will use its private identity, IMPI, when communicating with the IMS network. It will also do the registration for a specific public address, IMPU, which is the address that can later be used to contact it.

SIP registration is a 2 steps procedure:

- In the first step, SIP client sends a REGISTER message that is sent to P-CSCF. HSS provides authentication information to S-CSCF and a “401 Unauthorized” message is sent back to the client.
- Using challenge information contained in the “401 Unauthorized” message and its secret key, SIP client replies with a new REGISTER message that contains the result from computation. If this result matches the result stored in S-CSCF, Registration is accepted and S-CSCF will ask HSS for user profile download.

Consequently, it must be noted that following parameters are involved in the SIP registration:

- IMS Public address (IMPU),
- IMS Private address (IMPI),
- Secret key Ki.

When all of these must be obviously configured in the HSS, they also need to be stored on the client side. Usually, this information is available in the IMS SIM card (ISIM), for instance when there is a 5G user that has IMS credentials. In WP4, these credentials were hardcoded within On-Board and Trackside Gateways.

The used credentials are given in 3.2.1

No issue was raised related to the SIP registration.

3.5.2.2 MCX authentication (IdMS)

There is no specific feature related to MCX authentication, the process defined in TS33.180 was followed.

No issue raised on that topic.

3.5.2.3 MCX service authorization

The method used for MC service authorization is the one with SIP PUBLISH message defined in TS33.180.

Some issues were encountered with SIP header or MIME content (e.g., use of header for mcptt instead of MCData) but after alignments between MCX server provider and FRMCS gateways, these issues were solved.

3.5.2.4 MCX session establishment

MCX session establishment for LC applications is based on MCData-IPconn function defined in 3GPP rel. 16, TS 24.282, with some additional specific features when the 3GPP standards were not detailed enough.

Firstly, the GRE tunnel established at the end of the procedure is direct between both MCX clients (initiator and destination).

Secondly, the protocol used is GRE over IP, not GRE over UDP (GRE over IP was specified in 3GPP rel. 16, GRE over UDP is required since 3GPP rel. 17).

Then, it was necessary that client A (initiator) and client B (destination) agree on some items:

- DSCP value to be used at IP level for the GRE tunnel, in order to benefit from the correct QoS (see §3.8**)**
- GRE key value
- MCdata session ID

- **Optional**: binding between several MCdata sessions for multipath usage (with Alstom gateways only, where multipath is performed at service level and several MCdata sessions are established for the same applicative session)

Since the 3GPP specifications do not give any guidance on these points, each gateway provider uses its own way to exchange/negotiate these items. For example, new specific lines were added in the SDP part of the SIP INVITE transaction.

Conclusion on MCX session establishment:

Because of the lack of details in the 3GPP specifications of IPconn functions, which was not mature at the beginning of 5GRAIL, there were a lot of issues and alignment needed between gateway and server providers, but the interoperability between MCdata clients and MCdata servers was finally achieved (Alstom client with Kontron server, Kontron client with Kontron server, Kontron client with Nokia server).

This procedure will have to be reworked anyway because of the loss of backward compatibility between Rel.16 (used for 5GRAIL) and Rel.17 and further (to be used in FRMCS specifications) on IPconn function. For example, the use of GRE over UDP cancels the need to agree on a GRE key value.

3.5.3 Tight-coupled applications

The steps are identical for tight-coupled applications but initiated by the application instead of the FRMCS Gateway.

NOTE: The FRMCS V2 specifications will consider the other alternative defined in 3GPP on using SIP PUBLISH approach for registration.

3.6 Multi-talker control

The multi-talker control applies to designated MCPTT Groups and results in allowing several Participants talking simultaneously within the MCPTT Group. For example, multi-talker control is used by railway communication e.g., during shunting operation. The maximum number of simultaneous talkers is configured at the server level, according to 3GPP specifications. Authorized users can change the maximum number of simultaneous talkers at any time during a group call in the MCPTT Group configured for multi-talker control.

In case of number of MCPTT users requesting the permission to talk exceeds the maximum number of simultaneous talkers in the MCPTT Group, configured for multi-talker control, an override mechanism will be applied based on a priority hierarchy, depending on participant's type, urgent transmission types etc.

3.6.1 Feedback from multi-talker control functionality testing

The multi-talker test case was conducted in the WP3 test lab using a cab radio, a handheld device, and a controller terminal. The MCX Server was configured so that only two out of three users had permission to talk.

During test run 1, the handheld device did not have permission to talk. When the PTT button was pressed on the handheld device while the Cab Radio and the controller were holding their PTT buttons, there was no visual indication on the handheld screen that the request was sent or denied. A single sound was played (a beep), indicating a denial.

During test run 2, the same scenario was conducted, but this time the cab radio user had no permission to talk. When the PTT button was pressed on the Cab Radio, the message "Wait" was displayed first, followed by "Denied." The "Wait" message indicated that a successful message was sent to the MCX Server, and the "Denied" message was sent back to the Cab Radio from the MCS Server.

In the future, in cases where there are more call participants than allowed talkers, if the number of talkers exceeds the limit, the next call participant who requests the floor will be placed on a waiting list. When a talker releases the PTT button, the first waiting participant will be given the floor. However, the waiting list has not been implemented for the 5GRAIL project.

A CR, S1-232501, about waiting list mechanism (queuing) managing the request to transmit in the multi-talker control functionality, when the maximum number of simultaneous users is reached, was recently agreed in 3GPP stage 1.

3.7 REC implementation

The Railway Emergency Call (REC) for FRMCS V1 is an open topic, at system level, where the result of intensive evaluations was summarized by defining 4 potential options for further evaluation for V2. Based on that, the WP3 realization for 5GRAIL can be seen as “Pre-Standard”.

In the FRMCS-FIS specifications §8[22], the REC has been analysed and described as potential implementation options based on current or upcoming 3GPP MCX building blocks. One of the findings during this activity was to identify gaps of current 3GPP MCX standards.

In the scope of WP3 lab for 5GRAIL, we have implemented and tested the REC voice.

NOTE: Functional aliases are not considered in the REC establishment criterion.

The 4 potential options discussed for REC are (also refer to the Appendices §9.1 where some more details are described):

- Option 1: Client based approach using rule-based affiliation done by the client.
- Option 2: Server based approach. Server sends message to the clients based on rules that trigger the clients to perform an affiliation to the emergency group.
- Option 2A: Client Aware solution – continuous affiliation
- Option 2B: Client Aware solution – affiliation at setup

- Option 3: User regroup method: Server determines the clients, but a client to perform the active re-group.
- Option 4: Ad-hoc group method. Server based area definition and user determination (Target for 3GPP Rel-18)

It should be noted that the dynamic identification of the Area – based on the originator's location – and the further identification and affiliation of impacted clients according to their location, is a new concept in MCX standards which up to now were more focused on "controller-based Emergency Call use cases defined by the Public Safety / PPDR market, using a fixed list of participants.

For this reason, 5GRAIL considered to evaluate and test a server-based option (option 2A was selected). Note that today's discussions points rather to the realization of the (newly standardized) Option 4 (Ad Hoc Group) under standardization in 3GPP Rel. 18. However, the role and requirement on the server-based area calculation is comparable with Option 2, consequently valuable results could be derived from 5GRAIL test cases.

The main principles of this option 2A are the following:

- **Clients' configuration:** all clients initiate emergency-group calls to the currently selected group.

Below is the basic call flow used in WP3 lab implementation, except of the step 2a that was not applied and functional alias was not applied as a criterion. This call flow is also presented in the FIS-FRMCS specifications:

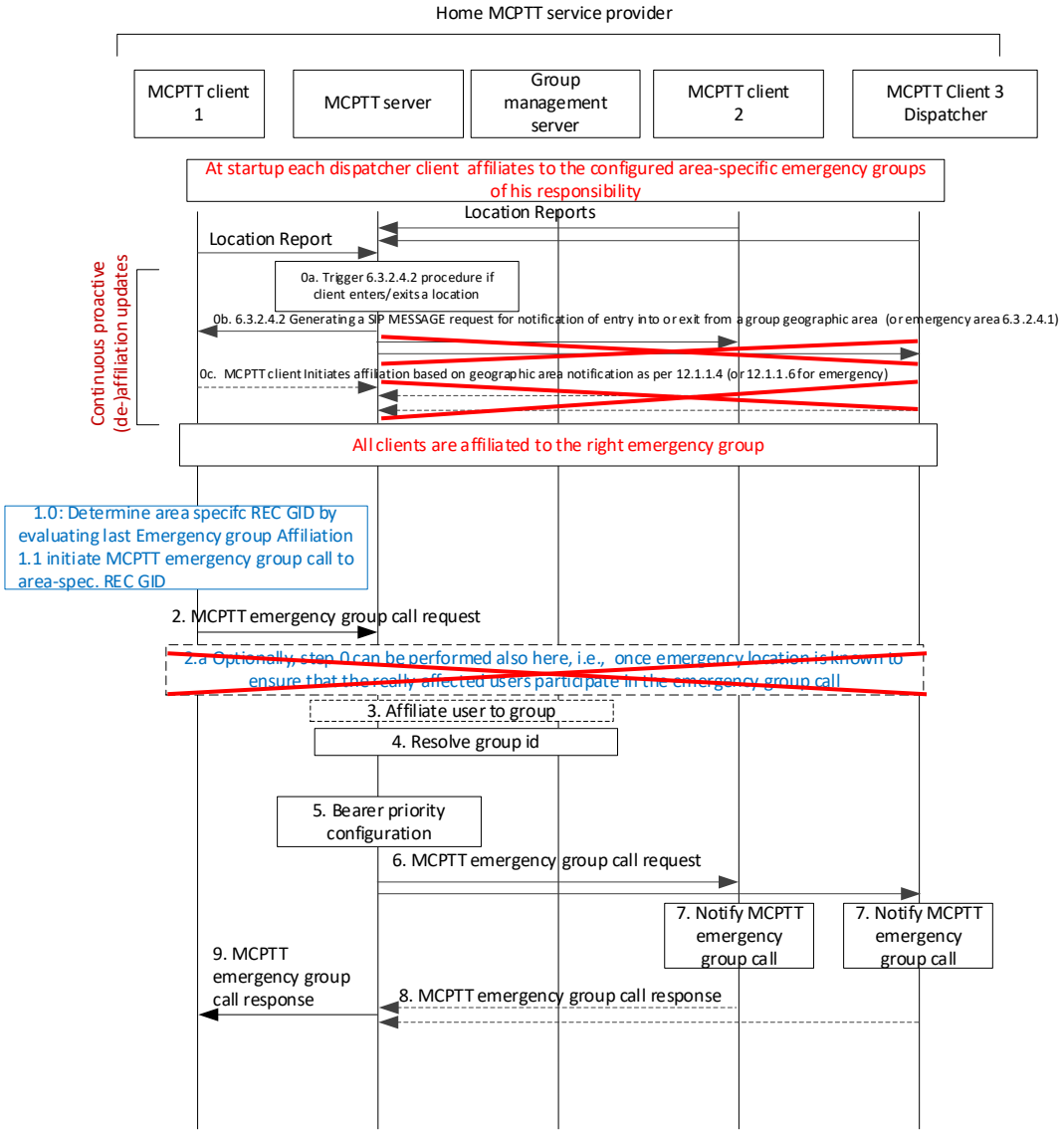


Figure 10:Basic call flow for REC option 2a

NOTE: The steps that are withdrawn in red are not implemented in the REC for 5GRAIL.

- **Prerequisites:**

Area specific predefined emergency group definitions are required.

Dispatchers are managed with static affiliation to the configured area specific emergency groups of his responsibility.

- **Description of the call flow:**

0. Continuous tracking of mobile clients based on location reporting.
   Server triggers mobile clients to perform continuously group affiliation/de-affiliation based on internal criteria (Functional Alias, location etc.)

1. Upon emergency initiated by user, the client automatically selects the last known emergency group (see affiliation step 0)
2. MCPTT emergency group call request

NOTE: Using client's 'mock journey GPS simulator' set to within the REC Area (based on the test REC area coordinates), the MCX Server is sending a SIP MESSAGE of Entering Geographic Area after every SIP MESSAGE from the client with such GPS coordinates (i.e., every 30 seconds). 3GPP TS 24.379 version 17.9.0 suggests it should send the message only on Entry into such an area, not repeatedly whilst in the same area. This currently has the knock-on effect of the client re-affiliating the group id. Whilst these do not affect the system behavior, it induces an additional network traffic. Regarding the latter, the client can be more discerning and not re-affiliate a group if it is already affiliated. This situation was accepted for 5GRAIL, but it has to be reconsidered for future REC implementation.

Based on the above call, two variants are tested in the WP3 lab:

3.7.1 REC initiated by the driver (cab radio)

The figure below presents the set-up of this test including one cab radio, one smartphone and one dispatcher:

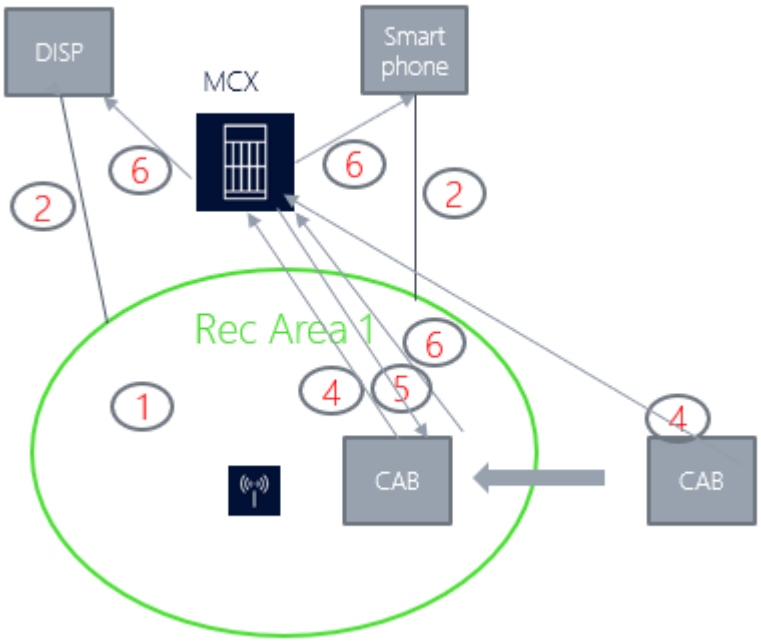


Figure 11:Driver initiated REC following FIS-FRMS specifications, option 2a

1. An Emergency Group is defined in the MCX Server related to Area 1 (polygon/rectangle)-> GPS Coordinates are used to define the Area 1.
2. Smartphone and Dispatcher are preconfigured for Group Area 1.
3. CAB radio using GPS Emulation for Area 1.

4. CAB radio sends continuous location report: firstly, outside the Area 1, after in the Area.
5. Dynamic group affiliation is performed for the CAB Radio when in Area 1.
6. CAB Radio initiates an MCX Emergency Call for Group Area 1: MCX Server also invites the Dispatcher and Smartphone.
7. Termination by the initiating driver or the dispatcher.

3.7.2 REC initiated by the dispatcher.

The figure below presents the set-up of this test including one cab radio, one smartphone and one dispatcher:

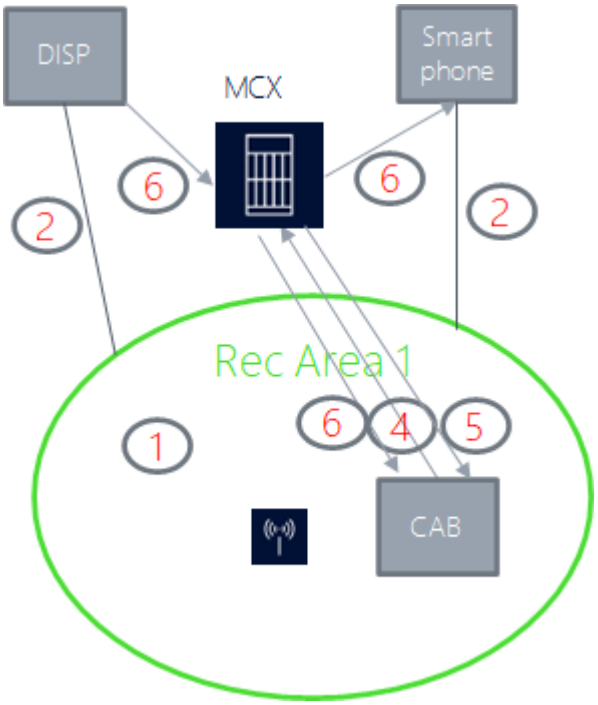
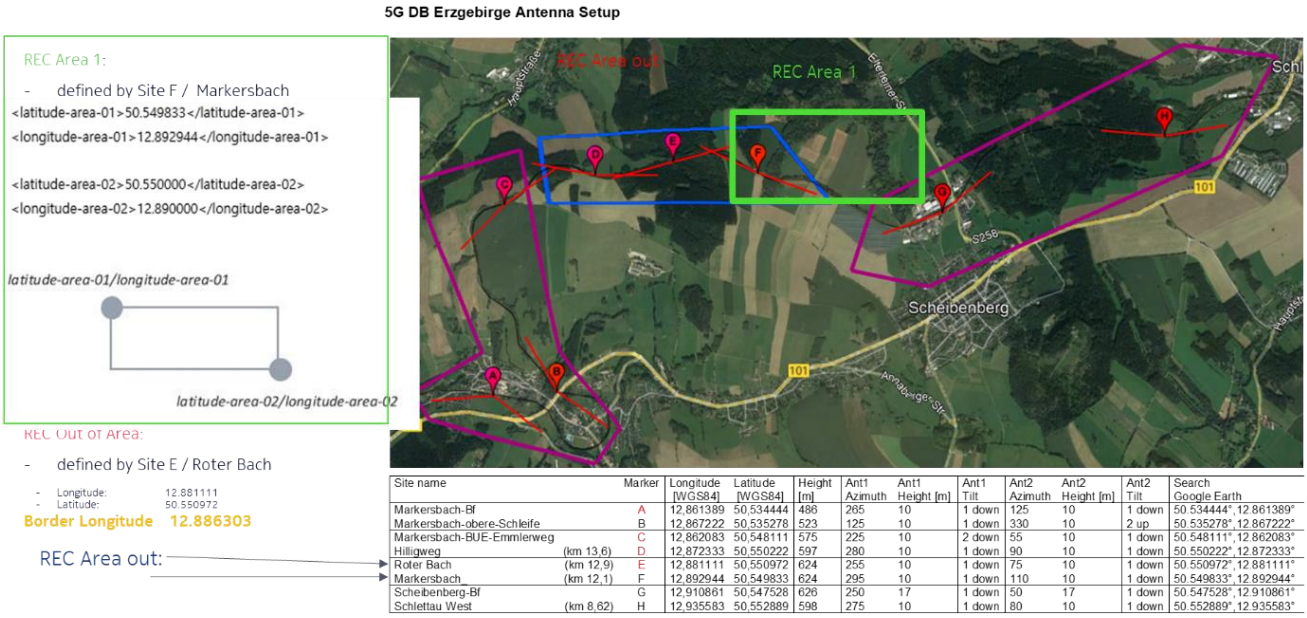


Figure 12:Controller initiated REC following FIS-FRMS specifications, option 2a

1. Emergency Group defined related to Area 1 (polygon)-> GPS Coordinates define the Area 1
2. Smartphone and Dispatcher are preconfigured for Group Area 1.
3. CAB radio using GPS emulation for Area 1
4. CAB radio sends location report in the Area 1
5. Dynamic group affiliation for CAB Radio
6. Dispatcher initiates an MCX Emergency Call for Group Area 1: MCX Server also invites the CAB radio and the Smartphone.

7. Termination by Dispatcher

Note that the GPS location in the lab has been emulated and for the field test cases in WP5 also emulated GPS coordinates have been used. The Area definition of the lab setup however is aligned with WP5 real coordinates. In 5GRAIL, the definition of an Area is done based on a Rectangle definition.



Site name		Marker	Longitude [WGS84]	Latitude [WGS84]	Height [m]	Ant1 Azimuth	Ant1 Height [m]	Ant1 Tilt	Ant2 Azimuth	Ant2 Height [m]	Ant2 Tilt	Search Google Earth
Markersbach-Bf		A	12,861389	50,534444	486	265	10	1 down	125	10	1 down	50.534444°,12.861389°
Markersbach-obere-Schleife		B	12,867222	50,535278	523	125	10	1 down	330	10	2 up	50.535278°,12.867222°
Markersbach-BUE-Emmlerweg		C	12,862083	50,548111	575	225	10	2 down	55	10	1 down	50.548111°,12.862083°
Hilligweg	(km 13,6)	D	12,872333	50,550222	597	280	10	1 down	90	10	1 down	50.550222°,12.872333°
Roter Bach	(km 12,9)	E	12,881111	50,550972	624	255	10	1 down	75	10	1 down	50.550972°,12.881111°
Markersbach_	(km 12,1)	F	12,892944	50,549833	624	295	10	1 down	110	10	1 down	50.549833°,12.892944°
Scheibenberg-Bf		G	12,910861	50,547528	626	250	17	1 down	50	17	1 down	50.547528°,12.910861°
Schlettau West	(km 8,62)	H	12,935583	50,552889	598	275	10	1 down	80	10	1 down	50.552889°,12.935583°

Figure 13: REC Area definition in WP5-DE

The test cases for late join / leave have been defined as optional and not been implemented following the dynamic calculation method of the server. However, the existing MCX functionality of Late Join (based on preconfigured groups) have been used to verify the test case for GSM-R Interworking and transition (see chapter §3.12).

3.8 Quality of Service (QoS) and Priority

3.8.1 Reminder

Railway applications exhibit different requirements, e.g., in terms of latency or reliability. Moreover, the FRMCS System offers bearer services with different characteristics. The main purpose of the Quality of Service (QoS) is to allocate a relevant bearer to a specific applicative session, compliant with the application requirement.

The most important QoS parameters that determine the quality of the transport system are **latency** of the user data and **reliability** of the communication. In addition, guaranteed bandwidth assures the continuation of critical communication.

QoS and Priority classification includes:

- A QoS characteristics (latency, reliability, throughput, setup time) expected from the FRMCS System in order to fulfil the required level of communication quality.
- A priority level, the priority in which the communication is handled by the FRMCS System

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 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 following figure reminds where the QoS is handled inside the FRMCS system, using the 5G QoS called 5QI, e.g., in the modem or in the transport side:

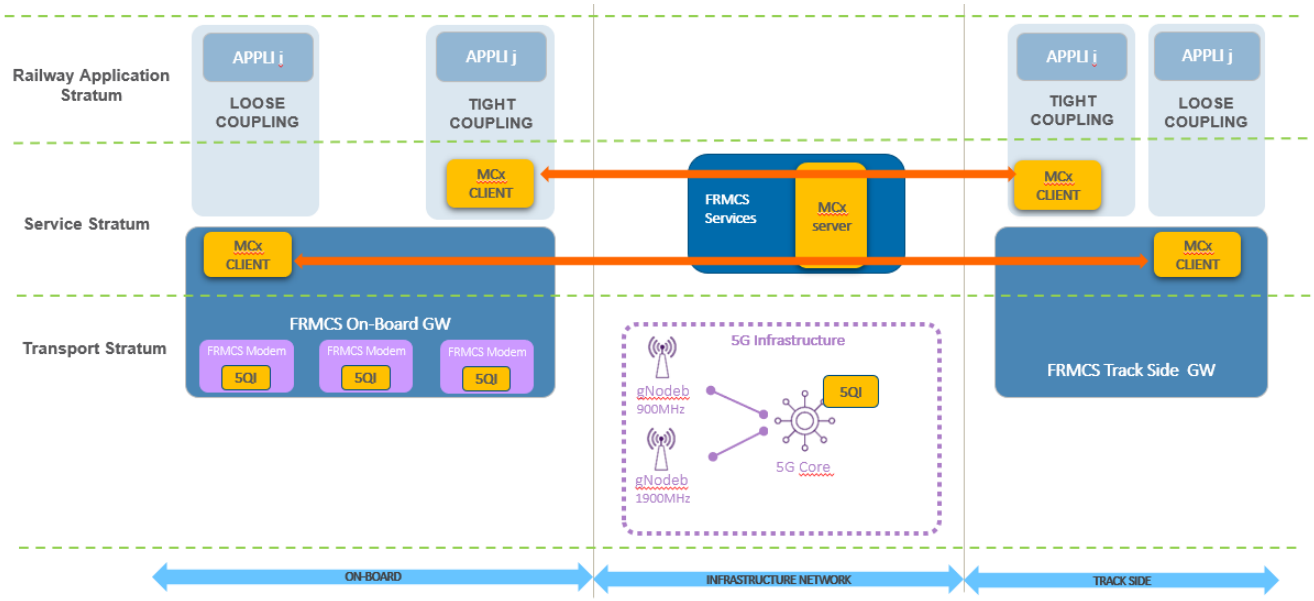


Figure 14: QoS function (Ref. D2.1)

- The FRMCS modem, provided by Thales and designed by Qualcomm, supports 5QIs from 1 to 9. Also, to mention that the used UE supports only Network initiated QoS, not UE initiated QoS.
- During the session start API request, an LC application asks for a “comm_profile”, and a specific QoS treatment is applied by the infrastructure for each comm_profile. The application is not aware of the used 5QI, due to the decoupling between application and transport. It is up to the OB_GTW to know the mapping between comm_profile and corresponding 5QI.
- In 5GRAIL implementation, no dynamic QoS (e.g., QoS requested by the MCX server for a specific session during its establishment) can be applied due to absence of PCF in both labs interacting with the MCX server to trigger dedicated QoS for a session. QoS is however statically managed by the core network, and the differentiation of QoS flows will be managed at the network level thanks to the DSCP value. 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.

For both labs, the mapping of comm_profile/DSCP values to the QoS parameters (5QI, ARP, etc.) depends on the network infrastructure.

Then, the DSCP value has two functions:

- Differentiate the UP flow in order to allow to the network/UE to use the relevant bearer. It is a relevant choice for LC application, because MCData-IPconn sessions relies on a GRE tunnel, which is not over TCP or UDP (then, no TCP/UDP ports can be used to identify the flow).
- Separate QoS parameters from application and transport point of view: the OB_GTW performs a mapping between a comm_profile (requested by the application with OBapp/TSapp API) and a DSCP value to be used to carry UP data; and the network performs a mapping between a DSCP value and a QoS rule (including 5QI for a 5GC).

- **NOTE:** In rel. 17, the 3GPP standard related to MCData-IPconn has recently changed and require using GRE-in-udp tunnel such defined in RFC8086, instead of GRE over IP. Thus, it becomes possible to use UDP port to differentiate the flow. But it does not allow the client (requesting an IPconn session) to reflect a QoS need, contrary to DSCP value (with a mapping table between DSCP value and comm_profile as described in 5GRAIL). There is no equivalent in FRMCS v1 specification today.

3.8.2 QoS handling in the scope of WP3.

As already described in D3-2 the QoS mechanisms used in the 5G core and radio access is configured for the different QoS classes with the help of filtering functionalities in the core network. This is required as for the time of 5GRAIL test activities, a PCF which is normally used to achieve Application specific end to end QoS setting in core and radio, was not available.

As agreed in WP1 the filtering for the different QoS classes is done by the DSCP marking received from the application settings. For TCMS, ETCS and Video different 5QI QoS classes were set based on the DSCP setting.

As 3GPP 23.501 §8 [11] states: The SMF may change the subscribed values for the default 5QI and the ARP and if received, the 5QI Priority Level, based on interaction with the PCF as described in TS 23.503 §8 [35] or, if dynamic PCC is not deployed, based on local configuration, to set QoS parameters for the QoS Flow associated with the default QoS rule.

This local configuration is realized using 3GPP ADC (Application Detection and Control) functionality in Nokia Core / SMF Traffic Steering function. This allows various options for detecting and assigning QoS flows based on filtering.

Some configuration option for differentiation can trigger based and may be included in the policy-rule-unit including direction (uplink, downlink, or both) and match criteria for:

- IP and local-port (list or range)
- IP and remote-port (list or range)
- tos-tc dscp (Type of Service/Traffic Class (ToS/TC) DSCP). Specifies the DSCP code point value.

Applications	OB_GTW		Infrastructure static configuration	Extract from TS23.501, Table 5.7.4-1		
comm_profile transmitted by the	DSCP value (bit)	DSCP value (decimal)	QoS parameters used for WP3	Packet Delay	Packet error rate	Comments
1- Voice (*)	101.101	43	5QI: 2, **ARP 7**, GBR	150ms	10^{-3}	Used for Conversational Video (Live Streaming) ?
2- Operational Voice	101.010	42	Not used			
3- Emergency voice (*)	101.001	41	5QI: 2, **ARP 1**, GBR	150ms	10^{-3}	Used for Conversational Video (Live Streaming) ?
4- Video	100.001	33	5QI : 7, non-GBR	100ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
5- Low latency Video	100.000	32	Not used			
6- Non harmonized Data (TCMS)	1.000	8	5QI:9, non-GBR	300ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) ?
7- Operational Data	10.011	19	Not used			
8- Emergency Data	10.111	23	Not used			
9- Low latency Data	10.110	22	Not used			
10 - ETCS	10.101	21	5QI 5, non-GBR	100ms	10^{-6}	Used for IMS signalling?

Table 3: QoS settings in WP3

However, a different filter had to be configured for the voice tests, as the CAB radio could not set a different ToS/DSCP value for the different test cases. Instead, a workaround has been realized by filtering for the IP address of the CAB radio to trigger the 5QI. This results in the setting of a GBR /Guaranteed Bit Rate setting for the voice bearer, but also for the signalling bearer (which is normally not required, and not impacting the test results.

For 5GRAIL, the Guaranteed Bitrate Class (GBR) for voice was set to 5QI-2 (Note. 5QI-1 requires additional signaling between a VoNR capable UE which is not supported by the 5GRAIL Modem.

For the measurement of voice related performance the KPI 1&2 have been used:

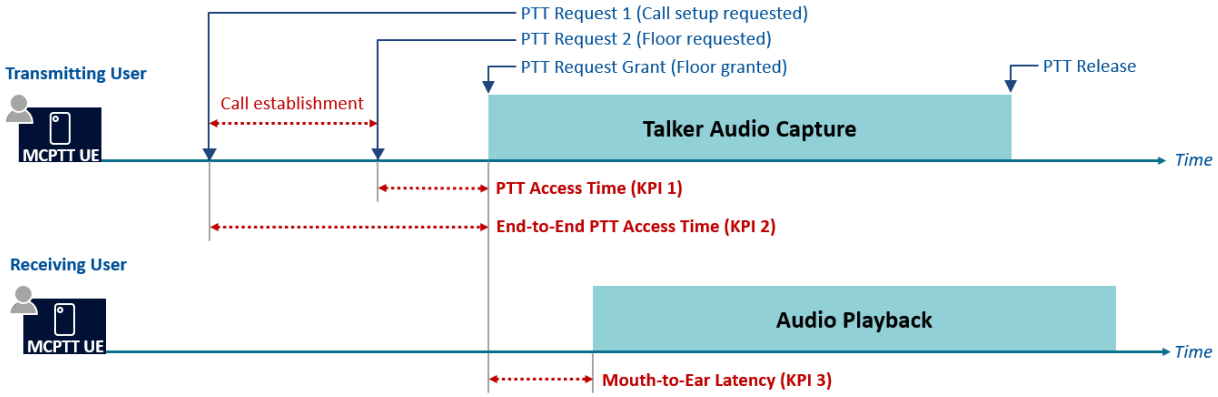


Figure 15: MCPTT KPIs for voice

KPI 1 and 2 are derived from SIP signalling messages captured on the devices and on a Wireshark monitoring PC.

Mouth-to-ear latency (KPI 3) will not be measured in detail but will be qualified and assessed by the person performing the test.

3.8.3 QoS demonstration with critical test cases versus non-critical ones in the scope of WP3

MCPTT KPI 1 and KPI 2 measurements, as defined in 3GPP TS 22.179 and recalled in D1.1 §16.5 were used for voice testing.

KPI 2 Measurements:

A limited number (~6) of measurements have been done for voice related tests giving a first indication on the end-to-end KPIs.

The measurement setup is shown in the following figure:

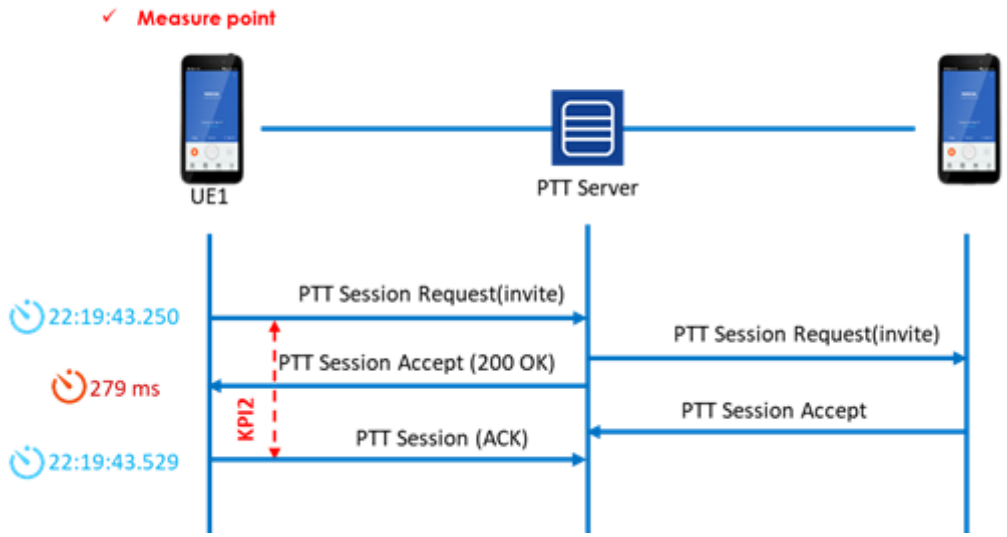


Figure 16 KPI2 Measurement Setup for Voice

3.8.3.1 Measurement of PTP / Private Calls:

Observations:

- Both directions fulfil the requirement of 3GPP TS 22.179 (1000 ms target)
- Direction from CAB Radio to Dispatcher shows values around 260 ms
- Direction from Dispatcher to CAB Radio shows values around 500 ms.

The following figure provides a performance view of the point-to-point call, referring to MCPTT KPI2, which was completely fulfilled in both directions from cab radio to dispatcher and vice-versa. However, higher values are observed in the dispatcher to cab radio direction due to the additional processing time at the receiving CAB radio.

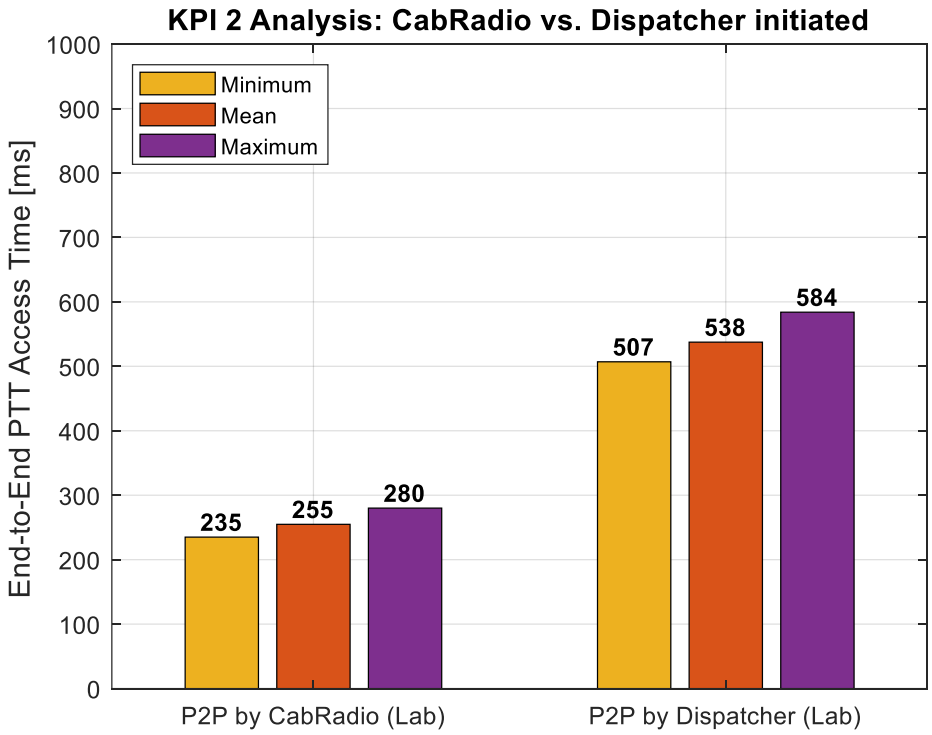


Figure 17 Comparison of MCPTT KPI2 values for point-to-point calls (Ref. D3.3v2)

3.8.3.2 MCPTT private point-to-point voice call (driver to controller) in parallel with MCData application (video) in normal and in degraded radio conditions.

The purpose of the tests is to demonstrate system behavior using simultaneously two applications requesting different MCX services, such as MCPTT service for voice application and MCData service for the data (video) application. The expected outcome of this test case is that in nominal radio conditions, each application keeps the standalone performances, and – important for railways – that the TOBA is capable to carry multiple applications, even of different MC services (e.g., MCPTT and MCData), over same device and interface, which is not the case for GSM-R.

The above combined scenario will be performed in WP3 lab, using an MCData application Video and TOBA-K, as FRMCS On-board gateway, on n78 band.

Initial state/configuration of both applications shall be applied before launching the combined scenario. The QoS (DSCP) configuration of each application is impacting the results of the combined scenarios, mainly in the degraded conditions. 5G QoS value for Video was set to 5QI=7, non-GBR and for voice 5QI=2, GBR, according to Table 3: QoS settings.

Note: As the cab radio does not support DSCP marking, the voice QoS (5QI) was set with a workaround using IP filtering rules instead of DSCP filtering.

Observation:

> The video view and object move within the view was smooth, no major jerks or picture blinking, trackside VMS indicated around 20-25 fps on the display overlay. This means the quality of the video was nearly perfect.
>
> The voice quality was clear and loud.

The interest of this combined scenario, MCPTT voice (configured as GBR) and MCData application (video) (configured as non-GBR), is in degraded conditions, using Vertex emulator. In such conditions the QoS, prioritization and radio resource management of voice application, as the most critical one, will be revealed, thanks to the QoS (DSCP) configuration of both applications.

5G QoS value for Video was set to 5QI=7, non-GBR and for voice 5QI=2, GBR, according Table 3

Simulation was done with two different train speeds: 50 km/h and 175 km/h. In both scenarios a propagation model with the most challenging condition, namely with double doppler effect was applied.

Couple of inter-gNodeB handovers were executed during the simulation, where also the so-called intra-frequency Xn handover was triggered (as per§8 [37] chapter 3.2.1)

Observations:

At simulated train speed of 50 km/h, the perceived video quality was acceptable. During handovers no degradation in video quality was observed. Sometimes the framerate was dropped, assumably due to temporary bandwidth degradations. The voice quality was clear and loud.

At simulated train speed of 175 km/h there was slight degradation of the perceived quality, but still acceptable. Framerate of the video stream was dropping frequently from 25 fps to 15 fps and above. Also, the bitrate was dropping from 1000 kbps to 600 kbps and above. During handovers buffering occurred, as framerate and as well as bitrate exceeded above 25 fps and 1000 kbps after the handover in order to send buffered data.

The voice was not affected much, however. The voice quality was clear and loud.

3.8.4 QoS demonstration with critical test cases versus non-critical ones in the scope of WP4

During WP4 execution, several test cases related to QoS and Priority function were performed:

- ATO session in parallel with a disturbing flow
- ATO and ETCS sessions in parallel.
- ETCS session in parallel with a disturbing flow
- ETCS session in parallel with Remote Vision
- Several kinds of PIS sessions (text message with normal priority, text message with high priority, log download) in parallel with a disturbing flow

iPerf tool was the flow generator used to create the disturbing traffic, using two dedicated devices (on-board and trackside). The iPerf flow is still using the comm_profile corresponding to the lowest priority (comm_profile 6, translated into DSCP value 8)

The table below gives the comm_profile used by each applicative session, the corresponding DSCP value applied by the FRMCS GTW, and the corresponding 5QI applied by the network for this DSCP value:

Type of session	comm_profile (API request)	DSCP value (GRE tunnel)	5QI applied by the network
ATO	11	20	2
ETCS	10	21	3
PIS: text message with normal priority	7	19	6
PIS: text message with high priority	8	23	5
PIS: log download	6	8	8
Disturbing flow (iPerf)	6	N/A	6

Table 4: QoS settings in WP4

Conclusion on QoS test cases in WP4

ETCS applicative session does not suffer from any disturbance in these test cases, no impact has been observed on the applicative logs compared with the nominal case.

For ATO applicative session, we observe an impact regarding the download of Segment profile, which is configured to be a voluminous download. The time to download it was increased when there is a disturbing flow in parallel, especially with downlink disturbing flow (27s in the nominal case without disturbing flow, 468s with the DL disturbing flow).

The difference of behavior between ETCS and ATO is linked to the fact that ETCS requires a very low bandwidth whereas ATO requires a high bandwidth for the Journey and Segment Profile (and then a low bandwidth when the download is over). **The 5QI used were not with guaranteed bitrate.**

Other QoS test cases were performed with PIS application:

- Text message with normal priority (comm_profile 7) in parallel with a disturbing flow (comm_profile 6, less prioritized) - KPI = time to receive the message
- Text message with high priority (comm_profile 8) in parallel with a disturbing flow (comm_profile 6, less prioritized) – KPI = time to receive the message
- Long download (comm_profile 7) in parallel with a disturbing flow (comm_profile 6, less prioritized) – no KPI measured on that test case.

For test cases 1 and 2, we observe a slight impact compared with the measurement without any disturbing flow (approximately 6,9s to receive the message instead of 5s), nevertheless the time to receive the message is still correct and compliant with the PIS requirement. There is no difference between the test cases 1 and 2, because in both cases the text message is on a more prioritized bearer than disturbing flow.

Another important feedback is that the internal QoS management of the OB_GTW/TS_GTW is also important. Initially, we were focused on the QoS in the radio layers only, but if the disturbing flow is coming from the train (this was the case in these WP4 test cases), the bottleneck can be the OB_GTW itself more than the radio link. Then, it should be required that the FRMCS Gateways has also a need (based on DSCP value too) in order to manage priority of flows before sending them to the modem.

3.8.4.1 RTT as a KPI representing the network impact to the ETCS application

A quick reminder of RTT:

Round Trip Delay Time (RTT): is the time between sending a message from a source to a destination (start) and receiving the acknowledgment from the destination at the source point (end). RTT is a specific metric to calculate the latency of the network. For example, the EVC will timestamp packets, and those packets will be sent to the RBC and the RBC will rebound them to the EVC. The time between packet sent and packet acknowledgement will be the RTT monitored.

The following diagrams show the evolution of RTT of ETCS in case of combined applications scenario with ETCS and remote vision application in nominal and degraded conditions to compare the results:

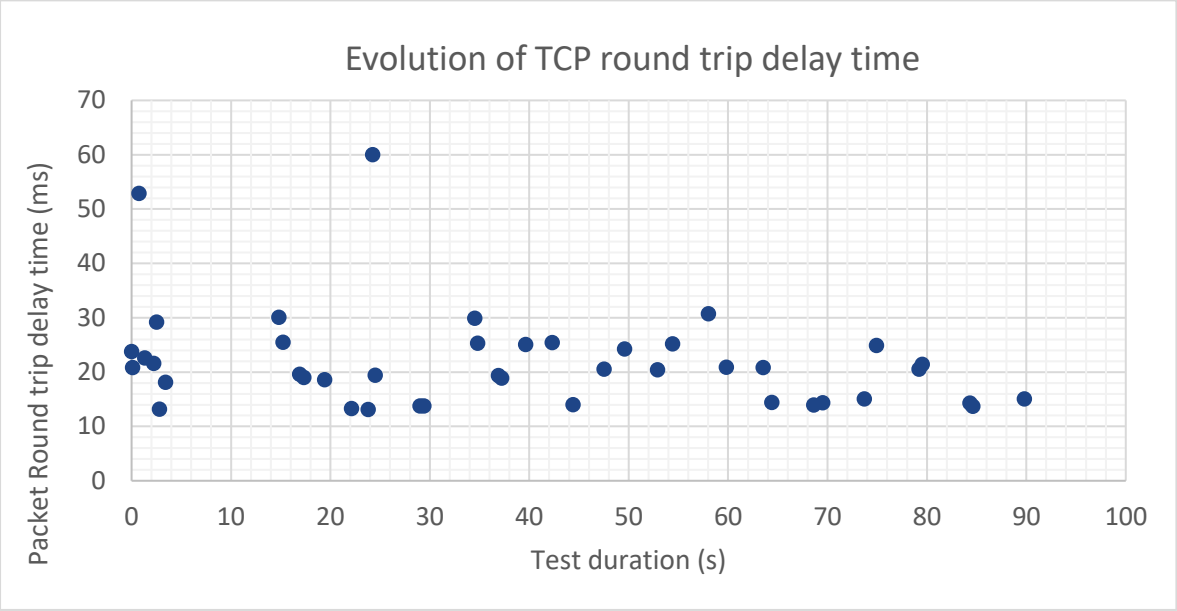


Figure 18 Round Trip Delay time observed with ETCS application in parallel with remote vision application. (Ref. D4.3v2)

These values are:

Average Round Trip Time = 12.82ms

Standard deviation Round Trip Time = 9.31ms

The value is calculated with 43 samples.

As expected, an increase of the TCP round trip delay time in degraded conditions is observed for ETCS without impact on the behaviour of the application:

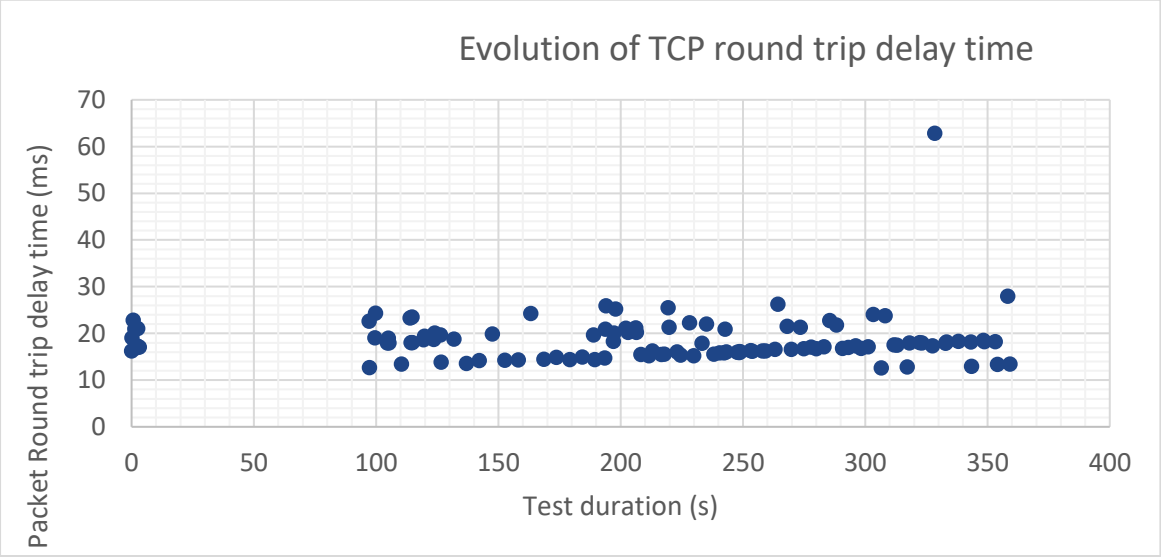


Figure 19 Round Trip Delay time observed with ETCS application in parallel with remote vision application, in degraded radio conditions. (Ref. D4.3v2)

The values observed are:

Average Round Trip Time = 18.51ms

Standard deviation Round Trip Time = 5.29ms

The value is calculated with 113 samples.

3.8.4.2 RTT as a KPI representing the network impact to the ATO application in parallel with a disturbing flow

In addition to the journey profile and segment profile which are the main inputs of the ATO functioning, the status report is also periodically exchanged between the On-board and trackside entities. The Packet Round Trip delay time is a KPI evaluating the impact on QoS of ATO application in presence of a disturbing flow.

The following graph shows the RTT values obtained for this test with uplink or downlink iPerf disturbing flows:

- Uplink iPerf disturbing flow:

The measured values are:

- Status report RTD Mean: 63.42 ms
- Status report RTD Standard deviation: 14.81ms

There was no impact observed in the ATO application's functioning with comparison to the nominal conditions:

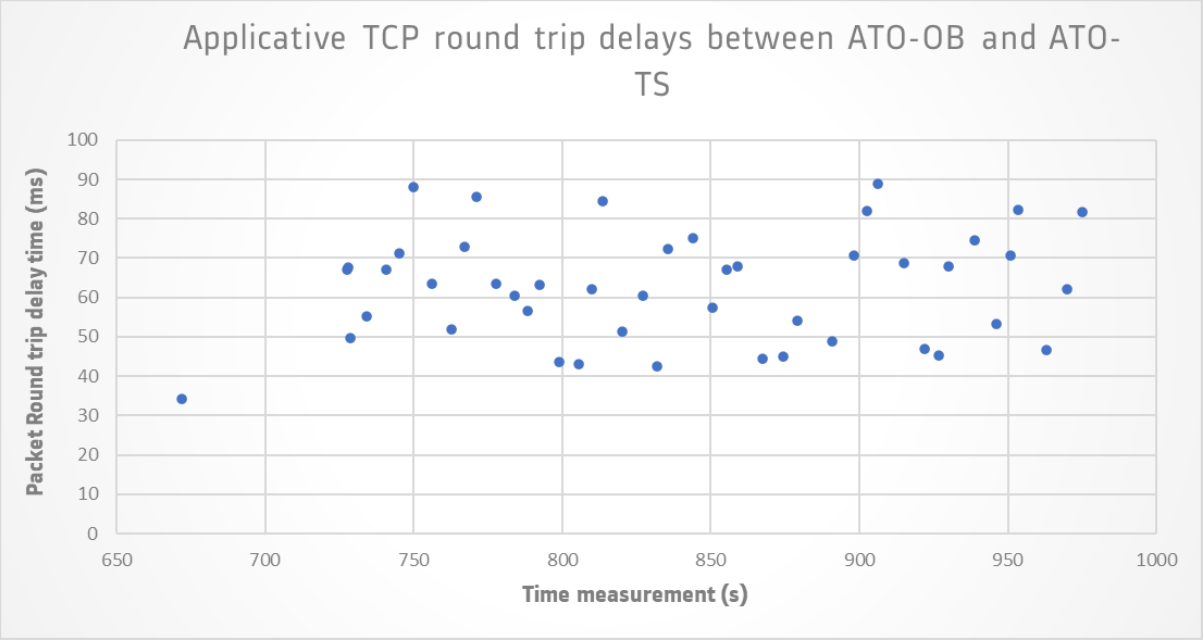


Figure 20 Packet Round Trip Delay time of ATO status report in parallel with highly disturbing uplink iPerf traffic. (Ref. D4.3v2)

- Downlink iPerf disturbing flow:

The measures values are:

- Status report RTD Mean: 67.26 ms.
- Status report RTD Standard deviation: 18.06ms

As previously, the KPI observed is the Packet Round Trip Time delay of the status report periodically exchanged between the On-board and trackside entities, in case of downlink iPerf disturbing traffic.

The measured values of that scenario are presenting in the following graph:

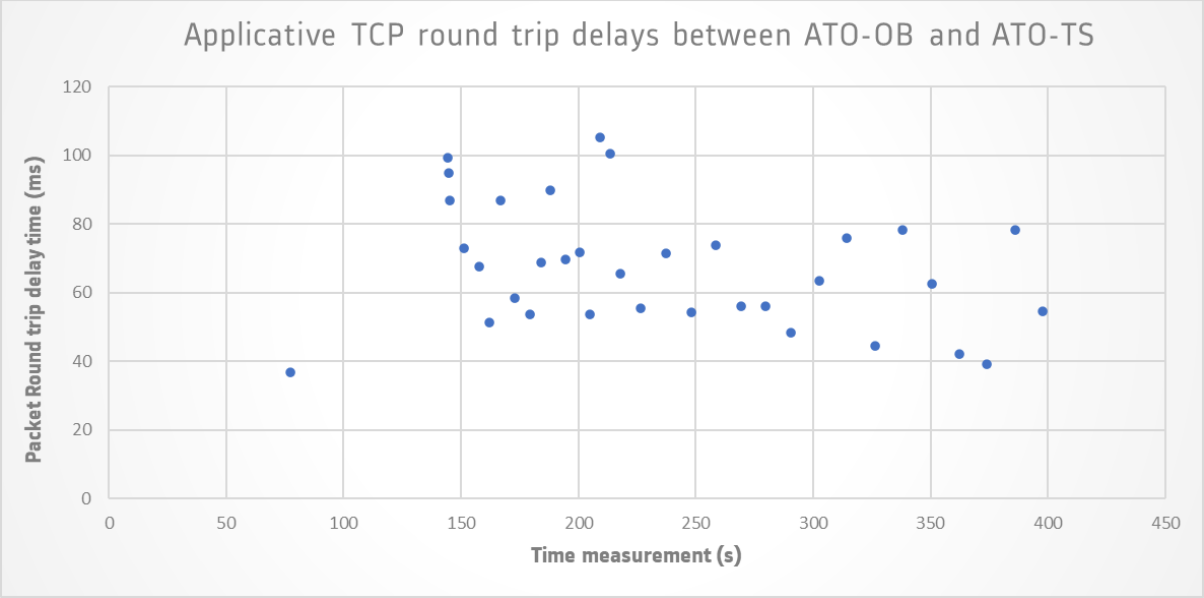


Figure 21 Packet Round Trip Delay time of ATO status report in parallel with highly disturbing downlink iPerf traffic. (Ref. D4.3v2)

In that case, a low impact was observed in comparison with the nominal conditions.

3.9 Bearer flex

3.9.1 Context

The bearer flexibility feature enhances the independency between the applications and the transport technologies. Bearer flexibility encompasses FRMCS Multi Access (same UE) and/or FRMCS Multipath (multiple UEs).

Bearer flexibility intends to improve service availability and performance.

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

For 5GRAIL execution, 4G modems are used in addition to exiting 5G modems to demonstrate bearer flexibility function. In addition, for these modems (4G), QoS will not be managed.

The choice of the 4G solution was taken due to issues on using 5G n8 frequencies in French field tests.

It is to be noted that the trackside gateway is mandatory to implement bearer flexibility for this as this is an end-to-end feature requirement. The Track Side Gateway is not yet specified in FRMCS specifications.

Bearer flex implementation for 5GRAIL is vendor dependent, it is not yet decided if these implementations will be the standardized option.

Two different approaches have been used:

Kontron's multi-connectivity based on Multipath TCP (MPTCP) for the transport layer, as presented in the following figure:

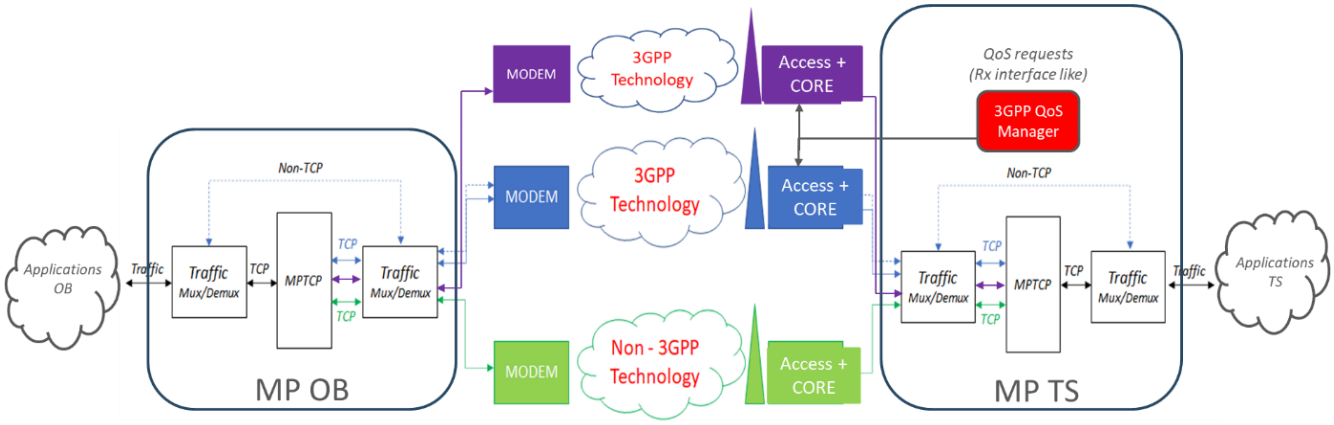


Figure 22: Kontron Multi-connectivity based on MPTCP (Ref. D2.1).

Alstom's approach is described below:

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

Bearer flex functions. So, the implementation is performed in the service layer. This is applicable in the User plane. For the MCX Signaling Plane, the multi-connectivity will depend on the capabilities of the MCX server to expose different databases for each radio network.

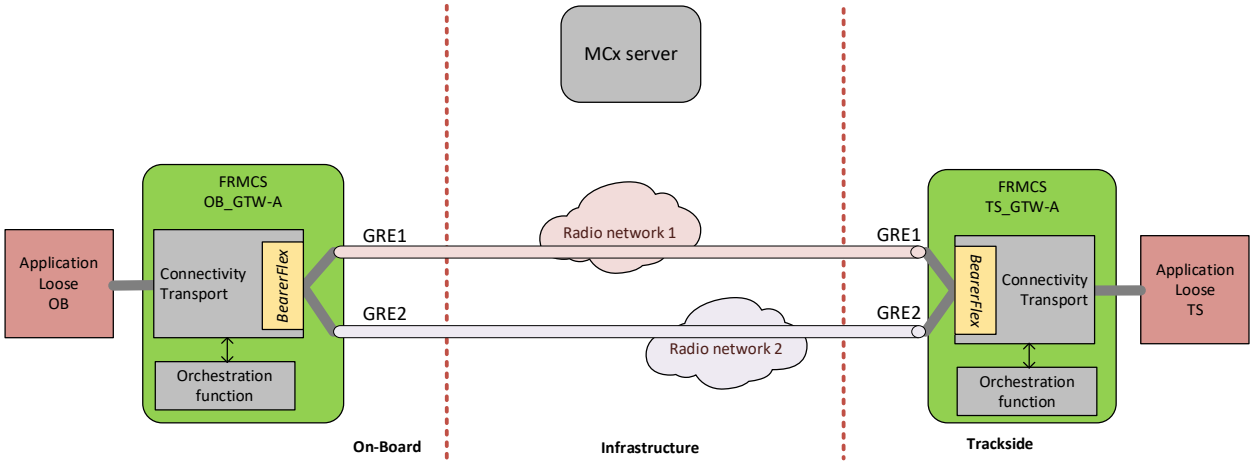


Figure 23: Alstom multi-connectivity - User Plane (Ref. D2.1)

We can distinguish the two kinds of solutions as follow:

- Kontron's approach is a multi-connectivity at transport level (only one MCData session, one GRE tunnel for MCData-ipconn session)
- Alstom's approach is a multi-connectivity at service level: two or more MCData-ipconn sessions, and the FRMCS GTW manages the use of these sessions for the applicative flow.

3.9.2 Bearer flex observations from WP4 loose coupled applications

Bearer flex testing used two different implementations of this feature, that were tested with the two gateways, TOBA-A and TOBA-K. The interest of having both FRMCS Gateways flavour is because of some features being available on TOBA-A but not on TOBA-K and vice-versa.

3.9.2.1 Tests performed with TOBA-A

- ATO Failover 5G to 4G and 4G to 5G with TOBA-A in n8 band (5G) and b38 band (4G)

There were 5G and 4G modem embedded in TOBA-A for this test. It is worth mentioning that the ATO application is configured to use 5G modem as primary link and 4G modem as secondary link. Consequently, 5G link is to be used as soon as it is available. Two MCdata-IPconn sessions are established (one per link) and TOBA-A/TS_GTW-A select the one to be used based on the signal strength and the configured priority.

The failure of the 5G link was simulated by disconnecting the radio wire (optical fiber between RRH and BBU). The switch from 5G link to 4G link was fully transparent for the application.

The test was successful with local binding and end-to-end communication established, independently of the bearer used.

- ETCS call continuation with OB-GW going from 4G to 5G coverage or from 5G to 4G coverage with TOBA-A in n8 band (5G) and b38 band (4G).

TOBA-A used one 5G modem and one 4G modem for this test, as well. The application profile used for ETCS application is also configured to use 5G modem as primary link and 4G modem as secondary link. Then, the 5G link is to be used as soon as it is available.
Two MCdata-IPconn sessions are established (one per link) and TOBA-A/TS_GTW-A select the one to be used based on the signal strength and according to the configured priority. To simulate the prioritization of one link over the other, in case 5G cell is switched on, 4G cell is progressively attenuated and vice-versa.

The test was successful without any impact on the ETCS application, even though there was a bearer changeover.

The following diagrams are showing the evolution of the RTT for ETCS application when going from 4G to 5G coverage and vice-versa. The average values of RTT delay are relatively stable whatever the bearer:

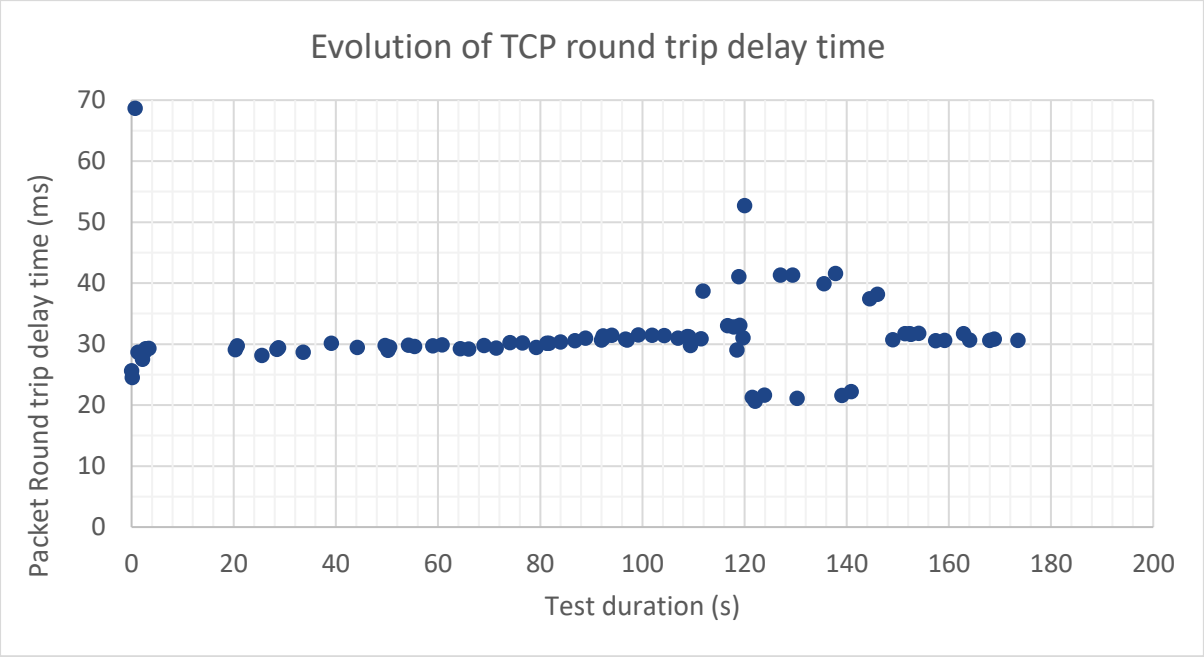


Figure 24: RTT delay of ETCS application when moving from 4G to 5G coverage, using bearer flex feature with TOBA-A (Ref.D4.3v2)

Average Round Trip Time = 31.23ms

Standard deviation Round Trip Time = 6.4ms

The value calculated on 81 samples.

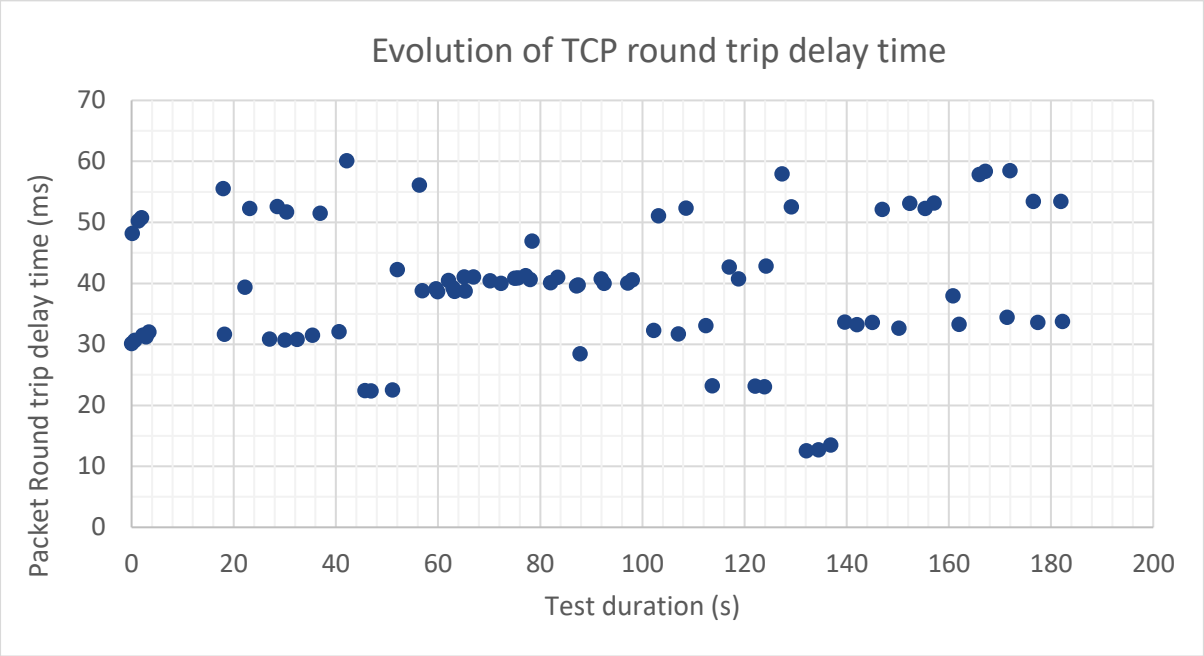


Figure 25: RTT delay of ETCS application when moving from 5G to 4G coverage, using bearer flex feature with TOBA-A (Ref.D4.3v2)

3.9.2.2 Tests performed with TOBA-K

- Aggregation use case: TOBA-K under overlapping 4G (b38 band) and 5G (n39 band) coverage is performing ETCS call using simultaneously both bearers. It moves under 4G only coverage and on-going call continues.

The network is configured to allow ETCS communication data to use both bearers simultaneously. To simulate the changeover from overlapping 5G and 4G coverage, to 4G only coverage, an attenuation of the 5G signal is progressively performed.

No impact was observed in the ETCS application.

3.9.2.3 Conclusion on multi-connectivity at service level tested in 5GRAIL:

- Works well for applicative TCP sessions. Switching between bearers was transparent at the application level.
- Several criteria possible to decide the link policy: Primary/backup policy (static policy configuration, i.e., one primary link used if available, the other link is back-up link), best link policy (i.e., several links have the same priority level and a quality measurement allow to decide the link to be used). A redundant mode (i.e., applicative data duplicated and sent on both links) have not been tested.

- Nevertheless, it implies more MCX clients (one per link) to be configured in the GTW and the MCX server, because the MCX server (at least the one used for 5GRAIL) does not support more than one IPconn session between the same couple of clients.
- The QoS can be managed independently on every links.

3.9.3 Bearer flex implementation and observations from WP3 loose coupled applications

According to UIC FRMCS specification FRMCS should provide two mechanisms to achieve Bearer Flexibility (refer to §8 [4] chapter 12.3.1): FRMCS Multi Access and FRMCS Multipath

Where FRMCS Multipath enables the (sequential or simultaneous) use of multiple UEs on the same or different transport domains, the FRMCS Multi Access enables the (sequential or simultaneous) use of multiple radio access technologies on a single UE and a single (FRMCS) Transport Domain.

For 5GRAIL, WP3 addresses the concept of FRMCS Multi Access (in contrast to WP4 focussing on Multipath approach). The use case is to utilize a second “access” with higher bandwidth to demonstrate a video archive upload from a train reaching the station (see chapter D1.1 §9.5.2)

Multi access capabilities by the 5G SA transport domain standardized in 3GPP defines the functionality required to serve different access using the ATSSS (Access Traffic Steering, Switching & Splitting). It is important to understand that in current 3GPP Rel. 17/18 the solution is limited to serve a 3GPP and a non 3GPP (e.g., Wi-Fi) access, but activities have been started for 3GPP Rel. 19 to evaluate enhancements of the ATSSS model to serve (at least) two different 3GPP access types as well. Appendix §9.2 we explain in more detail the concepts of ATSSS.

However, the support of multi access by the UE and infrastructure during 5RAIL does not allow to demonstrate ATSSS, instead a solution based on two subbands on the N78 bands was selected to demonstrate the behaviour of relying on an (high performant) second Uplink for the test case CCTV_TC_002 “CCTV offload from train to trackside with bearer-flex”. The following figure depicts the schematic setup:

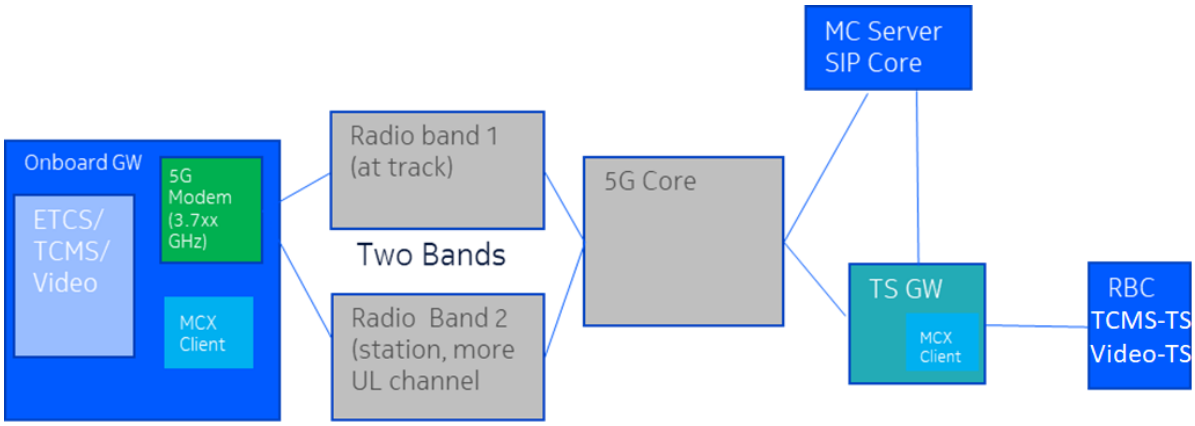


Figure 26 Schematic overview on Bearer Flexibility

Higher throughput of the second sub band was achieved by using TDD Frame Structure with higher number of UL channels. It is worth to mention that by this approach additional performance evaluation of different TDD frame structures related to uplink could be achieved – a result important for FRMCS, in general!

3.9.3.1 Observations from CCTV offload with bearer-flex functionality

In a CCTV offload system, FRMCS provides means for transferring video surveillance data between a mobile communication unit in the train and ground communication units located at the depot and at the stations and/or stops alongside the predetermined route of the train. Whenever the train approaches the stations and/or stops or arrives at the depot. FRMCS facilitates the communication between the mobile and ground communication unit with the 5G frequency available at stations and depots. FRMCS facilitates the communication between the mobile and ground communication unit outside of the depots or stops as well using other links / sub-bands with the frequency available along track. With this use case the bearer flexibility is demonstrated as multi access use case using two sub bands for track and station coverage.

During the test an inter-frequency Xn handover was executed with the help of the HYTEM attenuator in order to simulate the movement from Cell1 (track) to Cell2 (station). These cells were on different frequency subbands of N78.

During the test the radio condition was ideal, no fading effect. Cell1 and Cell2 were configured also with different frame structures to achieve higher bandwidth in Cell2

In Cell1 there was also background traffic generated to lower the available bandwidth for CCTV offload in Cell1.

5G QoS value for video was set to 5QI=7, non-GBR, according Table 3

From the integration point of view, it shall be mentioned that on the trackside two MCX clients were needed to handle CCTV offload. So, in total 3 MCX clients (2 in TS GW and 1 in OB GW) were required. This is because non-critical real time video streaming and Transfer of CCTV archives are also designed to support simultaneous operation of both applications, although this was not used in the scope of 5GRAIL.

At the beginning of the test, the CCTV offload, actually the upload of CCTV video surveillance data was transferred in Cell1 at about 11 Mbps, almost constantly, without any issue. Then background traffic was generated in Cell1, which lowered the bandwidth of CCTV offload to about 6 Mbps. After 2 minutes, the CCTV offload moved from Cell1 to Cell2, when suddenly the bandwidth of the CCTV offload increased to about 17 Mbps in Cell2.

The following diagram shows the impact of configuring more UL TSs in case of bearer-flex implementation with inter-band Xn handover:

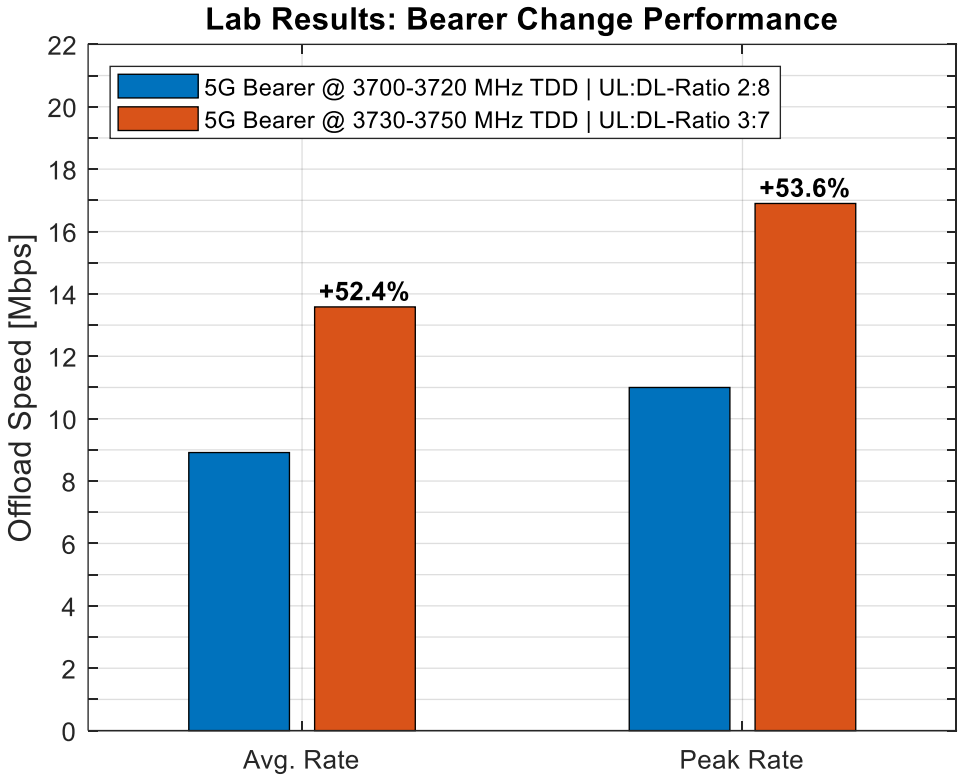


Figure 27 CCTV offload with bearer-flex implemented as inter-frequency Xn handover (Ref.D3.3).

3.10 Cross-border

3.10.1 Cross-border implementation from WP3 lab

Trains crossing the border is an essential requirement for FRMCS for the deployment of a Pan Europe Railway, allowing trains to seamlessly travel between the different countries. This is already a guiding principle for GSM-R which is included in the EU legal frame of Technical Specifications for Interoperability.

When it comes to FRMCS the different Strata of the FRMCS architecture are impacted and involved in Border Crossing scenarios:

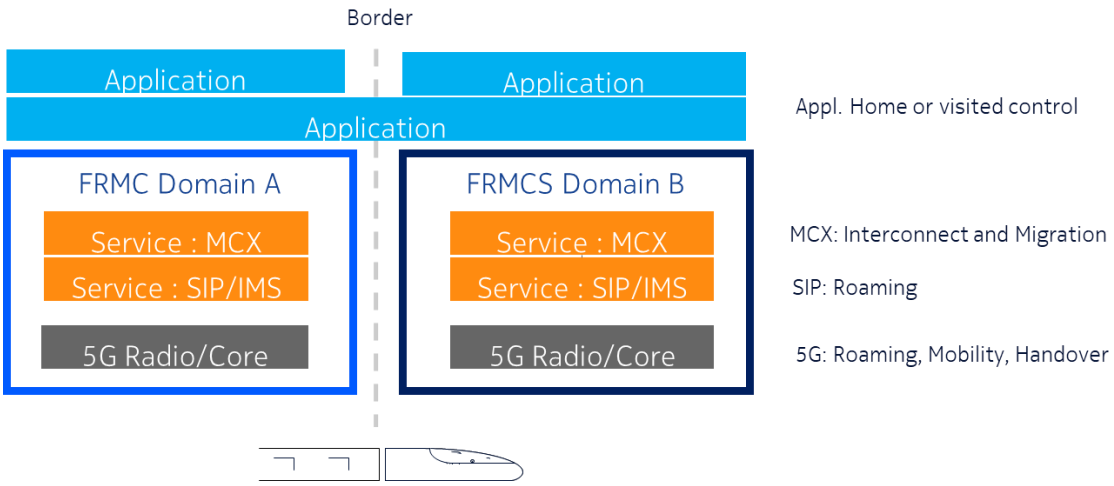


Figure 28 FRMCS Strata impacted by Border Crossing

The following topics are to be considered:

- On 5G Radio / Core measures for roaming and cell reselection or Inter PLMN to be considered
- On Session layer we have SIP roaming as the base to allow session handling between different countries, supporting MCX migration and interconnection.
- MCX lay interconnection and migration is not yet available, being under standardization in 3GPP (e.g., TS 23.280 / Rel. 18,) to allow border crossing in a MCX environment via the following mechanisms:
- Interconnection:
  Communication between MC systems whereby MC service users obtaining MC service from one MC system can communicate with MC service users who are obtaining MC service from one or more other MC systems. Interconnections between FRMCS domains is required.
- Migration:

  MC service user is able to obtain MC services from a partner MC system e.g., the MCX of the roaming PLMN. Therefore, User Profile data are migrated and then accessible to partner network to migrate, especially in cross border scenarios.

When it comes to the 5G NSA or SA evaluations for service continuity border crossing, different steps have been analysed and tested in the 5G CAM projects on potential improvements towards seamless service continuity support on 5G level with a focus on automotive requirements for border crossing between networks, mainly differentiating the following scenarios related to Network Reselection Improvements (cf. §8 [36]):

Scenario in 5G CAM projects	Description

Scenario 1 / Basic	UE roaming with new registration
Scenario 2	UE roaming with AMF relocation (idle mode mobility)
Scenario 3	(Inter PLMN) Handover, relying on NG/N2 based handover

Table 5: Cross-border scenario in other CAM projects

Scenario 1 is typically taking **up to several minutes** as no specific support is provided, and new search and registration phase as part of the roaming procedure is needed after losing the coverage with a new session setup (IP address change).

In **scenario 2** the improved idle mode mobility (with redirect function from source to target frequency and PLMN) allows to reduce **interruption time to about 1 second**, with same IP address kept.

Scenario 3 is the most demanding solution offering **interruption time as low as 0,1 seconds** with same IP Address as context is transferred.

One of the corner stone of Scenario 3 with Inter PLMN handover is the NG/N2 handover as a solution where the handover is not managed via interconnection of the gNb involved (X2 handover) but is realized via the core network.

Note: NG/N2 can be realized within one core network, or between two core networks. In an Inter PLMN Handover scenario, the exchange of session information between home and visited PLMN is required, this needs roaming interfaces between AMF (N14), as well as handling of SMF/UPF anchor transmission.

Annex §9.3 gives some more details on the evaluations in the Horizon 2020 CAM projects.

It should be noted that for concrete test setups the 5G system was based on 5G NSA (means relying on LTE core network) where functionality as Roaming is available since years.

Some scenarios are expected to be easier realized in FRMCS compared to CAM projects for the automotive sector, due to the stronger interconnection measures between railway operators. It is important to understand that – with difference to railway – CAM services rely on public operator networks, and thus for automotive sector the cooperation of mobile operator between networks is required, which is expected to be more challenge compared to the cooperation models typically done in railway (where already in GSM-R close cooperations between railways are in place to achieve seamless interworking and roaming across Europe (refer to GSM-R ENIR project).

5G RAIL implications:

For 5GRAIL the limits of the available infrastructure on Roaming and Handover capabilities in a 5G SA environment led to the solution to identify some of the building blocks defined above to derive benefits of the concepts for FRMCS, at least to validate principles and potential improvement of inter-PLMN handover and future usage of 1UE, as a cross-border solution.

However, it is worth mentioning that the set-up of both labs with one MCX server doesn't allow evaluating the impact of the MCX part which is mandatory for our critical applications. Moreover, MCX interconnection and migration, still in progress in 3GPP and FRMCS specifications.

The initially planned test case on Home Routing for TCMS services (refer to WP3 D3-2 delivery) could not been further tested due to the mentioned restrictions in 5G SA on roaming support (cf. Annex §9.3).

Instead, important building blocks of the 5G Inter PLMN and service continuity concepts have been analysed and tested using a Video Streaming application.

The following picture shows the overall architecture used to verify the border crossing functionality by emulating a second PLMN as roaming interfaces are not supported:

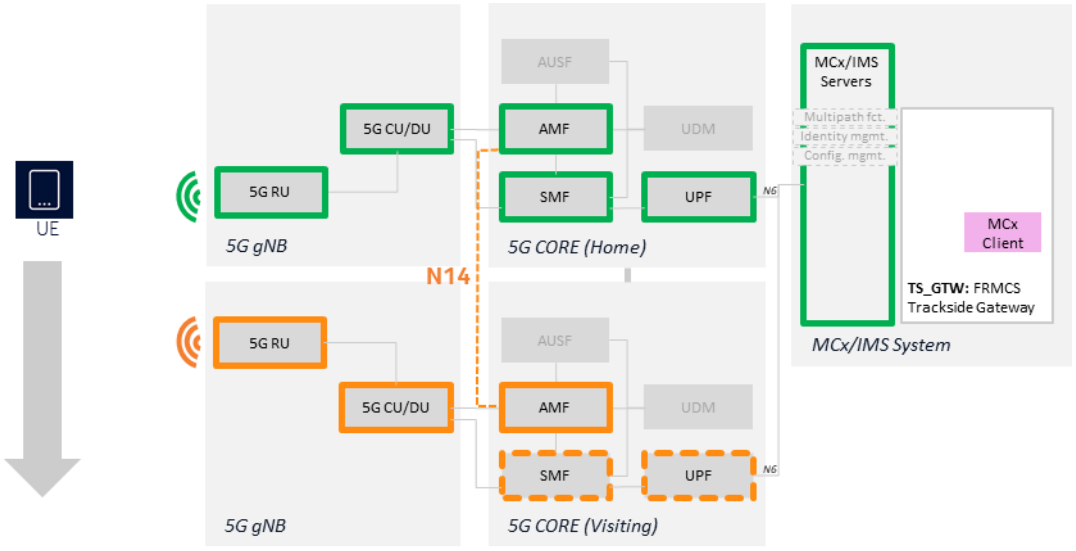


Figure 29 System overview for border crossing (Ref. D3.3)

NOTE:

- As the roaming interfaces are missing, the two-core systems are treated as same PLMN (this means the UDM/AUSF of the second visited PLMN is not used). This is also the reason this visited PLMN (emulated) is treated as the same network, although Ng handover using Inter AMF/SMF/UPF function (N14 interface) is part of an Inter PLMN Handover. We have therefore considered that this test is relevant for Inter-PLMN Handover since the major steps for this Domain Transition have been achieved.
- The realization of Inter AMF handover/connectivity as NG handover is tested by the capability of the N14 based interconnection of two AMF in Nokia core.

- Whether an UPF (or SMF) change can be realized is a matter of ongoing test activities and can only be realized optionally.

The Inter gNB NG/N2 Handover as a main building block for seamless Inter PLMN Handover scenario is depicted in following figure:

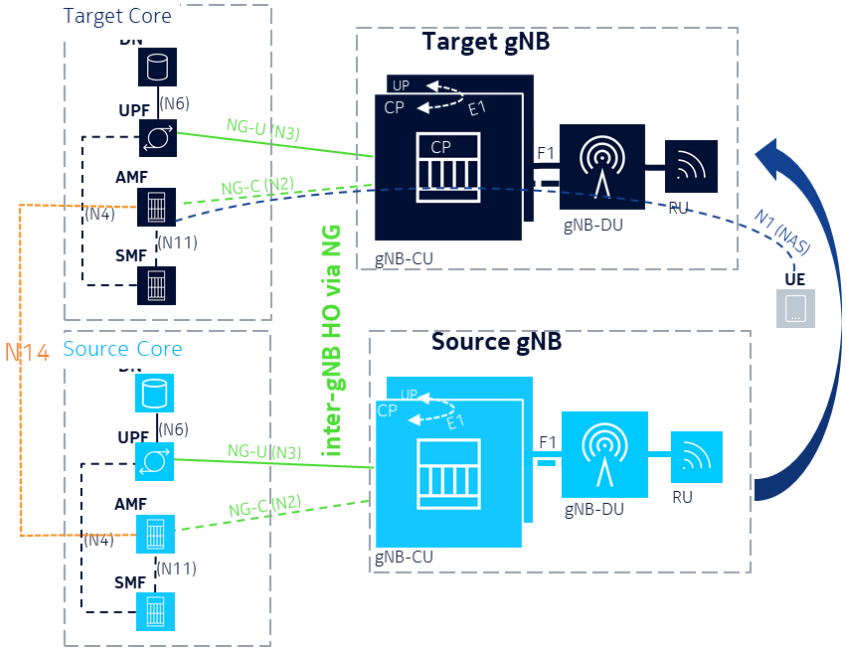


Figure 30: Inter gNB handover via NG/N2 over inter-AMF/inter-UPF

NOTE: the picture shows the target situation with two core/AMF configuration. An intermediate step (using two RAN but one Core) has been executed to first evaluate NG handover mechanisms on the radio side.

3.10.2 Introduction to Cross-border tests in WP4

WP4 was mainly focused on data applications (ETCS, ATO, PIS but also Remote Vision) consequently Cross-Border scenarios had to be foreseen for the most critical of these applications.

However, Cross-Border technical possibilities are numerous and it is worth to have a quick look at it before discussing what has been achieved in WP4.

The starting point is what is shown on Figure 31:

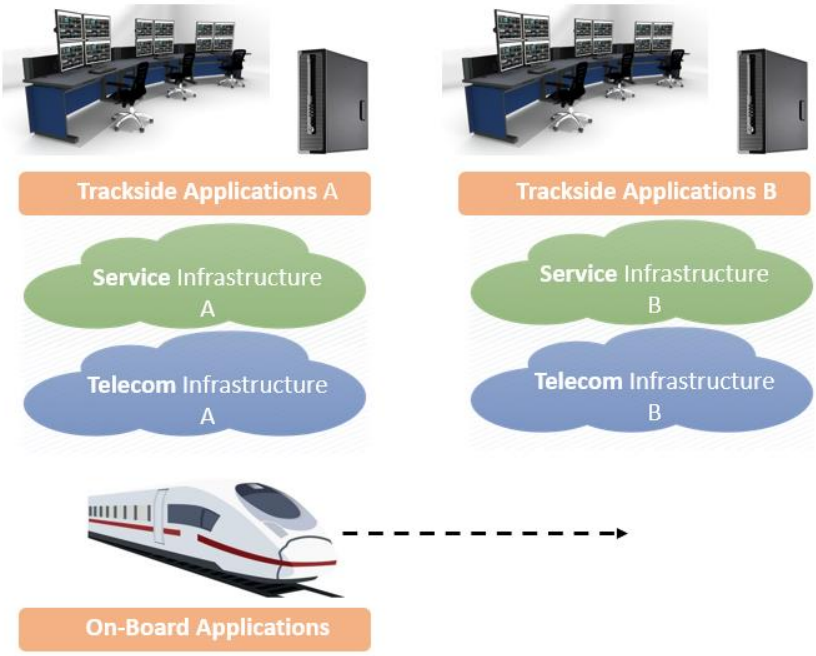


Figure 31: Cross-Border generic view

Train is moving from a Railway Operator A to a Railway Operator B, each of them managing their own:

- Telecom Infrastructure, i.e., a 5G SA network,
- Service Infrastructure, composed of a SIP Core/IMS network serving MCx application server,
- Trackside Applications servers.

What is known is that the train is going from Telecom Infrastructure A to Telecom Infrastructure B, but the possibles ways for On-Board Applications to reach Trackside counterparts are numerous:

- At Telecom Infrastructure Level:

  When using only one 5G modem in the TOBA, 5G SA roaming scenario with **Home-Routed** (HR) or **Local Break Out** (LBO) schemes can be used to manage the transition. LBO implying that

the 5G Modem will now get an IP address allocated by Telecom Infrastructure B, which is obviously a big difference compared to the situation before the crossing.

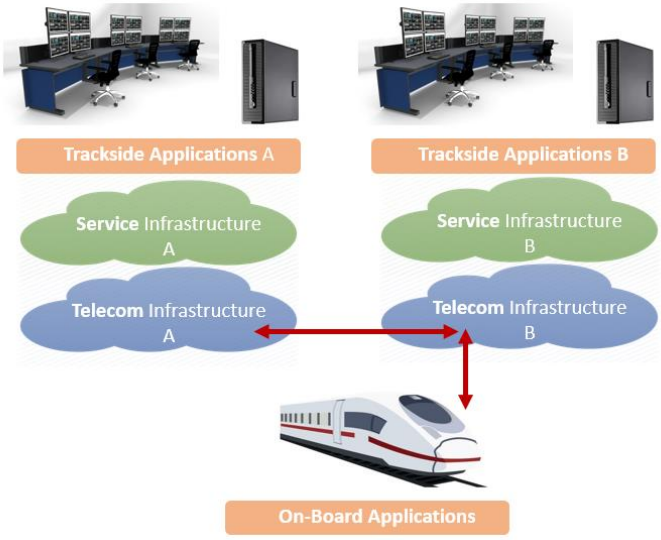


Figure 32: In HR scenario, the data flow exits directly in Network A

Not using such roaming schemes will result in a **disconnection from network A and re-connection to network B**, which is also a possible scenario, but it implies, in that case, a clear impact on continuity of service (cf. §9.3.1).

Use of a second modem in the TOBA to enable service continuity. In that case, the transition could look like a communication between Modem 1 and Telecom Infrastructure A being complemented by the communication between Modem 2 and Telecom Infrastructure B, whenever network B is reachable. Stopping the usage of Modem 1 can then be triggered by different factors (loss of Network A coverage, TOBA's decision based on some information). In the Cross-border implementation with two modems, TOBA will use the multi-connectivity feature in the scope of 5GRAIL. **It is worth mentioning that 2 GSM-R modems are already used in ETCS current border crossing scenarios**, which has influenced WP4 choice with the 2 5G UE approach.

- At Service Infrastructure Level:

  As soon as the TOBA gets a new IP address, it can communicate with the IMS/SIP Core of Operator A or the one of Operator B. Suppose that home network of the ISIM is network A, attaching on IMS/SIP Core B will result on IMS roaming.

  MCx service level that will be used should be the same as chosen IMS/SIP Core, so if MCx client is from Service Infrastructure A, it is possible that it uses MCx services of Service Infrastructure B. Specific MCx procedures can be used for that like MCx Migration procedures.

  Consequently, several technical schemes can be used when leaving Network A and attaching on Network B. WP4 could explore some of them, knowing that some scenarios are not yet

available due to industry's readiness on these topics (5G SA HR and LBO, MCx migration), during the set-up period of the project by 2021, knowing that public operators focused primarly on 5G NSA (i.e. 5G RAN connected to a 4G Core) and wide deployment of 5GA networks will come later.

3.10.2.1 Use of two modems 5G with ETCS application (Loose coupled) and TOBA-A multipath

The cross-border scenario tested with Alstom TOBA relies on multi-connectivity capability of the gateways. The high-level principle is depicted on Figure 33 and is based on preferred primary link whenever available, meaning that only one path is active each time:

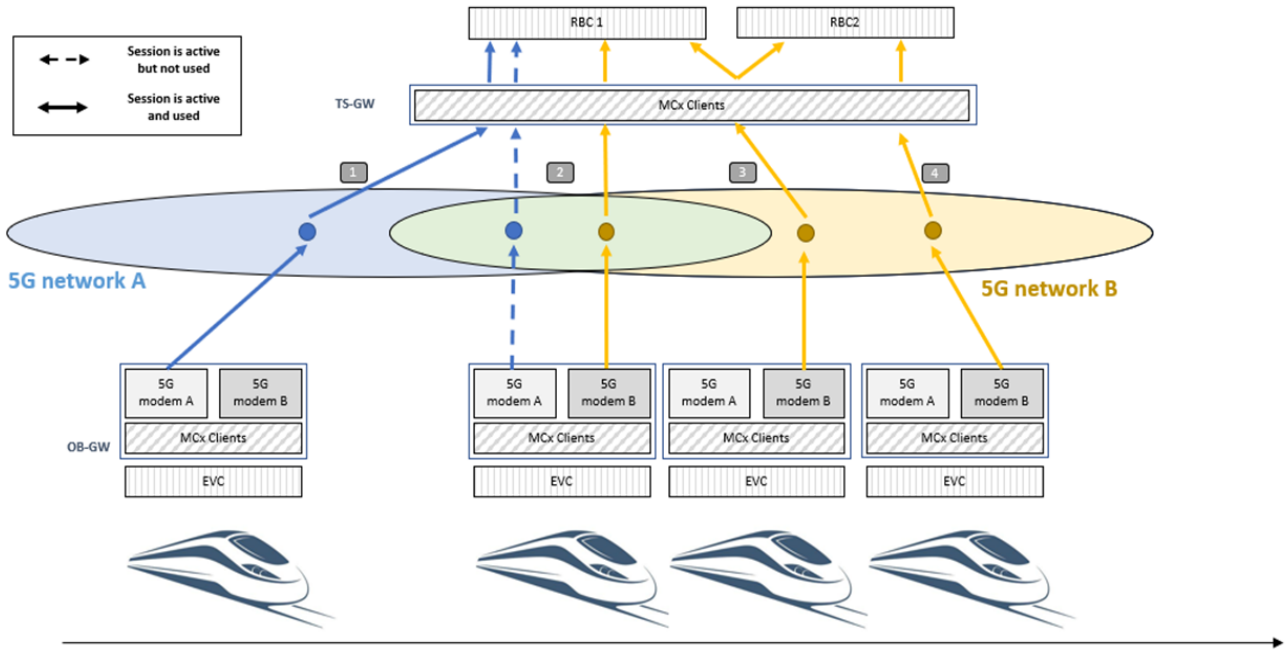


Figure 33: ETCS cross-border scenario with TOBA-A

To communicate, EVC can use two MCx clients: evc_a which can use Modem A, and evc_b which can use Modem B. Modem A is configured so that it can only attach to 5G network A, whereas Modem B can only attach to 5G network B.
At the very beginning, TOBA-A is under the coverage of 5G network A. Modem A is attached to it and there is a MCx session between evc_a and rbc_1a as shown on Figure 34. EVC can exchange ETCS information with RBC_1:

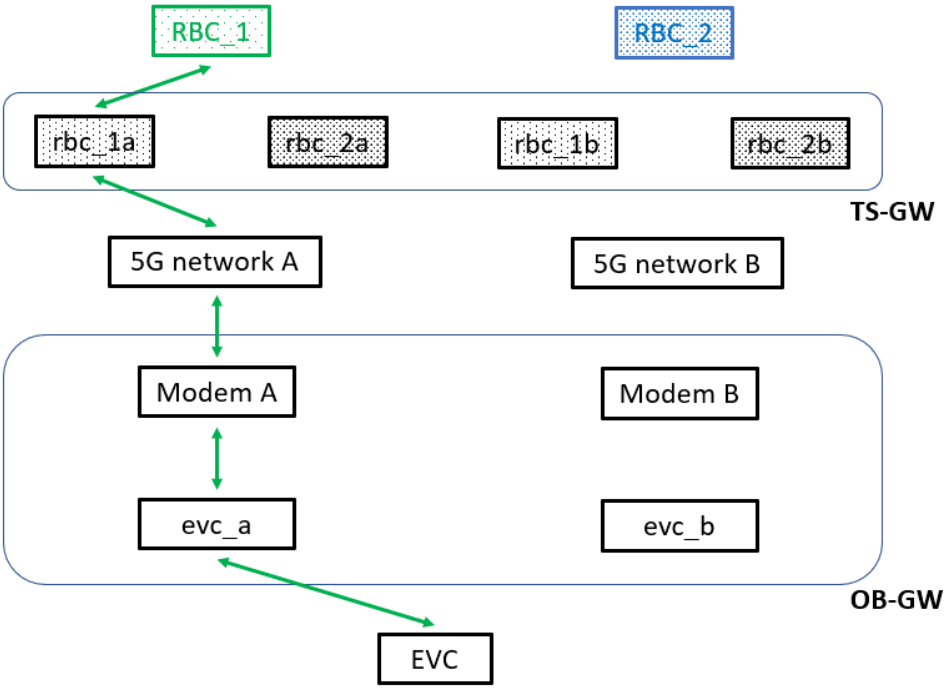


Figure 34: TOBA-A cross-border test – 1st step

TOBA-A now enter a zone where both 5G networks A and B are available. Consequently, modem B attaches on 5G network B and once connected, evc_b uses it in order to establish a MCx session with rbc_1b. EVC can now use *evc_a-rbc_1a* or *evc_b-rbc_1b* in order to send ETCS traffic to RBC_1. Note that the use of MCx clients evc_a and evc_b is transparent for EVC, as well as the use of rbc_1a and rbc_1b for RBC1; all being managed respectively by OB-GW and TS-GW. The second path can be set up as the preferred one so that in the second step of the cross-border scenario (cf.Figure 35), the ETCS traffic is now seamlessly handled by 5G network B:

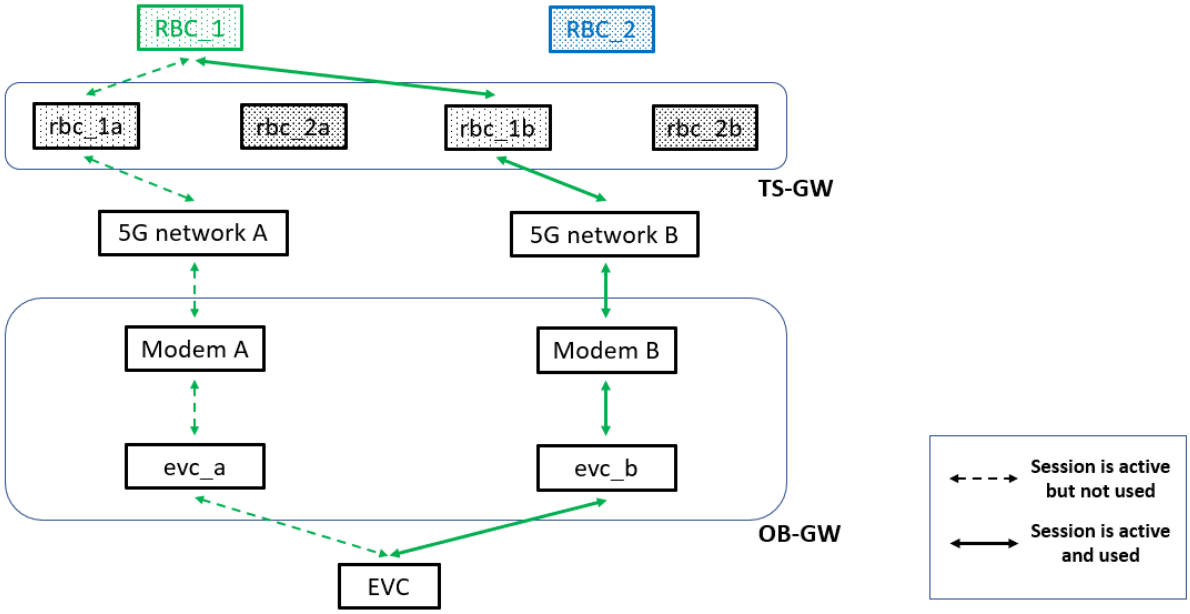


Figure 35: Cross-border scenario with TOBA-A – 2nd step

A simulated beacon then, requests EVC to connect to RBC_2. As shown onFigure 36, EVC now communicates with both RBC1 and RBC2:

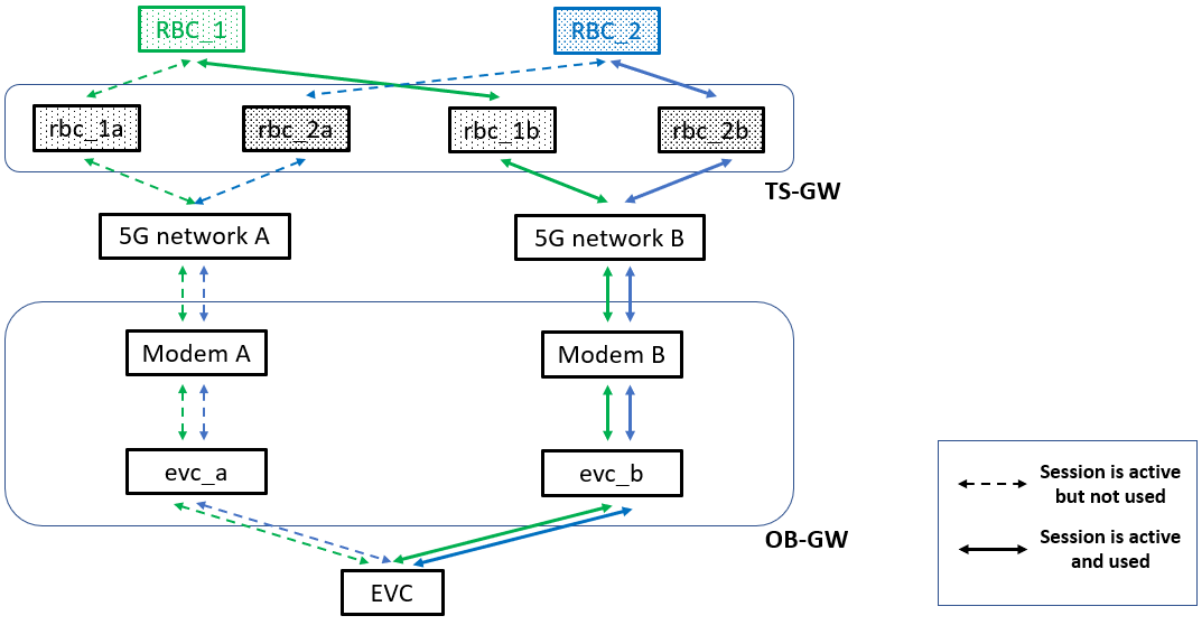


Figure 36: Cross-border scenario with TOBA-A - 3rd step

Then, another simulated beacon signals that communication with RBC_1 must be stopped. ETCS flows only to RBC_2 now:

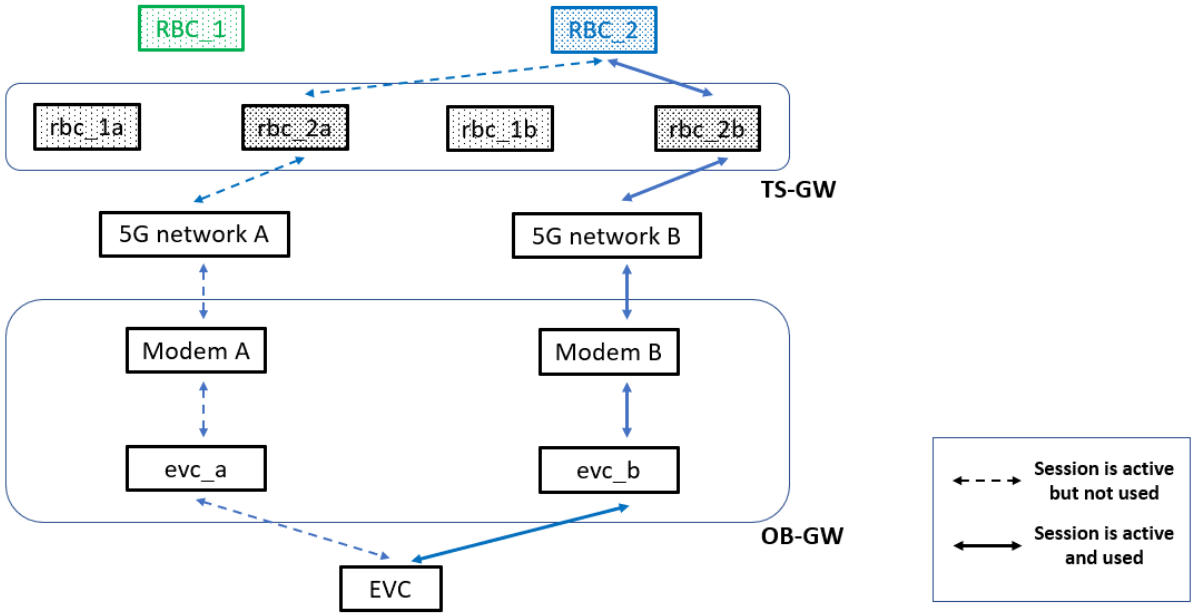


Figure 37: Cross-border scenario with TOBA-A - 4th step

The last step is achieved when TOBA-A exists the zone where 5G network A is available. ETCS is still managed without service interruption as shown on Figure 38:

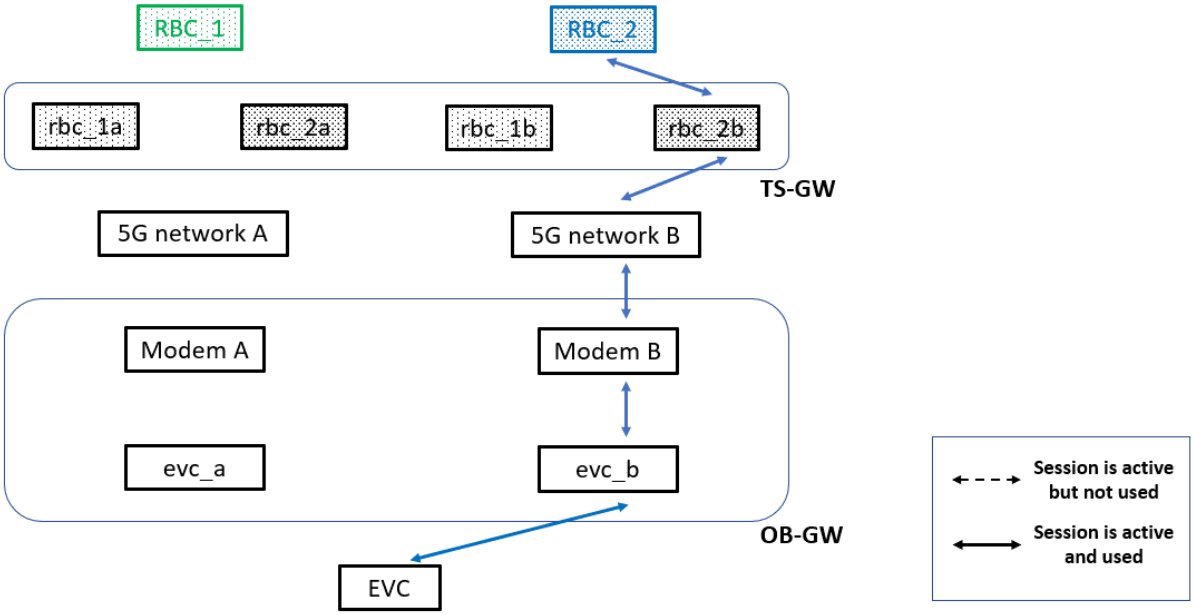


Figure 38: Cross-border scenario with TOBA-A - 5th step

3.10.2.1.1 RTT DELAY, AS A KPI FOR EVALUATION OF CROSS-BORDER SCENARIO WITH 2 5G UE

This chapter aims at giving additional details about cross-border scenario performed with ETCS application and TOBA-A using two 5G modems and two different 5G networks (named “blue” network and “red” network in the description below) and relying on the multipath function of TOBA-A to switch from a first 5G network to the second 5G network.

Especially, it illustrates the impact of border crossing in terms of RTT (round trip time) for ETCS applicative data, which is the main KPI used by ETCS to qualify the FRMCS communication.

The scatter plot below displays all the RTT for the applicative frames sent from EVC side (on-board) to RBC side (trackside) through FRMCS sessions established between TOBA-A and TS-GTW-A. The abscissa corresponds to the time where the TCP ACK of the packet is received (which is considered to compute the RTT). The first plot shows the full picture of the test, the second plot is a zoom around the key moments of the border-crossing, i.e., the change of network to carry the applicative data.

- Steps of the border-crossing:

In the two graphics below, blue points correspond to applicative frames carried on the blue network (tunnel 0xdbb168db for TOBA-A point of view), red points correspond to applicative frames carried on the red network (tunnel 0x17754811 for TOBA-A point of view).

NOTE:

- Tunnel 0xdbb168db through 5G modem 1, connected to 5G network A (“Blue” 5G network)
- Tunnel 0x17754811 through 5G modem 2, connected to 5G network B (“Red” 5G network)

T1 = 122.40s: last ETCS frames carried on the blue network by TOBA-A. RTT=45.3ms

T2 = **126.05s** (only visible on the second graphic): TOBA-A loss the connection to network A.

T3 = **127.05s** (only visible on the second graphic): TOBA-A decides to switch the applicative data to tunnel 0x17754811 (red network).

T4 = 127.61s: first ETCS frames carried on the red network. RTT=48.8ms

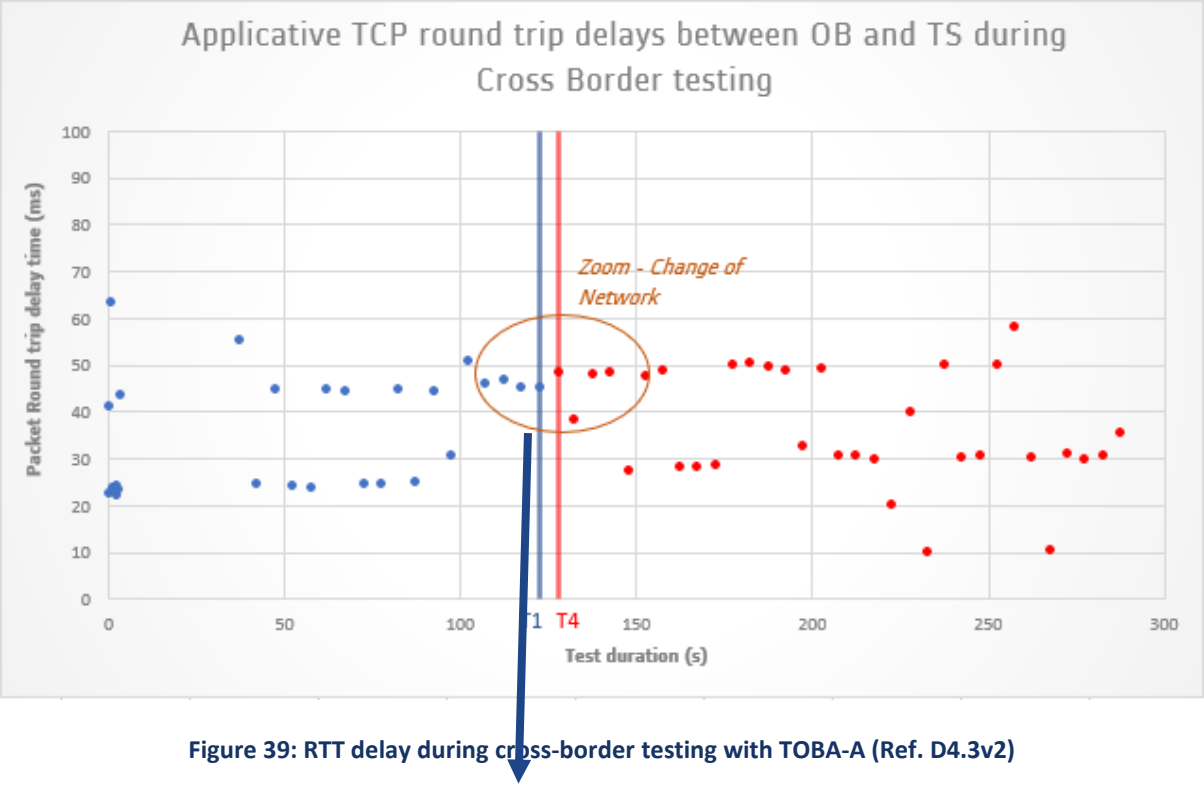


Figure 39: RTT delay during cross-border testing with TOBA-A (Ref. D4.3v2)

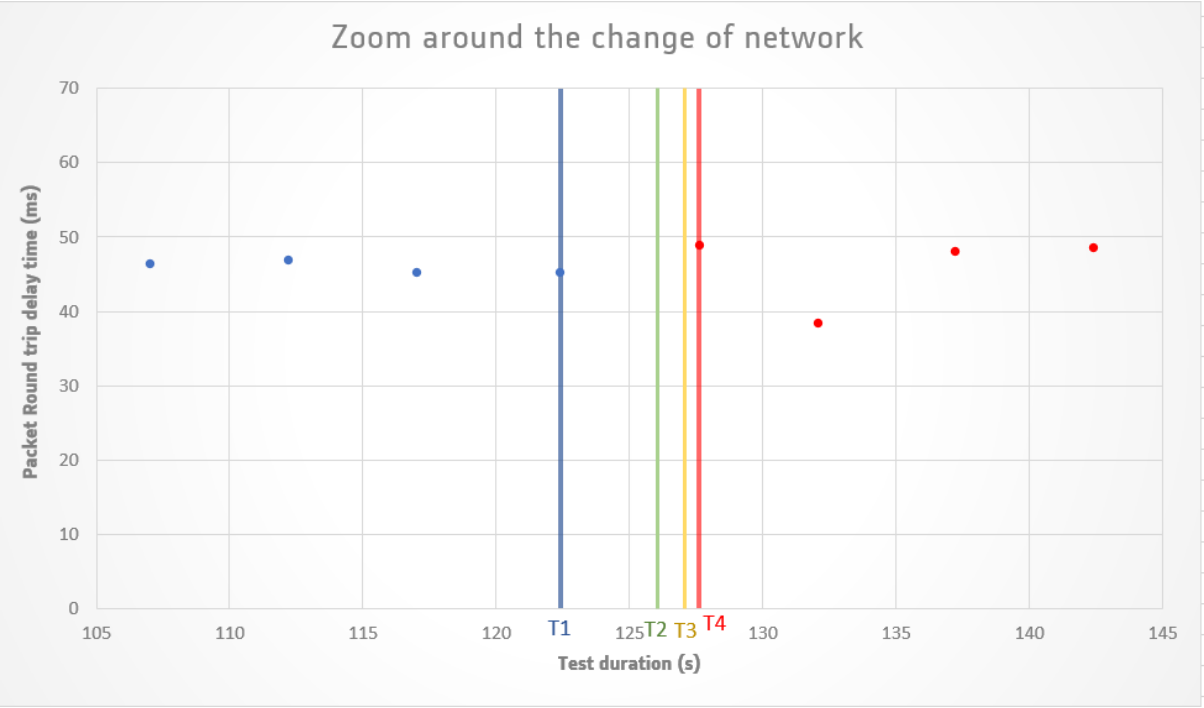


Figure 40: RTT delay detail around the change of the network during cross-border procedure (Ref. D4.3v2)

- **Comment on cross-border behaviour with TOBA-A:**

The change of network made by TOBA-A to carry ETCS applicative data has strictly no impact on the RTT seen by the application. The RTT just before and just after the transition is approximately the same (48.8ms vs 45.3ms).

It can be explained with the zoomed picture, the full transition from network A to network B occurs between T2 and T3 but there is no attempt of ETCS frames sending between T2 and T3, meaning that the change of network was fully done by TOBA-A between two consecutive frames. Hence, when the next applicative frame occurs (i.e., T4-45.3ms), the change of network has already been done and the frame is normally transported.

3.10.2.2 Use of two modems (4G and 5G) and TOBA-K multi-connectivity with ETCS application (Loose Coupled)

The border crossing scenario with TOBA-K is different from the one used by TOBA-A as the implementation of the multi-connectivity differs.
The first point to notice is that TOBA-K could not embark two 5G modems ES3 (the one that use the FRMCS 1900MHz band). Reason is that the heat dissipation of these modems, that use boosters, was not possible with the actual form factor of the equipment. Consequently, tests were done with one 4G modem and one 5G modem, knowing that the principles of the border crossing we envision here will stay the same. The second point is the ability to use at the same time several bearers for a given communication. Thus, Figure 41 sums up this ETCS cross-border scenario.

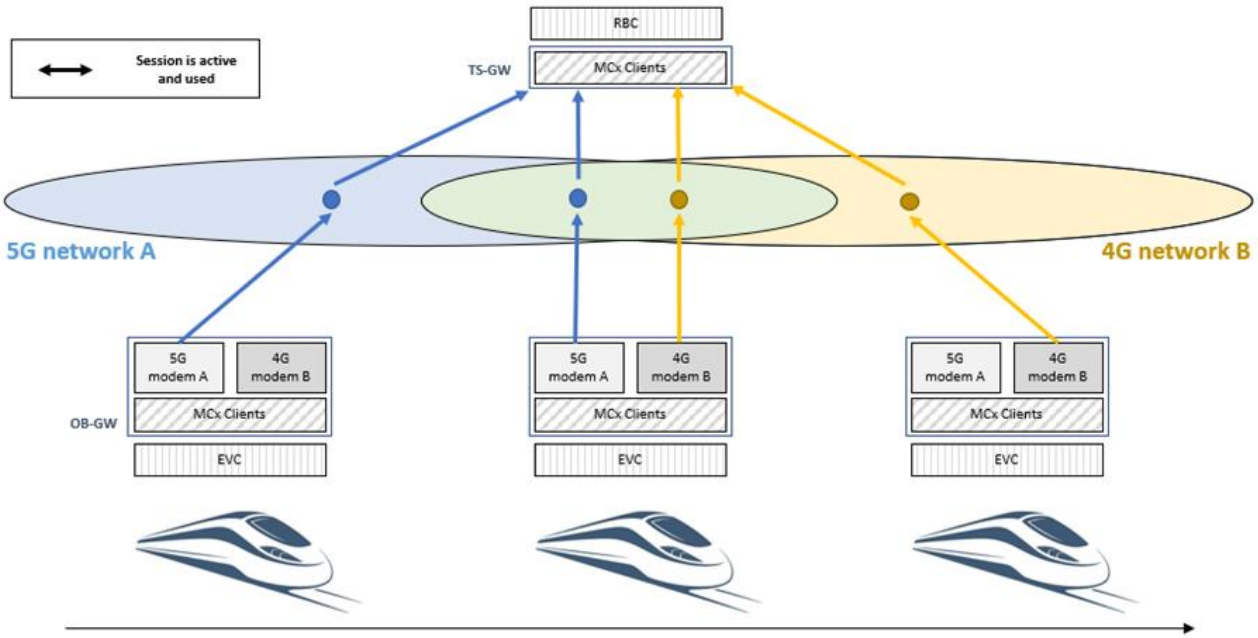


Figure 41: ETCS cross-border scenario with TOBA-K

As shown on Figure 42, the first step was to establish an EVC-RBC ETCS connection by using evc_a-rbc MCx communication while TOBA-K was under 4G only coverage:

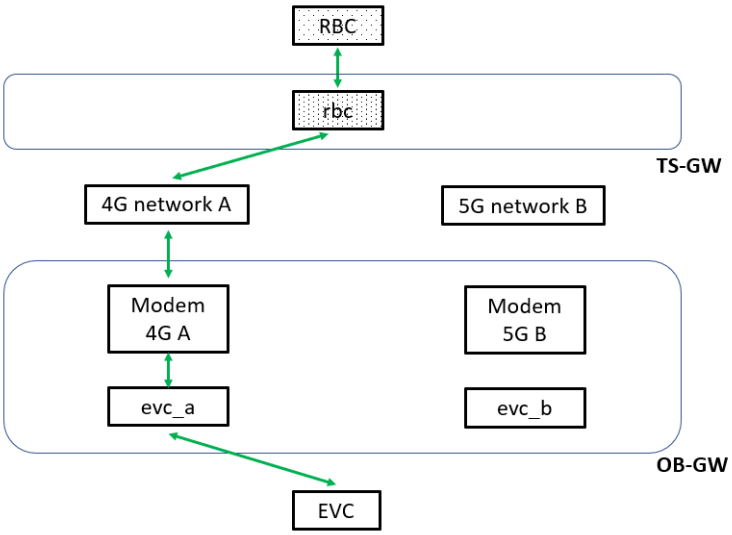


Figure 42: Cross-border scenario with TOBA-K - first step

Then, TOBA-K entered in an area where 4G coverage of Network A and 5G coverage of Network B were present. Then, using multi-connectivity feature, another MCx client on TOBA-K, evb_b, opens another stream with rbc for the same ETCS communication. Now, as shown on Figure 43, EVC use at the same time 4G and 5G link to communicate with RBC; this is a difference compared to TOBA-A behaviour where only one link was active at a time.

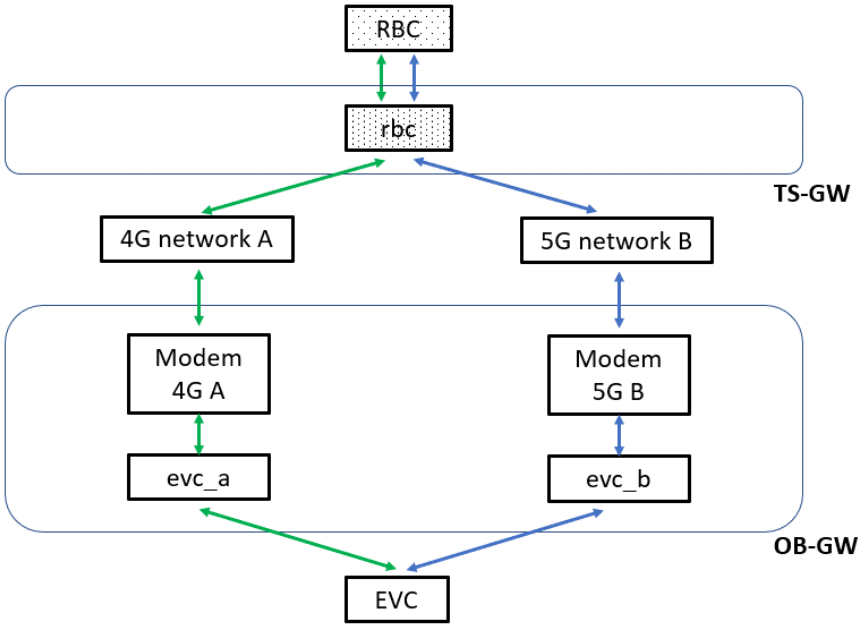


Figure 43: Cross-border scenario with TOBA-K - second step

Later, when TOBA-K gets completely into Network B and loses Network A coverage, the ETCS communication continued seamlessly on 5G network B as shown on Figure 44.

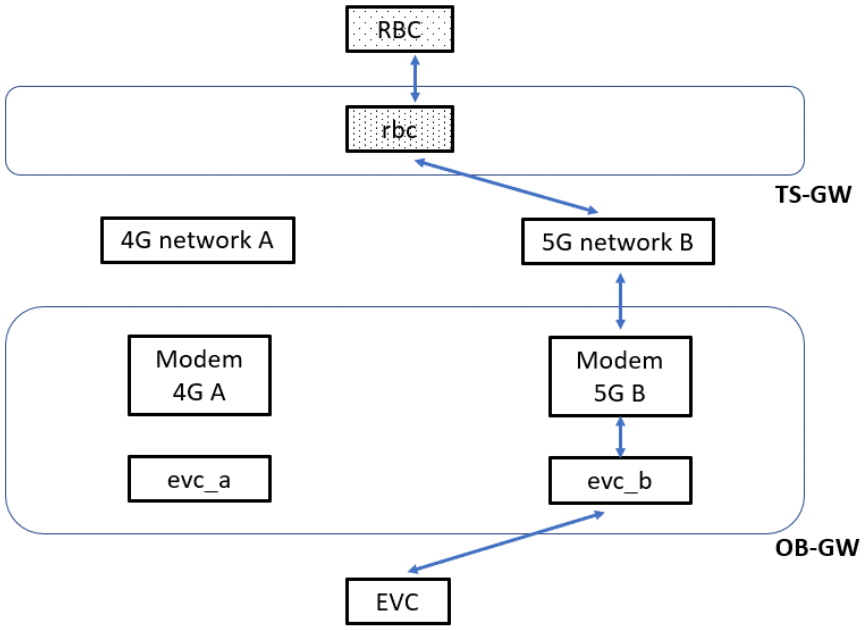


Figure 44: Cross-border scenario with TOBA-K - third step

This test enabled us to validate the multi-connectivity concept for cross-border scenario using a critical data application. Note that in this test, we used only one RBC and we didn't seek to test again RBC transition alike TOBA-A tests, considering it would have added complexity for little added value.

WP 4 Border Crossing Context:

As explained within WP3 Border Crossing context, to achieve a service continuity for a data application, we need to finalise the standardization of 3GPP MCX Interconnection and Migration.

As currently Railways need service continuity border crossing for ETCS and ATO only, in a first phase, we intend to use the two 5G modems method. We will of course pursuit our efforts to finalise the 3GPP work and look for reaching the capability to achieve a service continuity border crossing using only one modem, in the future.

3.10.2.3 Disconnection-Reconnection scenario with Remote Vision (Flat-Ip application)

In this configuration, the application is not using Obapp and Tsapp protocols, implying that the use of FRMCS gateways look, from applications point of vue, as if routers where used.
During WP4 test where Remote Vision application was used in a border-crossing scenario, we had the following steps:

a/ OB-GW is under radio coverage of Network A. The 5G modem attaches on it, then SIP/MCx client registers on Service part of Network A. After that, an MCdata communication is established between the OB and TS MCx clients. Once done, IP traffic coming from On-Board and Trackside applications can be routed to the IPConn tunnel in order to reach the other end.

b/ OB-GW now enters radio coverage of Network B and progressively loses radio contact with network A. There is now an outage for the application.

c/ 5G modems has to attach onto Network B radio, then register again on SIP/MCx, then re-establish the MCx call between MCx client (this was done automatically). Applications were then able to continue data traffic.

This scenario is interesting as **we can get a rough idea of the outage that one must undergo in step b : at least one minute during WP4 tests.** Using FRMCS application would of course have a greater impact on service due to the time taken on OBapp/TSapp to be aware of the cross-border and ask for a new communication set-up. This could mean that the network overlay could be required for some 3-5 km, which is reasonable (two cells). Other tests addressed this need by using two modems.

3.11 Arbitration

The FRMCS System shall be able to perform arbitration, based on the context of the communication. Arbitration means that the FRMCS System is able to determine the behaviour of the end user device in case of multiple competing communications. Additionally, the FRMCS System may ask the FRMCS User which communication to accept.

This function also saves the human user from interacting with the HMI in order to keep the attention on the railway operations when required.

Comments on arbitration testing:

Due to the lack of FRMCS arbitration standards, the 5GRail project adopted the GSM-R EIRENE arbitration tables. The test case conducted in WP3 included two FRMCS devices: one was the cab radio, and the other was a handheld device along with a controller terminal. The FRMCS devices were engaged in a point-to-point call when the controller terminal initiated a railway emergency call. As a result, the point-to-point call between the FRMCS devices was terminated, and the REC was established.

However, following the termination of the REC, the point-to-point call between the FRMCS devices was not restored. In the future, there could be an option to reconnect this call.

3.12 Interworking function

Since the migration period will take place progressively, interworking between FRMCS and GSM-R is required but without any changes in the GSM-R system. Depending on the migration scenario a Ground FRMCS User or a Driver can be attached to the FRMCS system, to the GSM-R system or both. Another scenario might be that the Driver can be attached either in the GSM-R system or in the FRMCS System. MCX functional identities are only applicable in FRMCS system.
To avoid impact on the development of the FRMCS On-board system, the migration functionality, the so called **'Coordinating Function'** should be part of the Application layer and not part of the FRMCS Service layer. 'Coordinating Function' uses the functionalities of the OBAPP reference point for an onboard application or the TSAPP reference point for a trackside application. that needs to interface with the FRMCS system, as presented in the figure below.

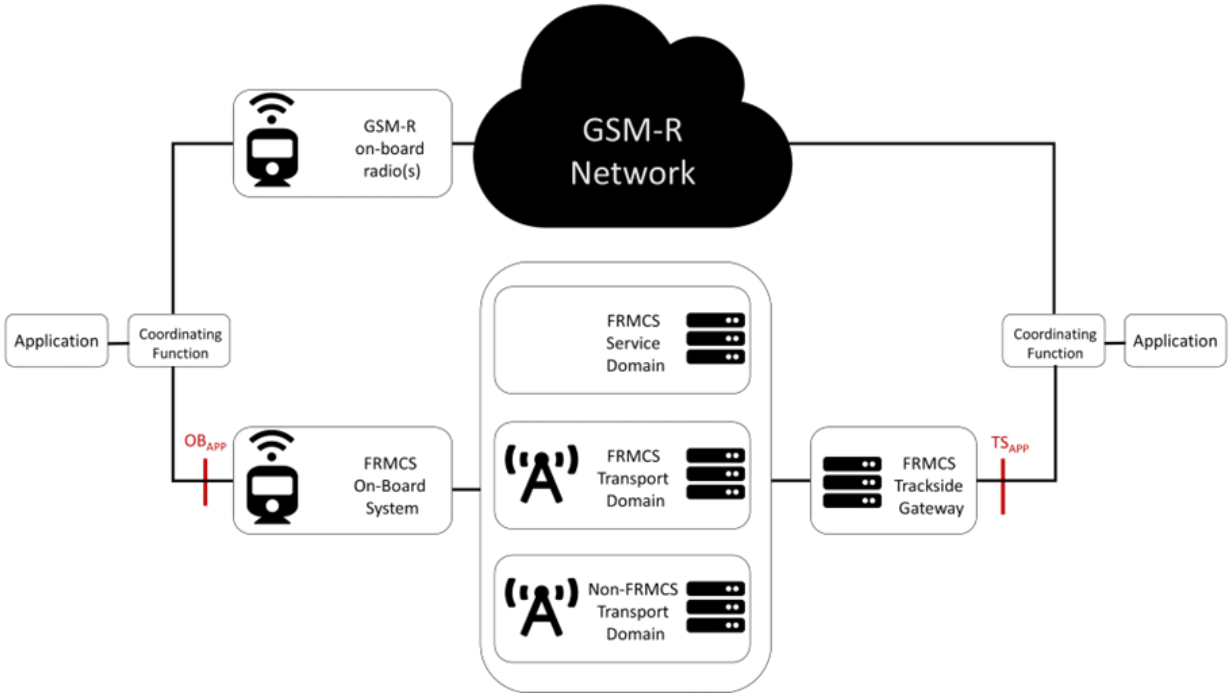


Figure 45: Coordinating function in relation with the FRMCS system. (Ref. UIC-SRS FW-AT 7800)

The following services are to be supported by the interworking function:

- Group call
- Emergency group call (REC)
- Individual call
- Short Data Service

In the scope of 5GRAIL mainly group calls and REC calls are tested in the framework of WP3 lab.

The principle consists in connecting the GSM-R core network to the SIP core of FRMCS system, via the newly developed interface called GSM-R IWF to MCX- Server. The solution integrated in WP3 lab is a pre-standard on based on the ETSI study on GSM-R FRMCS Interworking (TR 103 768) defining IWFg-x. Thanks to the IWF interface, an integrated mapping of Addressing schemes is provided.

It is worth mentioning that specifications of interworking function are still on-going in the ETSI standards workplan.

GSM-R – FRMCS Interworking is an important functionality during the transition phase where both technologies will be supported at the same time.

However, one important use case is the triggering of a Railway Emergency Call in a specific area for both technologies by the infrastructure to ensure that trains with either GSM-R or FRMCS capabilities can be reached. The principal realization in 5GRail was to automatically trigger a Railway Emergency Call on the GSM-R network when in the FRMCS system a corresponding REC is established by the CAB radio. for this the following setup was used for 5GRail:

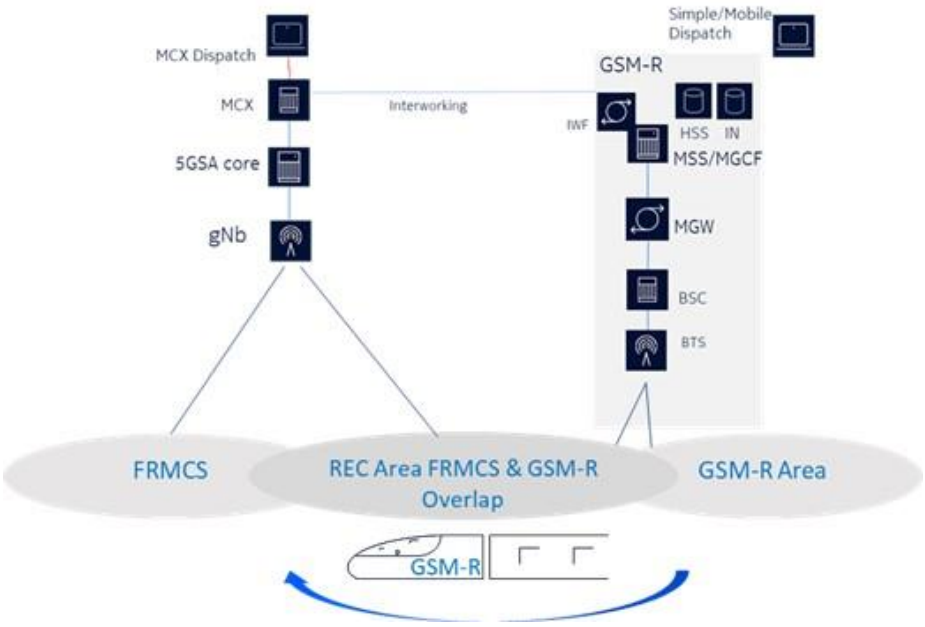


Figure 46: Setup for GSM-R to FRMCS system transition using IWF for Border Crossing

The implementation in the Nokia MSS therefore interprets incoming MCX messages defined in 3GPP for Interworking, and maps them to GSM-R messages inside the MSS , normally use by a dispatcher originated REC call.

Important aspect is that no floor control between the networks which lead to some specific behaviour on the terminal (CAB Radio/ Dispatcher). IPSecurity is not supported on the interfaces thus it must be switched off in the MCX server.

This configuration also serves the test case for border crossing for Voice with Transition from GSM-R to FRMCS. In this case a CAB radio connected to GSM-R receives the technology spanning REC call and is starting a network transition from GSM-R to FRMCS. By manual switching in the CAB radio the CAB radio will leave the GSM-R REC call and joins the ongoing REC call on the FRMCS side. We use the Pre-configuration / Pre-affiliation of the MCX group call on the FRMCS side to allow the CAB radio to do standard Late Join functionality.

3.13 Cybersecurity

The security framework protects the FRMCS System against attacks and threats, like misuse, Denial of Service (DoS), unauthorized access to services, interception, man-in-the-middle attacks, replay attacks and intended data modification. It encompasses the protection of security attributes confidentiality, privacy, integrity, availability.

FRMCS System security framework related service flows cover the following aspects:

- identity management;
- authentication;
- authorization;
- key management;
- data protection (regarding integrity, confidentiality, privacy, non-reputation);
- prevention of attacks;
- detection of attacks;
- reaction on detected attacks.

3.13.1 TLS implementation in TOBA-A – Local binding Reminder

In the cybersecurity scope, two locations are to be protected:

- For the control plane: local binding over TLS.
- For the user plane: TLS at application layers (E2E TLS)

The local binding function ensures 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, is based on certificate exchange.

The local binding of an on-board application is summarized in these two steps:

- Establish a TLS connection with the OB_GTW, using mutual authentication (mTLS). During the TLS handshake, client (application) and server (OB_GTW) authenticate themselves through the certificate exchange.
- Open a WebSocket connection (over the previous TLS layer) and perform the FRMCS_GTW_REGISTER As a result, the application retrieves a unique ID, named app_uuid, which is to be used for every further request in OB_{APP} API.

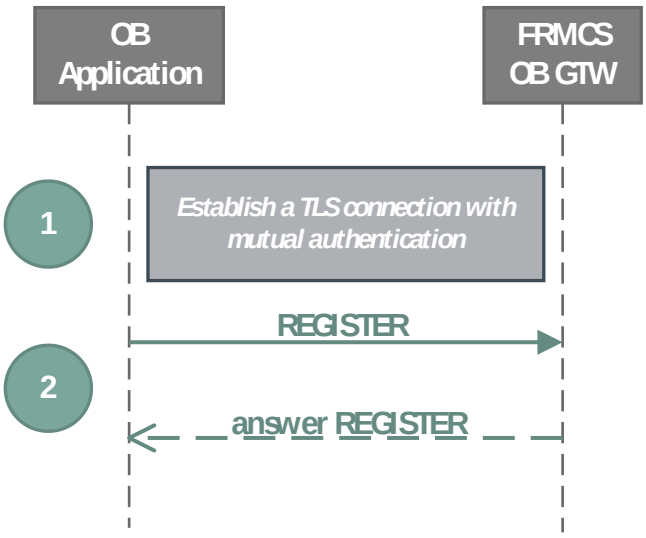


Figure 47: 2 steps in local binding (Ref. D2.1)

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).

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.

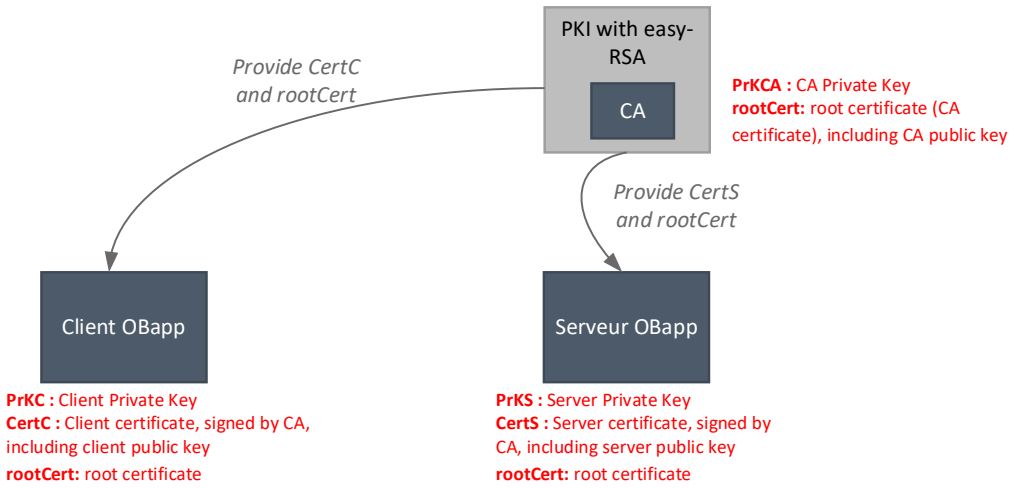


Figure 48: Needs for TLS connection (Ref.D2.1)

Signed certificates are provided by the PKI.

For the offline PKI used for local binding, easy-RSA is the simplest and light way to consider a small PKI for the 5GRAIL activities.

3.13.1.1 TLS for Local Binding

The purpose of this test was to check the use of secured WebSocket (i.e., WebSocket over TLS) for OBapp API, instead of unsecured WebSocket. In fact, in that case the WebSocket API between ATO-OB and TOBA-A is over TLS (instead of over plain TCP). Certificates were generated by an offline PKI and manually pushed on the involved devices (ATO-OB, ATO-TS, TOBA-A and TS_GTW-A). The root certificate (certificate authority which has signed the used client/server certificates) was also pushed on the same devices. With the above implementation, the TLS handshake and the subsequent OBapp API exchanges were successfully accomplished.

3.13.1.2 TLS for end-to-end ATO applicative session

The purpose of this test is to use end to end (E2E) TLS for the full applicative session between ATO OB and ATO-TS. The main difference is that the applicative TCP connection between ATO-OB and ATO-TS is over TLS. In that case, the certificates used for the TLS connection between ATO-OB and ATO-TS are managed by an online PKI on a virtual machine, hosted on the same device than ATO-TS. The TLS usage follows Subset-137. With the above implementation, the TLS handshake and the subsequent applicative messages were successfully exchanged.

3.13.2 Proposals about benefits based on introduction of Electronic Airgap and Session Border Controller

- Electronic Airgap

The principle of Electronic Air Gap function is an equipment with two sides, called gates. Whenever a packet reaches Gate A on a logical slot, the upper layers of the OSI model (4-7) will be extracted

from it, transferred to Gate B that will build new layers 1-3. Slots are paired one to one and configured with rules. For example, these rules will stipulate that any packet coming on Gate A with destination IP x.x.x.x and destination port y will be handled by Slot 1, and so automatically passed (after deconstructing) to Slot 1 of Gate B. This concept provides a protection related to the cyber-attacks targeting low level layers. Moreover, Gates A and B are managed by separated OAM parts with no connection between them, which is an additional advantage of this concept.

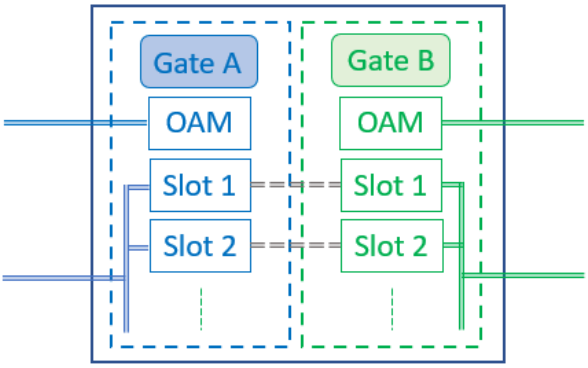


Figure 49: Electronic Air Gap device architecture (Ref. D4.3)

A representative use case with that equipment is by installing another IMS network next to the N6 LAN. In that case, user A is in the critical zone (FRMCS on the left) but needs to access some non-critical services that stands in another network of the railway operator (green part on the right). An interconnection point is needed and, in this case, we put an electronic air gap device (e.g., Sec-XN Seclab) because by doing so, there is a physical isolation of critical and non-critical networks, including OAM part: If for instance, OAM B is hacked because of an attack coming from OAM non critical zone, there is no way for hackers to go further in the critical zone.

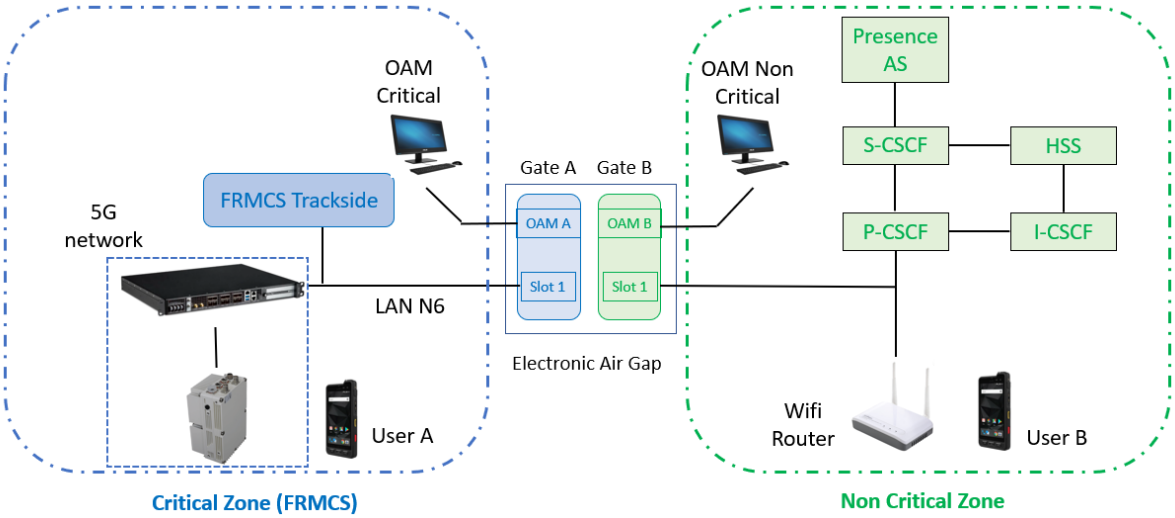


Figure 50: Electronic Air Gap device and non-critical IMS network inserted in WP4 lab (Ref.D4.3)

With this set-up including the Sec XN device, we put an IMS network on simulated non-critical zone (P-CSCF, I-CSCF, S-CSCF, HSS and a presence Server). User B, in the non-critical zone, reaches its

services thanks to a Wifi router. User A moves to the critical zone and, using for instance 5G SA connection, wants to connect its IMS client in order to access the non-critical services.

Some successful demonstration tests were performed in the scope of WP4 with this set-up, such as user A from the critical zone was successfully registered on non-critical IMS or voice calls established between users of critical and non-critical zones.

- Session Border Controller

WP4 studies about cybersecurity architecture raised the benefits of usage of Session Border Controllers (SBC) devices, whenever a SIP or IMS core is used, as it can bring many important features. For example, SBC is a device that is typically placed at the border between two different networks, such as between a service provider's network and a customer's network, to control and monitor the flow of voice and data traffic. As main entry point to the IMS core network, SBC is a critical device and the best place to put cybersecurity tools in order to protect what stands behind.

SBC can provide the so called “topology hiding” feature that consists in removing some information elements of some SIP messages and that gives information about all IMS nodes that were involved in the handling of the SIP method.

Another very useful protection is the ability of the SBC to fight Distributed Deny Of Service (DDOS) attacks thanks to the use of proprietary algorithms.

Our conclusion is that it is worth introducing SBC in the future FRMCS projects and evaluate benefits of its usage.

Conclusion:

We have tested both methods that are included in FRMCS V1 specifications, as well as methods that are supplementary, and under consideration (electronic air gap or session border controller).

This will help decisions for V2 cyber security mechanisms.

4 RECOMMENDATIONS ON RADIO CONFIGURATIONS AND OBSERVATIONS related to the used bands (n8, n39, n78)

The modem of TOBA-K in n39 is a key element of 5GRAIL but also for FRMCS, as it is the first modem with a chipset that functions in 1900 MHz FRMCS band. So, the configurations applied in both labs and behaviour of the modem are important considerations, to provide guidelines for further FRMCS deployment.

It is worth mentioning that n8 is in FDD mode where n39 and n78 are TDD modes. For example, the TDD pattern used in WP4 lab in n39 is 2uplink TS and 7downlink TSs because the applications tested are not bandwidth demanding. However, in field remote vision is planned to be tested and there is a need for more uplink TSs, since this application is more bandwidth demanding.

5 LAB EXPERIENCE AS A FACILITATOR OF FIELD ACTIVITIES IN WP5

Both labs have started by firstly evaluating the TOBA-K performances due to the different frequencies used mainly n39 and n78 which are also used for field tests. Some experiences were performed in WP4 by simulating:

- Attenuation level
- Fading and multipath profile
- Simulated Doppler effect reflecting change of train speed.

5.1 TOBA-K tests on 5G N39 band

5.1.1 TOBA-K HO intra gNodeB

The set-up to perform this test is the following:

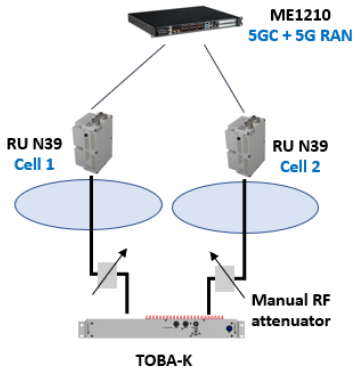


Figure 51: TOBA-K intra gNodeB HO test setup (Ref. D4.3)

Based on the field RF measurements, a path loss of approximately 105dB reflects the conditions of HO at cell edge. Below this level, communication might be lost. So, this can be considered as a worst-case scenario.

As a conclusion, the intra gNodeB HO test could be performed without restriction in WP5-FR field tests.

5.1.2 TOBA-K HO inter gNodeB

The set-up to perform this test is the following:

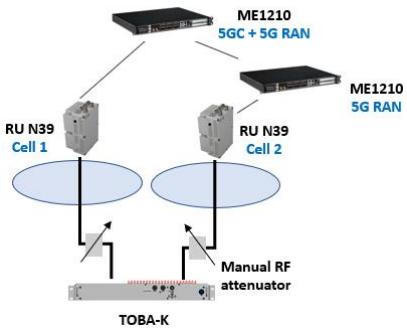


Figure 52: TOBA-K inter gNodeB HO test setup (Ref. D4.3)

Same path loss of 105dB were assumed for inter gNodeB HO. Since no issue was reported during this activity. Consequently, there was no restriction to perform this kind of test in WP5-FR field tests.

5.1.3 Total loss of radio. Reconnection

This test is interesting because it simulates the cross-border conditions in case one UE is used. In that case a complete RF loss happens for a while. The recovery time for the UE when getting attached to the other 5GC is usually less than 35s, which provides an indication for the field tests of WP5-FR.

5.1.4 Iperf uplink test and Attenuation impact

This test is also useful for the performances in terms of data rate for TOBA-K in n39, with changing radio conditions. An Iperf session of 100 seconds is launched on TOBA-K.

The set-up used for this test is the following:

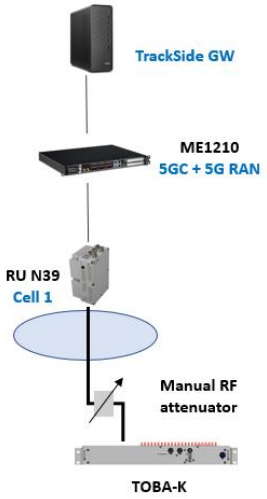


Figure 53: TOBA-K throughput performance evaluation test setup (Ref. D4.3)

The results below correspond to the WP4 configuration with 7 DL slots and 2 UL slots in n39 TDD, when in degraded conditions of 106dB, the data rate is 660kb/s. So, for WP5-FR where remote vision, which is more bandwidth demanding will be used, this gives an indication to increase the UL slots.

Path Loss (dB)	Uplink Data Rate (kb/s)	Jitter (ms)
66	2780	2.6
76	1200	6.7
86	880	9.1
96	830	9.2
106	660	12.4
115	Communication Lost	

Table 6: Uplink data rate according to Path Loss with TOBA-K on N39 (Ref. D4.3)

5.1.5 Iperf uplink with speed and fading impact

This test aims at checking simulated speed and fading impact on uplink data rate, using Vertex simulator tool.

- Test consists in launching Iperf client on TOBA-K while Iperf server runs on Trackside Gateway. The objective is to monitor the uplink throughput when changing simulated speed with fixed pathloss conditions to 105 dB.
- The considered speed change is between 10-50Km/h. For each speed value, an Iperf session of 100 seconds is launched. We do not consider higher train speeds as WP5-FR runs, correspond to this speed range.

The table below demonstrates that speed at this range is not impacting the data rate

Path Loss (dB)	Fading Model	Speed (km/h)	Uplink Data Rate (kb/s)	Jitter (ms)
105	GSM TU 12 path	10	320	23.6
105	GSM TU 12 path	20	320	25.5
105	GSM TU 12 path	30	290	28.8
105	GSM TU 12 path	40	300	25.8
105	GSM TU 12 path	50	280	24.8

Table 7: Impact of speed on Uplink data rates (Ref. D4.3)

5.1.6 RTD measurement and RF attenuation impact

The purpose of this test is to check if the attenuation might have an impact on the round-trip delay. Ping is done towards the P-CSCF as it is the entry point of many procedures where delay matters (IMS registration for instance). Attenuation is performed using RF attenuators.

The following table shows that there is no impact.

Path Loss (dB)	RTD (ms)
68	52
78	47
88	50
97	50
105	45

Table 8: Results of RTD measurement test with RF attenuation (Ref. D4.3)

5.1.7 Forcing the attachment of 5G modem to the network

The following situations were observed with the modem, where the usage of specific AT commands was necessary:

- The modem is attached but cannot automatically retrieve PDP context. This situation can be resolved via AT command: **cgact= »ci »,1**
- Sometimes, even though the modem recognizes the 5G coverage, it doesn't succeed attachment. The following AT commands force the registration, as an example:
  - **AT+CREG=1**
  - **AT+COPS=1,2, »20890 »**
- Also, the following command seemed efficient enough in cross-border conditions: **AT^SET_PLMN=208,90** ou **208,85**, this command was very useful for a quick reconnexion when changing PLMN, e.g., in case of cross-border with one UE.

6 TESTING OUTCOMES IMPACTING SPECIFICATIONS (FRMCSv1 as well as3GPP R18 AND BEYOND)

The following table summarizes all the domains where 5GRAIL activities have impacted specifications:

							Impacted specifications		
Domain	**Impact**	**Description**	**Context**	**Issue resolved**	**WP involved**	**Partner**	**UIC-FRMCS specs**	**3GPP specs**	**ETSI specs**
Functional alias	Core network, MCX	Call restriction based on subparts/elements of functional alias	Existing call restriction is based on source and destination MCX User identities (including functional alias(es)). It is not allowed to deny/permit calls based on subpart/elements of functional alias(es) of MCX Users.	The proposed changes allow call restriction based on subparts/elements of functional aliases.	5GRAIL-WP3	Nokia		CR S1-221238, TS 22.280 - CR 0152	

			An example of a Railway functional alias of an MCX User is a specific driver on a specific train assigned to a particular Railway organization. An example of a subpart/element of a functional alias of MCX Users is their role e.g., all train drivers.						
Location information and clarification of location terms	Radio Access Network, Core Network, MCX	Additional parameters for Location Information and clarification of Location terms	Position of an MCX UE can be described by various means e.g., geographic coordinates, 3GPP-based location information (e.g., serving cell of an MCX UE), velocity and direction of an MCX UE, but also using location labels such as a railway track area (as required in clause 6.4 of TR 22.989). Allowed formats for	Railways and other verticals' needs are not fully covered	5GRail - WP3	Nokia		CR S1-221239, TS 22.280 - CR 0153	

			Location information have to be described. In addition, clarification is required on definitions of Location vs Location information (the latter is extensively used in TS 22.280).						
FRMCS - GSM-R interworking	Core network, MCX, GSM-R MSS, IWF	Coexistence of FRMCS - GSM-R	During migration from GSM-R to FRMCS railway tracks will be covered with both technologies. Establishing a voice group call (especially an emergency call) in one domain should trigger a corresponding group call in the other domain. The innovation is beyond current standard, it triggers by interworking of the FRMCS MCX Server with a GSM-R MSS System the setup of	Allows group calls and emergency voice calls between FRMCS and GSM-R users	5GRail - WP3	Nokia			ETSI TS 103 792

			group calls with the possibility of communication between UEs of both domains. The IWF function can be realized in different deployment schemes, it maps 3GPP MCX messages from FRMCS/MCX domain to GSM-R messages. In the project the IWF is integrated in the GSM-R MSS						
MCdata-IPconn	Session establishment	GRE key negotiation	If GRE over IP is used, how to negotiate the GRE key to be used between both ends of the tunnel?	Rel 17 seems to require GRE over UDP and cancels the need of GRE key.	5GRAIL - WP2	Alstom		TS 24.282; TS 24.582	
MCdata-IPconn	Session establishment	SDP content and DIAMETER request for QoS	Which TFT filters to be used to trigger a request for dedicated bearer/QoS flow for an MCdata-Ipconn session? How to transmit the corresponding information to the		5GRAIL - WP2	Alstom		TS 24.282; TS 24.582	

			MCx AS which perform the request to the PCRF/PCF? With GRE over IP, no TCP/UDP ports possible; DSCP value could be used but it needs to be transmitted and understood by the MCx AS. With GRE over UDP, use of UDP ports are possible but the mechanism to build the DIAMETER request from an IPconn SIP INVITE is not tackled						
MCdata-IPconn	User Plane	GRE tunnels: end to end between both clients, or endpoints at each involved MCx AS (participating and controlling)?	Rel 16 seems to let implementation dependant details; tunnels can be "end to end" or hop by hop through MCx AS.	Rel 17 seems to require endpoints at each involved MCx AS. It is not what has been implemented in 5GRAIL.	5GRAIL - WP2	Alstom		TS 24.282 ; TS 24.582	

Local binding		WebSocket over TLS vs http2			5GRAIL - WP2	Alstom	FFFIS/TOBA		
Registration/authentication	Call flow (SIP REGISTER/SIP PUBLISH)		SIP PUBLISH: no need to wait for access token with for SIP registration		5GRAIL - WP3	Nokia	FIS		
MCdata-Ipconn - Ipconn Session termination	Session termination	After a connection loss and recovery, how to notify the other "side" of the session?	Considering an Mcdata-IPCONN session between client A and client B. If client A loses the connection and retrieves it (potentially after changing of IP address), how MCx AS will be informed and what will be notified to the other side (client B). A solution could be that the client A has to deactivate and reactivate SIP registration and MCData authorization (e.g., send a SIP		5GRAIL - WP2	Alstom	SRS		

			PUBLISH with expire=0; then a SIP PUBLISH with a normal expire), then the MCx AS would terminate the related remaining sessions to client B. This behavior has to be specified.						
WebSocket vs HTTP2			These tests allowed to raise some new issues in the OBapp API interoperability (not detected with ATO tests because the dynamic used for ETCS application is not the same). For example, ETCS-OB monitors the local WebSocket connection using the native ping/pong mechanisms (see RFC 6455 for WebSocket specifications) with a timeout at 500ms. Sometimes, the OB_GTW-K took too long time to answer		5GRAIL - WP2	Alstom	SRS		

			to the ping monitor message, and ETCS-OB closed the connection accordingly. The situation has been improved on OB_GTW-K and the issue has disappeared. Such a timing performance should have been specified between applications and gateway.						
MCdata-Ipconn - Multipath	Session management		Phase 2.3 tests allowed to raise the difficulty to implement a multipath based on several MCData-IPconn sessions in parallel. The use of SIP forking was initially tried, but this is not compliant with the MCx server. Then, another solution using multiple clients (with different		5GRAIL - WP2	Alstom	SRS		

			MCdata ID, and SIP URI) was implemented. After several attempts and SW modifications, a final version for Phase 2.4 was released end of December to improve Multipath feature. A minor update was done end of January (no impact on the applications), then it corresponds to the final version of OB_GTW-A and TS_GTW-A software for 5GRAIL.						
Location update	REC, Location dependent calls (?)		The MCX Server is sending a SIP MESSAGE of Entering Geographic Area after every SIP MESSAGE from the client with such GPS coordinates (i.e., every 30 seconds). 3GPP TS 24.379 version 17.9.0		5GRAIL – WP3	Nokia		3GPP TS 24.379 version 17.9.0	

			suggests it should send the message only on Entry Into such an area, not repeatedly whilst in the same area. This currently has the knock-on effect of our client re-affiliating the group id. Whilst these do not affect the functioning of the system, this implies a waste of network traffic. Regarding the latter, the client can be more discerning and not re-affiliate a group if it already is affiliated.						

7 CONCLUSIONS

The purpose of D1.2, as defined in the GA was to summarize the observations and outcomes of lab testing in the scope of WP3 and WP4 with the intention to correct/improve FRMCS V1 specifications targeting the next step, which is FRMCS V2 specifications and the associated field testing (e.g., MORANE2). This purpose is achieved and moreover 5GRAIL has in some cases even guided instead of validating FRMCS V1 specifications, as labs have performed many pre-standard implementations. To this, can be added CRs and discussions that have impacted 3GPP and ETSI specifications.

5GRAIL contributed to understand a set of issues of the first FRMCS architecture. Thanks to that, the project supported the equipment providers to first create and during the project lifetime to improve their prototypes. Moreover, an excellent collaboration between the partners was developed, towards a common target which is the FRMCS 1st edition deployment success, also considering coexistence period with GSM-R

When it comes to the border-crossing topic, which is considered as one of the very important topics of the project, it is worth mentioning that 5GRAIL is probably the only project trying to reproduce in lab and field (even in the commercially operational field testbed of SNCF) almost the real cross-border conditions, involving critical railway applications, supported by **3GPP MCX building blocks, in the early stages of 5GSA deployment.** Based on that and the issues raised, 5GRAIL has clearly identified the axes of improvement, to make the FRMCS completely cross-border interoperable.

The following table summarizes some of the 5GRAIL findings:

Domain	5GRAIL outcome description
OBapp API	• Maximum time to answer API request needs to be specified. • OB_GTW shall supports **session_start** request under a non-coverage area, when the MCX clients is not registered yet.
SIP/MCX addressing	• Secure update and storage of credentials • Multipath implementation solution (at service or transport layer) implies a slightly different MCX/SIP addressing. • SIP Proxy is needed for tight coupled applications
REC	Pre-standardized REC implementation, server based, using location criterion
QoS	In the absence of PCF, usage of DSCP method to map the application comm_profile
Bearer flex	• Multipath implementation either in the transport or service level for Kontron or Alstom GTW respectively • Multiaccess using two subbands of n78 with different bandwidth capabilities (WP3 lab and WP5-DE field testing
Cross-border	• Pre-standardized implementation of cross-border with two UEs • Inter-gNodeB handover via AMF

IWF	Usage for group call and REC GSM-R FRMCS transition test case
Cybersecurity	• For the control plane: local binding over TLS. • For the user plane: TLS at application layers (E2E TLS) with ATO application • Two additional method studied
n39	Testing of n39 radio capabilities with TOBA-K

We encourage the reader to go through the deliverable and realize how the outstanding work performed in each lab has validated the FRMCS principles and contribute to a future improvement of them. The lab outcomes will be completed by the field-testing outcomes, captured in the upcoming D1.4 document.

8 REFERENCES

id	DOCUMENT TITLE	REFERENCE, VERSIONS
[1]	FRMCS User Requirements Specification,	FU-7100
[2]	FRMCS Use cases	MG-7900
[3]	FRMCS Functional Requirement Specification (FRMCS FRS)	FU- 7120
[4]	System Requirements Specification (FRMCS SRS)	AT- 7800
[5]	Study on Future Railway Mobile Communication System, Stage 1 (Release 16 & Release 17)	3GPP TR22.889 V17.4.0 3GPP TR22.889 V16.6.0
[6]	Technical Specification Group Services and System Aspects, Mission Critical Services over 5G System, Stage 2 (Release 17)	3GPP TS 23.289 V1.0.0
[7]	Technical Specification Group Services and System Mission Critical Services Common Requirements (MCCoRe) Stage 1 (Release 17)	3GPP TS 22.280 V17.4.0
[8]	Technical Specification Group Services and System Aspects Mission Critical Push to Talk (MCPTT) Stage 1(Release 17)	3GPP TS 22.179 V17.0.0
[9]	Technical Specification Group Services and System Aspects Mission Critical Data services Release 16	3GPP TS22.282 V16.4.0
[10]	Group Services and System Aspects Security of the Mission Critical (MC) service (Release 17)	3GPP TS 33.180 V17.2.0
[11]	Technical Specification Group Services and System Aspects System architecture for the 5G System (5GS) Stage 2(Release 17)	3GPP TS 23.501 V17.0.0
[12]	Technical Specification Group Services and System Aspects. Mobile Communication System for Railways Stage 1(Release 17)	3GPP TS22.289 V17.0.0

[13]	Technical Specification Group Services and System Service requirements for the 5G system Stage 1 (Release 18)	3GPP TSTS22.261 V18.2.0
[14]	ETSI- Study on FRMCS System Architecture	ETSI TR 103 459 V1.2.1 (2020-08)
[15]	ETSI-GSM-R/FRMCS Interworking	ETSI TR 103 768 V0.0.4 (2021-062)
[16]	D2.1 TOBA Architecture report	REV3 – 31/01/2023
[17]	D3.1 First Lab Integration and Architecture Description	13/09/2021 – v1 31/03/2022 – v2
[18]	D4.1 Second Lab Integration and Architecture Report	14/09/2021 – v1 25/03/2022 – v2
[19]	Grant Agreement number: 951725 — 5GRAIL — H2020-ICT-2018-20 / H2020-ICT-2019-3	
[20]	D3.2 First Lab Setup Report	28/02/2022 - v1 30/06/2022 – v2
[21]	D4.2 Second Lab Setup Report	25/02/2022 – v1
[22]	Functional Interface Specification	FIS – 7970
[23]	Form Fit Functional Interface Specification	FFFIS-7950
[24]	ERTMS/ETCS GSM-R Bearer Service Requirements	Subset 093 – v4.0.0
[25]	Radio Transmission FFFIS for EuroRadio	V13.0.0
[26]	Subset-037	v3.2.0
[27]	Functional architecture and information flows to support Mission Critical Push to Talk (MCPTT); Stage 2 - (Release 17)	3GPP TS 23.379 v17.8.0

[28]	Mission Critical Push To Talk (MCPTT) media plane control; Protocol specification	3GPP TS 24.380 v17.6.0
[29]	Subset 126 – Appendix A	Issue: 0.0.10
[30]	D1.1 Test plan	RV4
[31]	D4.3 Second Lab Test report	RV1
[32]	Technical Specification Group Services and System Mission Critical Services Common Requirements, Stage 2 (Release 17)	3GPP TS23.280 v17.9.0
[33]	Technical Specification Group Core Network and Terminals Mission Critical Data (MCData) signalling control Protocol specification (Release 17)	3GPP TS24.282 v17.9.0
[34]	Technical Specification Group Core Network and Terminals. Mission Critical Push To Talk (MCPTT) call control; Protocol specification (Release 17)	3GPP TS24.379 v17.11.0
[35]	Technical Specification Group Services and system Aspects; Policy and charging control framework for the 5G System (5GS) Stage 2 (Release 17)	3GPP TS23.503 v17.9.0
[36]	Cross-Working Group Work Item: Network Reselection Improvements (NRI) – 5GAA Automotive Association Technical Report	V1.0
[37]	D3.3 First Lab Test report	RV1
[38]	Inter-PLMN Mobility Management Challenges for Supporting Cross-Border Connected and Automated Mobility (CAM) Over 5G Networks. K. Trichias, P. Demestichas, N. Mitrou	5G-MOBIX, Journal of ICT Standardization, Vol.9_2

9 APPENDICES

NOTE: The information of this chapter provides some insights to understand the state of the art of UIC and 3GPP specifications as well as the outcome of other CAM projects for crucial topics such as: a**) Pre-standard Railway Emergency Call b) Bearer Flexibility in 5G c) Border-crossing.** Many parts can also be found in D3.3v2 but are repeated in this document for the reader to avoid using many documents in parallel.

9.1 Railway Emergency Call – FRMCS – FIS V1 Specification options

UIC FIS evaluated the following 4 options for V1 in UIC FIS specifications:

	Option 1	Option 2 Option 2A and Option 2B	Option 3	Option 4
Type	Client based approach based on rules based affiliation done by the client	Server based approach. Server sends message to the clients based on rules that trigger the clients to perform an affiliation **Option 2A:** using continuous affiliation/de-affiliation after client movements based on Areas and Roles **Option 2B:** server triggered explicit affiliation of clients based on Area and Roles subsequent to client initiating a generic emergency alert.	User regroup method: Server determines based group and area definition the clients that have to be included in the call). Then originating client performs user regroup and initiates group call using the newly defined group Client based affiliation	Adhoc group method Server based area definition and user determination

The following high level flow diagram is a generic one showing the different phases required to realize a Railway Emergency Call setup fulfilling railway requirements:

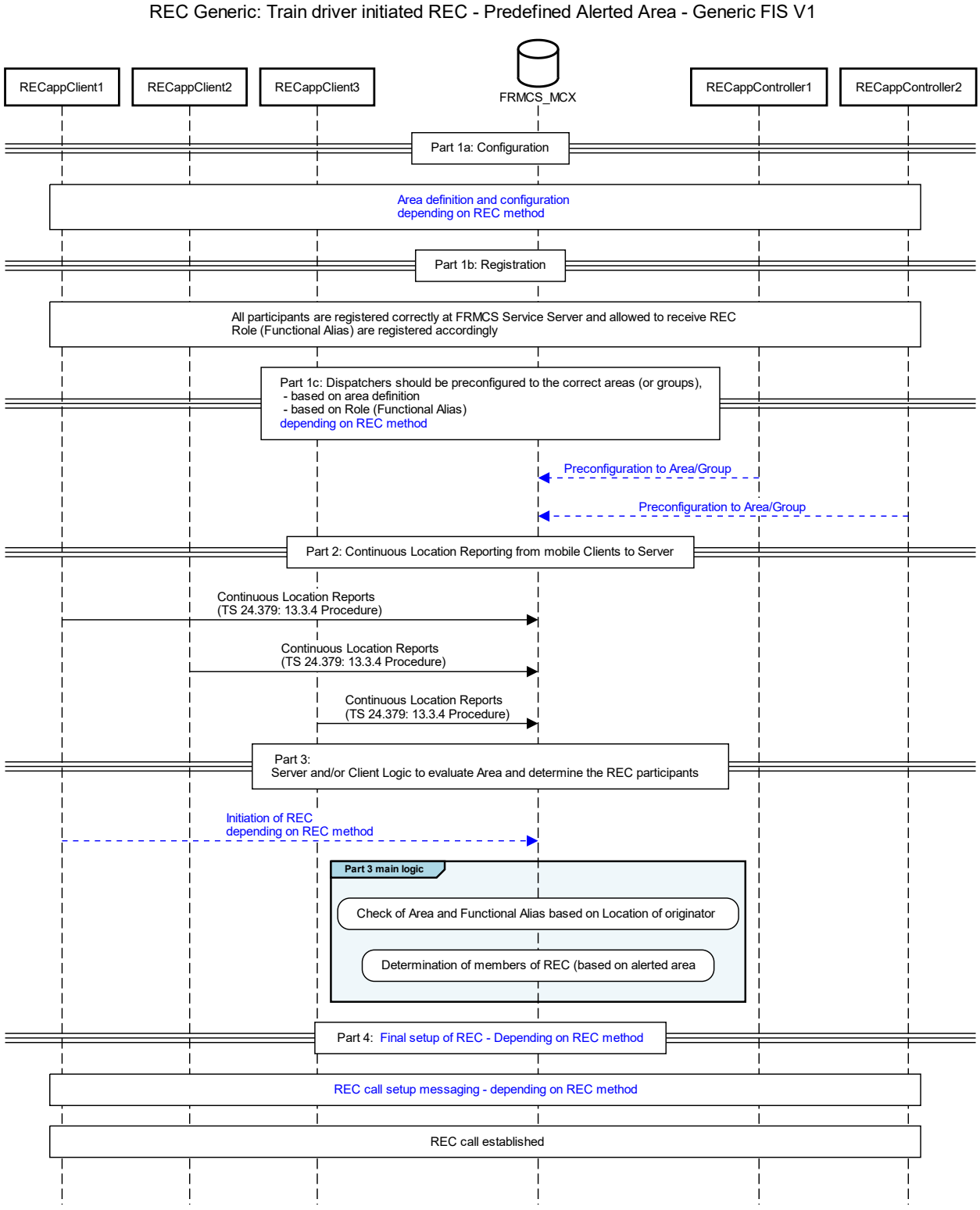


Figure 54: Generic Call Flow for REC

The following steps are described (not supported function in 5GRAIL are marked as strikethrough):

Part 1a: Configuration and Prerequisites

- System is configured with Area definition
- All participants are correctly configured in the FRMCS Service Server (MCX Server)

Part 1b: Registration

- All participants are registered correctly at FRMCS Service Server and allowed to receive REC
- Controller is registered in a controller's identity
- ~~Roles (Functional Alias) have been registered accordingly by all participants~~

Part 1c: Dispatcher configuration

- Dispatchers should be preconfigured/registered to the correct areas (or groups),
    - based on area definition
    - ~~based on Role (Functional Alias)~~
- depending on REC method

Part 2: Continuous Location Reporting from mobile Clients to Server

- All mobile clients shall report continuously their location as per the MCX location rules.
- Thus, the FRMCS Service Server (MCX Server) is aware of current location of all mobile clients.

Part 3: Server and/or Client Logic to evaluate Area and determine the REC participants.

- After initiation of the REC a logic shall
    - Shall check the area based on the location of the originator.
    - ~~Shall check the Functional Alias and associated permissions of the originator.~~
    - Shall eventually determine the members of the REC (based on the above evaluations and the addressed area)

Part 4: Final setup of REC – depending on REC method.

- Initiation of REC call setup signalling – depending on REC method

9.2 Bearer Flexibility in 5G: ATSSS (Access Traffic Steering, Switching & Splitting)

To allow to serve non 3GPP access like Wi-Fi using a 5G SA core network, mediation functionality (e.g., a N3IWF) is needed to map to 5G NSSAP signalling capable to be understood by the 5G Core. Following architecture from 3GPP TS 23.501 shows the concept:

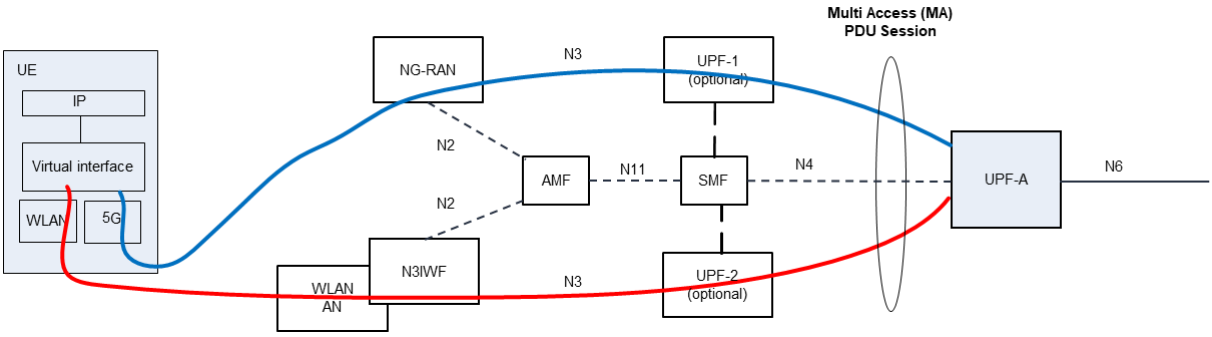


Figure 55: ATSSS architecture

ATSSS (Access Traffic Steering, Switching & Splitting) between one 3GPP access and one non-3GPP access encompasses following functions.

- Access Traffic **Steering** (to one 3GPP access or to one non-3GPP access): Selecting an access network for a new data flow and transferring the traffic of this data flow over the selected access network.
- Access Traffic **Switching** (between one 3GPP access and one non-3GPP access): Moving all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow.
- Access Traffic **Splitting** (between one 3GPP access and one non-3GPP access): Splitting the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access.
- ATSSS considers any type of access network, including untrusted and trusted non-3GPP access networks, wireline 5G access networks.

This is achieved by a Multi-Access PDU Session concept with a new type of PDU session to serve the two accesses. On the establishment of the sessions the UE includes an "MA-PDU capability" indication. User planes are established on each access when possible (either both at same time, or one first and the other when the UE registers to the access).

9.3 Border Crossing in related CAM projects

Horizon 2020 ICT CAM projects as 5GCroCo, 5G Carmen et al have evaluated in detail available measures and potential improvements to improve service continuity for the automotive sector when crossing borders (refer to §8[S36]). It is important to understand that – in contrast to railway – CAM services rely on public operator networks, and thus for automotive sector the cooperation of mobile operator between networks is required, which is expected to be more challenge compared to the cooperation models typically done in railway (where already in GSM-R close cooperation between

railways are in place to achieve seamless interworking ad roaming across Europe (refer to GSM-R ENIR project.

The following steps have been described and partly tested to improve service continuity between different mobile operator PLMNs with respect to the capabilities of the (4G and) and 5G NSA/SA core and radio network:

Scenario in 5G CAM projects	Description
Scenario 1 / Basic	UE roaming with new registration
Scenario 2	UE roaming with AMF relocation (idle mode mobility)
Scenario 3	(Inter PLMN) Handover, relying on NG/N2 based handover

The below architecture shows the two main interfaces where improvements have been evaluated:

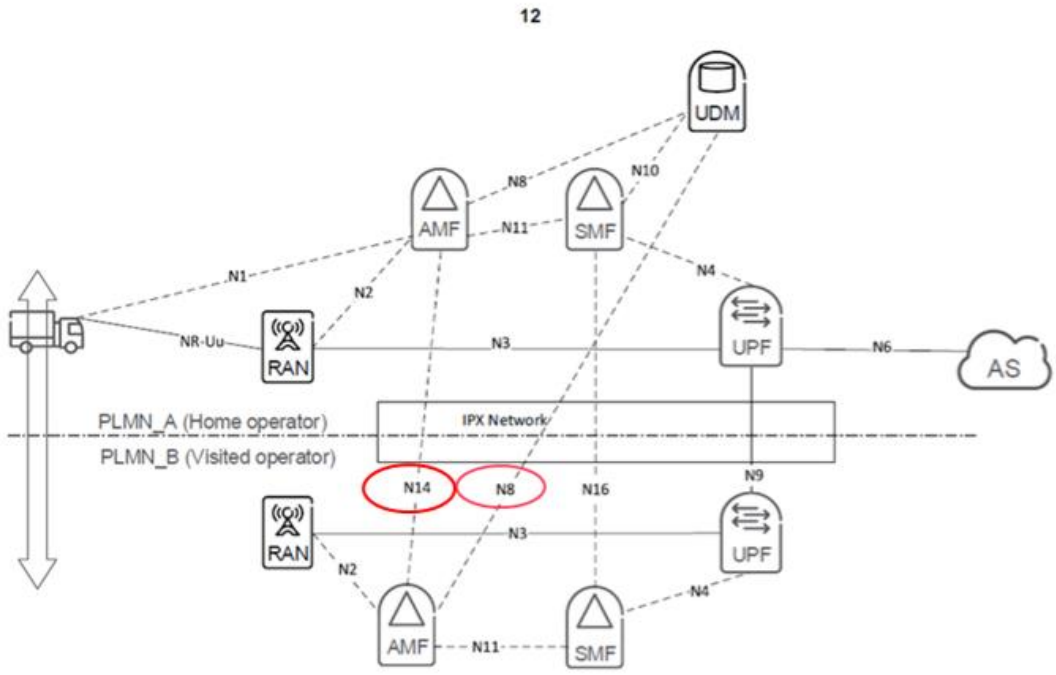


Figure 56 5G SA Reference architecture for cross border evaluations

The following scenarios have been studied:

Scenario 1: UE roaming with new registration.

- Once a UE loses connection with a serving operator, the roaming procedure will take place. As described in [TS23.122], the UE will perform PLMN selection and identify the most suitable PLMN (according to its configuration).
- In any case, the delay to attach to a VPLMN is 100 seconds on average because of the sequential process and the context transfer procedure. In the case of the HPLMN the registration requires significant time as well – in the range of 9 seconds according to the same measurements' analysis.
- This solution is implemented using the N8 interface among the operators and does not require deployment of N14.

Scenario 2. UE roaming with AMF relocation (idle mode mobility)

Following improvements have been evaluated in this scenario:

- Redirecting
  This is addressed by including redirect information in the release message. I.e., the controlling RAN is configured to inform the UE (as part of the release) about available target frequency bands to allow the UE to immediate tune to a carrier (without the need to scan the spectrum).
- Use of the "Equivalent PLMN" function, i.e., the UE is informed about PLMNs it is allowed to use, removing the need for blind attachment attempts.
- Optimizing registration/authentication with the additional roaming interface between AMFs (N14), this interface allows the AMF in the Visited PLMN to fetch the UE context from the source AMF.
- Optimizing the user plane re-established on the new network also using N14 interface, since the new network is made aware of used UPF and UE IP address and that the user plane is re-established as part of the tracking area update in the new network.

Scenario 3 (Inter PLMN) Handover

An additional step to improve roaming would be to support handover, as defined by 3GPP between the networks. In this case, it would involve a core network type of handover, not using Xn between base stations (gNBs) because they are not normally used between networks. In this scenario the above architecture needs to be configured or factor in the handover functions.

In short, the source (controlling) network gets information from the UE about potential handover candidates in the target network, the source network contacts the potential target network and asks for resources. If granted, the source network sends a 'handover command' to the UE with information about the target network, the UE then tunes into and connects to the new network. The PLMNs need to be configured to execute the NG/N2 Handover between gNB and PLMNs.

It is assumed that the 5G scenario can anticipate similar interruption times to 4G, i.e., around 100 ms.

9.3.1 Mechanisms for Improved Mobility management

To support the URLLC functionality over 5G, upgraded MM mechanisms have proposed by 3GPP, to minimize the interruption time introduced by inter-PLMN HO or trying to optimize the data routing through PLMNs for a more efficient resources usage or reduction of end-to-end latencies. These are known as **Session and Service Continuity and Home Routing vs Local Break-Out.**

Session continuity is defined as the capability of a node to maintain its ongoing IP sessions when changing network (different IP address). The simultaneous switching of the application server and host as well, while maintaining full operational capacity for the application is defined as service continuity.

There are 3 types of SSC Modes in 3GPP §9[11] as explained below and presented in the following figure:

- **SSC Mode 1**: With SSC mode 1, the 5G network preserves the connectivity service provided to the UE. For the PDU session, the IP address is preserved. In this case the User Plane function (UPF) acting as the PDU session anchor is maintained (remains same) till the release of the PDU session by the UE.
- **SSC Mode 2:** With SSC mode 2, the 5G network may release the connectivity provided to the UE, i.e., the PDU Session can be released. If the PDU Session is being used to transfer IP packets, then the allocated IP address is also released. It works on break and make framework i.e., PDU session will be release from first serving UPF and then a new PDU session is established at new UPF (break-before-make).
- **SSC Mode 3:** With SSC mode 3, if the Anchor UPF changes but the change procedure will ensure that connectivity is preserved, i.e., connectivity towards the new Anchor UPF is established before releasing the connection to the old Anchor UPF (make-before-break).

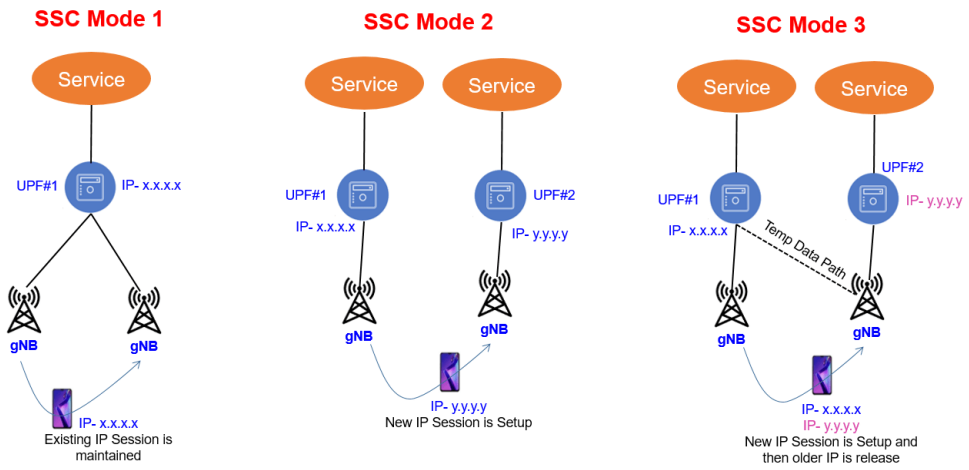


Figure 57 https://www.techplayon.com/ssc-modes-session-and-service-continuity-in-5g/

The following figure presents the Home Routing and Local Break-Out architecture for 5G SA (CAM use case):

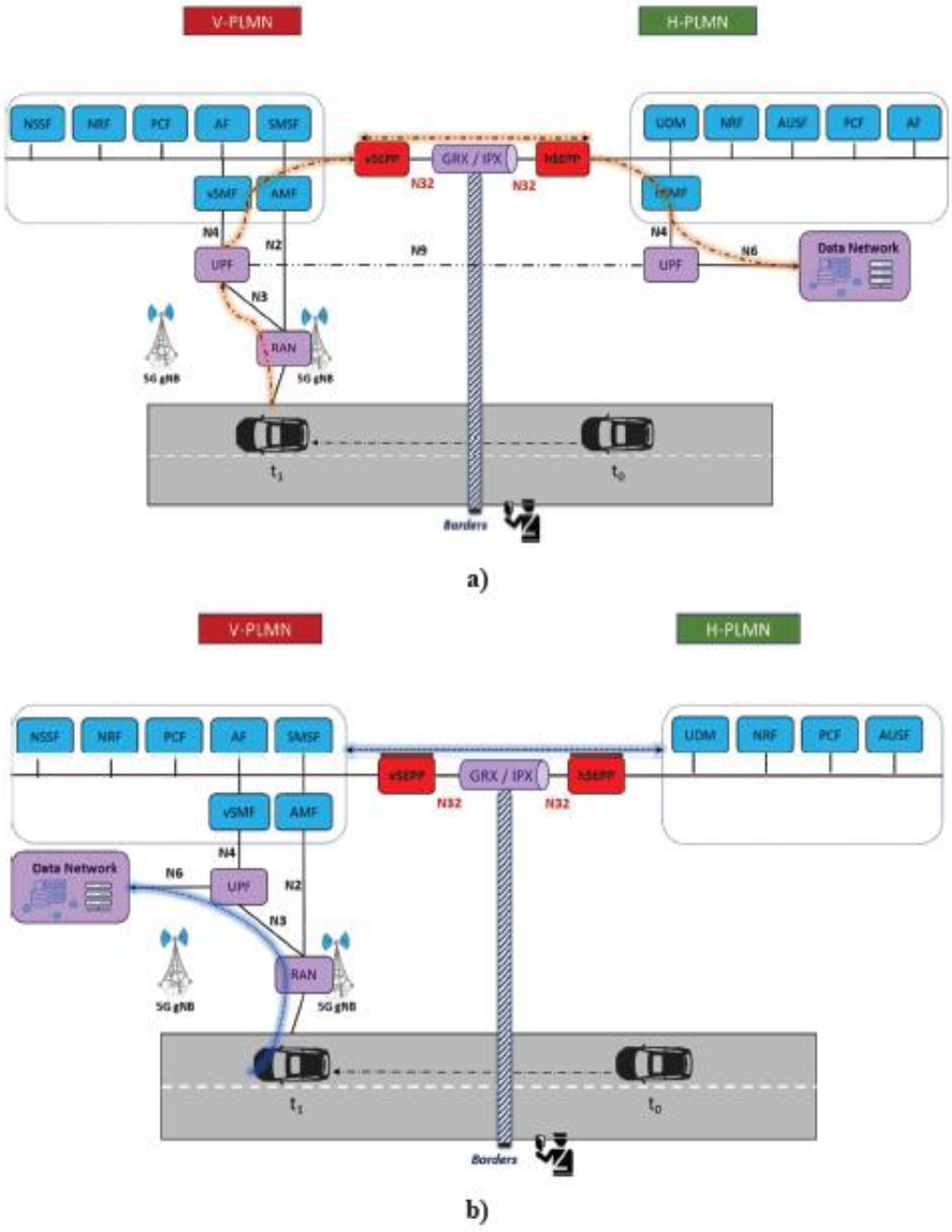


Figure 58 5G SA based roaming architecture with (a) Home-Routing (HR) and (b) Local Break-Out (LBO) (Ref. §9 [38])

In **Local Break Out**, roamer uses a visited network UPF to access a Data Network

In **Home Routed**, roamer uses a home network UPF to access a Data Network

Based on the above explanations, in case of 5G SA network deployment from both sides of the borders, the SSC mode 3 seems to be the best solution for cross- border.

When 5GSA will be widely deployed, improvements will appear from the usage of dedicated interfaces, as specified by 3GPP [TS29.573], such as N32 which is used between the Security Edge Protection Proxies (SEPP) of the H-PLMN and V-PLMN during roaming scenarios. The initial handshake between the networks and the negotiation of the roaming parameters to be applied on the actual messages going over the N32 interface, is performed over the N32-c (control plane) interface, which is followed by the N32-f (forwarding) interface, used for communication between Network Functions (NF) of the two networks.

Besides the N32 interface, the N9 interface is also established to facilitate the direct communication among the UPF of the H-PLMN and the V-PLMN. As in LBO mode the SMF and all UPFs sessions are under the control of the V-PLMN UPF, while in HR both instances of the SMFs and UPFs are utilized, the N9 reference point for user plane traffic is only applicable to the HR scenario. Both the N32 and N9 interfaces, depicted in the above in figure aim to facilitate the direct communication among the necessary two neighboring PLMNs and as such streamline the roaming process between two 5G SA networks, improving the experienced QoS and the relevant KPIs.

Grant agreement
No 951725