Deliverable D4.2

Second Lab Test Setup Report

Grant agreement
No 951725

5GRAIL

5G for future RAILway mobile communication system

D4.2 Second Lab Test Setup Report

Due date of deliverable: 31/12/2021

Actual submission date: 27/02/2023

Leader/Responsible of this Deliverable: KONTRON

Reviewed: Y

Document status		
Revision	**Date**	**Description**
0.1	17/02/2022	Draft Version
0.2	22/02/2022	Update from WP leader based on comments from members of the consortium
1.0	25/02/2022	Consolidation of the first deliverable version
2.0	26/08/2022	Update from WP leader based on latest lab integration tests
3.0	30/01/2023	Update based on last lab integration tests and comments from reviewers

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	✓
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

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

Executive Summary

The purpose of this deliverable titled “D4.2 – Second Lab Test Setup Report” is firstly to give details on the network integration of the various components provided by WP4 collaborating suppliers: While Kontron is in charge of the setting of the whole telecommunication network, including 5G, Alstom and Thales respectively had to interconnect ETCS/ATO and PIS equipment’s onto it. This report will provide information on how these tasks have been achieved and will also give all the details on the current lab setup.

This report will then shed light on the integration of the first WP2 FRMCS Gateways into the network. WP2 prototypes providers, namely Kontron and Alstom, were indeed able to deliver their first OB and TS Gateways modules to WP4 team. As it will be described later in this document, WP4 dedicated Gateways were then in place in the lab and some end to end integration tests could be done with OB and TS Gateways.

Finally, having explained the integration of these various elements, a perspective on foreseen tests setup will be given by explaining how the different scenarios and use cases defined by WP1 will be tested in WP4 lab, with a time plan for these lab trials.

To conclude, it has to be noticed that a phased approach has been privileged for this D4.2 document due to some constraints that induced delay in the availability and test of some WP2 deliveries and some WP4 lab components. This third version is the final one as it includes all information that could be provided by WP2 team.

Abbreviations and Acronyms

Abbreviation	Description
3GPP	3rd Generation Partnership Project
5G NSA	5G Non StandAlone
5G SA	5G StandAlone
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programmable Interface
AS	Application Server
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATSSS	Access Traffic Steering, Switching and Splitting
BBU	Base Band Unit
BIOS	Basic Input Output System
BSC	Base Station Controller
BTS	Base Transceiver Station
CAM	Connected and Automated Mobility
CCS	Control Command and Signalling
CCTV	Closed Circuit TeleVision
CP	Control Plane
CPU	Central Processing Unit
CSCF	Call/Session Control Functions
CSFB	Circuit Switched Fall Back
DC	Direct Current
DMI	Desktop Management Interface
DMZ	Demilitarized Zone
DN	Domain Name
DNS	Domain Name System
DRCS	Data Radio Communication System
DSD	Driver Safety Device

E2E	End To End
EDOR	ETCS Data Only Radio
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EU	European Union
EVC	European Vital Computer
FDD	Frequency Division Duplexing
FFFIS	Form Fit Functional Interface Specification
FIS	Functional Interface Specification
FRMCS	Future Railway Mobile Communication System
FRS	Functional Requirements Specification
FW	Firewall
GA	Grant Agreement
GBR	Guaranteed Bit Rate
GCG	Ground Communication Gateway
GNSS	Global Navigation Satellite System
GoA	Grade of Automation
GRE	Generic Routing Encapsulation (RFC8086) -> Tunnel GRE
GTW or GW	GaTeWay or GateWay
HDMI	High Definition Multimedia Interface
HLR	Home Location Register
H2020	Horizon 2020 framework program
HSS	Home Subscriber System
HW	Hardware
IMPI	IP Multimedia Private Identity
IMPU	IMS Public User Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IWF	Inter Working Function

JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LAN	Local Area Network
LED	Light Emitting Diode
LTE	Long Term Evolution
MCC	Mobile Country Code
MCG	Mobile Communication Gateway
MCPTT	Mission Critical Push To Talk
MCx	Mission Critical Voice/Data/Video
MGW	Media Gateway
MIMO	Multiple Input Multiple Output
MMI	Man Machine Interface
MNC	Mobile Network Code
MNO	Mobile Network Operator
MPTCP	MultiPath Transmission Control Protocol
MQTT	Message Queuing Telemetry Transport
N3IWF	Non-3GPP Inter Working Function
NR	New Radio
NSA	Non-Stand Alone (5G Core architecture)
OAM	Operation Administration Maintenance
OB	On Board
OB_GTW	On-Board Gateway
OBA	On-Board Application (e.g. ETCS on-board, ATO on-board)
OBU	On-Board Unit
OM	Operation & Maintenance
OMC	Operation & Maintenance Centre
OTA	Over The Air
OTT	Over The Top
PCB	Printed Circuit Board

PCRF	Policy and Charging Rules Function
PCU	Packet Control Unit
PDN	Packet Data Network
PIS	Passenger Information Service
PSS	Process Safety System
PTT	Push To Talk
QoS	Quality Of Service
RAM	Random Access Memory
RAN	Radio Access Network
RAT	Radio Access Technology
RBC	Remote Block Centre
REST	REpresentational State Transfer
RPC	Remote Procedure Call
RF	Radio Frequency
SA	Stand Alone (5G Core architecture)
SDWAN	Software-Defined Wide Area Network
S-CSCF	Servicing-CSCF (Correspondence IMPU - @ IP)
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMA	Subminiatures version A, type of coaxial RF connectors
SRS	System Requirements Specification
TCMS	Train Control Management System
TCN	Train Communication Network
TCU	TransCoder Unit
TFT	Traffic Flow Template
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
UP	User Plane
URLLC	Ultra-Reliable Low-Latency Communications (5G)
URS	User Requirements Specification
VPN	Virtual Private Network
WP1	Work Package 1
WP2	Work Package 2
WP3	Work Package 3
WP4	Work Package 4
WP5	Work Package 5

CONTENTS

Table of figures

List of tables

1 INTRODUCTION

Within 5Grail project, WP4 lab can be seen as a place for validation of WP2 deliveries and preparation of WP5 field tests. While the latter is taken into account by WP1 in choosing the right derisking tests cases to be executed in WP4, the former appears clearly when considering Figure 1 :

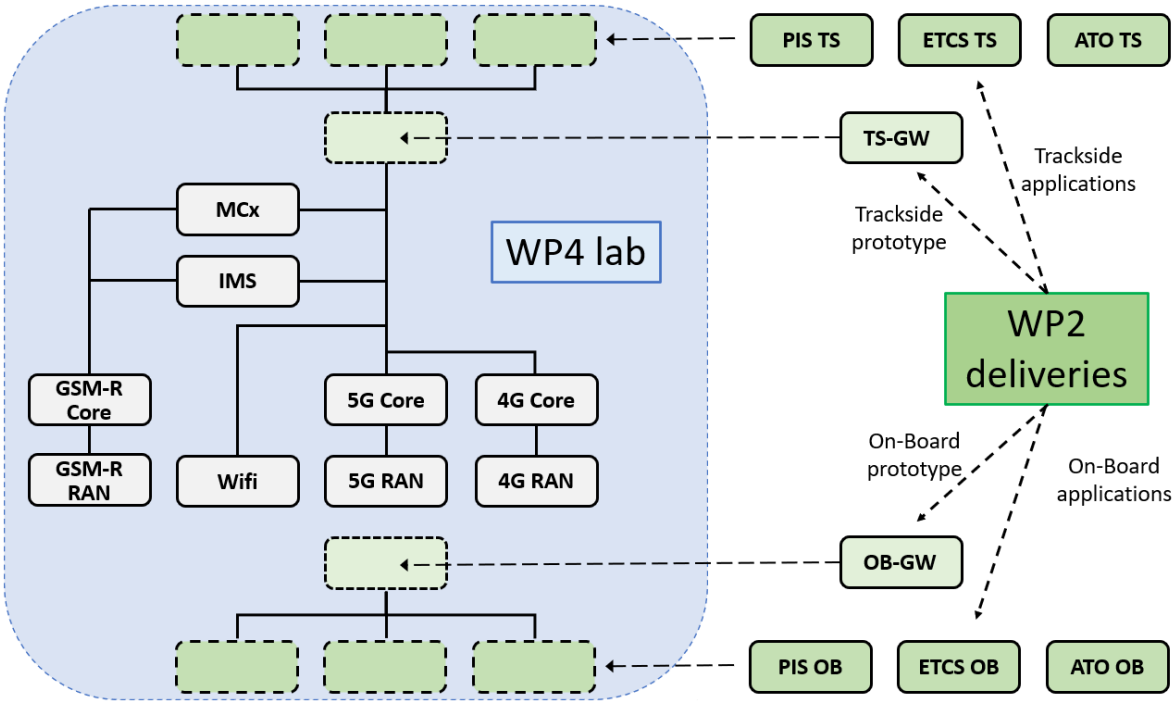


Figure 1: WP2 deliveries mapping into WP4 lab

On that picture, we can see that WP4 lab is composed of an hybrid telecommunication network (5G, 4G, Wi-Fi, GSM-R), fitted with an upper IMS/MCx service, on which FRMCS Gateways can be inserted. These On-Board and Trackside Gateways, developed by Alstom and Kontron, use the telecommunication part to communicate with each other according to the FRMCS standards.
Besides, some railway applications use the FRMCS Gateways in order to provide a specific service: PIS, ETCS and ATO. These applications, located On-Board or Trackside, communicate with the Gateways respectively through the FRMCS OBapp and TSapp interfaces. They are also part of WP2 deliveries and in a sense, they also find in WP4 lab a place for end-to-end validation.

WP4 lab design has been described in D4.1 document [S20], and especially which hardware will be used and how the network should be set-up. For its part, D4.2 document shows, among others, how the lab has been actually built and which integration tests have been performed in order to ensure that work package is on track for the next step, i.e. lab execution of the WP1 test cases assigned to WP4.
To be more precise, 5GRail Grant Agreement defined the objectives of D4.2 delivery as follow:

"This report outlines the lab setup and details the different lab test phases for each application and TOBA based on WP1 definition. It documents the work done and details the achieved results for the integration of prototypes into the 5G infrastructure and the validation of the communication capabilities in the lab environment in line with the lab test strategy document elaborated in WP1. "

D4.2 document should then address several topics:

- Show how the different elements of WP4 lab (telecommunication network, FRMCS gateways, FRMCS applications) have been put in place,
- Explain how the integration of these elements have been done to ensure the right behaviour,
- Give details on how WP4 lab will be configured in order to test what is defined in D.1.1 document and provide a planning for execution.

It should be noted that WP2 deliveries spanned over a long period of time and so did WP4 work of integration. This explains that this document used a phased approach with reporting on integration described progressively in v1 and v2 documents. Final version now gives a complete view of this WP4 task, knowing that some late features to be delivered by WP2 will be directly tested in WP4 test phase, with results directly reported in D4.3 document [S21] (multi-connectivity tests on TOBA-K, cross border scenarios).

In order to ease the reading of the document, the following Table 1 can be used when looking for a specific information related to the previous objectives:

Topic	Sections in D4.2 Document	Comment
5G Network setting up	2.1.2 & 2.1.3	
5G Network integration tests	2.1.4	Contains tests with N8, N39 and N78 RUs.
IMS/MCx Network setting up	2.2.1	
IMS/MCx Network integration tests	2.2.2	
GSM-R Network setting up	2.3.1	
GSM-R/MCx hybridation integration tests	2.3.2	
4G Network setting up	2.4.1	
4G Network integration tests	2.4.2	
Wi-Fi Network setting up	2.5.1	
Wi-Fi Network integration tests	2.5.2	
5G SA smartphone integration tests	2.2.22.1.4.4	
Integration testing with N39 modem	2.1.4.1	When ES3 modem was delivered by WP2
QoS management in 5G	2.1.4.3	DSCP method is used
5G HO tests	2.1.4.2	
Radio degraded tool setting up	6.1.3	
Protocol analysers setting up	6.1.1	

PIS application setting up	3.1	Describes hardware and software used to provide PIS TS and OB applications and the way it has been connected to WP4 lab
PIS integration tests	3.2	
ATO and ETCS applications setting up	4.1	Describes hardware and software used to provide ATO and ETCS TS and OB applications and the way it has been connected to WP4 lab
ATO and ETCS integration tests	4.2	
OB and TS FRMCS Gateways of Alstom setting up and integration	5.1	
OB and TS FRMCS Gateways of Kontron setting up and integration	5.2	Includes N39 band testings
WP4 configurations to be used during test phase	6.1	
WP4 planning	9.3	

Table 1: List of topics addressed in D4.2 v3 document

Note that all information that has been recorded during the integration phase has been stored by each partner on a private repository. Traces and logs that are given in this document stand on these repositories.

2 WP4 telecommunication modules set-up and integration

This chapter describes the integration of the telecommunication services of WP4 lab. All the elements, which appeared in green on Figure 2, are provided by Kontron WP4 team and are located in the Montigny office, France.

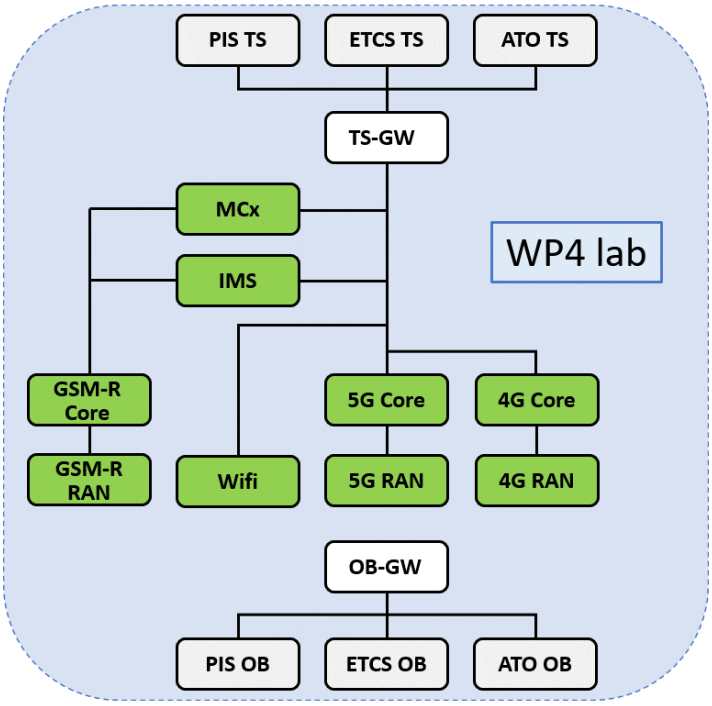


Figure 2: Telecommunication modules of WP4 lab

These telecommunication modules make the communication part of WP4 lab network, in which entities delivered by WP2 can be tested.

2.1 5G Network installation and integration

2.1.1 Introduction

5G network is the main component of WP4 lab as nearly all test cases will use it in the next phases. Indeed, foreseen use cases to be considered express the need to install two 5G networks. It is very important to underline that 5G network must be in Standalone mode (5G SA). 5G SA ecosystem in the industry is currently less rich than for other modes: we for instance discovered that, albeit lots of 5G smartphones available on the market claim to be 5G compliant, 5G SA compliant ones are quite rare (at the end of WP4 we could get only two kinds of them). Available 5G core features also appear progressively and for instance, PCF function was not available; this lead to the use of DSCP method for QoS tests.

As depicted hereafter, WP4 team achieved the setting of these networks and the following sections will describe how 5G RANs and Cores are currently arranged and configured.

2.1.2 5G RAN

2.1.2.1 Frequencies to be used and number of RUs available

5Grail project decided to focus on three 5G frequencies:

- **N8** band around 900 MHz
- **N39** band around 1900 MHz (**FRMCS band**)
- **N78** band around 3.5 GHz

Considering project scope, it is clear that the N39 band is of great interest. WP4 consequently ordered 4 RUs in that band in order to be able to address various radio topologies. It should be noted that these RU does not exist in the market and had then to be especially designed for our purposes. Along with these RUs, WP4 also ordered 4 RUs N8 and 2 RUs N78. Globally 10 RUs have then been installed in WP4 lab, in Montigny France.

Note also that WP4 lab was asked to be used during WP5 french field tests, these ones having to be done in N39 band. WP4 N39 RUs have then to be moved to WP5 location at the end of WP4.

2.1.2.2 CU/DU function and its engineering

As explained in D4.1 document [S20], RU is managed by a CU/DU unit hosted in Kontron *ME1210* product (see Figure 3: Kontron ME1210 product hosts CU/DU function).

Figure 3: Kontron ME1210 product hosts CU/DU function

We have set two CU/DU and consequently, we have two gNodeB in the lab. It is interesting to notice that a CU/DU can be connected to several RUs at the same time. The ME1210 having 4 CPRI optical fibre ports, it is for example possible to have the setup of Figure 4: gNodeB with 4 RUs where a gNodeB with 4 cells is built:

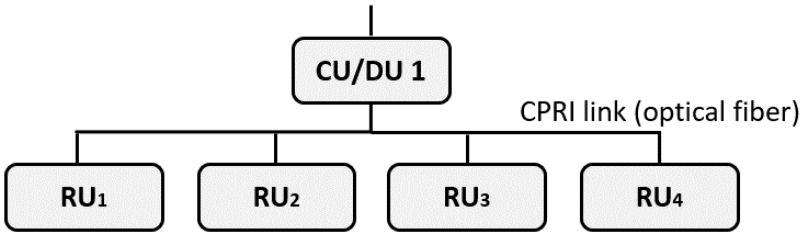


Figure 4: gNodeB with 4 RUs

We have also the possibility to do “drop and insert” configuration in order to have even more RUs connected to CU/DU (as shown on Figure 5: gNodeB using 4 RUs in chain configuration). This topology fits very well railways operator’s needs as more suitable for linear coverage. With Kontron ME1210, the chain can gather up to 4 RUs on the same CPRI port.

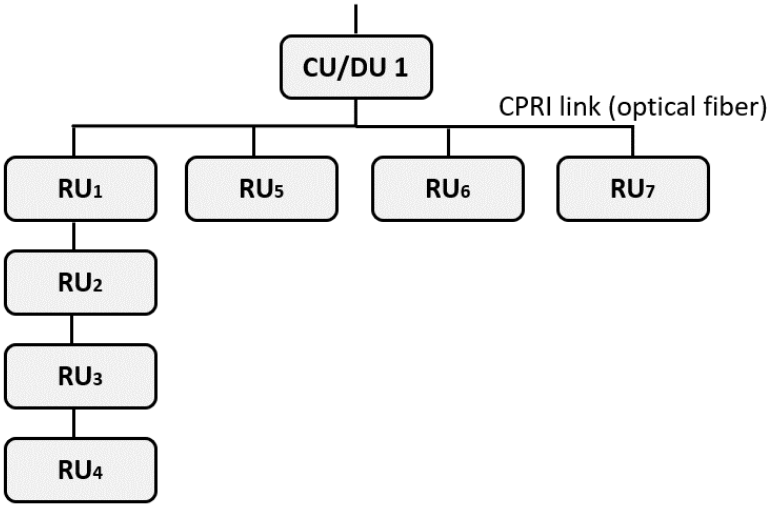


Figure 5: gNodeB using 4 RUs in chain configuration

Considering RUs that can be used under the same Kontron ME1210, there is no specific limitation so that hybrid configurations, where we have for example N8 and N39 RUs under the same gNodeB, are feasible.

2.1.2.3 Radio link: direct cabling and Faraday cage

In field conditions, RU is linked to an antenna that radiates radio signal. However, in lab activities, it is forbidden to use such equipment due to safety and health requirements. Consequently, direct RF cables (see Figure 6: WP4 lab uses direct coaxial cables between RU (left) and OB-GW (right)) must be used between radio modems and RUs.

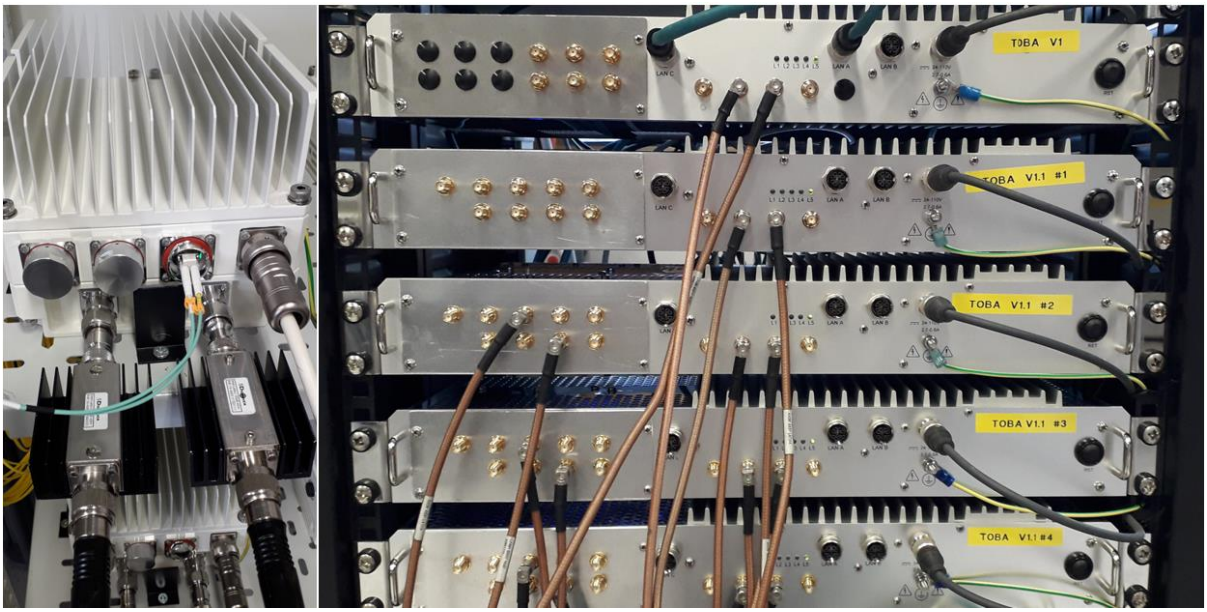


Figure 6: WP4 lab uses direct coaxial cables between RU (left) and OB-GW (right)

Note that a Faraday cage has also been installed in WP4 lab: It will then be possible to put a small antenna and a 5G modem or a smartphone in it (see Figure 7: Antenna and 5G modem in WP4 Faraday cage). Radio link would then be entirely on the air in case some tests would need it.

Figure 7: Antenna and 5G modem in WP4 Faraday cage

In many tests, we used the ES1 Thales modem that was delivered by WP2 team. This modem is shown on Figure 8. Later, ES3 modem was delivered by Thales and could be also tested. ES3 modem is N39 capable.

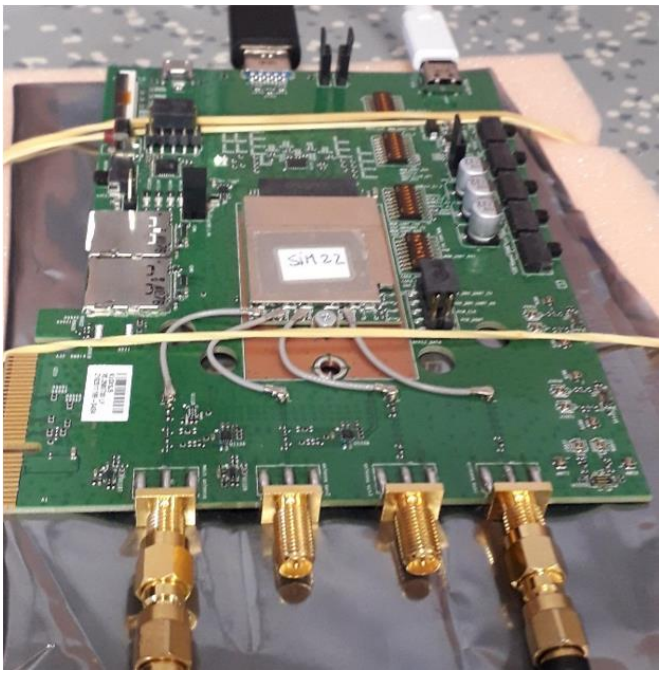


Figure 8: Thales modem ES1

2.1.2.4 Attenuators for handover tests

In order to perform handover tests, manual RF attenuators will be used (see Figure 9: Manual RF attenuator used in WP4 lab). Some specific commands on 5G RAN equipment's can also be launched to force the handover of an UE.

Figure 9: Manual RF attenuator used in WP4 lab

2.1.2.5 Smartphones

It is not essential to have smartphones in WP4 lab as work package focuses on data applications that are provided by WP2 and connected only to air interface through OB-GW. Yet, as Kontron has already a FRMCS MCx voice solution (an Android app in smartphone combined with a MCx AS in core network), some optional tests could be foreseen on that part too and we started looking at 5G SA smartphones.

With collaboration of WP3, led by Nokia, we managed to get a XR20 Nokia smartphone N78 5G SA capable running in the lab. Even if this smartphone can be found easily in the market, the ability to run in 5G SA mode requires a specific firmware and some debug commands for activation. Integration tests of this smartphone with the 5G WP4 network is described in 2.1.4.4. Later in the project, we also had the opportunity to successfully test another smartphone in 5G SA : SONIM XP10. Availability and successful tests with these smartphones was indeed a very good news for WP4 as it enables us to foresee the execution of the optional voice tests defined by WP1.

2.1.2.6 Conclusion

Summary of WP4 5G RAN is shown on Figure 10. Ten available RUs (2 N8, 4 N39 and 4 N78) can be set under the two CU/DU according to test needs. All RUs are installed and powered in racks and adding/removing RU only consists in cabling the right fibre optic for CPRI link connection with CU/DU.

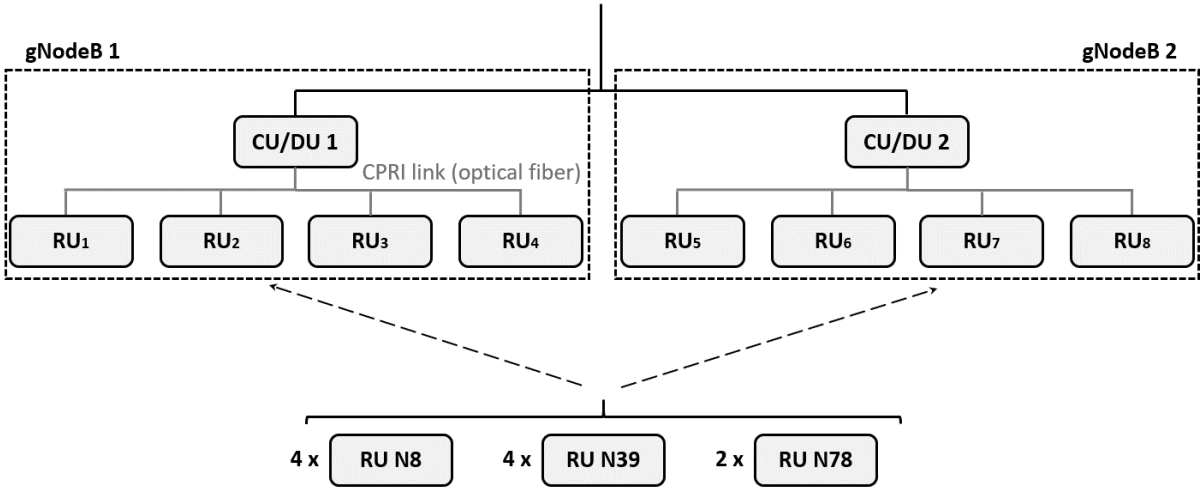


Figure 10: 5G RAN of WP4 lab

For the ergonomic of the platform, in terms of radio connection, all RUs are now connected to a network of RF cables with a cross-connect termination panel. RF attenuators and FRMCS OB Gateways are also connected to that panel in order to trigger handovers as shown on Figure 11. RF connections are then easily possible thanks to the use of this panel.

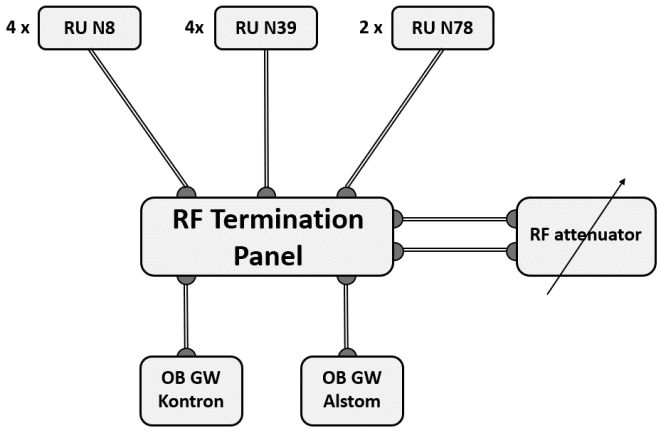


Figure 11: Use of termination panel for easy RF connections

2.1.3 5G Core Networks

2.1.3.1 Functional view

5G Core network application consists in a software that is also installed on the ME1210 Kontron product of Figure 3: Kontron ME1210 product hosts CU/DU function. The functions that are available with the current software level are AMF, SMF, AUSF, UDM and UPF as shown on Figure 12:

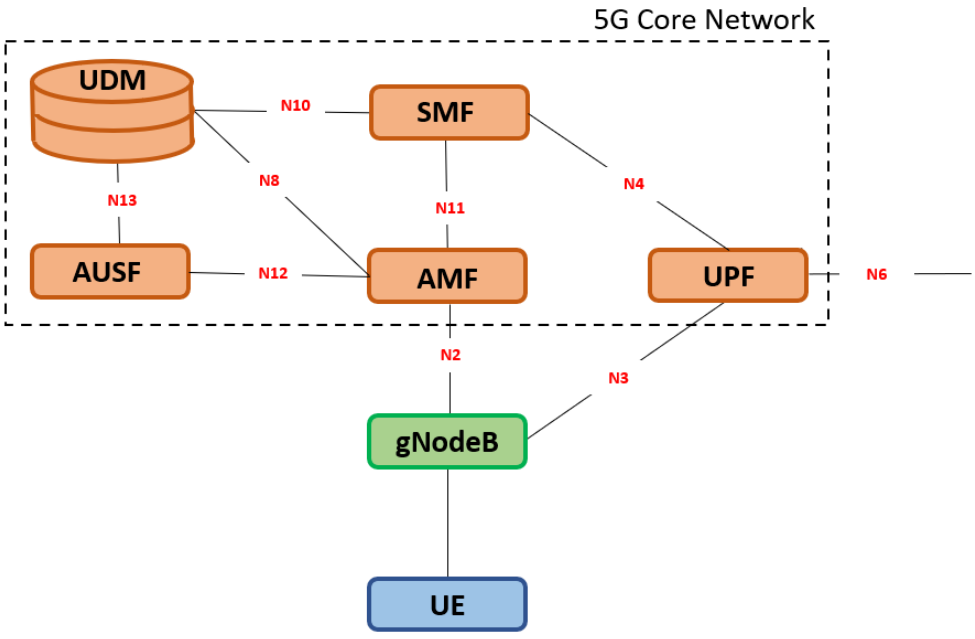


Figure 12: 5G Core functions available in WP4 lab

As we have two ME 1210 equipment, we installed one 5G Core on each of them.

PCF function is not available with this software and QoS is then managed using DSCP as explained in section 2.1.4.3.

Besides, we have chosen not to use NAT at N6 interface (neither on 4G SGi) as there is no recommendation on that point for the moment. UPF's pool of IP addresses that are allocated to UEs are consequently routed at the UPF N6 interface.

2.1.3.2 Possible setups with 5G RAN

When there is a need of having only one gNodeB for testing, configuration of Figure 13 can be used. In that case, a single ME1210 equipment is needed.

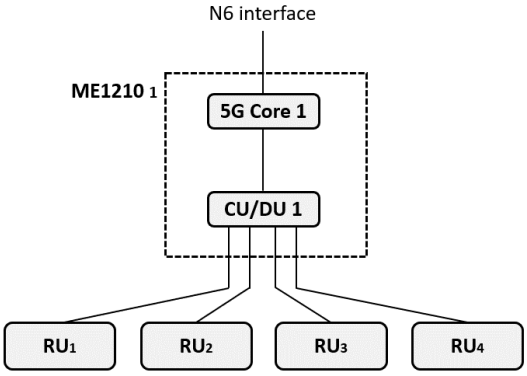


Figure 13: Using a single ME1210 to have one gNodeB under a 5G Core

When there is a need of having two gNodeB for testing, configuration of Figure 14Figure 14 can be used. In that case, two ME1210 equipment's are needed.

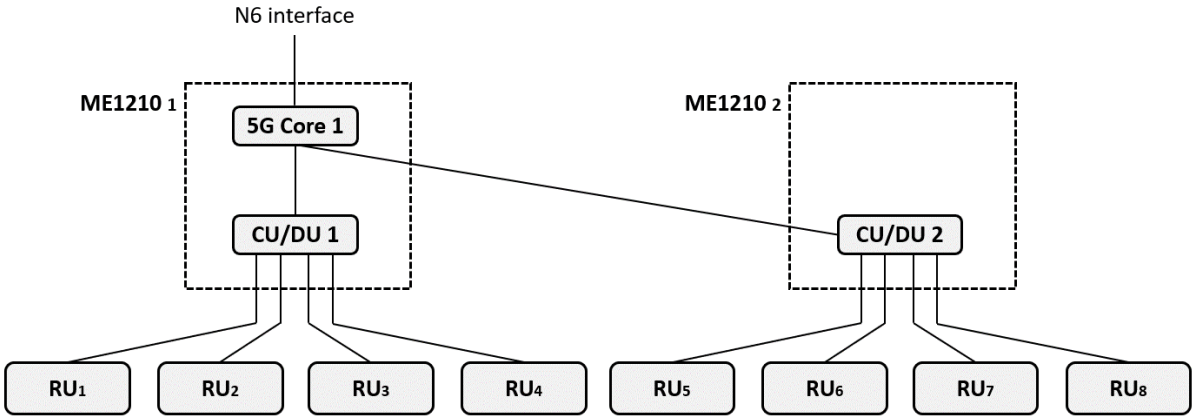


Figure 14: Configuration used to have two gNodeB under a 5G Core

2.1.4 5G network integration testing's

In this section, we give some details on the integration tests that have been done with the 5G network in order to check its correct behaviour.

2.1.4.1 5G tests with available frequencies

In order to check 5G network basic behaviour, some tests have been performed quite soon with the Thales ES1 modem, and OB-GW Kontron when available. Thales ES3 modem, which can work on N39 band, was received later. As soon as WP4 received it, we were able to test it and evaluate the N39 RU. These tests are summarized in Figure 15:

Test	Comment	Trace
5G UL transfer test on N78	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G UL Transfer N78 OB GW-K.pcap
5G DL transfer test on N78	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G DL Transfer N78 OB GW-K.pcap
5G UL transfer test on N8	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G UL Transfer N8 OB GW-K.pcap
5G DL transfer test on N8	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G DL Transfer N8 OB GW-K.pcap
5G UL transfer test on N39 using ES3	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G UL Transfer N39 ES3.pcap
5G DL transfer test on N39 using ES3	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G DL Transfer N39 ES3.pcap
5G RTD test on N78	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_5G RTD N78 OB GW-K.pcap
5G RTD test on N39	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_5G RTD N39 ES3.pcap
5G RTD test on N8	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_5G RTD N8 OB GW-K.pcap
5G HO between RU N8 and RU N78	Both ways	5GRail_WP4_Kontron_D4.2_5G HO N8 N78 OB GW-K.zip

Figure 15: Basic 5G integration tests done with Thales ES1 and ES3 modems

N39 band being very important for the project, we did the test above with the Vertex radio channel tool in order to change radio path conditions. Vertex tool was also sent for calibration just before in order to ensure its behaviour.

2.1.4.2 HO testing's

In order to ensure handover capability of the lab, one 5G HO test has been done between a N8 RU and a N78 one, both ways (see Figure 16). This test was successful and connection was not lost.

Test	Comment	Trace
5G HO between RU N8 and RU N78	Both ways	5GRail_WP4_Kontron_D4.2_5G HO N8 N78.zip

Figure 16: 5G HO test

2.1.4.3 QoS management within 5G network

WP4 5G network having no PCF, it has been discussed with WP2 other ways of triggering specific QoS in the network and the DSCP-based method has been chosen.

2.1.4.3.1 DSCP TEST SETUP

DSCP method has been checked by Alstom with the same core network as depicted in Figure 17**:**

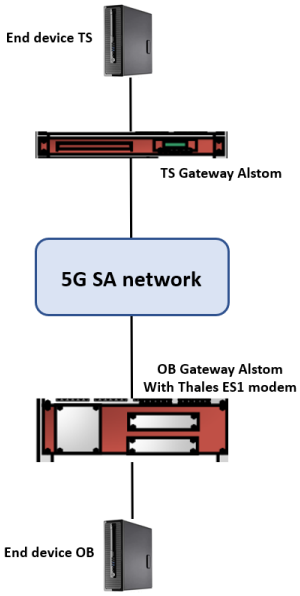


Figure 17: Architecture for DSCP tests

Thales ES-1 modem is controlled by Alstom OB_GTW. It is connected to the 5G SA network with the APN "internet". End devices OB and TS simply host iperf application that is used to generate traffic.

There are static QoS rules configured in the 5G network for this apn. Basically, we have the following QoS flows configuration for the apn "internet":

- QoS flow #1 = default one
- QoS flow #2 :
  - 5QI 3 (gBR)
  - gBR UL/DL = 100kbit/s
  - max BR UL/DL = 1Mbits/s
  - tft filtering: for DSCP value 110 000 (CS6)
- QoS flow #3:
  - 5QI 5 (non gBR)
  - tft filtering: for DSCP value 101 000 (CS5)

On the On-Board end device and trackside end device, we use iPerf to generate traffic. DSCP marking is performed by the OB_GTW and TS_GTW depending on the test that we want to perform. We will generate traffic with DSCP 110 000 and check that it goes on qos_flow #2. Then, we will generate traffic with DSCP 101 000 and check that it goes on qos_flow #3.

Additionally, there is a permanent data flow with no specific DSCP marking (or another one than 110 000 and 101 000) and this flow should go on qos_flow #1 (default one).

To check which qos_flow is used, we run a command on the simulator (named "ue_get") which gives the total bytes amount on each qos_flow for the selected UE.

2.1.4.3.2 TEST RESULTS

The test sequence and corresponding results are given in the following table:

Step	Description/Results	Total bytes in QoS flow #1 (default)	Total bytes in QoS flow #2 (for DSCP 110000)	Total bytes in QoS flow #3 (for DSCP 101000)
0	Initial step. Permanent data flow with DSCP CS0 (000 000) Only default QoS flow is used.	"dl_total_bytes": 34542, "ul_total_bytes": 22770,	"dl_total_bytes": 0, "ul_total_bytes": 0	"dl_total_bytes": 0, "ul_total_bytes": 0
1	We start a TCP flow with DSCP 110 000 (CS6), with iPerf during 30s. We can see that the traffic in Qos flow #2 has increased.	"dl_total_bytes": 102046, "ul_total_bytes": 66116,	"dl_total_bytes": 4338104, "ul_total_bytes": 237964	"dl_total_bytes": 0, "ul_total_bytes": 0
2	We stop the flow with DSCP 110 000, and wait for 80s approximately We can see that the traffic in Qos flow #2 does not increase anymore.	"dl_total_bytes": 157222, "ul_total_bytes": 101678,	"dl_total_bytes": 4338104, "ul_total_bytes": 237964	"dl_total_bytes": 0, "ul_total_bytes": 0
3	We start a UDP flow with DSCP 101 000 (CS5) in the DL only, with iPerf during 30s. We can see that the traffic in Qos flow #3 has increased for DL only.	"dl_total_bytes": 248960, "ul_total_bytes": 160660,	"dl_total_bytes": 4338104, "ul_total_bytes": 237964	"dl_total_bytes": 213544998, "ul_total_bytes": 0
4	We stop the previous flow (UDP DL with DSCP 101 000). We start the same flow in UL only, with iPerf during 30s. Lower data rate than step 3 (because of UL limitations) We can see that the traffic in Qos flow #3 has increased for UL only.	"dl_total_bytes": 332538, "ul_total_bytes": 214344,	"dl_total_bytes": 4338104, "ul_total_bytes": 237964	"dl_total_bytes": 213544998, "ul_total_bytes": 30180042

Table 2: DSCP tests with Thales EVB1 5G modem

Then, we could check that the behaviour of the modem was correct:

- Traffic with DSCP 110 000 (CS6) goes into ***qos_flow #2***.
- Traffic with DSCP 101 000 (CS5) goes into ***qos_flow #3***.
- Other traffic goes into default ***qos_flow #1***.

And consequently, DSCP can be used for all WP4 tests that need a specific 5G QoS to be applied.

Traces of the tests done in this section are stored under Alstom's repository under the name 5Grail_WP4_Alstom_testDSCP_21-12-07.zip

2.1.4.4 5G SA tests with Nokia XR 20 smartphone and SONIM XP10 smartphone

We first received a 5G SA capable smartphone in WP4 lab and then, we could start some integration tests with it on our 5G SA network. This smartphone can only work on 5G SA N78 and it is consequently the 5G frequency we used for the tests.

Objective being to perform some optional voice tests with it, we installed Kontron MCx application on the smartphone and checked few call scenarios :

- MCPTT point to point call from Wifi to 5G without floor control (**associated trace *MCPTT_PTP_from_Wifi_to_5G_without_floor_control.pcapng***)
- MCPTT point to point call from Wifi to 5G with floor control (**associated trace *MCPTT_PTP_from_Wifi_to_5G_with_floor_control.pcapng***)
- MCPTT point to point call from 5G to Wifi without floor control (**associated trace *MCPTT_PTP_from_5G_to_Wifi_without_floor_control.pcapng***)
- MCPTT point to point call from 5G to Wifi with floor control (**associated trace *MCPTT_PTP_from_5G_to_Wifi_with_floor_control.pcapng***)
- MCPTT emergency call from 5G to Wifi (**associated trace *MCPTT_EGC_from_5G_to_Wifi_Emergency_Group_Call.pcapng***)

All tests were successful and no misbehaviour has to be reported. Later, we received another 5G SA capable smarphone : SONIM XP10. This one can operate on 5G SA N8 band and similarly, we did the same kind of check tests with it after having installed an MCx client software on it.

Unfortunately, neither of these smartphone can work on N39 5G SA, this band being quite specific for FRMCS usage. Anyway, after these basic testings, we could foresee to be able to run some optional voice tests on 5G SA during the WP4 test period.

2.2 MCx and IMS network installation and integration

2.2.1 IMS and MCx network installation

MCx and IMS softwares have been installed on a HP GEN-10 server, in WP4 server room, as shown on Figure 18:

Figure 18: HP Gen-10 equipment installed in WP4 lab for IMS/MCx functions hosting

These applications run on several Virtual Machines and provide the functions that appear on Figure 19. It is also shown there that IMS and MCx networks are connected to the "N6 LAN" which can be reached by on board and trackside FRMCS gateways (more details on WP4 lab architecture is given in section Detailed WP4 lab architecture2.6). Consequently, all MCx clients from On Board and Trackside can reach IMS and MCx network.

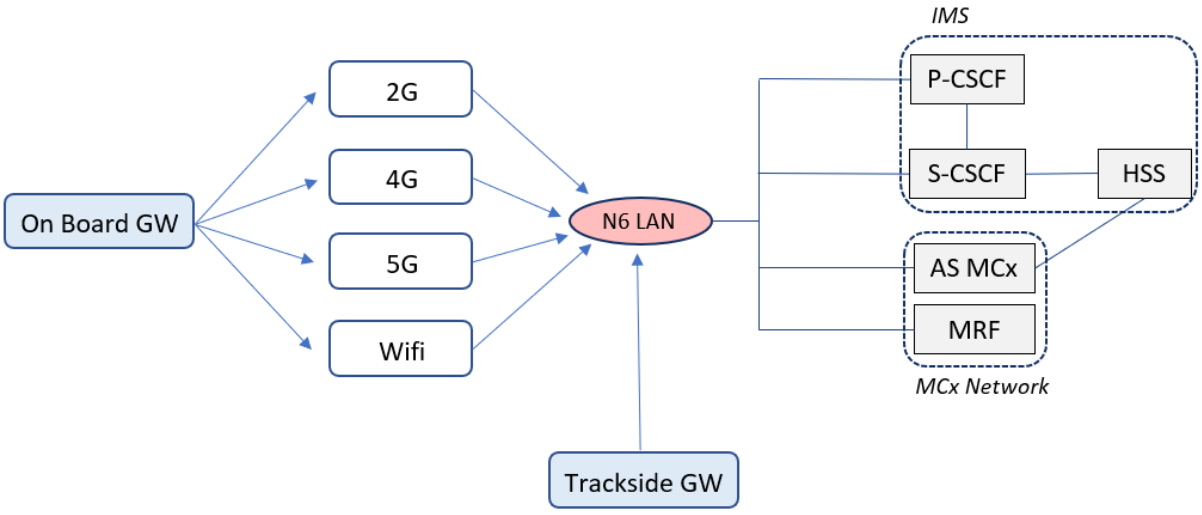


Figure 19: IMS and MCx functions installed in the lab

Besides, whenever a call has to be made between an on-board application and its trackside peer, a MCx client from on-board side will connect to a MCx client hosted in the Trackside Gateway, both clients communicating with the MCx AS which sets up the call.

2.2.2 IMS and MCx integration testing

Once IMS and MCx parts were installed, it was possible to check the correct behaviour of these components by using smartphones with MCx client applications.

Kontron MCx application is able, among other things, to launch MCx point to point calls, group calls and data transfer. After configuration of clients in the network, integration tests of Figure 20 were performed:

Test	Comment	Trace
Client registration	IMS and MCx Registration	5GRail_WP4_Kontron_D4.2_IMS-MCx Registration.pcap
Voice private call without floor control	Mcvoice call without push to talk function	5GRail_WP4_Kontron_D4.2_MCx PtP voice call.pcap
Voice private call with floor control	Mcvoice group call with 3 clients	5GRail_WP4_Kontron_D4.2_MCx PtP voice call with PTT.pcap
Group call with floor control	Mcvoice call with push to talk function	5GRail_WP4_Kontron_D4.2_MCx Group call with PTT.pcap
Mcdata FD	File delivery using Mcdata	5GRail_WP4_Kontron_D4.2_MCx FD.pcap
MCx Emergency voice group call	Automatic answer of all MCx clients	5GRail_WP4_Kontron_D4.2_MCx EGC.pcap

Figure 20: MCx integration tests performed in WP4 lab

Mobiles were using Wi-Fi connection as smartphones able to connect 5G SA were not yet available on in the lab at that moment. Kontron MCx client application was running on Android system, the interface of this application can be seen on Figure 21 where a point to point MCptt call is ongoing:

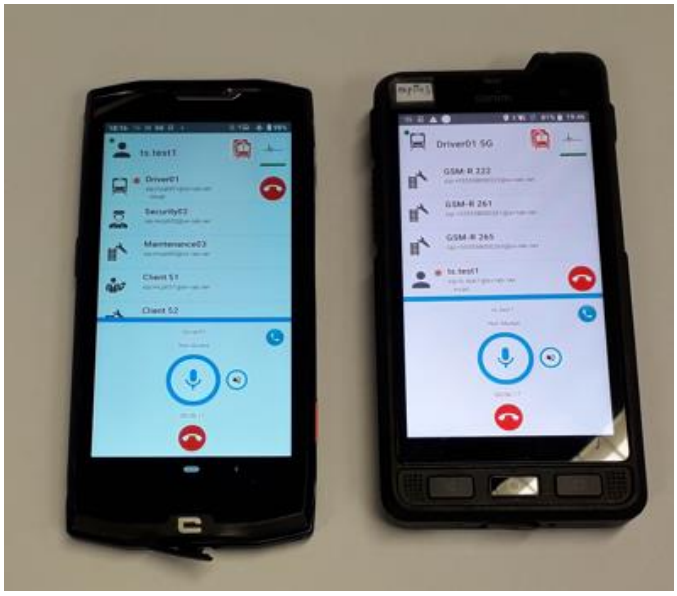


Figure 21: MCx private voice call

Group calls with Push to Talk token management where also checked during that integration test period (see Figure 22), as well as emergency voice calls.

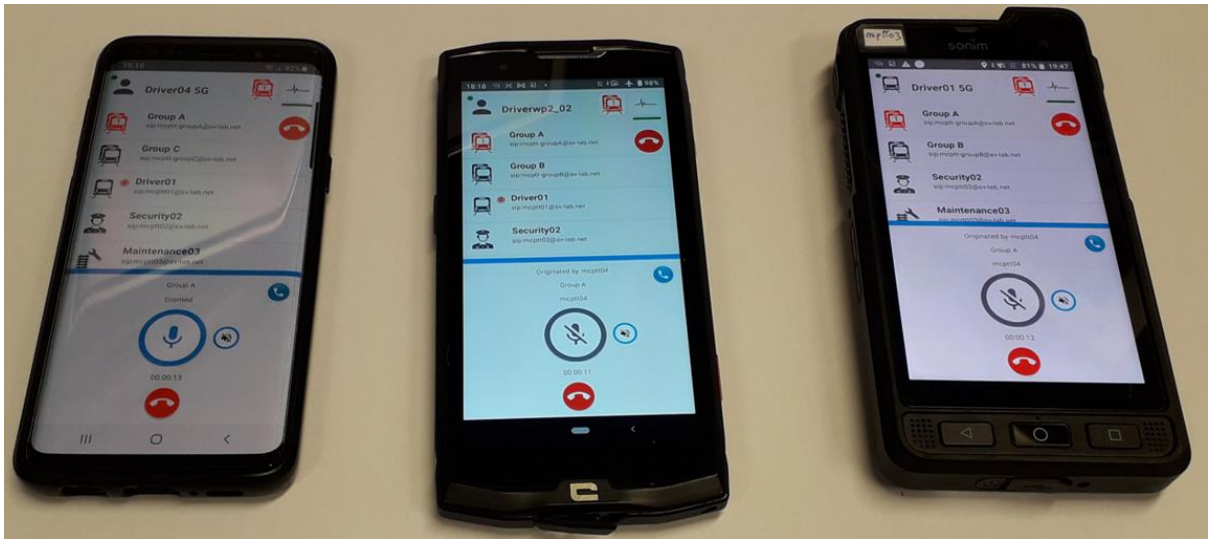


Figure 22: MCx group call test

Overall, it appeared that IMS/MCx system was operational and ready to be used by other WP4 entities, especially OB and TS FRMCS Gateways. Besides, as soon as a 5G SA capable smartphone was available in the lab, we were able to run some MCPTT voice tests after having installed Kontron MCx client on it.

2.2.3 IMS and MCx parameters

2.2.3.1 IMS/MCx network main parameters

Main default parameters of IMS/MCx network are given in appendix 9.4

2.2.3.2 MCx clients configuration

A specific workstream has been initiated by WP2 in order to discuss MCx clients configuration in WP3 and WP4 labs. As concerns WP4, ETCS, ATO and PIS users profiles have been defined at that time.

Figure 23 shows the identifiers that have been consequently configured in the system to prepare connections of these WP2 applications (if needed later, other clients could be created).

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

Figure 23: IMS/MCx users configuration for ETCS, ATO and PIS applications

2.3 GSM-R network installation and integration

2.3.1 GSM-R network installation

A GSM-R network, including dedicated BSC and BTS, was connected to the IMS/MCx network in order to enable hybridation tests. Radio cables from BTS were installed in WP4 lab room in order to connect them to radio devices, including two GSM-R handsets (see Figure 24):

Figure 24: GSM-R handsets installed in WP4 lab

2.3.2 GSM-R integration testing

As shown on Figure 25, GSM-R network was connected to the IMS/MCx network through the N6 LAN for the GSM-R/MCx hybridation. To be more precise, signalling flow can be exchanged between MSC-CS and S-CSCF while user plane data is exchanged between MGW and MRF.

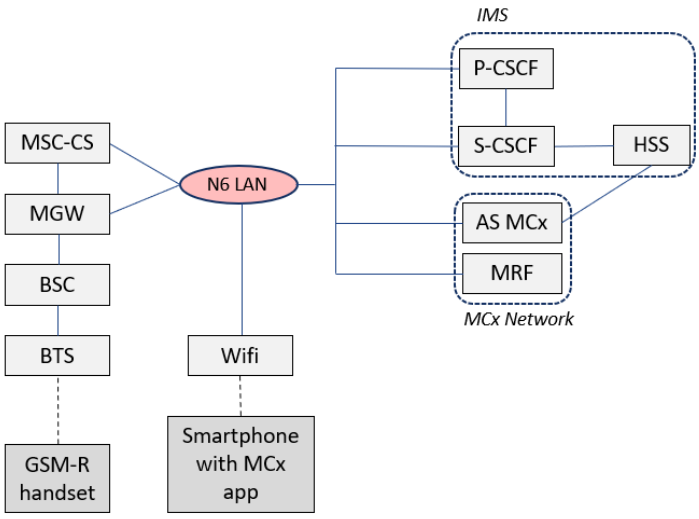


Figure 25: GSM-R/MCx hybridation

In order to check the setup, basic scenario were tested: point to point call from GSM-R side to a MCx user (a MCx client on a smartphone connected via Wi-Fi to IMS/MCx network) and vice versa (see Figure 26).

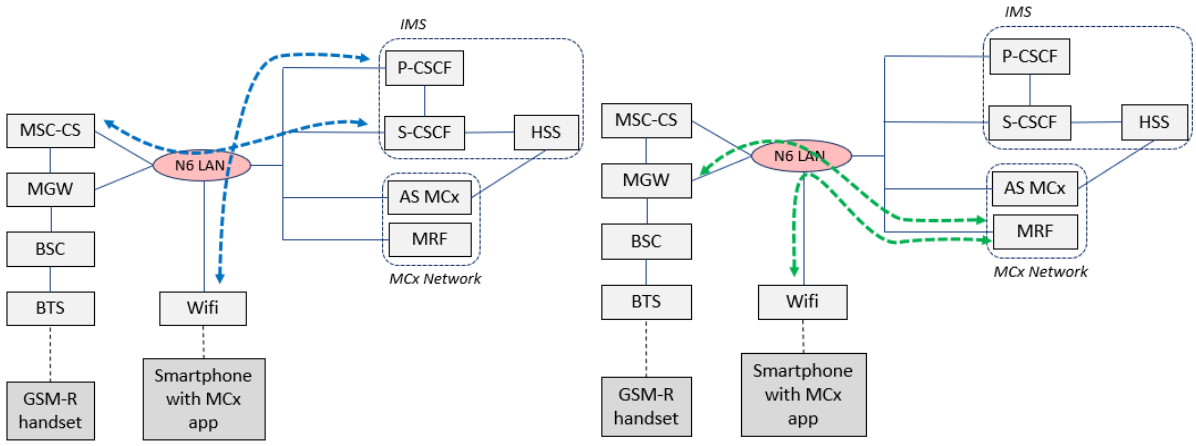


Figure 26: Signalling flow (blue) and User plane (green) for GSM-R hybridation tests

For the moment, no group call were tested there, neither push to talk. List of tests with traces references are given in Figure 27:

Test	Comment	Trace
Voice call from GSM-R handset to MCx client	No PTT	5GRail_WP4_Kontron_D4.2_Voice GSM-R to MCx.pcap
Voice call from MCx client to GSM-R handset	No PTT	5GRail_WP4_Kontron_D4.2_Voice MCx to GSM-R.pcap

Figure 27: GSM-R integration tests

2.4 4G service installation and integration

2.4.1 4G network installation

The need for a 4G network in the WP4 setup is linked to WP5 activities as, in field, there will be some limitation in the possibility of using some 5G bands. Consequently, the use of 4G in WP5 has been considered for some tests and, in order to de-risk WP5 activity, WP4 must also set-up a 4G network.

There is no specific hardware to be added in order to provide 4G access: We've seen that ME1210 product, described in section 2.1.2.2, is able to host a CU/DU and a 5G Core but these function can be turned to BBU and 4G core using the same software. The switching shown on Figure 28 is easy and only a question of minutes.

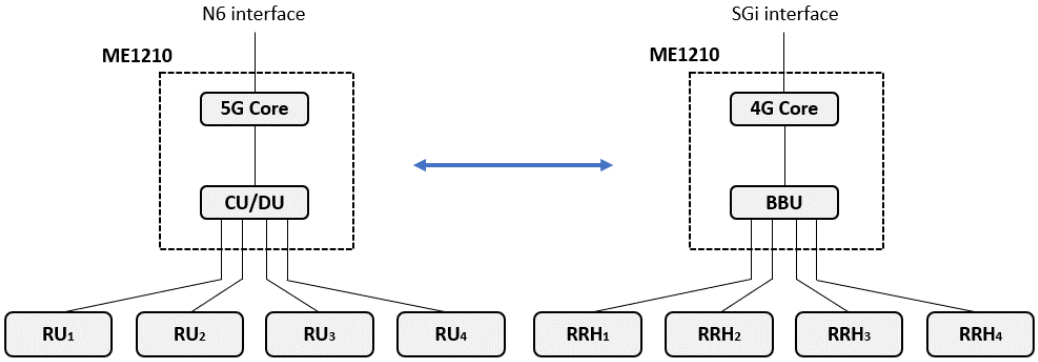


Figure 28: Software switching to activate 4G or 5G functions on the same ME1210

Besides, still within the same ME1210 equipment, we can have both 4G and 5G networks running at the same time, whatever number of RUs and RRHs, the only constraint being the maximum use of 4 ports for RUs and RRHs connections. Figure 29 shows an example of such configuration:

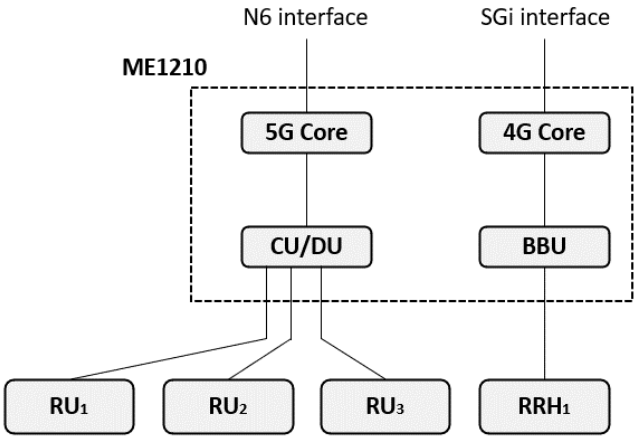


Figure 29: 4G and 5G networks running at the same time under the same ME1210

As regards RRHs, it is expected that WP5 will use B38 (2.6 GHz) in France. Consequently, that kind of RRH has been installed in WP4 lab and some validation tests have been done with it.

2.4.2 4G network integration

Few tests have been performed in order to check that 4G service is correctly provided by the system, they are shown on Figure 30:

Test	Comment	Trace
4G UL transfer test on B38	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_4G_UL_Transfer B38.pcap
4G DL transfer test on B38	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_4G_DL_Transfer B38.pcap
4G RTD test on B38	Ping P-CSCF from modem	5GRail_WP4_Kontron_D4.2_4G_RTD B38.pcap

Figure 30: Integration tests of 4G network

2.5 Wi-Fi service installation and integration

2.5.1 Wi-Fi service installation

Wi-Fi router has been installed in the lab as shown on Figure 31:

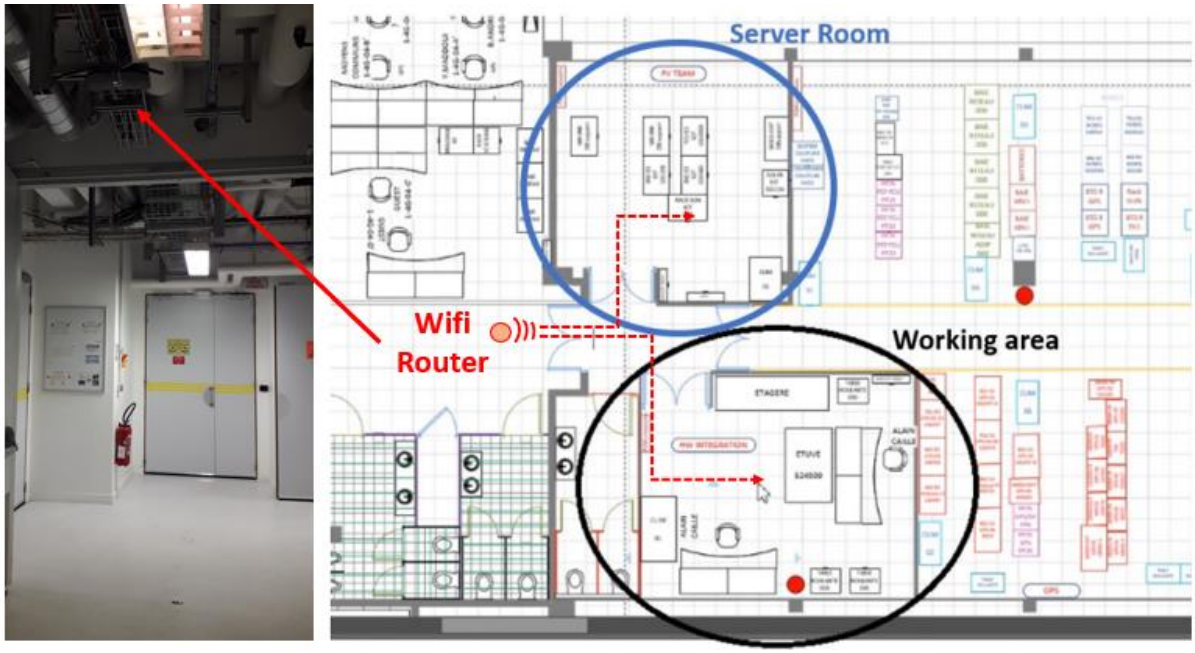


Figure 31: Wi-Fi access point set up in WP4 lab

Wi-Fi is the only RF signal that is going over the air in WP4 lab: GSM-R, 4G and 5G signals use RF coaxial cables.

2.5.2 Wi-Fi service integration

Minimal tests were done in order to ensure signal strength at locations where FRMCS OB Gateways and Smartphones will be located, that is to say in WP4 Server room and in WP4 Working area. List of tests that have been done are given on Figure 32:

Test	Comment	Trace
Wifi UL transfer test in Server Room	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_Wifi_UL_Server Room.pcap
Wifi DL transfer test in Server Room	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_4G_DL_Server Room.pcap
Wifi RTD transfer test in Server Room	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_4G_RTD_Server Room.pcap
Wifi UL transfer test in Working Area	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_Wifi_UL_Working Area.pcap
Wifi DL transfer test in Working Area	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_Wifi_DL_Working Area.pcap
Wifi RTD transfer test in Working Area	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_Wifi_RTD_Working Area.pcap

Figure 32: Wi-Fi integration tests

2.6 Detailed WP4 lab architecture

2.6.1 Functional view of WP4 lab

The functional components described in the previous sections are connected together to make WP4 lab as given on Figure 33, where ethernet switches and router components are not detailed to ease the reading.

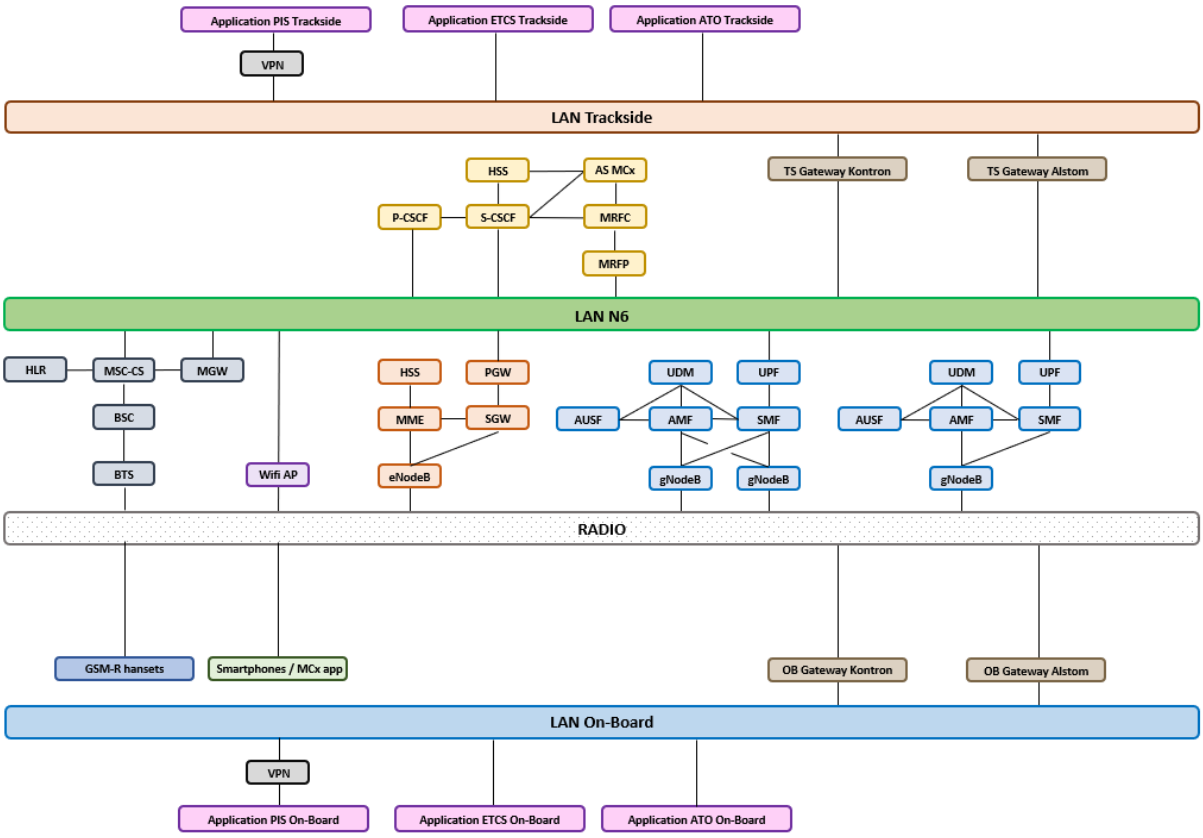


Figure 33: Functional view of WP4 lab

As foreseen in document D4.1 [S20], three LANs are particularly important:

- LAN “On-Board”: it connects all the On-Board applications to the FRMCS OB Gateways
- LAN “Trackside” : it connects all the Trackside applications to the FRMCS TS Gateways
- LAN “N6” : it connects all the radio access networks (GSM-R, Wi-Fi, 4G, 5G) to IMS/MCx core (so that FRMCS OB Gateways are able to connect to MCx core), and also a connection between TS Gateways and IMS/MCx core (so that FRMCS TS Gateways are able to connect to MCx core).

IP plan of these LAN are given in section 2.6.3

VPNs between partners, that are not fully detailed on this picture, were also put in place and tested during the integration phase. Precisely, it deals with:

- VPN between Thales and Kontron which is used to bridge OB and TS PIS applications, that stands on Thales premises, with WP4 lab (i.e. make a connection with LAN “On-Board” and LAN “Trackside”). More details are given in chapter 3.
- VPN between Alstom and Kontron which is used by Alstom engineers to remotely control the equipment they shipped and installed in Montigny lab. More details are given in chapter 4.

2.6.2 Hardware view of WP4 lab

Hardware view of WP4 lab is given on Figure 34. Switch, routers, and details about VPN connection are not described on that figure.

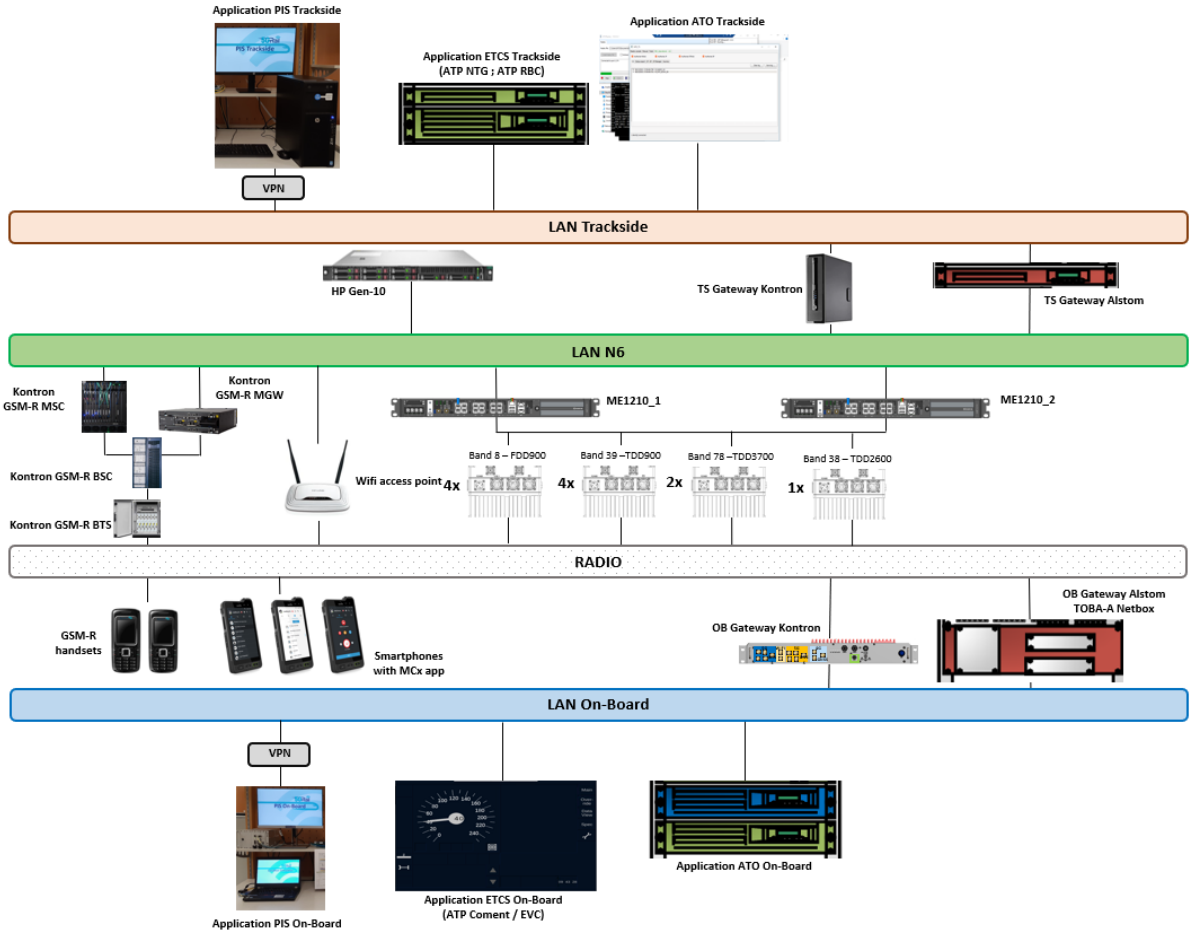


Figure 34: Global hardware view of WP4 lab

2.6.3 IP Plan of WP4 lab

Ip plan of the three LANs described in section 2.6.1 can be found in following figures Figure 35, Figure 36 and Figure 37.

172.21.160.160 /27 "LAN On-Board"	172.21.160.160	255.255.255.224	Reserved (Subnet)
	172.21.160.161	255.255.255.224	
	172.21.160.162	255.255.255.224	OBapp - OB Appli (PC1) VM
	172.21.160.163	255.255.255.224	
	172.21.160.164	255.255.255.224	Kontron DNS_OB
	172.21.160.165	255.255.255.224	OBapp - OB GW v1.1 #2 VM
	172.21.160.166	255.255.255.224	
	172.21.160.167	255.255.255.224	OBapp - OB GW v1.1 #3 VM
	172.21.160.168	255.255.255.224	
	172.21.160.169	255.255.255.224	
	172.21.160.170	255.255.255.224	Alstom OB comet
	172.21.160.171	255.255.255.224	Alstom OB nbx
	172.21.160.172	255.255.255.224	Alstom OB odb
	172.21.160.173	255.255.255.224	Alstom OB ato-ob
	172.21.160.174	255.255.255.224	
	172.21.160.175	255.255.255.224	OBapp - OB GW v1.1 #4 VM
	172.21.160.176	255.255.255.224	
	172.21.160.177	255.255.255.224	OBapp - OB GW v0 VM
	172.21.160.178	255.255.255.224	
	172.21.160.179	255.255.255.224	
	172.21.160.180	255.255.255.224	OBapp - OB GW v1 VM
	172.21.160.181	255.255.255.224	
	172.21.160.182	255.255.255.224	OBapp - OB GW v1.1 #1 VM
	172.21.160.183	255.255.255.224	OBapp - Simu
	172.21.160.184	255.255.255.224	OBapp - front-end
	172.21.160.185	255.255.255.224	OBapp - OB Appli (PC1) VM Simu(websocket)
	172.21.160.186	255.255.255.224	
	172.21.160.187	255.255.255.224	
	172.21.160.188	255.255.255.224	
	172.21.160.189	255.255.255.224	
	172.21.160.190	255.255.255.224	
	172.21.160.191	255.255.255.224	Reserved (Broadcast)

Figure 35: IP Plan of the On-Board LAN

172.21.160.128 /27 "LAN Trackside"	172.21.160.128	255.255.255.224	Reserved (Subnet)
	172.21.160.129	255.255.255.224	Gateway (uCPE FW2)
	172.21.160.130	255.255.255.224	
	172.21.160.131	255.255.255.224	TSapp - TS GW #1 VM
	172.21.160.132	255.255.255.224	
	172.21.160.133	255.255.255.224	
	172.21.160.134	255.255.255.224	Kontron DNS_TS
	172.21.160.135	255.255.255.224	
	172.21.160.136	255.255.255.224	
	172.21.160.137	255.255.255.224	
	172.21.160.138	255.255.255.224	
	172.21.160.139	255.255.255.224	
	172.21.160.140	255.255.255.224	Alstom ATP-NTG
	172.21.160.141	255.255.255.224	Alstom ATO-TS
	172.21.160.142	255.255.255.224	Alstom DNS-TS-ED
	172.21.160.143	255.255.255.224	Alstom TS GW eno1
	172.21.160.144	255.255.255.224	
	172.21.160.145	255.255.255.224	TSapp - OB Appli (PC1) VM
	172.21.160.146	255.255.255.224	TSapp - TS GW #2 VM
	172.21.160.147	255.255.255.224	
	172.21.160.148	255.255.255.224	
	172.21.160.149	255.255.255.224	
	172.21.160.150	255.255.255.224	
	172.21.160.151	255.255.255.224	TSapp - Appli VM (PC3)
	172.21.160.152	255.255.255.224	TSapp - Simu VM (PC1)
	172.21.160.153	255.255.255.224	TSapp - front-end
	172.21.160.154	255.255.255.224	TSapp - Front End (PC3) VM Simu(websocket)
	172.21.160.155	255.255.255.224	
	172.21.160.156	255.255.255.224	
	172.21.160.157	255.255.255.224	
	172.21.160.158	255.255.255.224	
	172.21.160.159	255.255.255.224	Reserved (Broadcast)

Figure 36: IP Plan of the Trackside LAN

Vlan 622 - 172.21.160.64 /26 "LAN N6"			
	172.21.160.64	255.255.255.192	Reserved (Subnet)
	172.21.160.65	255.255.255.192	Default GW
	172.21.160.66	255.255.255.192	IP 3750 Vlan 622 (Router1)
	172.21.160.67	255.255.255.192	Reserve (Router2)
	172.21.160.68	255.255.255.192	p-cscf-a1
	172.21.160.69	255.255.255.192	sdp-a1
	172.21.160.70	255.255.255.192	Ubuntu MCx Client
	172.21.160.71	255.255.255.192	Ubuntu MCx Client 2
	172.21.160.72	255.255.255.192	Ubuntu VM , Media router
	172.21.160.73	255.255.255.192	
	172.21.160.74	255.255.255.192	Simkloud1 UPF GW
	172.21.160.75	255.255.255.192	WP2 TS Gateway 1 on the N6
	172.21.160.76	255.255.255.192	IMS S-CSCF GSM-R IWF
	172.21.160.77	255.255.255.192	Simkloud2 UPF GW
	172.21.160.78	255.255.255.192	
	172.21.160.79	255.255.255.192	
	172.21.160.80	255.255.255.192	Alstom TS GW eno2
	172.21.160.81	255.255.255.192	Alstom TS GW eno2:1
	172.21.160.82	255.255.255.192	Alstom TS GW eno2:2
	172.21.160.83	255.255.255.192	Alstom TS GW eno2:4
	172.21.160.84	255.255.255.192	Kontron DNS_N6
	172.21.160.85	255.255.255.192	
	172.21.160.86	255.255.255.192	
	172.21.160.87	255.255.255.192	
	172.21.160.88	255.255.255.192	
	172.21.160.89	255.255.255.192	
	172.21.160.90	255.255.255.192	
	172.21.160.91	255.255.255.192	
	172.21.160.92	255.255.255.192	
	172.21.160.93	255.255.255.192	
	172.21.160.94	255.255.255.192	
	172.21.160.95	255.255.255.192	
	172.21.160.96	255.255.255.192	
	172.21.160.97	255.255.255.192	
	172.21.160.98	255.255.255.192	
	172.21.160.99	255.255.255.192	
	172.21.160.100	255.255.255.192	
	172.21.160.101	255.255.255.192	
	172.21.160.102	255.255.255.192	
	172.21.160.103	255.255.255.192	
	172.21.160.104	255.255.255.192	
	172.21.160.105	255.255.255.192	
	172.21.160.106	255.255.255.192	
	172.21.160.107	255.255.255.192	
	172.21.160.108	255.255.255.192	
	172.21.160.109	255.255.255.192	
	172.21.160.110	255.255.255.192	
	172.21.160.111	255.255.255.192	
	172.21.160.112	255.255.255.192	N6 - TS GW #2 VM
	172.21.160.113	255.255.255.192	N6 - TS GW #1 VM
	172.21.160.114	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.115	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.116	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.117	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.118	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.119	255.255.255.192	TPLink wifi router / wifi IP (reserved)
	172.21.160.120	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.121	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.122	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.123	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.124	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.125	255.255.255.192	TPLink wifi router / wifi IP
	172.21.160.126	255.255.255.192	TPLink wifi router IP
	172.21.160.127	255.255.255.192	Reserved (Broadcast)

Figure 37: IP plan of N6 LAN

3 WP4 PIS application integration

PIS application, provided by Thales, fits into WP4 lab as depicted in Figure 38. It consists in an on-board part, linked to OB-GW, and a trackside part, linked to TS-GW. Both parts communicate with each other in order to offer PIS service.

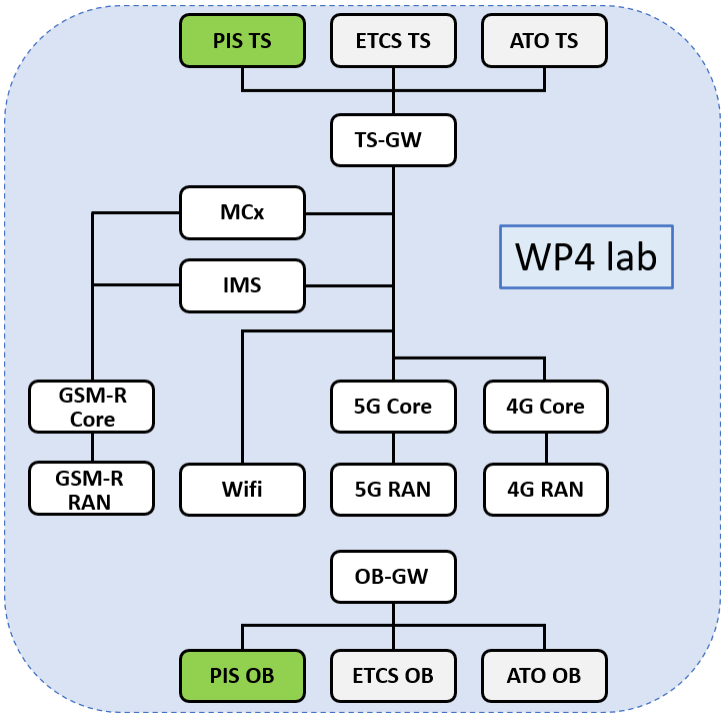


Figure 38: PIS OB and TS applications in WP4 lab

3.1 Description of PIS lab

3.1.1 Lab location and high level description

PIS lab is located on two different geographical sites:

- In Kontron's premises at Montigny-Le-Bretonneux, France.
- In Thales SGF's premises at Vélizy, France.

Figure 39: Geographical situation of PIS Lab

In Kontron's premises are installed, among others:

- 5G Radio Access Network and Core Network,
- IMS and MCx systems,
- FRMCS On-Board and TrackSide Gateways,
- VPN Gateway for the remote access with Thales Lab.

In Thales SGF's premises are installed:

- PIS TrackSide and On-Board equipment,
- VPN Gateway for the remote access with Kontron Lab

Note: The description of the different equipment is given in document D4.1 [S20].

In order to be able to execute functional PIS test cases (i.e. send trackside to on-board and on-board to trackside messages and display accurate train location information to the passengers like the current and next stops), a secure VPN connection must be considered between the two sites to interconnect PIS equipment to the FRMCS infrastructure.

Thales SGF 5GRAIL Lab is protected by three firewalls:

- "FW-Internet" firewall protects Thales SGF's infrastructure against attacks coming from Internet,
- "FW-5GRAIL-TS" and "FW-5GRAIL-OB" firewalls dedicated to 5GRAIL project. They create a DMZ in order to isolate Thales SGF's WP4 5GRAIL Lab from other Thales' Lab.

Kontron 5GRAIL Lab is also protected by three firewalls:

- "FW-K1" protects Kontron infrastructure against attacks coming from Internet,
- "FW-K2-A" and "FW-K2-B" a DMZ in order to isolate 5GRAIL Lab from other Kontron's Lab.

These firewalls implement the matrix of PIS flows (see Figure 44).

In order to set-up a VPN connections with Thales SGF 5GRAIL Lab, a VPN endpoint is setup in Montigny lab: this is the so called uCPE platform.

In order to set-up a VPN with Kontron's lab, Thales SGF will use a SDWAN connection, based on Velocloud/VMware solution. In order to achieve this, a Velocloud VCE520 box is installed in Thales SGF's premises.

The above equipment is provided and configured by Kontron.

Note: The description of the above equipment is provided in document D4.1 [S20].

Figure 40 provides a high-level view of the WP4-PIS Lab.

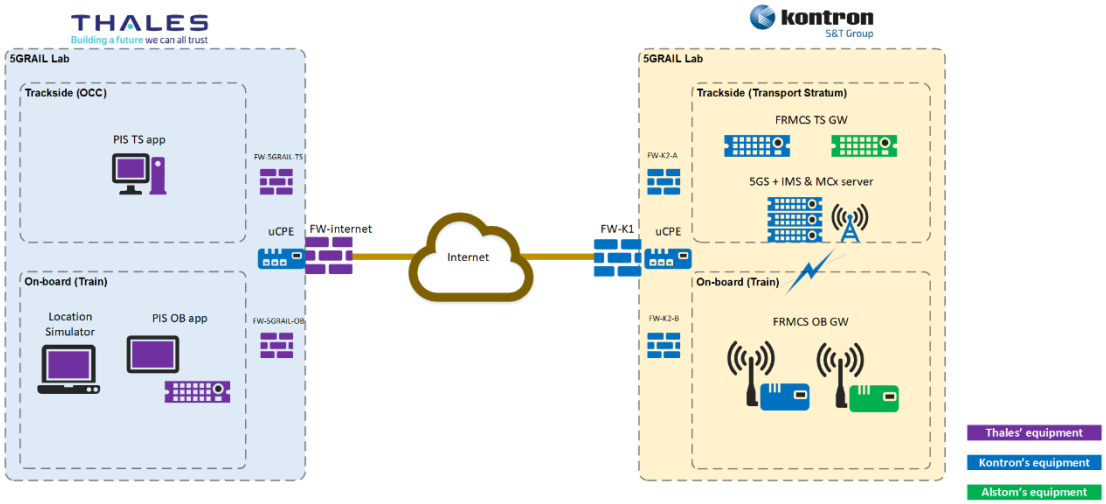


Figure 40: High-level view of WP4-PIS Lab

PIS application is constituted of "trackside" and "on-board" equipment:

- PIS trackside server hosts PIS trackside application. It allows the passenger information manager to send information to passengers in the train.
- PIS on-board server hosts PIS on-board application. This application handles messages sent by PIS trackside application and dispatches them to display device.
- The on-board display device displays text information like train timetables sent by the passenger information manager to the passenger in the train.
- Location simulator provides the location of the train. Indeed, PIS application needs to know train's location in order to provide accurate information to the passengers such as real-time train schedules and other operator service information. At this stage of the FRMCS specifications, available for 5GRAIL project, no FRMCS equipment has been specified to be responsible to provide location information to the applications that need it.

The description of the above equipment is given in document D4.1 [S20].

Connections between the on-board and the trackside sides of the application go through two gateways (provided by Kontron and Alstom), located on both sides of the 5G infrastructure (provided by Kontron):

- The FRMCS on-board Gateway, connected to the applications through OB_{app} interface and to the 5G radio access networks, through a set of FRMCS modems;
- The FRMCS trackside Gateway, connected to the applications through TS_{app} interface and to the 5G core infrastructure.

FRMCS Gateways and the equipment of the 5G infrastructure are installed in Kontron's lab.

The description of the set-up of FRMCS Gateways and the 5GS is provided in chapter 5 and section 2.1.

Equipment housed on Thales SGF's premises is installed in two rooms. One room hosts the equipment managing the remote connection and the second room hosts the equipment of the PIS application.

Figure 41: WP4-PIS Lab in Thales SGF's premises.

Note: For security and confidentiality rules, only photos of PIS equipment are allowed.

See chapter 2 for the description of Kontron's Lab.

3.1.2 WP4 PIS lab setup

Figure 42 illustrates the detailed network architecture of the WP4-PIS Lab.

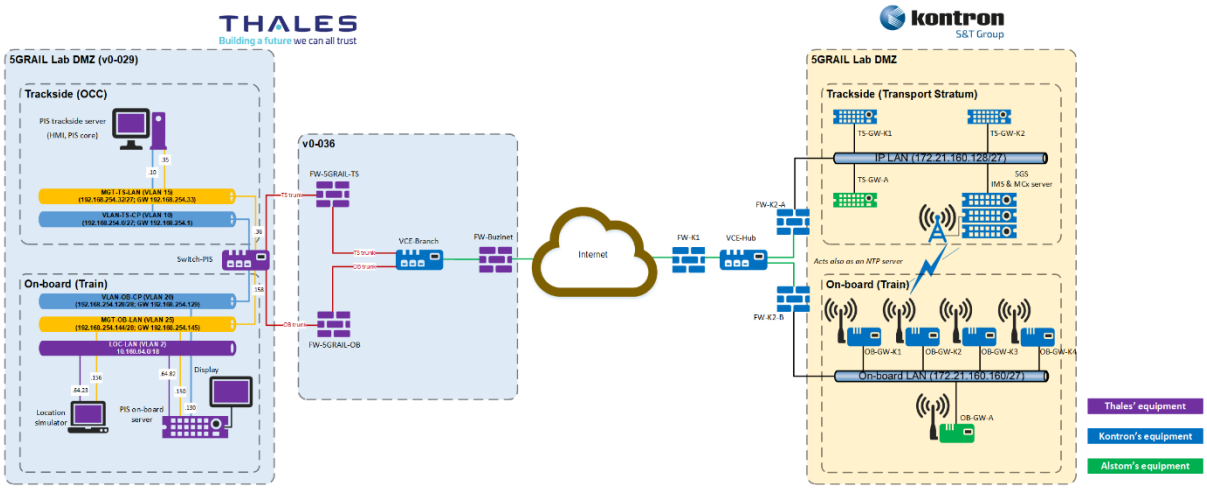


Figure 42: Detailed network architecture of WP4-PIS Lab

On Thales SGF side of the WP4-PIS Lab, 5 different VLANs have been configured in order to separate the trackside and the on-board parts of the application and to segregate the PIS flows (for security):

- VLAN 10 for PIS trackside Control Plane and User Plane flows (e.g. send information messages to passengers, synchronization of the train mission database),
- VLAN 15 for trackside management flows (e.g. OM session, logs synchronization),
- VLAN 20 for PIS on-board Control Plane and User Plane flows (e.g. reception of the messages sent from trackside and train mission database),
- VLAN 25 for on-board management flows (e.g. O&M session, logs synchronization),
- VLAN 2 for local on-board communication between the Location simulator and the PIS on-board server.

Note: At this stage, the segregation of the Control Plane and the User Plane is not considered in FRMCS loose API described in [S19].

In Kontron's Lab, the relevant subnets to consider for PIS application are:

- Subnet Trackside,
- Subnet On-board.

See section 2.6 for the full description of the IP plan configured in Kontron's Lab.

3.1.2.1 IP Plan

Figure 43 provides the IP plan of all equipment involved in WP4-PIS Lab for PIS functional tests.

PIS IP plan			
Location	**LAN**	**Equipment**	**IP/mask**
THALES			
Trackside	VLAN-CP (VLAN 10) 192.168.254.0/27 (GW: 192.168.254.1)	PIS trackside	192.168.254.10/27
	MGT-LAN (VLAN 15) 192.168.254.32/27 (GW: 192.168.254.33)	PIS trackside	192.168.254.35/27
		Switch	192.168.254.36/27
On-board	VLAN-CP (VLAN 20) 192.168.254.128/28 (GW: 192.168.254.129)	PIS on-board	192.168.254.130/28
	MGT-LAN (VLAN 25) 192.168.254.144/28 (GW: 192.168.254.145)	PIS on-board	192.168.254.150/28
		Loc simulator	192.168.254.156/28
		Switch	192.168.254.158/28
	LOC-LAN (VLAN 2) 10.160.64.0/18	PIS on-board	10.160.64.82
		Loc simulator	10.160.64.23
KONTRON			
Trackside	DATA	TS-GW-K1	172.21.160.151/27
	DATA	TS-GW-K2	172.21.160.146/27
	DATA	TS NTP server	172.21.160.129/27
On-board	DATA	OB-GW-K1	172.21.160.175/27
	DATA	OB-GW-K2	172.21.160.177/27
	DATA	OB-GW-K3	172.21.160.180/27
	DATA	OB-GW-K4	172.21.160.182/27
	DATA	OB NTP server	172.21.160.161/27
ALSTOM			
Trackside	DATA	TS-GW-A	172.21.160.143/27
On-board	DATA	OB-GW-A	172.21.160.171/27

Figure 43: IP plan of WP4-PIS Lab

3.1.2.2 Network flow matrix

The matrix (illustrated by Figure 44) provides the flows to consider as filtering rules to authorise in the firewalls in order to allow the execution of PIS functional tests.

PIS flow matrix							
Rules id	**Src @IP**	**Hostname Src**	**Hostname Dst**	**Dst @IP**	**Protocol**	**Dst Port**	**Comment**
1	172.21.160.129/27	TS NTP server	PIS trackside	192.168.254.35/27	UDP	123	Trackside NTP sync
2	172.21.160.161/27	OB NTP server	PIS on-board	192.168.254.150/28	UDP	123	On-board NTP sync
3	172.21.160.161/27	OB NTP server	Loc simulator	192.168.254.156/28	UDP	123	On-board NTP sync
4	192.168.254.35/27	PIS trackside	TS NTP server	172.21.160.129/27	UDP	123	Trackside NTP sync
5	192.168.254.150/28	PIS on-board	OB NTP server	172.21.160.161/27	UDP	123	On-board NTP sync
6	192.168.254.156/28	Loc simulator	OB NTP server	172.21.160.161/27	UDP	123	On-board NTP sync
7	192.168.254.10/27	PIS trackside	TS-GW-A	172.21.160.143/27	TCP	443	TS_{app} loose messages with Alstom's trackside GW
8	192.168.254.10/27	PIS trackside	TS-GW-K1	172.21.160.151/27	TCP	8443	TS_{app} loose messages with Kontron's trackside GW1
9	192.168.254.10/27	PIS trackside	TS-GW-K2	172.21.160.146/27	TCP	8443	TS_{app} loose messages with Kontron's trackside GW2
10	192.168.254.130/28	PIS on-board	OB-GW-A	172.21.160.171/27	TCP	443	OB_{app} loose messages with Alstom's on-board GW
11	192.168.254.130/28	PIS on-board	OB-GW-K1	172.21.160.175/27	TCP	8443	OB_{app} loose messages with Kontron's on-board GW1
12	192.168.254.130/28	PIS on-board	OB-GW-K2	172.21.160.177/27	TCP	8443	OB_{app} loose messages with Kontron's on-board GW2
13	192.168.254.130/28	PIS on-board	OB-GW-K3	172.21.160.180/27	TCP	8443	OB_{app} loose messages with Kontron's on-board GW3
14	192.168.254.130/28	PIS on-board	OB-GW-K4	172.21.160.182/27	TCP	8443	OB_{app} loose messages with Kontron's on-board GW4
15	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2223	Sending E2E text messages with a high priority
15b	192.168.254.10/27	PIS trackside	PIS TS - virtual IP	192.168.3.0/24	TCP	2223	To take into account virtual IP address for Sending E2E text messages with a high priority
15c	192.168.2.0/24	PIS OB - virtual IP	PIS on-board	192.168.254.130/28	TCP	2223	To take into account virtual IP address for Sending E2E text messages with a high priority
16	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2222	Sending E2E text messages with a normal priority Train mission DB sync to display accurate location information
16b	192.168.254.10/27	PIS trackside	PIS TS - virtual IP	192.168.3.0/24	TCP	2222	Take into account virtual IP Sending E2E text messages with a normal priority
16c	192.168.2.0/24	PIS OB - virtual IP	PIS on-board	192.168.254.130/28	TCP	2222	Take into account virtual IP Sending E2E text messages with a normal priority
17	192.168.254.130/28	PIS on-board	PIS trackside	192.168.254.10/27	UDP	514	Offloading of the on-board log files
17b	192.168.254.130/28	PIS on-board	PIS OB - virtual IP	192.168.2.0/24	UDP	514	Take into account virtual IP for Offloading of the on-board log files
17c	192.168.3.0/24	PIS TS virtual IP	PIS trackside	192.168.254.10/27	UDP	514	Take into account virtual IP for Offloading of the on-board log files
18	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	22	PIS O&M
18b	192.168.254.10/27	PIS trackside	PIS TS - virtual IP	192.168.3.0/24	TCP	22	Take into account virtual IP for PIS O&M
18c	192.168.2.0/24	PIS OB - virtual IP	PIS on-board	192.168.254.130/28	TCP	22	Take into account virtual IP for PIS O&M
19	192.168.254.10/27	PIS trackside	TS Robot	172.21.160.152/27	TCP	8443	TS_{app} loose messages with Kontron's trackside robot
20	192.168.254.130/28	PIS on-board	OB Robot	172.21.160.183/27	TCP	8443	OB_{app} loose messages with Kontron's on-board robot
21	192.168.254.10/27	PIS trackside	TS-GW-A	172.21.160.143/27	TCP	8765	TS_{app} loose messages with Alstom's trackside GW
22	192.168.254.130/28	PIS on-board	OB-GW-A	172.21.160.171/27	TCP	8765	OB_{app} loose messages with Alstom's on-board GW

Figure 44: WP4-PIS Lab flow matrix

3.2 Phasing approach for WP4 PIS lab integration

Three phases are considered to validate the integration of PIS prototype in FRMCS infrastructure:

- Phase 1: Validate equipment in Thales SGF's lab reaches equipment in Kontron's lab and vice-versa,
- Phase 2: Validate the implementation of the PIS flow matrix in the firewalls,
- Phase 3: Validate basic PIS functional test cases.

In the following chapters, describing PIS test cases, the notation using "$" is a Linux terminal command that does not require "super user" privileges to be executed:

```
$ command
```

On the contrary, the notation using "#" is a Linux terminal command that requires "super privileges" to be executed:

```
# command
```

3.2.1 Phase 1: Validate the reachability between PIS equipment & FRMCS infrastructure

The purpose of this phase is to validate the remote connection set-up which interconnects equipment in Thales SGF's premises and equipment in Kontron's premises.

Figure 45 illustrates the network architecture used during the execution of the tests.

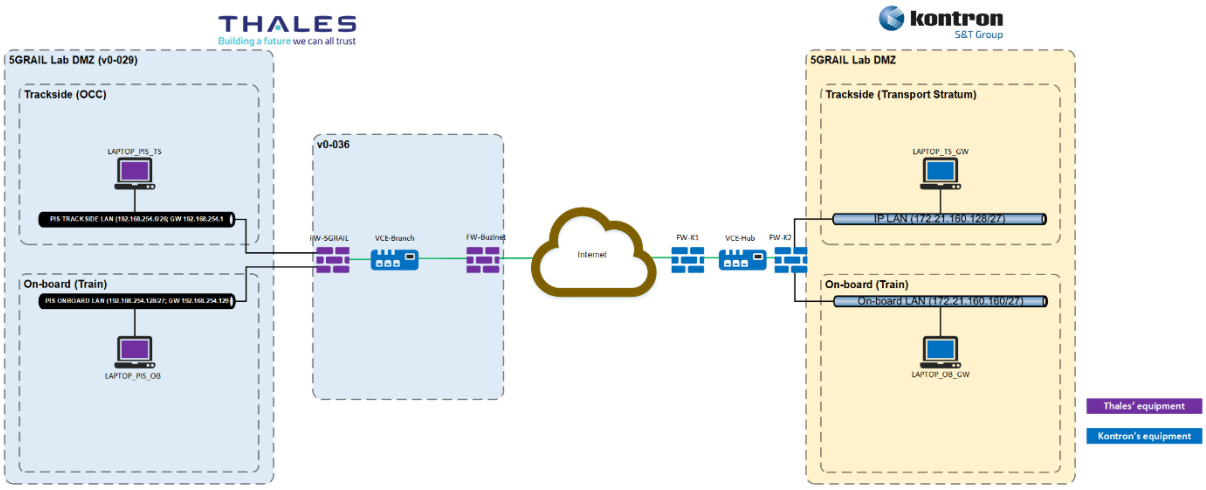


Figure 45: Network architecture used for reachability tests

Basically, the aim is to verify that the "VCE-Branch" installed in Thales SGF's premises is capable of establishing an SDWAN tunnel with the VCE-hub installed in Kontron's premises i.e. Thales SGF "FW-Buzinet" and Kontron "FW-K1" authorize the corresponding network flows to permit the communication between PIS and FRMCS equipment.

Therefore, the network flow matrix (see Figure 44) is not implemented in the firewalls. Only ICMP protocol is authorized in "FW-5GRAIL", "FW-K2" and in "FW-Buzinet", "FW-K1" (in addition to SDWAN protocol) and WP4-PIS Lab is simplified. Four laptops are used to simulate PIS equipment and FRMCS gateways:

- LAPTOP_PIS_TS simulates the PIS trackside server,
- LAPTOP_PIS_OB simulates the PIS on-board server,
- LAPTOP_TS_GW simulates the FRMCS trackside gateway,
- LAPTOP_OB_GW simulates the FRMCS on-board gateway.

These laptops send ICMP messages to each other in order to verify the reachability.

Table 3 gives the IP addresses used by the different equipment involved in the tests.

Equipment	IP address
LAPTOP_PIS_TS	192.168.254.10/26
LAPTOP_PIS_OB	192.168.254.130/27
LAPTOP_TS_GW	172.21.160.162/27
LAPTOP_OB_GW	172.21.160.130/27

Table 3: IP plan of phase 1 Test Cases

Notes:

1. *The tests described in the following chapters were executed in June 2021.*
2. *When the tests were executed, the IP plan was not yet clearly defined. This is the reason why the subnets differ from those configured in phase 2.*

3.2.1.1 TC_001: Reachability of on-board equipment

3.2.1.1.1 PURPOSE

The purpose of this test is to validate the ability of the PIS on-board equipment to reach the FRMCS on-board Gateway and the FRMCS on-board Gateway to reach the PIS on-board equipment. Figure 46 depicts the network equipment routing the ICMP packets used to validate the on-board equipment reachability.

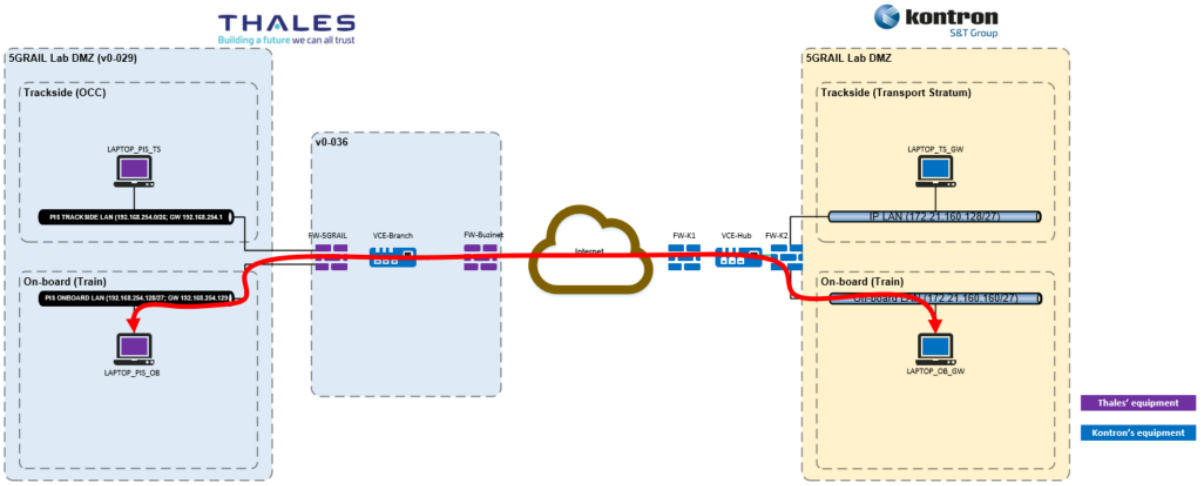


Figure 46: Ping route between PIS OB and FRMCS OB GW

3.2.1.1.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

The initial state covers the following steps:

- Laptops are configured and up,

- Kontron VCE are configured and up,
- The firewalls of Thales SGF and Kontron are configured to authorize ICMP packets between the different equipment,
- The internal firewall of the laptops is deactivated,
- Network protocol analyser (e.g. Wireshark) is started and configured to capture traffic on the network interfaces involved in the test.

3.2.1.1.3 TEST PROCEDURE 1: PIS ONBOARD EQUIPMENT REACHES FRMCS ON-BOARD GATEWAY

Step	Action	Expected result(s)
01	Execute “ping” command to send ICMP ECHO-REQUEST messages from LAPTOP_PIS_OB to the IP address of LAPTOP_OB_GW.	LAPTOP_PIS_OB shall receive ICMP ECHO-REPLY messages from LAPTOP_OB_GW with an acceptable latency.

Table 4: Reachability of on-board equipment - test procedure 1

3.2.1.1.4 TEST PROCEDURE 2: FRMCS ONBOARD GATEWAY REACHES PIS ONBOARD EQUIPMENT

Step	Action	Expected result(s)
01	Execute “ping” command to send ICMP ECHO-REQUEST messages from LAPTOP_OB_GW to the IP address of LAPTOP_PIS_OB.	LAPTOP_OB_GW shall receive ICMP ECHO-REPLY messages from LAPTOP_PIS_OB with an acceptable latency.

Table 5: Reachability of on-board equipment - test procedure 2

3.2.1.1.5 TEST OBSERVATIONS

Remarks	Impossible to deactivate the firewall of LAPTOP_OB_GW (credentials of Administrator account unknown). The consequence was the ICMP ECHO-REQUEST sent by LAPTOP_PIS_OB were blocked. Nevertheless, the requests were accepted by FW_K2. Therefore, Kontron & Thales decided to modify the test procedure 1. Indeed, the ICMP ECHO-REQUEST messages sent by the LAPTOP_PIS_OB were sent to FW_K2 (172.21.160.129) instead of LAPTOP_OB_GW.
Tested by	Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE1_TC001.pcapng
Test result	Passed

Table 6: Reachability of on-board equipment - test observations

3.2.1.2 TC_002: Reachability of trackside equipment

3.2.1.2.1 PURPOSE

The purpose of this test is to validate the ability of the PIS trackside equipment to reach the FRMCS trackside Gateway and the FRMCS trackside Gateway to reach the PIS trackside equipment. Figure 47 depicts the network equipment routing the ICMP packets used to validate the trackside equipment reachability.

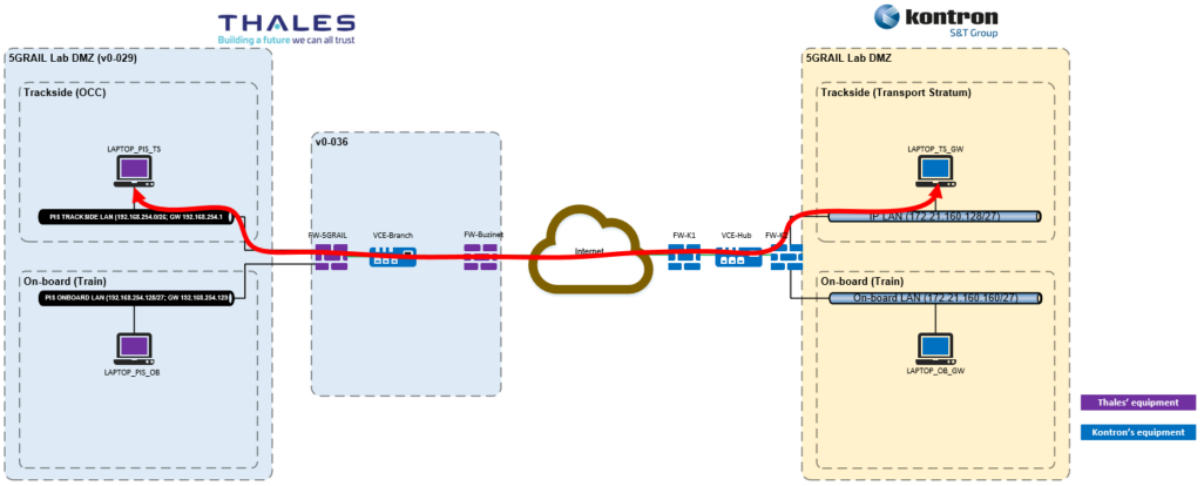


Figure 47: Ping route between PIS TS and FRMCS TS GW

3.2.1.2.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

The initial state covers the following steps:

- Laptops are configured and up,
- Kontron VCE are configured and up,
- The Firewalls of Thales SGF and Kontron are configured to authorize ICMP packets between the different equipment,
- The internal firewall of the laptops is deactivated,
- Network protocol analyser (e.g. Wireshark) is started and configured to capture traffic on the network interfaces involved in the test.

3.2.1.2.3 TEST PROCEDURE 1: PIS TRACKSIDE EQUIPMENT REACHES FRMCS TRACKSIDE GATEWAY

Step	Action	Expected result(s)
01	Execute “ping” command to send ICMP ECHO-REQUEST messages from LAPTOP_PIS_TS to the IP address of LAPTOP_TS_GW.	LAPTOP_PIS_TS shall receive ICMP ECHO-REPLY messages from LAPTOP_TS_GW with an acceptable latency.

Table 7: Reachability of trackside equipment - test procedure 1

3.2.1.2.4 TEST PROCEDURE 2: FRMCS TRACKSIDE GATEWAY REACHES PIS TRACKSIDE EQUIPMENT

Step	Action	Expected result(s)
01	Execute "ping" command to send ICMP ECHO-REQUEST messages from LAPTOP_TS_GW to the IP address of LAPTOP_PIS_TS.	LAPTOP_TS_GW shall receive ICMP ECHO-REPLY messages from LAPTOP_PIS_TS with an acceptable latency.

Table 8: Reachability of trackside equipment - test procedure 2

3.2.1.2.5 TEST OBSERVATIONS

Remarks	Impossible to deactivate the firewall of LAPTOP_TS_GW (credentials of Administrator account unknown). So, the ICMP ECHO-REQUEST sent by LAPTOP_PIS_TS were blocked. Nevertheless, the requests were accepted by FW_K2. Kontron & Thales decided this result is acceptable to validate the test.
Tested by	Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE1_TC002.pcapng
Test result	Passed

Table 9: Reachability of trackside equipment - test observations

3.2.2 Phase 2: Validate the implementation of the PIS flow matrix

The network architecture used in the following tests is described in Figure 42. The flow matrix to consider is given by Figure 44.

Note: At this stage, only FRMCS gateways provided by Alstom are available and therefore usable for end-to-end tests.

3.2.2.1 TC_001: Time synchronization test cases

3.2.2.1.1 PURPOSE

The purpose of this test is to validate that:

- PIS trackside server is able to synchronize its clock with the trackside NTP server,
- PIS on-board server and the Location Simulator are able to synchronize their clocks with the on-board NTP server.

Figure 48, Figure 49 and Figure 50 respectively depict the network equipment routing NTP packets for the time synchronization of the PIS trackside/on-board servers and the Location Simulator.

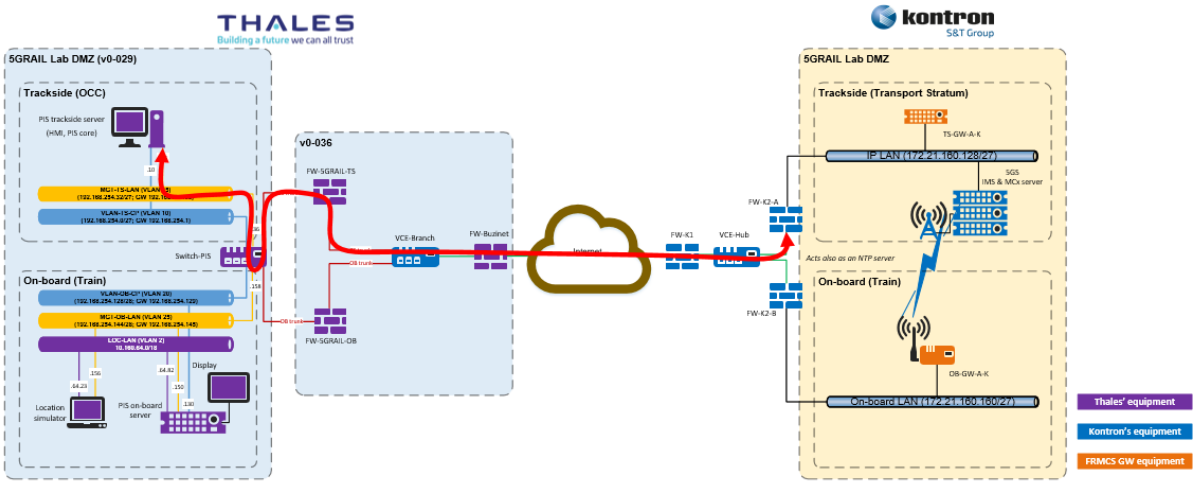


Figure 48: NTP synchronization of PIS TS server

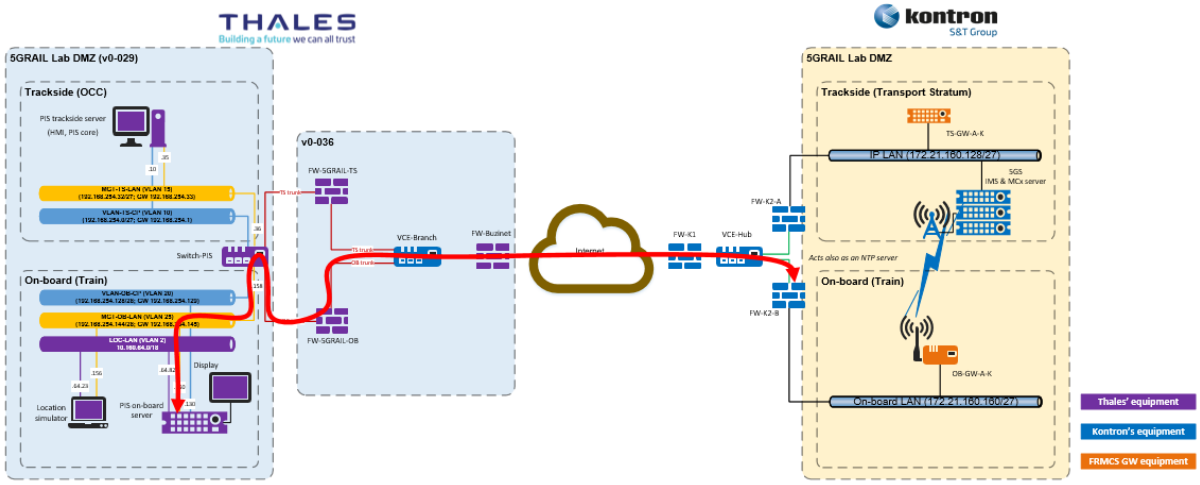


Figure 49: NTP synchronization of PIS OB server

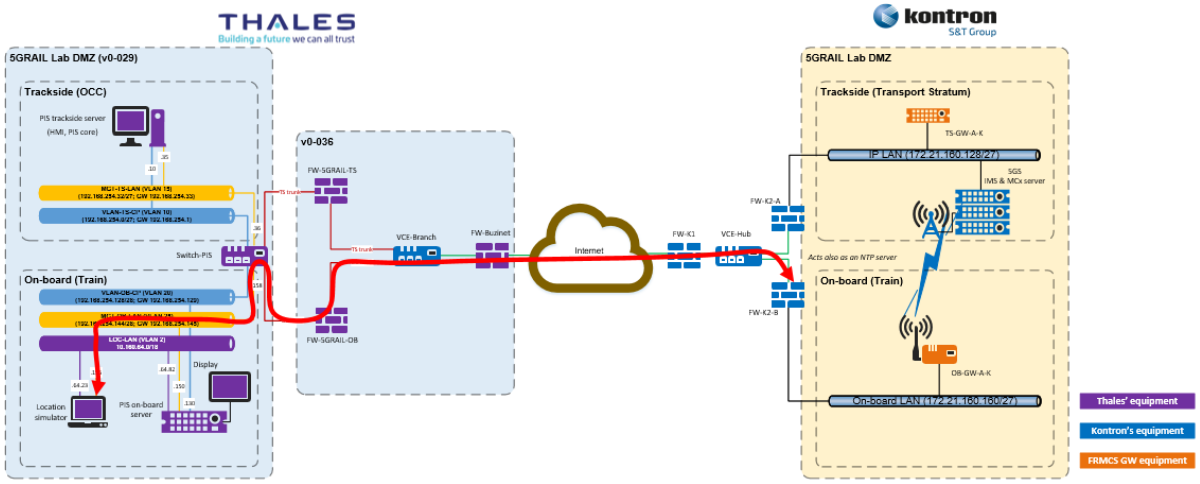


Figure 50: NTP synchronization of Location simulator

3.2.2.1.2 DESCRIPTION OF INITIAL STATE/CONFIGURATION

The firewalls of Thales SGF and Kontron shall authorize the following flows (extract from the WP4-PIS flow matrix, see Figure 44):

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
172.21.160.129/27	TS NTP server	PIS trackside server	192.168.254.35/27	UDP	123
172.21.160.161/27	OB NTP server	PIS on-board server	192.168.254.150/28	UDP	123
172.21.160.161/27	OB NTP server	Loc simulator	192.168.254.156/28	UDP	123
192.168.254.35/27	PIS trackside server	TS NTP server	172.21.160.129/27	UDP	123
192.168.254.150/28	PIS on-board server	OB NTP server	172.21.160.161/27	UDP	123
192.168.254.156/28	Loc simulator	OB NTP server	172.21.160.161/27	UDP	123

The PIS trackside and on-board servers are running.

The Location simulator is running.

The NTP client of PIS trackside server is configured to synchronize its clock to trackside NTP server (IP address is 172.21.160.129/27) as NTP master clock.

The NTP clients of PIS on-board server and the Location Simulator are configured to synchronize their clocks to the on-board NTP server (IP address is 172.21.160.161) as NTP master clock.

The trackside and on-board NTP servers are configured as an NTP master clock and authorize the PIS trackside and on-board servers and the Location Simulator to synchronize their clocks to it.

A protocol analyser like Wireshark is running on:

- PIS trackside & on-board servers and the Location Simulator
- Thales SGF's & Kontron's firewalls.

3.2.2.1.3 TEST PROCEDURE 1: SUCCESSFUL TIME SYNCHRONIZATION OF THE PIS TRACKSIDE SERVER

Step	Action	Expected result(s)

01	From the PIS trackside server, open a Linux terminal in order to execute the Linux command `chronyc`.
	`$ sudo chronyc sources -v`
		The protocol analyser displays the NTP packets exchanges between the TS NTP server 172.21.160.129 and the PIS trackside server 192.168.254.35.
		
		The output of the command shall indicate that the clock of the server is synchronized with the master clock:
		`$ sudo chronyc sources -v`
		`…`
		`MS Name/IP address Stratum Poll Reach LastRx Last sample`
		`==========`
		`^* 172.21.160.129...`
		`…`

Table 10: Validate the implementation of the PIS flow matrix - test procedure 1

3.2.2.1.4 TEST PROCEDURE 2: SUCCESSFUL TIME SYNCHRONIZATION OF THE PIS ON-BOARD SERVER

Step	Action	Expected result(s)

01	From the PIS on-board server, open a Linux terminal in order to execute the Linux command `ntpq`.
	`# ntpq -p`
		The protocol analyser displays the NTP packets exchanges between the OB NTP server 172.21.160.161 and the PIS on-board server 192.168.254.150.
		The output of the command `ntpq` shall indicate that the clock of the server is synchronized with the master clock:
		`# ntpq -p`
		`remote refid st t when poll reach delay offset jitter`
		…
		`*172.21.160.161 …`

Table 11: Validate the implementation of the PIS flow matrix - test procedure 2

3.2.2.1.5 TEST PROCEDURE 3: SUCCESSFUL TIME SYNCHRONIZATION OF THE LOCATION SIMULATOR

Step	Action	Expected result(s)

01	From the PIS Location Simulator server, open a Linux terminal in order to execute the Linux command `ntpq`.
	`$ sudo ntpq -p`
		The protocol analyser displays the NTP packets exchanges between the TS NTP server 172.21.160.161 and the Location simulator 192.168.254.156.
		The output of the command shall indicate that the clock of the server is synchronized with the master clock:
		`$ sudo ntpq -p`
		`remote refid st t when poll reach delay offset jitter`
		…
		`*172.21.160.161 …`

Table 12: Validate the implementation of the PIS flow matrix - test procedure 3

3.2.2.1.6 TEST OBSERVATIONS

Tested by	**Kontron** **Thales**
Attachments (log/trace file)	Traces taken from the PIS trackside server • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP01.log (proves that the PIS trackside server and trackside NTP server are time-synchronized). • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP01.pcapng (proves that NTP packets are exchanged between PIS trackside server and the trackside NTP server). Traces taken from the PIS on-board server • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP02.log (proves that the PIS on-board server and on-board NTP server are time-synchronized). • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP02.pcapng (proves that NTP packets are exchanged between the PIS on-board server and the on-board NTP server). Traces taken from the Location Simulator • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP03.log (proves that the Location Simulator and on-board NTP server are time-synchronized). 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC001_TP03.pcapng (proves that NTP packets are exchanged between the Location Simulator and the on-board NTP server).
Test result	Passed

Table 13: Validate the implementation of the PIS flow matrix - test observations

3.2.2.2 TC_002: FRMCS loose API test cases

3.2.2.2.1 PURPOSE

The purpose of this test is to validate that the port 443/TCP used to exchange FRMCS loose API messages is authorized in the firewalls.

Figure 51 and Figure 52 depict the network equipment routing FRMCS loose packets for trackside and on-board connections.

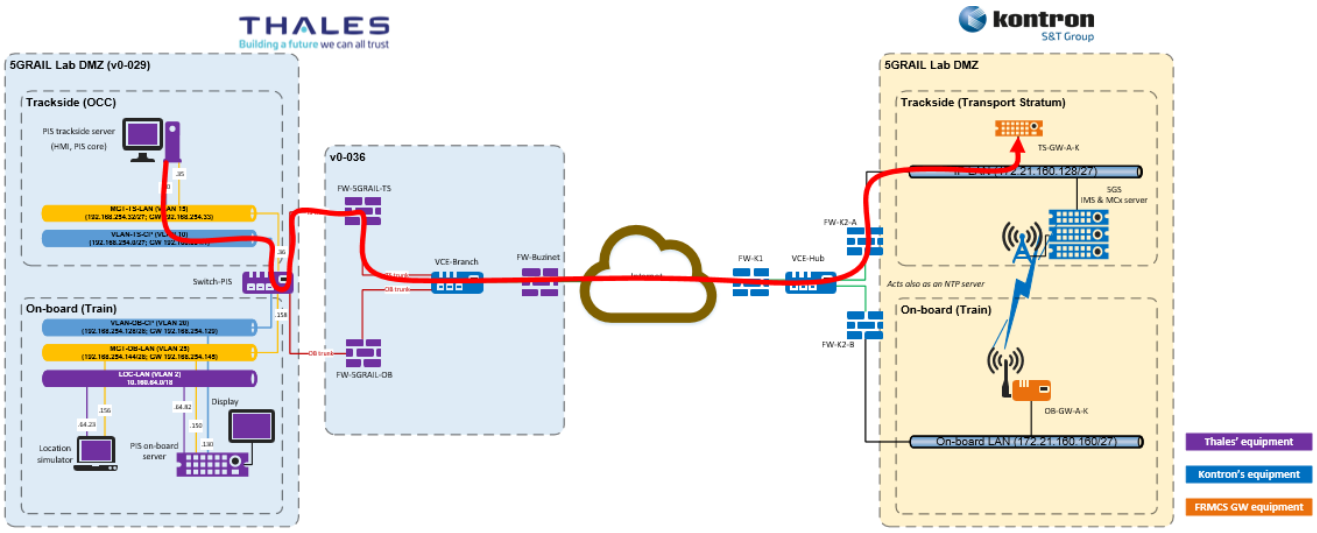


Figure 51: FRMCS TS loose connection

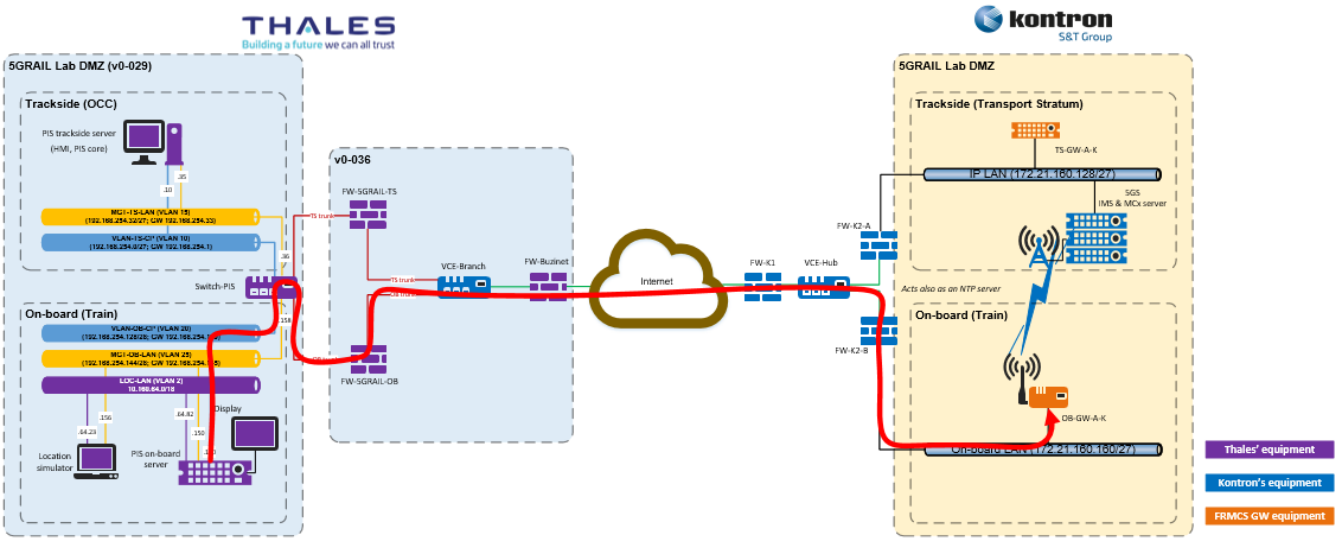


Figure 52: FRMCS OB loose connection

3.2.2.2.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

The firewalls of Thales SGF and Kontron shall authorize the following flows (extract from the WP4-PIS flow matrix, see Figure 44):

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
192.168.254.10/27	PIS trackside	TS-GW-A	172.21.160.143/27	TCP	443
192.168.254.10/27	PIS trackside	TS-GW-K1	172.21.160.151/27	TCP	443
192.168.254.10/27	PIS trackside	TS-GW-K2	172.21.160.146/27	TCP	443
192.168.254.130/28	PIS on-board	OB-GW-A	172.21.160.171/27	TCP	443
192.168.254.130/28	PIS on-board	OB-GW-K1	172.21.160.175/27	TCP	443
192.168.254.130/28	PIS on-board	OB-GW-K2	172.21.160.177/27	TCP	443
192.168.254.130/28	PIS on-board	OB-GW-K3	172.21.160.180/27	TCP	443
192.168.254.130/28	PIS on-board	OB-GW-K4	172.21.160.182/27	TCP	443

Note: Telnet protocol will be used to simulate the exchanges of FRMCS loose messages. Therefore, depending on the Firewall provider, the port 23/TCP will have to be temporarily authorized in the firewalls for these tests.

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
192.168.254.10/27	PIS trackside	TS-GW-A	172.21.160.143/27	TCP	23
192.168.254.10/27	PIS trackside	TS-GW-K1	172.21.160.151/27	TCP	23
192.168.254.10/27	PIS trackside	TS-GW-K2	172.21.160.146/27	TCP	23
192.168.254.130/28	PIS on-board	OB-GW-A	172.21.160.171/27	TCP	23
192.168.254.130/28	PIS on-board	OB-GW-K1	172.21.160.175/27	TCP	23
192.168.254.130/28	PIS on-board	OB-GW-K2	172.21.160.177/27	TCP	23
192.168.254.130/28	PIS on-board	OB-GW-K3	172.21.160.180/27	TCP	23
192.168.254.130/28	PIS on-board	OB-GW-K4	172.21.160.182/27	TCP	23

The PIS trackside and on-board servers are running.

The Location simulator is running.

A protocol analyser like Wireshark is running on:

- PIS trackside and on-board servers,
- Thales SGF's & Kontron's firewalls.

3.2.2.2.3 TEST PROCEDURE 1: SUCCESSFUL FRMCS TRACKSIDE LOOSE CONNECTION

Step	Action	Expected result(s)
01	From the PIS trackside server, open a Linux terminal and execute the Linux command `telnet` to join the Alstom's FRMCS trackside GW: `$ telnet 172.21.160.143 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS trackside server 192.168.254.10 to the Alstom's FRMCS trackside GW 172.21.160.143 with destination port = 443/TCP.
02	From the PIS trackside server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS trackside GW1: `$ telnet 172.21.160.151 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS trackside server 192.168.254.10 to the Kontron's FRMCS trackside GW1 172.21.160.151 with destination port = 443/TCP.
03	From the PIS trackside server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS trackside GW2: `$ telnet 172.21.160.146 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS trackside server 192.168.254.10 to the Kontron's FRMCS trackside GW2 172.21.160.145 with destination port = 443/TCP.

Table 14: FRMCS loose API test cases - test procedure 1

3.2.2.2.4 TEST PROCEDURE 2: SUCCESSFUL FRMCS ON-BOARD LOOSE CONNECTION

Step	Action	Expected result(s)
01	From the PIS on-board server, open a Linux terminal and execute the Linux command `telnet` to join the Alstom's FRMCS on-board GW: `$ telnet 172.21.160.171 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS on-board server 192.168.254.130 to the Alstom's FRMCS on-board GW 172.21.160.171 with destination port = 443/TCP.
02	From the PIS on-board server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS on-board GW1: `$ telnet 172.21.160.175 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS on-board server 192.168.254.130 to the Kontron's FRMCS on-board GW1 172.21.160.175 with destination port = 443/TCP.
03	From the PIS on-board server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS on-board GW2: `$ telnet 172.21.160.177 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS on-board server 192.168.254.130 to the Kontron's FRMCS on-board GW2 172.21.160.177 with destination port = 443/TCP.
	From the PIS on-board server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS on-board GW3: `$ telnet 172.21.160.180 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS on-board server 192.168.254.130 to the Kontron's FRMCS on-board GW3 172.21.160.180 with destination port = 443/TCP.
	From the PIS on-board server, open a Linux terminal and execute the Linux command `telnet` to join the Kontron's FRMCS on-board GW4: `$ telnet 172.21.160.182 443` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS on-board server 192.168.254.130 to the Kontron's FRMCS on-board GW4 172.21.160.182 with destination port = 443/TCP.

Table 15: FRMCS loose API test cases - test procedure 2

3.2.2.2.5 TEST OBSERVATIONS

Remarks	In PCAPNG log files, there are packet retransmissions. Indeed, at this stage no service/program is running on the FRMCS GWs to treat TCP/443 messages. The purpose of this test is to validate that the port 443/TCP used to exchange FRMCS loose API messages is authorized in the firewalls.
Tested by	Kontron Thales
Attachments (log/trace file)	Traces taken from PIS trackside server • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_002_TP01.pcapng (proves that TCP/443 packets are exchanged between the PIS trackside server and the FRMCS trackside GWs). Traces taken from FW-K2-A which manages PIS trackside flows • 5GRail_WP4_Thales_D4_2_PIS_packetcapture-FW2A-TCP443.cap Traces taken from PIS on-board server • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_002_TP02.pcapng (proves that TCP/443 packets are exchanged between the PIS on-board server and the FRMCS on-board GWs). Traces taken from FW-K2-B which manages PIS on-board flows 5GRail_WP4_Thales_D4_2_PIS_packetcapture-FW2B-TCP443.cap
Test result	Passed

Table 16: FRMCS loose API test cases - test observations

3.2.2.3 TC_003: Sending test messages to train

3.2.2.3.1 PURPOSE

The purpose of this test is to validate the ports 2222/TCP & 2223/TCP are authorized in the firewalls. These ports are used to send text messages with a normal or a high priority from trackside to on-board.

Figure 53 depicts the network equipment routing PIS text messages.

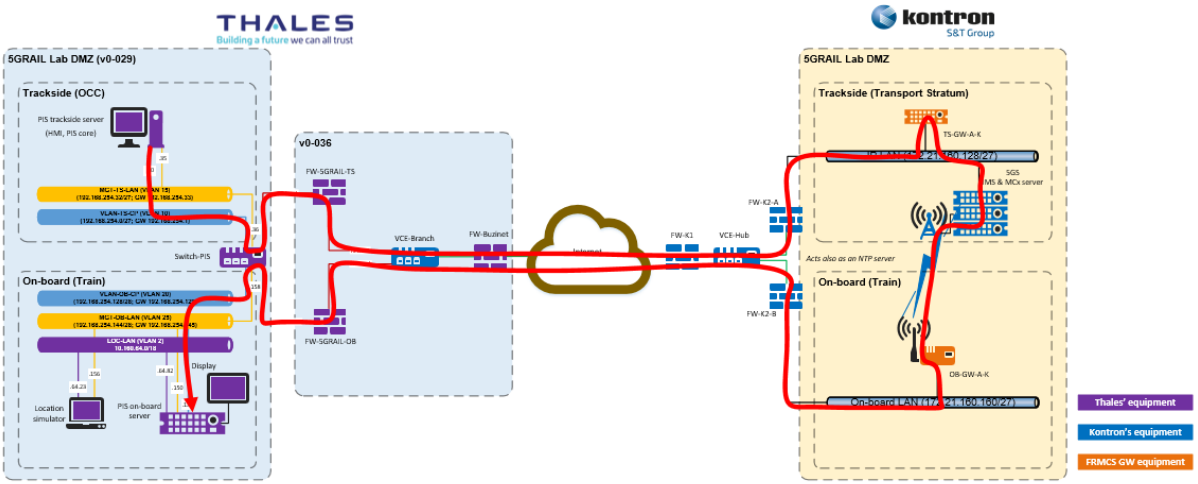


Figure 53: Test messages flow from TrackSide to Train

3.2.2.3.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

The firewalls of Thales SGF and Kontron shall authorize the following flows (extract from the WP4-PIS flow matrix, see Figure 44):

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2222
192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2223

The PIS trackside server is running.

The PIS manager is connected to the PIS Web Interface (hosted by the PIS trackside server, see Figure 54) and ready to compose and send text messages.

Figure 54: HMI allowing the PIS manager to send text messages to trains

A protocol analyser like Wireshark is running on

- PIS trackside & on-board servers,
- Thales SGF's & Kontron's firewalls,
- Alstom's FRMCS gateways.

3.2.2.3.3 TEST PROCEDURE 1: SUCCESSFUL SENDING OF A MESSAGE WITH A NORMAL PRIORITY

Step	Action	Expected result(s)
01	The PIS manager composes his message by choosing a normal priority and send it.	The protocol analysers display TCP packets sent from the PIS trackside server 192.168.254.10 to the PIS on-board server 192.168.254.130 with destination port = 2222/TCP.

Table 17: Sending test messages to train - test procedure 1

3.2.2.3.4 TEST PROCEDURE 2: SUCCESSFUL SENDING OF A MESSAGE WITH A HIGH PRIORITY

Step	Action	Expected result(s)
01	The PIS manager composes his message by choosing a high priority and send it.	The protocol analysers display TCP packets sent from the PIS trackside server 192.168.254.10 to the PIS on-board server 192.168.254.130 with destination port = 2223/TCP.

Table 18: Sending test messages to train - test procedure 2

3.2.2.3.5 TEST OBSERVATIONS

Tested by	Alstom Kontron Thales
Attachments (log/trace file)	Traces taken from the PIS trackside & on-board servers proving that the port 2222/TCP is opened (test procedure 1, see chapter 3.2.2.3.3) in the firewalls and the E2E traffic is correctly routed • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_003_TP01_TS.pcapng • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_003_TP01_OB.pcapng Traces taken from the PIS trackside & on-board servers proving that the port 2223/TCP is opened (test procedure 2, see chapter 0) in the firewalls and the E2E traffic is correctly routed • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_003_TP02_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_003_TP02_OB.pcapng
Test result	Passed

Table 19: Sending test messages to train - test observations

3.2.2.4 TC_004: Offloading of the on-board logs

3.2.2.4.1 PURPOSE

The purpose of this test is to validate the port 514/UDP is authorized in the firewalls.

Figure 55 depicts the network equipment routing PIS log flows.

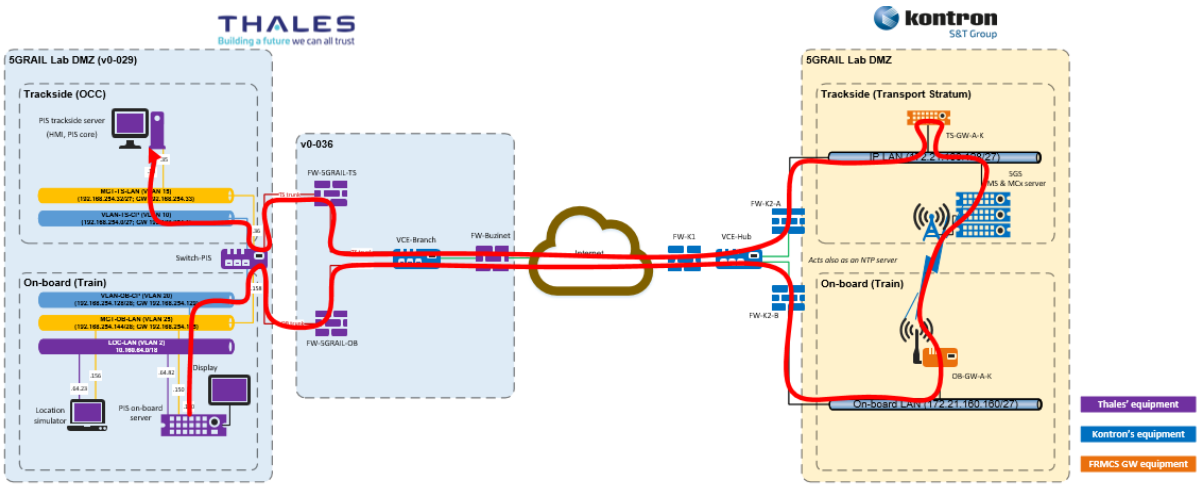


Figure 55: Offloading of OB logs from Train to Trackside

3.2.2.4.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

The firewalls of Thales SGF and Kontron shall authorize the following flows (extract from the WP4-PIS flow matrix, see Figure 44):

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
192.168.254.130/28	PIS on-board	PIS trackside	192.168.254.10/27	UDP	514

The PIS on-board server is running.

The Linux log manager is configured to download its logs to the PIS trackside server.

A protocol analyser like Wireshark is running on the PIS on-board server and on Thales SGF's & Kontron's firewalls.

3.2.2.4.3 TEST PROCEDURE

Step	Action	Expected result(s)
01		The protocol analysers display UDP packets sent from the PIS on-board server 192.168.254.130 to the PIS trackside server 192.168.254.10 with destination port = 514/UDP.

Table 20: Offloading of the on-board logs - test procedure

3.2.2.4.4 TEST OBSERVATIONS

Tested by	**Alstom** **Kontron** **Thales**
Attachments (log/trace file)	Traces taken from the PIS trackside & on-board servers proving that the port 514/UDP is opened in the firewalls and the E2E traffic is correctly routed • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_004_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_004_OB.pcapng
Test result	Passed

Table 21: Offloading of the on-board logs - test observations

3.2.2.5 TC_005: OM flows

3.2.2.5.1 PURPOSE

The purpose of this test is to validate the port 22/TCP is authorized in the firewalls.

Figure 56 depicts the network equipment routing PIS O&M flows.

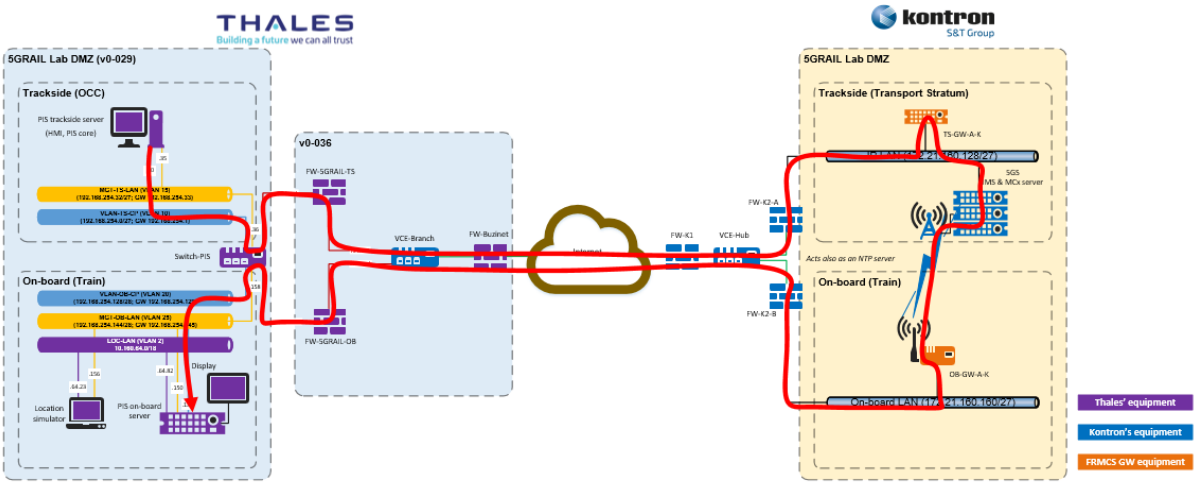


Figure 56: O&M flows from TrackSide to Train

3.2.2.5.2 DESCRIPTION OF INITIAL STATE/CONFIGURATION

The firewalls of Thales SGF and Kontron shall authorize the following flows (extract from the WP4-PIS flow matrix, see Figure 44):

Source IP address	Source Hostname	Destination Hostname	Destination IP address	Protocol	Destination Port Number
192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	22

The PIS trackside server is running.

A protocol analyser like Wireshark is running on the PIS trackside server and on Thales SGF's & Kontron's firewalls.

3.2.2.5.3 TEST PROCEDURE

Step	Action	Expected result(s)
01	From the PIS trackside server, open a Linux terminal and execute the Linux command `telnet` to join the Alstom's FRMCS trackside GW: `$ telnet 192.168.254.130 22` You do not need to use `sudo` command.	The protocol analysers display telnet packets sent from the PIS trackside server 192.168.254.10 to the PIS on-board server 192.168.254.130 with destination port = 22/TCP.

Table 22: OM flows - test procedure

3.2.2.5.4 TEST OBSERVATIONS

Tested by	**Alstom** **Kontron** **Thales**
Attachments (log/trace file)	Traces taken from the PIS trackside & on-board servers proving that the port 22/TCP is opened in the firewalls and the E2E traffic is correctly routed • 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_005_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE2_TC_005_OB.pcapng
Test result	Passed

Table 23: OM flows - test observations

3.2.3 Phase 3: Validate basic PIS functional test cases

This is the last phase to validate the WP4-PIS Lab set-up. PIS application was used with TOBA-A on N8.

Phases 1 and 2 focus mainly on the validation of the remote connection configuration. The purpose of this phase is to validate basic end-to-end PIS functional scenario.

At this stage, two phases are considered for functional PIS integration:

- PIS in flat-IP mode starting in November 2021
- PIS in loose mode starting in May 2022

Therefore, this “validation” phase is divided in two sub-phases:

- Phase 3.a: Validate basic PIS functional scenario in flat-IP mode,
- Phase 3.b: Validate basic PIS functional scenario in loose mode.

3.2.3.1 Phase 3.a: Validate basic PIS functional scenario in flat-IP mode

The network architecture used in the following tests is described in Figure 42. The flow matrix to consider is given by Figure 44.

Figure 57 provides the DSCP and 5QI values to configure in the FRMCS Gateways and in the 5G Core.

PIS flow matrix							QoS		
Rules id	Src @IP	Hostname Src	Hostname Dst	Dst @IP	Protocol	Dst Port	DSCP value/name	5QI	Comment
15	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2223	40/CS5	5	Sending E2E text messages with a high priority
16	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	2222	16/CS2	6	Sending E2E text messages with a normal priority Train mission DB sync to display accurate location information
17	192.168.254.130/28	PIS on-board	PIS trackside	192.168.254.10/27	UDP	514	8/CS1	8	Offloading of the on-board log files
18	192.168.254.10/27	PIS trackside	PIS on-board	192.168.254.130/28	TCP	22	8/CS1	8	PIS O&M

Figure 57: Mapping of DSCP and 5QI values for PIS application

Note: At this stage, only Alstom’s FRMCS GW are capable of configuring QoS and at this time only DSCP value from CS0 to CS7.

In the following test cases, the PIS trackside software is configured if the content of its configuration file “/tsPis/config.xml” is:

```
<config>
    <mode>flat-ip</mode>
    <test>extern</test>
    <parameters>
        <rsyslogInit>/etc/init.d/rsyslog</rsyslogInit>
        <retry>5</retry>

<loosePrerequisite>/tsPis/prerequisites/TSPIS_test_loose.sh</loosePrerequis
ite>

<flatipPrerequisite>/tsPis/prerequisites/TSPIS_test_flatip.sh</flatipPrereq
uisite>
        <registrationNames>
            <msg_ts_pis>msg.ts.pis</msg_ts_pis>
            <mgt_ts_pis>mgt.ts.pis</mgt_ts_pis>
```

```
            <log_ts_pis>log.ts.pis</log_ts_pis>
        </registrationNames>
    </parameters>
    <python>/usr/bin/python2</python>
    <ipGateway>171.21.160.143</ipGateway>
    <portGateway>443</portGateway>
    <gatewayPath>/v0</gatewayPath>
    <env>trackside</env>
    <ssl>False</ssl>
    <certificate>/tsPis/cert.crt</certificate>
</config>
```

Note: The IP address of the FRMCS trackside gateway configured in "ipGateway" parameter may be modified depending on the gateway used (TS-GW-K1, TS-GW-K2 or TS-GW-A).

To start the PIS trackside software, execute the command:

```
# /tsPis/tsPis.sh run
```

To make sure the prerequisites are met, the status given by the command "/tsPis/tsPis.sh status" shall be [OK]:

```
# /tsPis/tsPis.sh status
mode: flat-ip
test: extern
status interface data:        [OK]
status interface mgt:         [OK]
status interface internal:    [OK]
status chronyd:               [OK]
status time synchronization:  [OK]
status apache2:               [OK]
status mysql:                 [OK]
status rsyslog:               [OK]
```

The PIS on-board software is configured if the content of its configuration file "/obPis/config.xml" is:

```
<config>
    <mode>flat-ip</mode>
    <test>extern</test>
```

```
    <rsyslog_server>192.168.254.10</rsyslog_server>
    <rsyslog_server_intern>10.0.0.2</rsyslog_server_intern>
    <parameters>
        <rsyslogInit>/etc/init.d/rsyslog</rsyslogInit>
        <rsyslogConf>/etc/rsyslog.conf</rsyslogConf>

<flatipPrerequisite>/obPis/prerequisites/OBPIS_test_flat_ip.sh</flatipPrere
quisite>

<loosePrerequisite>/obPis/prerequisites/OBPIS_test_loose.sh</loosePrerequis
ite>
        <registrationNames>
            <msg_ob_pis>msg.ob.pis</msg_ob_pis>
            <mgt_ob_pis>mgt.ob.pis</mgt_ob_pis>
            <log_ob_pis>log.ob.pis</log_ob_pis>
        </registrationNames>
    </parameters>
    <python>/usr/bin/python2</python>
    <ipGateway>171.21.160.171</ipGateway>
    <portGateway>443</portGateway>
    <gatewayPath>/v0</gatewayPath>
    <env>on-board</env>
    <ssl>False</ssl>
    <certificate>/obPis/cert.crt</certificate>
</config>
```

Note: The IP address of the FRMCS on-board gateway configured in “ipGateway” parameter may be modified depending on the gateway used (OB-GW-K1, OB-GW-K2, OB-GW-K3 or OB-GW-A).

To start the PIS on-board software, execute the command:

```
# /obPis/obPis.sh run
```

To make sure the prerequisites are met, the status given by the command “/obPis/obPis.sh status” shall be [OK]:

```
# /obPis/obPis.sh status
mode: flat-ip
test: extern
```

```
status interface eth0.20:           [OK]
status interface eth0.25:           [OK]
status interface eth0.2:            [OK]
status /Thales/obifModule/ntpd:     [OK]
status time synchronization:        [OK]
status tcmsAdapter.sh:              [OK]
status location simulation:         [OK]
```

3.2.3.1.1 TC_001: SEND TEXT MESSAGE WITH A NORMAL PRIORITY TO TRAINS

See PIS TC_001 in flat-IP test case scenarios in [S22].

Specific test configuration	Alstom GW with ES1 modem
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_001_TS.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_001_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_001_OB.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_001_OB.pcapng 5GRail_WP4_Kontron_D4.2_Thales_Alstom_PIS_DSCP_Test_15_16_17_18.txt
Test result	Passed

Table 24: Sending normal priority test messages to train (Flat-IP) - test observations

3.2.3.1.2 TC_002: SEND TEXT MESSAGE WITH A HIGH PRIORITY TO TRAINS

See PIS TC_002 in flat-IP test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_002_TS.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_002_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_002_OB.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_002_OB.pcapng 5GRail_WP4_Kontron_D4.2_Thales_Alstom_PIS_DSCP_Test_15_16_17_18.txt
Test result	Passed

Table 25: Sending high priority test messages to train (Flat-IP) - test observations

3.2.3.1.3 TC_003: DISPLAY TRAIN LOCATION INFORMATION

See PIS TC_005 in flat-IP test case scenarios in [S22].

Specific test configuration	Alstom GW with ES1 modem
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_003_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_003_OB.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_003.png 5GRail_WP4_Kontron_D4.2_Thales_Alstom_PIS_DSCP_Test_15_16_17_18.txt

Test result	Passed

Table 26: Display train location information (Flat-IP) - test observations

3.2.3.1.4 TC_004: ON-BOARD PIS LOGS DOWNLOADED ON THE FLY IN NORMAL CONDITIONS

3.2.3.1.4.1 PURPOSE

The purpose of this test is to validate the ability to send on the fly with a high priority the on-board PIS logs to trackside.

3.2.3.1.4.2 DESCRIPTION OF INITIAL STATE/CONFIGURATION

The initial state covers the following steps:

- PIS trackside and on-board equipment are installed, configured and started,
- PIS trackside and on-board software are configured and are running,
- FRMCS trackside and onboard Gateways are installed, configured and started,
- PIS trackside equipment is connected to the FRMCS trackside Gateway,
- PIS on-board equipment is connected to the FRMCS on-board Gateway,
- 5G system (Radio Access Network & Core Network) is operational,
- FRMCS on-board Gateway is connected to 5G Core Network (i.e., 5 Core Network has provided an IP address to the gateway).
- GRE tunnels between FRMCS trackside & on-board are operational and FRMCS gateways can communicate with each other,
- On-board logs centralization in trackside is configured,
- NTP server is configured and operational,
- NTP server, PIS trackside equipment, FRMCS trackside equipment, 5G system, FRMCS on-board equipment and PIS on-board equipment are time synchronized (date & time),
- Wireshark tool is running on PIS trackside and on-board equipment; it is capturing in/out traffic,
- PIS log flows are configured in the 5G system to use critical (i.e., corresponding to “Critical Data”) 5QI,
- FRMCS trackside and on-board Gateways internal traffic flow scheduler is configured to treat PIS log messages with a high priority (i.e., corresponding to “Critical Data”),
- Remote connection between Thales SGF lab and WP4 lab is operational (i.e., all PIS IP flows are authorized in the firewalls according to the flow matrix).

3.2.3.1.4.3 TEST PROCEDURE

Step	Action	Expected result(s)
01	On-board PIS logs are sent on the fly to trackside	On-board PIS logs are received on trackside in real time by the PIS trackside server. It can be verified by executing the Linux command “tail” from PIS trackside server: `# tail -f /var/log/congatec-qa3-64/obpis`

Table 27: Validate basic PIS functional test cases - test procedure

3.2.3.1.4.4 TEST OBSERVATIONS

Tested by	**Alstom** **Kontron** **Thales**
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_004_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_004_OB.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_004.png 5GRail_WP4_Kontron_D4.2_Thales_Alstom_PIS_DSCP_Test_15_16_17_18.txt
Test result	Passed

Table 28: Validate basic PIS functional test cases - test observations

3.2.3.1.5 TC_005: OPEN A “TRACKSIDE TO ON-BOARD” MANAGEMENT SESSION WITH A HIGH PRIORITY

3.2.3.1.5.1 PURPOSE

See PIS flat-ip TC_007 in document D1.1 [S22].

The purpose of this test is to validate the ability to open a “trackside to on-board” management session with a critical priority during a significant time (e.g., 15 minutes) for PIS O&M operations.

3.2.3.1.5.2 DESCRIPTION OF THE INITIAL STATE/CONFIGURATION

- The initial state covers the following steps:
- PIS trackside and on-board equipment are installed, configured and started,
- PIS trackside and on-board software are configured and are running,
- FRMCS trackside and onboard Gateways are installed, configured and started,
- PIS trackside equipment is connected to the FRMCS trackside Gateway,
- PIS on-board equipment is connected to the FRMCS on-board Gateway,
- 5G system (Radio Access Network & Core Network) is operational,
- FRMCS on-board Gateway is connected to 5G Core Network (i.e., 5G Core Network has provided an IP address to the gateway).
- GRE tunnels between FRMCS trackside & on-board are operational and FRMCS gateways can communicate with each other,
- NTP server is configured and operational,
- NTP server, PIS trackside equipment, FRMCS trackside equipment, 5G system, FRMCS on-board equipment and PIS on-board equipment are time synchronized (date & time),
- Wireshark tool is running on PIS trackside and on-board equipment; it is capturing in/out traffic,
- PIS O&M traffic flows are configured in the 5G system to use critical (i.e., corresponding to “Critical Data”) 5QI,
- The traffic flow scheduler of the FRMCS trackside and on-board gateways is configured to manage PIS O&M flows with a high priority corresponding to “Critical Data”,
- Remote connection between Thales SGF Lab and WP4 lab is operational (i.e., all PIS IP flows are authorized in the firewalls according to the flow matrix).

3.2.3.1.5.3 TEST PROCEDURE

Step	Action	Expected result(s)
01	From trackside PIS server, PIS maintainer opens an SSH connection to on-board PIS equipment using on-board PIS O&M IP address. Execute the script KeepAliveCon.sh to maintain the SSH connection alive for 15 minutes. `# ./KeepAliveCon.sh`	No disconnection of the trackside to on-board SSH connection for 15 minutes.

Table 29: Open a “trackside to on-board” management session with a high priority – test procedure

3.2.3.1.5.4 TEST OBSERVATIONS

Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_005.txt 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC005_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC005_OB.pcapng 5GRail_WP4_Kontron_D4.2_Thales_Alstom_PIS_DSCP_Test_15_16_17_18.txt
Test result	Passed

Table 30: Open a "trackside to on-board" management session with a high priority – test observations

3.2.3.2 Phase 3.b: Validate basic PIS functional scenario in loose mode

3.2.3.2.1 TC_001: SEND TEXT MESSAGE WITH A NORMAL PRIORITY TO TRAINS

See TC_013 PIS Loose test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem On TS side loose mode: “auto_reject” / On OB side loose mode: “auto_accept”
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_001_TS.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_001_TS.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_001_OB.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_001_OB.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng
Test result	Passed

Table 31: Sending normal priority test messages to train (auto-accept mode) - test observations

3.2.3.2.2 TC_002: SEND TEXT MESSAGE WITH A HIGH PRIORITY TO TRAINS

See TC_014 PIS Loose test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem On TS side loose mode: “auto_reject” / On OB side loose mode: “auto_accept”
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_002_TS.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_002_TS.pcapng

	5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_002_OB.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_002_OB.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng
Test result	Passed

Table 32: Sending high priority test messages to train (auto-accept mode) - test observations

3.2.3.2.3 TC_003: DISPLAY TRAIN LOCATION INFORMATION

See TC_017 PIS Loose test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_003_TS.txt
Test result	Passed

Table 33: Display train location information (auto-accept mode) - test observations

3.2.3.2.4 TC_004: ON-BOARD PIS LOGS DOWNLOADED ON THE FLY IN NORMAL CONDITIONS

See TC_018 PIS Loose test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem On TS side loose mode: “auto_accept” / On OB side loose mode: “auto_reject”
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_004_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_004_OB.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_004_logs.txt
Test result	Passed

Table 34: Offloading of the on-board logs (auto-accept mode) - test observations

Specific test configuration	Alstom GW with ES1 modem On TS side loose mode: “not_auto” / On OB side loose mode: “auto_reject”
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_004_TS_not_auto.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_004_OB_not_auto.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_004_logs_not_auto.txt
Test result	Passed

Table 35: Offloading of the on-board logs (not-auto mode) - test observations

3.2.3.2.5 TC_005: OPEN A “TRACKSIDE TO ON-BOARD” MANAGEMENT SESSION WITH A HIGH PRIORITY

See TC_019 PIS Loose test case scenarios in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem On TS side loose mode: “auto_reject” / On OB side loose mode: “auto_accept”
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRail_WP4_Thales_D4_2_PIS_PHASE3_TC_005_TS.pcapng 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_005_OB.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng
Test result	Passed

Table 36: Open a “trackside to on-board” management session with a high priority (loose mode) – test observations

3.2.3.2.1 TC_006: CHECK CONNECTION TO FRMCS SERVICES

See PIS Loose TC_020 in document D1.1 [S22].

Specific test configuration	Alstom GW with ES1 modem
Tested by	Alstom Kontron Thales
Attachments (log/trace file)	5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TC_006_TS.png 5GRail_WP4_Thales_D4_2_PIS_PHASE3B_TC_006_TS.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_TS_LOOSE_all_TCs.pcapng 5GRAIL_WP4_Thales_D4_2_PIS_PHASE3B_OB_LOOSE_all_TCs.pcapng
Test result	Passed

Table 37: Check FRMCS status of PIS application (loose mode) – test observations

4 ATO/ETCS applications integration

ETCS and ATO applications, provided by Alstom, fit into WP4 lab as depicted in Figure 58.

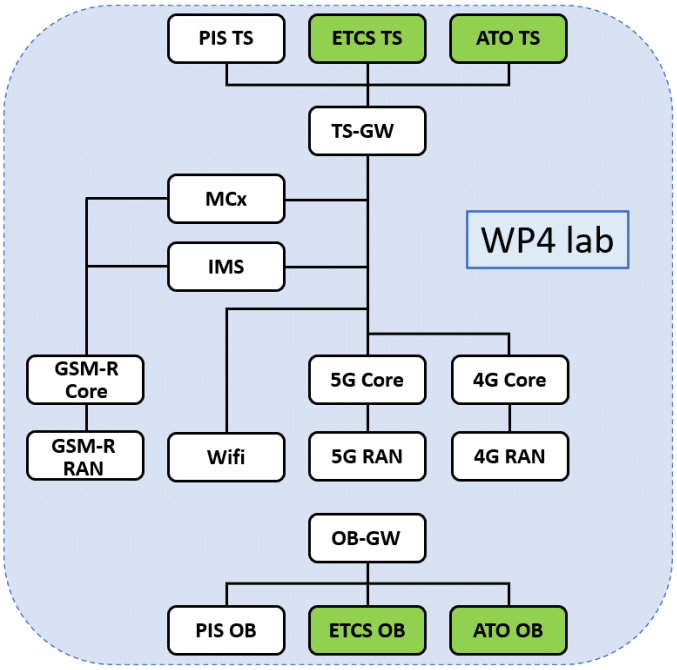


Figure 58: ETCS/ATO OB and TS applications in WP4 lab

4.1 Description of Alstom ETCS and ATO lab in WP4

Alstom ETCS and ATO devices for WP4 are installed in Kontron labs at Montigny-Le-Bretonneux, France. Besides, an IPsec remote connection is established between Kontron lab in Montigny and Alstom labs in Villeurbanne (France) and Charleroi (Belgium) to allow Alstom engineers to remotely monitor and control their devices.

The list of ETCS equipment for WP4 is the following:

- On board part:
  - COM-STS (simulator)
  - COMET board (EVC board)
  - DMI (driver machine interface)
  - Others: switch for local network, IPX800 to remotely restart the equipment
- Trackside part:
  - RBC simulator
  - NTG

Further details are given in D4.1 document [S20].

The list of ATO equipment for WP4 is the following:

- On-board part:
  - ATO-OB (on-board part of ATO)
  - ATO-TE (test bench device) which is installed on the same HW than ATO-OB
- Trackside part:
  - ATO-TS (trackside part of ATO)

Further details are given in D4.1 document [S20].

Besides ETCS and ATO devices, Alstom provides also an OB_GTW and a TS_GTW (see chapter **5** for further details), respectively named NetBox and OCC, and two end devices (Raspberry Pi) for testing purposes. The full diagram of Alstom test bench in WP4 labs is given in Figure 59, with the corresponding IP addresses. All these Alstom equipment are integrated in the same rack.

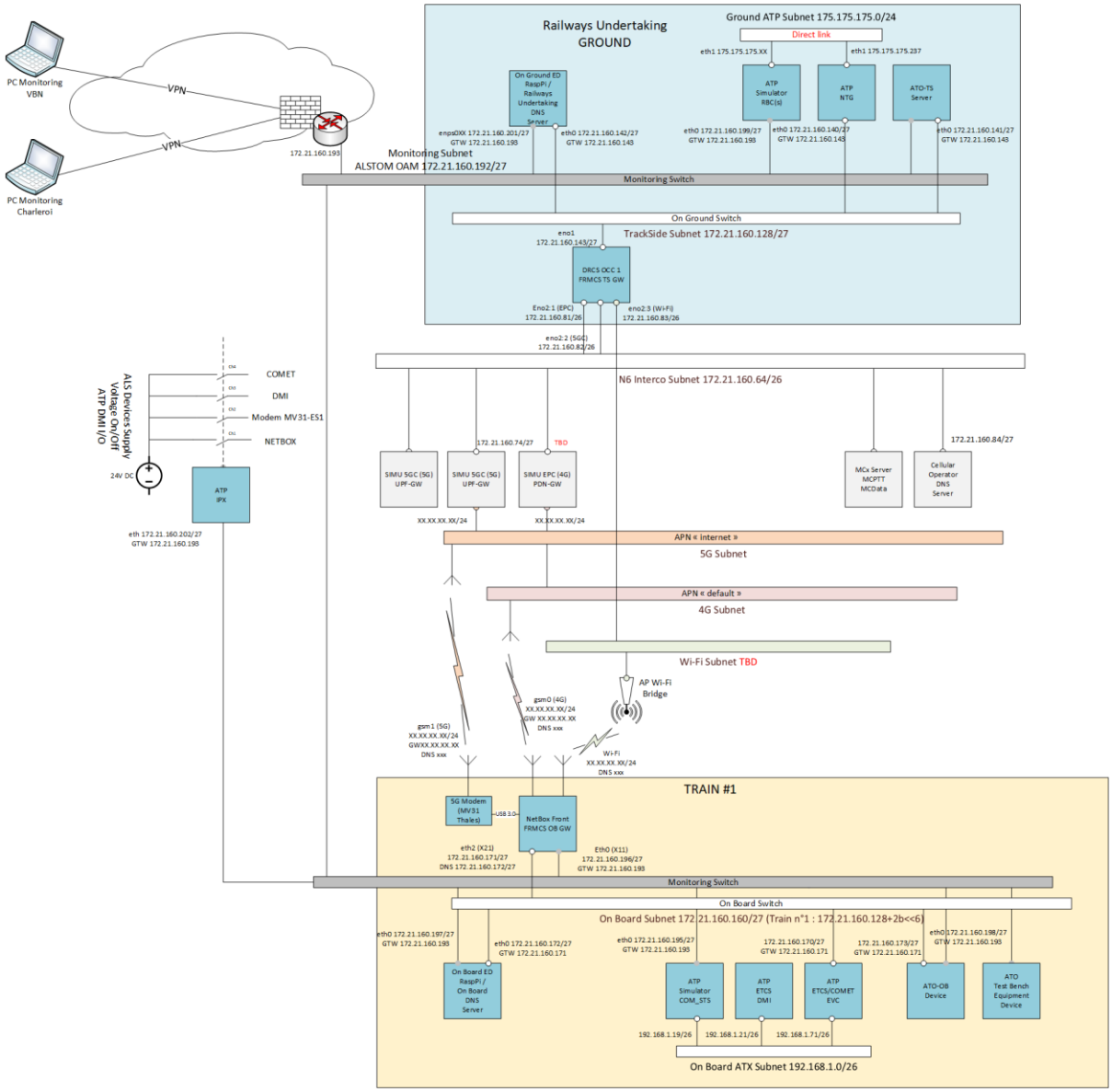


Figure 59: Schema of Alstom testbench

4.2 ALSTOM integration in Kontron lab

The integration of Alstom equipment for ETCS and ATO in Kontron lab for WP4 was performed in five successive steps described below. This integration and the integration of Alstom OB-GTW and TS-GTW were jointly done.

4.2.1 Pre-integration in Alstom labs and test

Alstom discussed with Kontron the addressing plan to define all the IP addresses for the equipment provided by Alstom and other participants. With this addressing plan, Alstom prepared the integration by reproducing the Kontron's Testbench in its Lab in Villeurbanne (France).

For the pre-integration in the Alstom lab, all Alstom devices were preconfigured with the IPs provided by Kontron in the three networks: Trackside, Onboard and Alstom OAM (Management and supervision). After those configurations, the OB_GTW-A and TS_GTW-A were connected through the network simulator in Alstom lab.

Once this train to ground connection was established, Alstom tested if the data traffic between the train and the ground was operational (with ICMP traffic and UDP/TCP). Then, the pre-integration tests described in D2.2 deliverable were performed. Basically, it consists in connecting the application (ATO and ETCS) to the OB_GTW-A and TS_GTW-A, and performing applicative tests under nominal and degraded conditions.

When those tests were successful, they sent their equipment to Kontron lab.

4.2.2 VPN creation between Kontron and Alstom labs and test

Alstom established a VPN tunnel with Kontron lab in Montigny to allow Alstom's engineer to remotely access their equipment through SSH and Remote desktop (RDP).

From Alstom side, they access to the VPN through a virtual desktop deployed by Alstom IT. From this virtual computer and only from this one, they can remotely access their equipment for maintenance and supervision purposes.

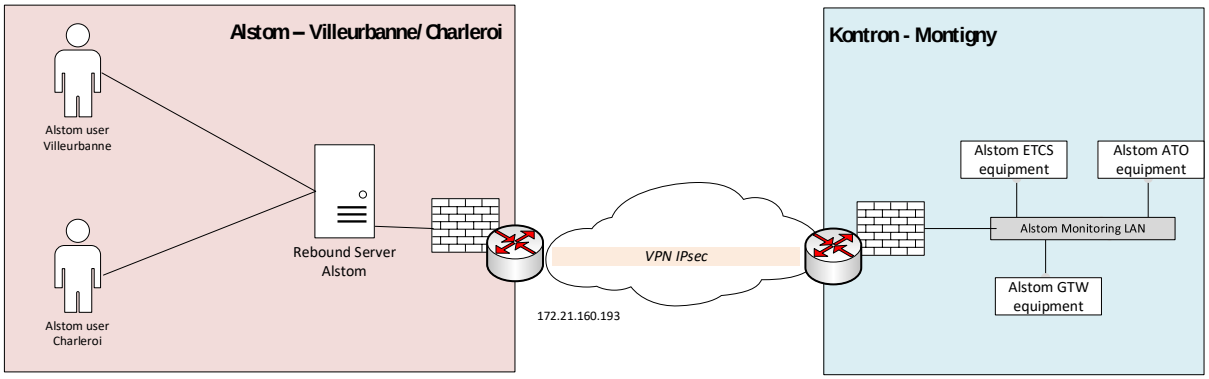


Figure 60: VPN between Alstom and Kontron labs

The firewalls on Alstom side allow only SSH and RDP from the Virtual Desktop to the tunnel. On Kontron side, more protocols can be allowed but for now only SSH and RDP are enabled.

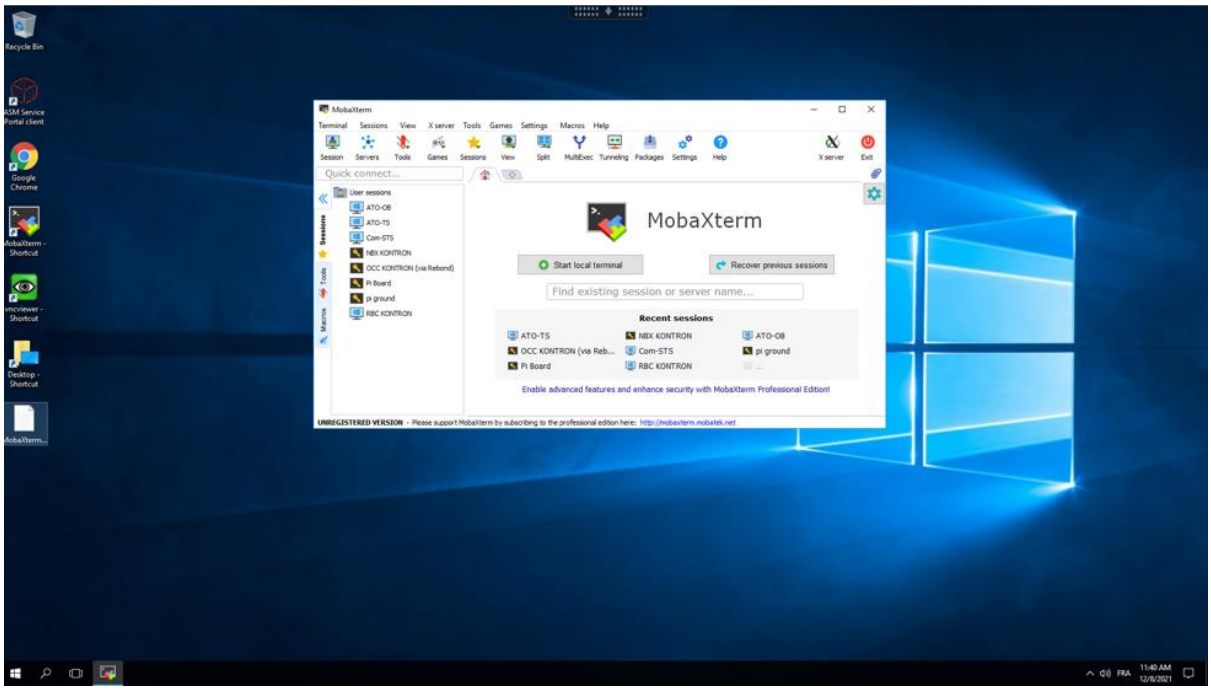


Figure 61: VPN access via Windows virtual desktop

In order to test the VPN connection, Kontron provided two devices, one with a Linux base OS and one under Windows to test the SSH and the RDP connection from Alstom to Kontron lab before the beginning of the Alstom devices installation .

During the installation of the equipment, Alstom planed a remote session with one of their engineers stayed at Villeurbanne to check they can access all their equipment from their lab. It was working properly, all equipment were accessible for maintenance, update, and supervision.

A MobaXterm file was provided to all Alstom engineers who must access the equipment remotely.

4.2.3 Test Bench installation at Montigny

This section describes what was done by the Alstom team during the installation of their equipment.

First, Alstom checked all their equipment they received in Kontron Lab, (check that everything was present and not damaged).

Then, they started the installation of their equipment in the rack provided by Kontron. For the installation, Alstom follows the schematic below:

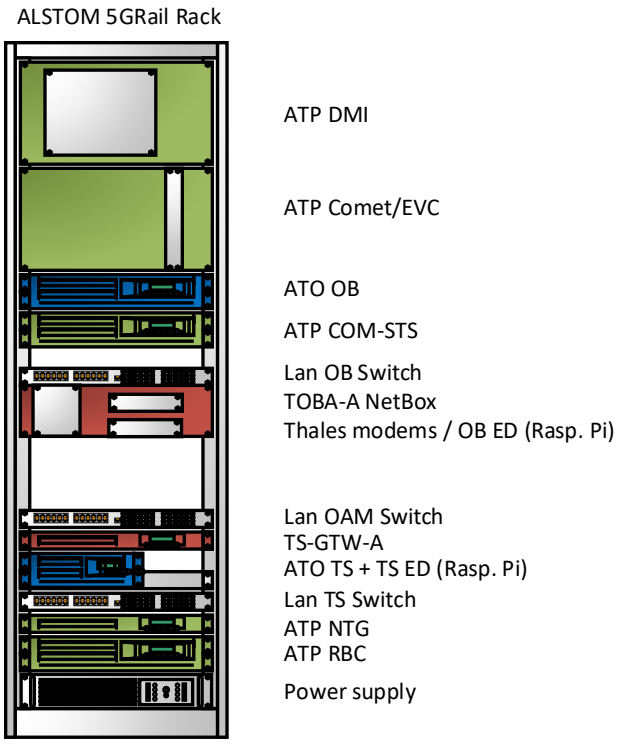


Figure 62: Alstom devices in testbench cabinet

On this schematic, the upper part represents the train and its applications, and the lower part (below "Lan OAM Switch") represents the ground server's applications.

ATP equipment are coloured in green, ATO in blue and communication part in red.

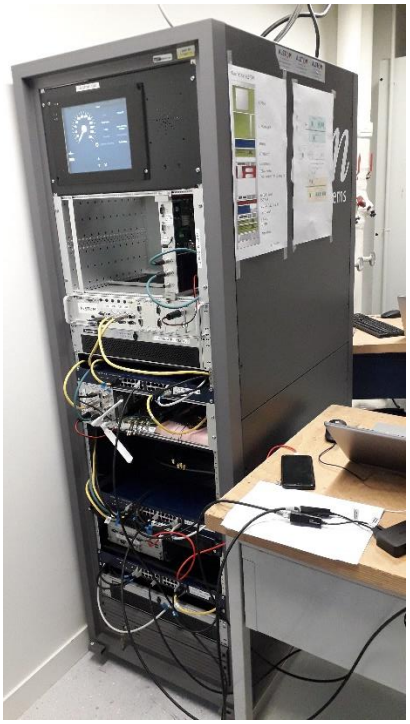


Figure 63: Picture of Alstom cabinet in Kontron lab

Figure 64: Train part of Alstom cabinet

Figure 65: Ground part of Alstom cabinet

When all the equipment were installed in the rack, Alstom connected all of them to the uninterruptible power supply except the 2 ATO PCs, the OB_GTW-A and the 2 ED. Those equipment are not sensitive to power cut, but it is planed with Kontron to move them on the uninterruptible power supply later. The next step was to connect all other cable (ethernet, serial) as it is described in the schema in Figure 59.

After all equipment were connected and powered, Alstom proceeded with some tests to check the local access on the OAM Lan (SSH connection, remote desktop, and http). When all equipment were up and running, Alstom started to work on the connectivity with some ping tests to check everything is properly connected on the TS Lan and on the OB Lan. Then, Kontron provided the cables to connect the Alstom Lan to the labs Lan.

The next step was to enable the connectivity between the TS GTW and the OB GTW.

At this step, Alstom and Kontron decided to freeze the setup and the cable connection, and to label all ethernet cables to be able to solve any issue in the cabling.

4.2.4 Network connection

This step consists in checking the network connection of OB_GTW and TS_GTW, and the connectivity between these gateways through the different radio links. This is not really an ETCS/ATO test, so it is described in chapter **5**.

4.2.5 Connectivity and application test

Once, the network connection is correct, the last step consisted in performing first application tests to check the connectivity between ETCS-OB and ETCS-TS devices, and between ATO-OB and ATO-TS devices for the applicative sessions ATO and ATP.

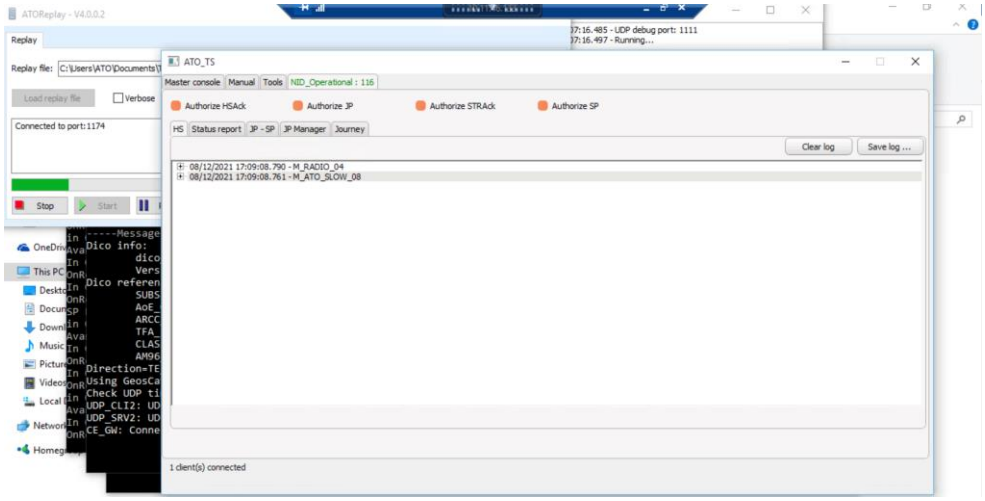


Figure 66: ATO TS interface

The connectivity between ATO-OB and ATO-TS is checked on the ATO-OB IHM. More detailed tests with application data exchange are then performed in chapter **4.3.1**.

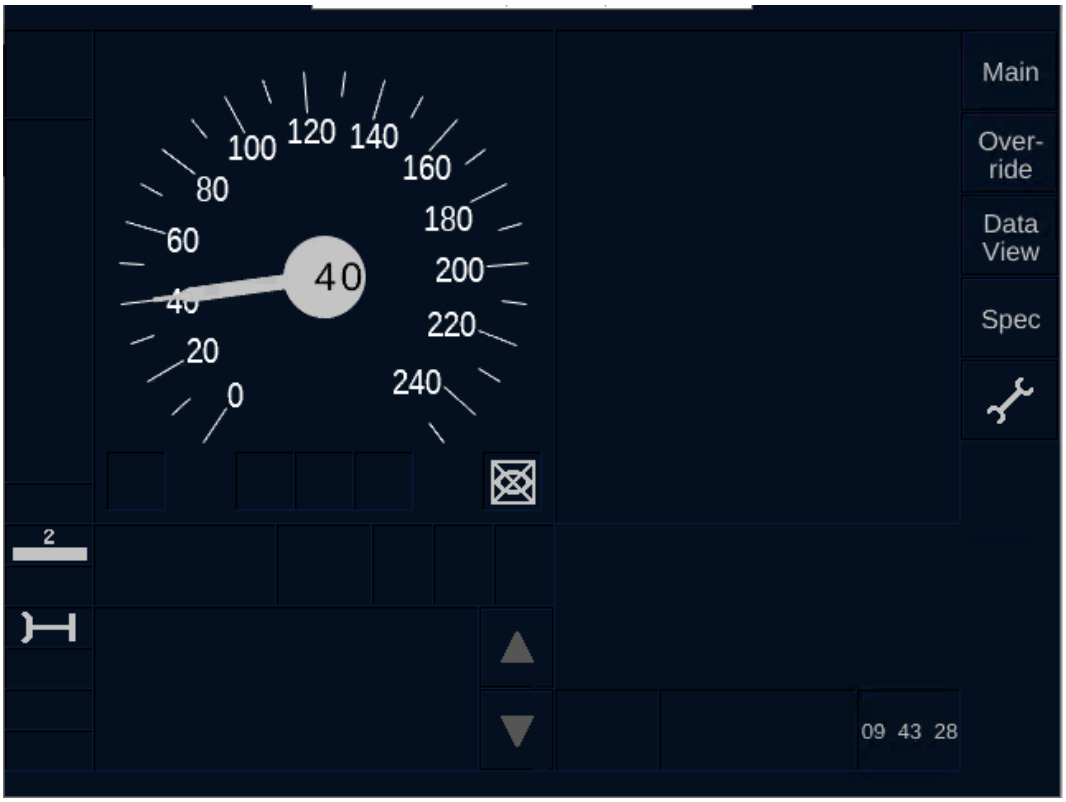


Figure 67: ETCS DMI view in nominal mode

The connectivity between ETCS on-board and trackside equipment is also checked. Basically, the EVC (COMET board) received data from the COM-STS (to simulate train movement) and from the trackside RBC (such as movement authority), and we can see the corresponding behaviour on the DMI (see Figure 67).

The next figure shows the on-board and trackside equipment which are connected each other:

- ETCS: EVC (on-board) and RBC (trackside) through the NTG : see the red line
- ATO: ATO-OB (on-board) with ATO-TS (Trackside): see the green line

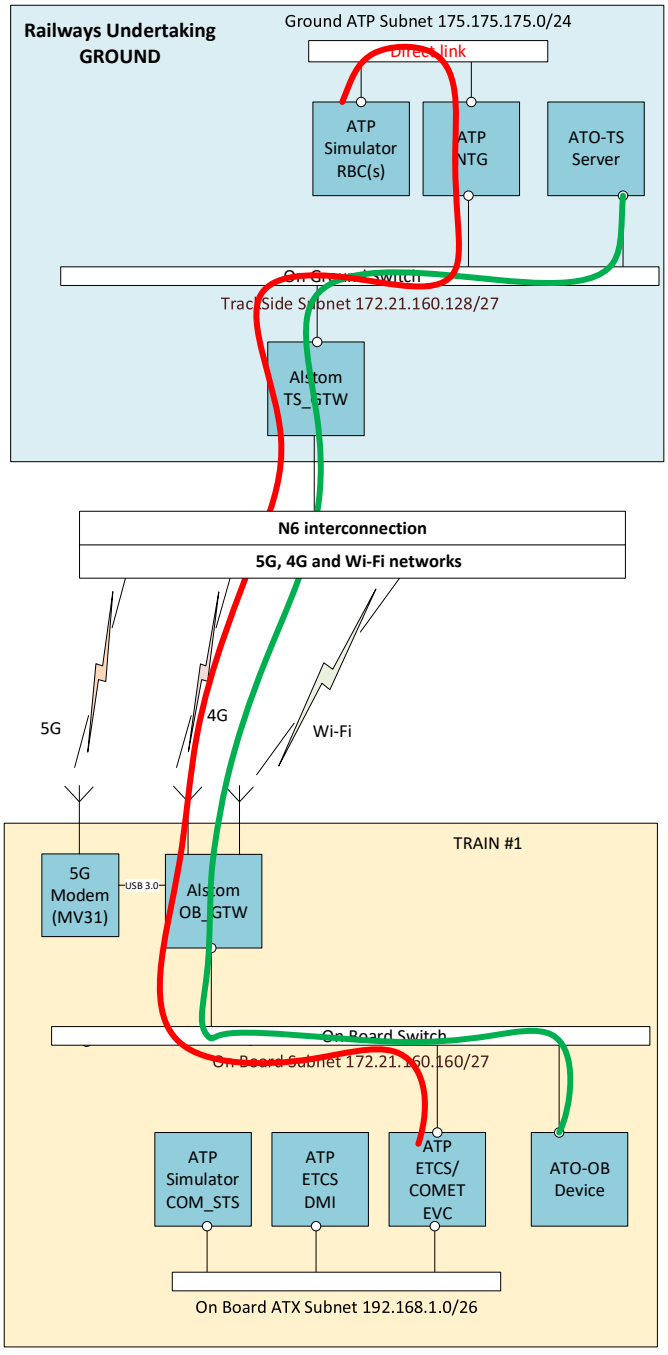


Figure 68: ETCS and ATO connectivity

As shown above, both ATP and ATO application are running in Kontron lab. For the ATO, the OB ATO application and the TS ATO server can exchange information over the radio network through the OB and TS Gateways.

Thus, the prerequisite to perform ETCS and ATO tests that are defined in D1.1 document are OK. The results of these tests would be given in D4.3 document [S21].

4.3 Phasing approach and additional tests for Phase 1

4.3.1 ATO

4.3.1.1 Phasing approach

At this stage, two phases are considered for Alstom ATO:

- Phase 1: application in Flat-IP only
- Phase 2.1: Loose couple approach, OB_{APP} and TS_{APP} implementation for ATO-OB and ATO-TS. No TLS implemented for the OB_{APP} and TS_{APP} API, nor for the end to end communication.
- Phase 2.2: Same than phase 2.1 with an implementation of TLS for the OB_{APP} /TS_{APP} API, and for the end to end communication.

End to End connectivity was checked in section 4.2.5. Furthermore, phase 1 tests were already performed with ATO OB and TS equipment, using OB_GTW-A and TS_GTW-A in flat IP. These tests are described below.

4.3.1.2 Phase 1 test in nominal conditions

The communication between the ATO-OB and the ATO-TS is provided by the 5G network during the test.

Note: in the following table, PROBE is the name of the Alstom ATO diagnostic/debugging tool.

Step	Action	Expected result(s)	Test result	Comments (after the test)
01	Launch all softs: by opening the cmd files Start_5Grail_OB and Start_5Grail_TE	All applications are going to open (ATO_CE simulator, ATO_PROBE, SS130, SS139, SS126, ATO_SLOW, ATO_FAST, DO, ATO_REPLAY, ATO_TS)	Passed	
02	Go to the application ATO_REPLAY , and load the scenario TEST_5G.STrm then launch it	If everything is OK, ATO_onboard will send a handschake request to the ATO trackside If not, nothing will happen	Passed	

03	Check in the PROBE, ATO_trackside and SS126 the Handshake request issued by the ATO-onboard		Passed	
04	Check in the ATO-trackside the content of the received Handshake request		Passed	
05	Check the PROBE, ATO_trackside and SS126 the handshake Acknowledgement issued by the ATO-trackside		Passed	
06	Check at ATO-onboard level if the handshake Acknowledgement is coherent with the message sent by the ATO-trackside	we should observe the same message as on ATO-trackside	Passed	
07	Check the PROBE, ATO_trackside and SS126 the Journey Profile request issued by the ATO-onboard		Passed	
08	Check the ATO-trackside and PROBE the content of the received Journey profile request		Passed	
09	Check the PROBE and ATO_trackside the journey profile issued by the ATO-trackside		Passed	
10	Check at ATO-onboard level if the Journey profile is coherent with the message sent by the ATO-trackside	we should observe the same message as on ATO-trackside	Passed	
11	Check in the PROBE the segment profile request issued by the ATO-onboard		Passed	
12	Check in the ATO-trackside the content of the received segment profile request		Passed	
13	Check in the PROBE, ATO_trackside and SS126 the segment profile issued by the ATO-trackside		Passed	Some errors appeared during tests the firsts attempts to send a SP, the ss126gateway showed a

				checksum error and stopped the SP from being sent to the CE, but after some tries, the SP sent by the ATO-TS is accepted and forwarded to the CE. Maybe some data have been lost during transfer.
14	Check at ATO-onboard level if the segment profile is coherent with the message sent by the ATO-trackside	we should observe the same message as on ATO-trackside	Passed	
15	Check in the PROBE the status report issued by the ATO-onboard		Passed	
16	Check in the ATO-trackside the content of the received status report		Passed	
17	Check in the PROBE the status report acknowledgment issued by the ATO-trackside		Passed	
18	Check at ATO-onboard level status report acknowledgment is coherent with the message sent by the ATO-trackside	we should observe the same message as on ATO-trackside	Passed	

Table 38: ATO - Phase 1 test in nominal conditions

The capture files corresponding to these tests are saved on Alstom's repository under the name 5Grail_WP4_Alstom_Test_ATO_ph1.zip

4.3.1.3 Phase 1 test in degraded conditions

The communication between the ATO-OB and the ATO-TS is ensured by the 5G network (primary). To apply a degradation on the radio link, the 5G modem interface of the OB_GTW-A was shutdown. The 5G link was cut, in order to use the Wi-Fi link (secondary), the aim is to observe the impact of the transition between these two modes of communication.

The same scenario as in nominal mode was processed.

No alteration of the behaviour is observed, the communications remain operational and the transition time between the communication modes is too fast to impact the exchanges between the ATO-OB and the ATO-TS.

4.3.1.4 Update and tests for ATO Phase 2.1

In February 2022, the ATO-OB and ATO-TS software was updated in order to evolve to Phase 2.1 (OB_{APP} and TS_{APP} implementation). This update was performed remotely by Alstom team thanks to the VPN link described in chapter 4.2.2.

Before pushing the update in the WP4 labs, it had been internally tested in Alstom lab with an Alstom OB_{APP}/TS_{APP} simulator shared in WP2. The corresponding capture files are saved in Alstom's repository under the name "5Grail_WP2_Alstom_2022-03-04_ATO_simu-A.zip".

Secondly, after software update in WP4 lab, it was tested with Kontron gateways (OB_GTW-K and TS_GTW-K) under nominal conditions (no link failure). The same scenario as in 4.3.1.2 was proceed. The test allows to emphasize some minor differences between Kontron and Alstom implementation of OB_{APP}/TS_{APP}. that were transmitted to WP2 and were easily solved (examples: url for opening the WebSocket, use of lowercase or uppercase in the API parameters,…). The corresponding capture files are saved in Alstom's repository under the name "5GRAIL_WP4_Alstom_2022-03-10_testATO"

Then, it was tested with Alstom gateways (phase 2.1 of OB_GTW-A and TS_GTW-A, see 5.1.3) under nominal conditions (no link failure). The same scenario as in 4.3.1.2 was proceed. No issue was encountered. The corresponding capture files are saved in Alstom's repository under the name "5GRAIL_WP4_Alstom_2022-04-06_testATO_ph2.1_ALS"

Finally, once the Alstom gateways were updated with multipath function (phase 2.2 of OB_GTW-A and TS_GTW-A, see 5.1.3), the same tests than in 4.3.1.3 were performed. The corresponding capture files are saved in Alstom's repository under the name "5GRAIL_WP4_Alstom_2022-06-01_ATO_multipath". No alteration of the behaviour is observed in ATO probe, the communications remain operational and the transition time between the communication modes is too fast to impact the exchanges between the ATO-OB and the ATO-TS. Nevertheless, it appears that ATO application is not the best candidate to evaluate multipath capability of the FRMCS gateways, because once the different profiles are fully downloaded by ATO-OB (journey profile, segment profile,…), the flow between ATO-OB and ATO-TS is quite sporadic (status report, approximately) and light, thus it does not really allow to observe an accurate impact of an eventual change of link.

4.3.1.5 Update and tests for Phase 2.2

In December 2022, ATO-OB and ATO-TS software was updated in order to evolve to Phase 2.2. The new supported features are:

- Use TLS for local binding (WebSocket over TLS for the API exchange between OB_GTW and ATO-OB, and between TS_GTW and ATO-TS) --> control plane
- Use TLS for the end to end applicative session between ATO-OB and ATO-TS –> user plane.

This update was performed remotely by Alstom team thanks to the VPN link described in chapter 4.2.2.

The local binding TLS was successfully tested in January with OB_GTW-A and TS_GTW-A, using certificates manually stored in the ATO-OB, ATO-TS, OB_GTW-A and TS_GTW-A.

For End to end TLS, a PKI was installed on a trackside device (to be more accurate, it is a virtual machine hosted on the ATO-TS). Then ATO-TS has obviously access to the PKI.

ATO-OB can also reach the PKI through a “flat-IP” session established between OB_GTW-A and TS_GTW-A. Then, ATO-OB and ATO-TS are able to open a TLS connection between them. This was successfully tested end of January. The results will be given in D4.3 document [S21].

4.3.2 ETCS

4.3.2.1 Phasing approach

At this stage, two phases are considered for Alstom-ETCS:

- Phase 1: application in Flat-IP only
- Phase 2: Loose-coupling approach, OB_{APP} implemented for OB part

For ETCS, end to end connectivity tests between RBC (trackside) and EVC (on-board) was done and described in chapter 4.2.5. The success of this connectivity was shown on the DMI display.

The next E2E tests for ETCS application will be performed in Phase 2 with OB_{APP} implementation for the control plane, and the corresponding test results will be included in D4.3 document.

Note: phase 1 tests with Alstom ETCS were already performed during the pre-integration stage in Alstom lab (see D2.2 document).

4.3.2.2 Update for phase 2

In November 2022, the ETCS-OB software was updated in order to evolve to Phase 2 (OB_{APP} Loose-coupling implementation). This update was performed remotely by Alstom team thanks to the VPN link described in chapter 4.2.2.

Before pushing the update in the WP4 labs, it had been internally tested in Alstom lab with a mirrored test bench with an OB_GTW-A and TS_GTW-A.

First tests (connectivity, registration, session establishment) with OB_GTW-A and TS_GTW-A 7 in WP4 lab were done during Week 47 (2022).

First tests with OB_GTW-K and TS_GTW-K 7 in WP4 lab were done during Week 48 (2022).

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 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.

During January, several test sessions were planned with OB_GTW-A/TS_GTW-A and OB_GTW-K/TS_GTW-K, in order to fill the expected test cases.

The corresponding results would be given in D4.3 document [S21].

OB_GTW-A and TS_GTW-A have been updated in order to support a border-crossing scenario as specified in D2.1 document (using two 5G modems). The corresponding test case would be given in D4.3 document [S21].

5 FRMCS Gateways installation and integration in WP4 lab

5.1 OB and TS Gateways provided by Alstom

5.1.1 First integration of OB_GTW Alstom

5.1.1.1 Description and first steps of integration

The OB_GTW-A is composed of one internal Wi-Fi modem, one internal 4G only modem and one external 4G/5G modem (a MV31-W modem provided by Thales). More details are given in D4.1 document [S20].

As explained in chapter 4, Alstom OB_GTW and TS_GTW were installed together with ETCS and ATO devices. The different steps of pre-integration in Alstom labs, VPN creation and test bench installation are already described in chapters 4.2.1 to 4.2.3. Especially, the installation of OB_GTW-A in Alstom rack is defined in 4.2.3.

5.1.1.2 Connection to 5G, 4G and Wi-Fi networks

Kontron provides Wi-Fi access and SIM cards to allow the OB_GTW-A to connect to the 5G and 4G radio networks. Alstom team configured the OB_GTW-A to access the radio network and be able to connect Train to Ground application.

The Wi-Fi was the first link configured by Alstom while Kontron Teams were connecting the 5G hardware to allow a cable RF connection with the OB_GTW-A.

Secondly, Kontron installed the 5G setup close to the Alstom rack and connected a N8 RU to the 5G core. Then they connected it to the OB_GTW-A with RF cable to avoid radio emission in the lab. Then Alstom configured the Thales Modem MV31-W with the network parameters given by Kontron (APN, roaming). The OB_GTW-A was successfully able to connect to 5G SA network provided by Kontron on band N8.

Finally, the last radio link to be installed was the 4G. Kontron was able to provide the 4G network through the same core and another dedicated RRH.

5.1.1.3 Connection with TS_GTW-A

The aim here is to check the interconnection between OB_GTW-A and TS_GTW-A through the different radio links (5G, 4G, Wi-Fi).

Firstly, Alstom tested the Wi-Fi connection to allow the Train to Ground communication. This link was working properly and enabled Alstom engineer to test the communication and then the applications.

Then, the connectivity between OB_GTW-A and TS_GTW-A through the 5G network was checked. It works correctly with the current 5G network configuration applied in WP4.The 4G link is also available

using the external 5G modem and internal 4G modem. In order to prove the connection between OB_GTW-A and TS_GTW-A, Alstom started an iperf3 traffic between On-board End device and Trackside end device (Raspberry Pi), as we can see below. The terminal on the left called Pi ground is an end device in the TS Lan and receives the TCP traffic from the "Pi Board" (on the right) which is in the OB Lan. Then, Alstom tested the switching of the data from the primary link (5G) to a backup link (Wi-Fi) and it worked successfully.

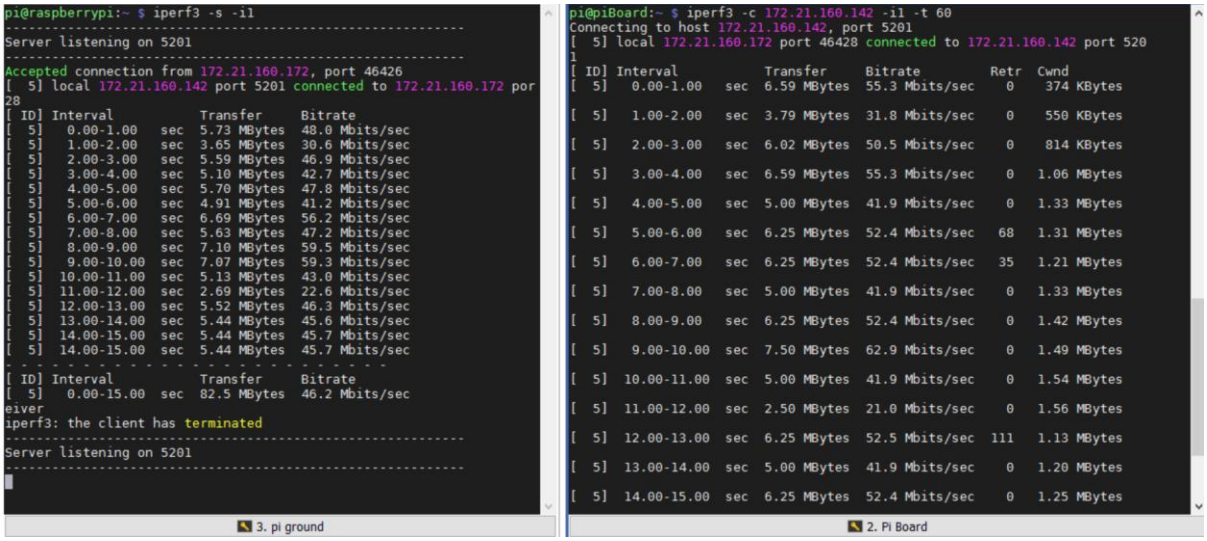


Figure 69: End to end Iperf train to ground communication

5.1.2 First integration of TS_GTW Alstom

5.1.2.1 Description and first steps of integration

The details relative to the TS_GTW-A are given in document D4.1 [S20]. As explained in chapter 4, Alstom OB_GTW and TS_GTW were installed together with ETCS and ATO devices. The different step of pre-integration in Alstom labs, VPN creation and test bench installation are already described in chapters 4.2.1 to 4.2.3. Especially, the installation of TS_GTW-A in Alstom rack is defined in 4.2.3.

5.1.2.2 Connection to the N6 LAN

For the Train to Ground connectivity, Alstom firstly connected their TS-GTW-A to the N6 Lan to allow the connection between the TS Gateway and the 5G and 4G network core and with the Wi-Fi.

Alstom checked the connection to the N6 Lan by pinging the radio network core, the MCx server and the Wi-Fi access point.

5.1.2.3 Connection with OB_GTW-A

The tests performed to show the connection between TS_GTW-A and OB_GTW-A are described in section 5.1.1.3.

5.1.3 Phasing approach and software/hardware updates

5.1.3.1 Phasing approach

At this stage, the following phases are considered for OB_GTW-A and TS_GTW-A:

- Phase 1: Flat-IP mode only
- Phase 2.1: integration of OB_{APP} and TS_{APP} API, and QoS management using DSCP values
- Phase 2.2: integration of multipath
- Phase 2.3: integration of MCdata-IPconn for session management.
- Phase 2.4: integration of TLS in the API exchanges.

The initial software used for the 1st integration described above corresponds to Phase 1.

Then, few software updates have been remotely performed by Alstom team on the OB_GTW-A and TS_GTW-A in order to make it evolve to the next phases.

5.1.3.2 Software updates

The table below sums up the different software updates already performed since the 1st integration, and the corresponding details:

Actions	Date of achievement	Capture files
Phase 2.1		
SW update of OB_GTW-A and TS_GTW-A in WP4 lab	1/04/2022	NA
Test in WP4 lab with ATO See chapter 4.3.1.4.	6/04/2022	5GRAIL_WP4_Alstom_2022-04-06_testATO_ph2.1_ALS
Test in WP4 lab with PIS	27/04/2022	5GRAIL_WP4_Alstom_2022-04-27-Thales_testPIS
Phase 2.2		
SW update of OB_GTW-A and TS_GTW-A in WP4 lab	18/05/2022	NA
Test in WP4 lab with ATO see chapter 4.3.1.5.	1/06/2022	5GRAIL_WP4_Alstom_2022-06-01_ATO_multipath

SW update of OB_GTW-A and TS_GTW-A in WP4 lab	18/05/2022	NA
Tested with generic OBapp/TSapp application simulator.	28/09/2022	5GRAIL_WP4_Alstom_2022-09-28_testMCdata_MP
Tested with PIS application	06/10/2022	5GRAIL_WP4_Alstom_2022-10-06_testPIS
See Phase 2.3 delivery.		
SW update to improve multipath feature (and others improvements)	23/12/2022 24/01/2023	NA
Tested with ATO and ETCS	Second half of January	See D4.3 document [S21] for test results.

Phase 2.1 tests with PIS application allow to show that the correct values of DSCP is used by the OB_GTW-A/TS_GTW-A in the GRE tunnel carrying the applicative data. It is the first step to satisfy QoS requirement. Nevertheless, the use of the corresponding dedicated QoS flow in the 5G network is still to be checked.

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 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.

5.1.3.3 Hardware update

The first integration of OB_GTW-A was done with MV31-W modem. Then, it has been substituted in February 2022 by Thales modem ES1.x

In January 2023, a hub USB and a second ES1 modem were connected and integrated to the OB_GTW-A additionally to the one ES1 modem already connected. Then, the OB_GTW-A has two 5G modems (Thales ES1). This modification aims at supporting border-crossing test case as described in D2.1 document, between two 5G networks.

At this day, Thales modems ES2 and ES3 have also been received in Alstom lab but have not been integrated with the OB_GTW-A in WP4 lab.

5.2 OB and TS Gateways provided by Kontron

5.2.1 OB and TS Gateways Kontron installation in WP4 lab

Kontron WP2 team delivered an OB Gateway and a TS Gateway to WP4, these modules being dedicated to WP4 activities only.

OB Gateway has been installed in a rack of the WP4 working area (see Figure 70: WP4 dedicated OB GW Kontron) while TS Gateway VM is hosted on a dedicated PC connected to Trackside and N6 LANs.

Figure 70: WP4 dedicated OB GW Kontron

Before being used by WP4, OB and TS GW Kontron were tested during a pre-integration phase. The report that deals with these pre-integration tests is D2.2 delivery [S23].

Integration testing of the gateways consisted in checking the basic behaviour of the Gateways while inserted into the WP4 lab.

5.2.2 OB and TS Gateways Kontron integration tests

5.2.2.1 Integration tests focusing on OB Gateway Kontron behaviour in N8 and N78

Having connected the OB GW to the various RANs, some tests were done in order to check its basic behaviour. Tests linked to 5G access are reported in Figure 71: 5G Integration tests with OB GW Kontron :

Test	Comment	Trace
5G UL transfer test on N78	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G UL Transfer N78 OB GW-K.pcap
5G DL transfer test on N78	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G DL Transfer N78 OB GW-K.pcap
5G UL transfer test on N8	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G UL Transfer N8 OB GW-K.pcap
5G DL transfer test on N8	Check that traffic is stable	5GRail_WP4_Kontron_D4.2_5G DL Transfer N8 OB GW-K.pcap
5G RTD test on N78	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_5G RTD N78 OB GW-K.pcap
5G RTD test on N8	Ping P-CSCF	5GRail_WP4_Kontron_D4.2_5G RTD N8 OB GW-K.pcap
5G HO between RU N8 and RU N78	Both ways	5GRail_WP4_Kontron_D4.2_5G HO N8 N78 OB GW-K.zip

Figure 71: 5G Integration tests with OB GW Kontron

All these tests proved the good basic 5G behaviour and the successful integration of the OB GW Kontron in the lab.

At the time of submission of the first version of D4.2 version 1 delivery, 5G N39, 4G and Wi-Fi capabilities were not available in OB GW-K and couldn't be tested with it.

5.2.2.2 Integration tests focusing on OB Gateway Kontron behaviour in N39

Kontron's OB GW with N39 capabilities has been delivered by WP2 beginning of October 2022. Same kind of tests than 5.2.2.1 were then performed in order to check that the integration of the ES3 modem within Kontron's OB GW form factor did not alter its behavior.

As N39 OB Gateway Kontron is the key element of WP5 tests in France, a specific chapter of D4.3 test document [S21] will give details and measurements taken during these tests that appear on Table 39: TOBA-K N39 evaluation tests

Test Title	TOBA	5G Band	Status
1_TOBA-K HO intra gNodeB	TOBA-K	N39	Executed 28/11/2022
2_TOBA-K HO inter gNodeB	TOBA-K	N39	Executed 28/11/2022
3_Total loss of radio. Reconnection	TOBA-K	N39	Executed 23/11/2022
4_Iperf test uplink_Attenuation impact	TOBA-K	N39	Executed 22/11/2022
5_Iperf test downlink_Attenuation impact	TOBA-K	N39	Executed 22/11/2022
6_Iperf test uplink_Speed-Fading impact	TOBA-K	N39	Executed 30/11/2022
7_Iperf test downlink_Speed-Fading impact	TOBA-K	N39	Executed 30/11/2022
8_RTD measurement_Attenuation impact	TOBA-K	N39	Executed 23/11/2022

Table 39: TOBA-K N39 evaluation tests

5.2.2.3 End to end integration tests with OB and TS Gateways Kontron

This sections describes the steps that have been executed in order to achieve an end to end integration of all FRMCS components. As ATO application was chosen, the objective was to make a first ATO call, using OBapp/TSapp interface with OB/TS Gateways Kontron.

5.2.2.3.1 INTEGRATION OF OB AND TS GATEWAYS KONTRON

Once installed in WP4 lab, an OB GW and TS GW connection test has been done in order to check the right behaviour with 5G, IMS and MCx networks. It consists in using an embedded tool that launches, on each Gateway, a registration of MCx clients then an IPconn MCdata connection between them.

Figure 72 sums up the setting for this integration step; traces have been recorded and stored on repository under the following name: 5Grail_WP4_Kontron_D4.2_OBTS GWs integration.zip

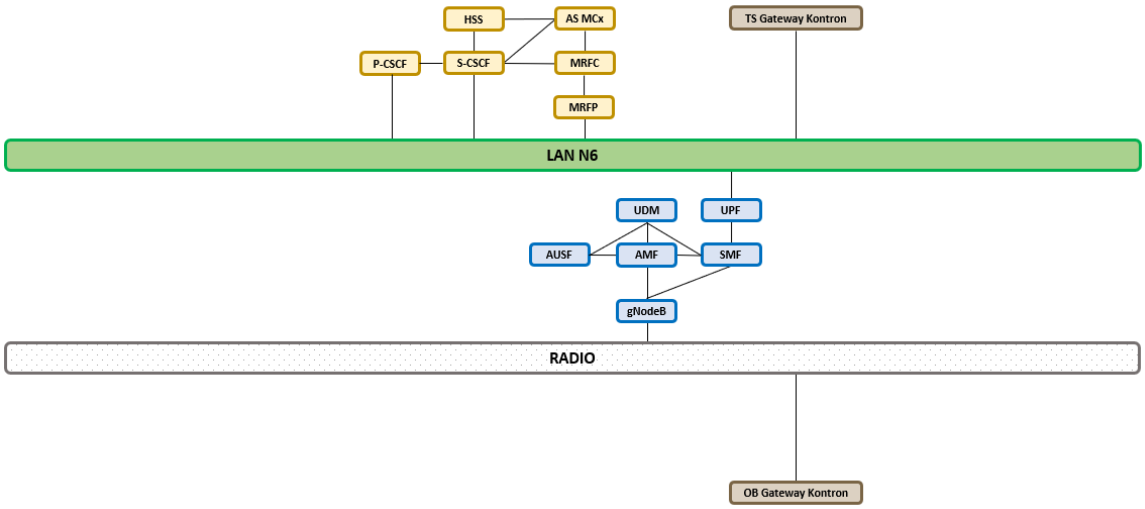


Figure 72: Integration test of OB and TS GWs Kontron with 5G, IMS and MCx networks

5.2.2.3.2 INSTALLATION OF WP2 KONTRON OBAPP/TSAPP VALIDATION TOOL

WP2 delivered an OBapp/TSapp validation tool to be used by every 5Grail application supplier. It consists in a VM, connected to LAN On-Board and LAN Trackside, to which OB and TS application can connect to in order to validate that the OBapp/TSapp messaging matches the one developed by OB and TS GW-K engineers.

Once the test with the validation tool is passed, OB and TS applications are ready to be connected to the real OB and TS GWs. Note that only signalling plane is checked at that step, user plane is not in the scope of the tool, also called OBapp/TSapp robot.

ATO OB and TS applications have then been connected to the validation tool (see Figure 73) and, after few changes in the code, they were reported to be compatible on OBapp/TSapp.

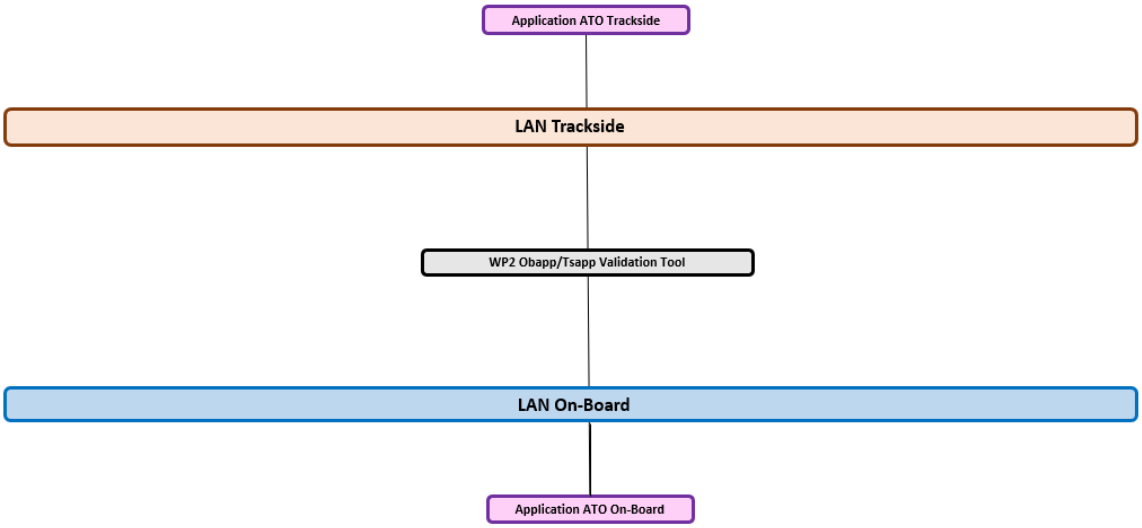


Figure 73: ATO applications validation step with WP2 OBapp/TSapp tool

5.2.2.3.3 END TO END ATO COMMUNICATION USING KONTRON FRMCS GATEWAYS OVER 5G

The last step was the connection of ATO OB and ATO TS applications to respectively OB and TS GTW Kontron as shown on Figure 74:

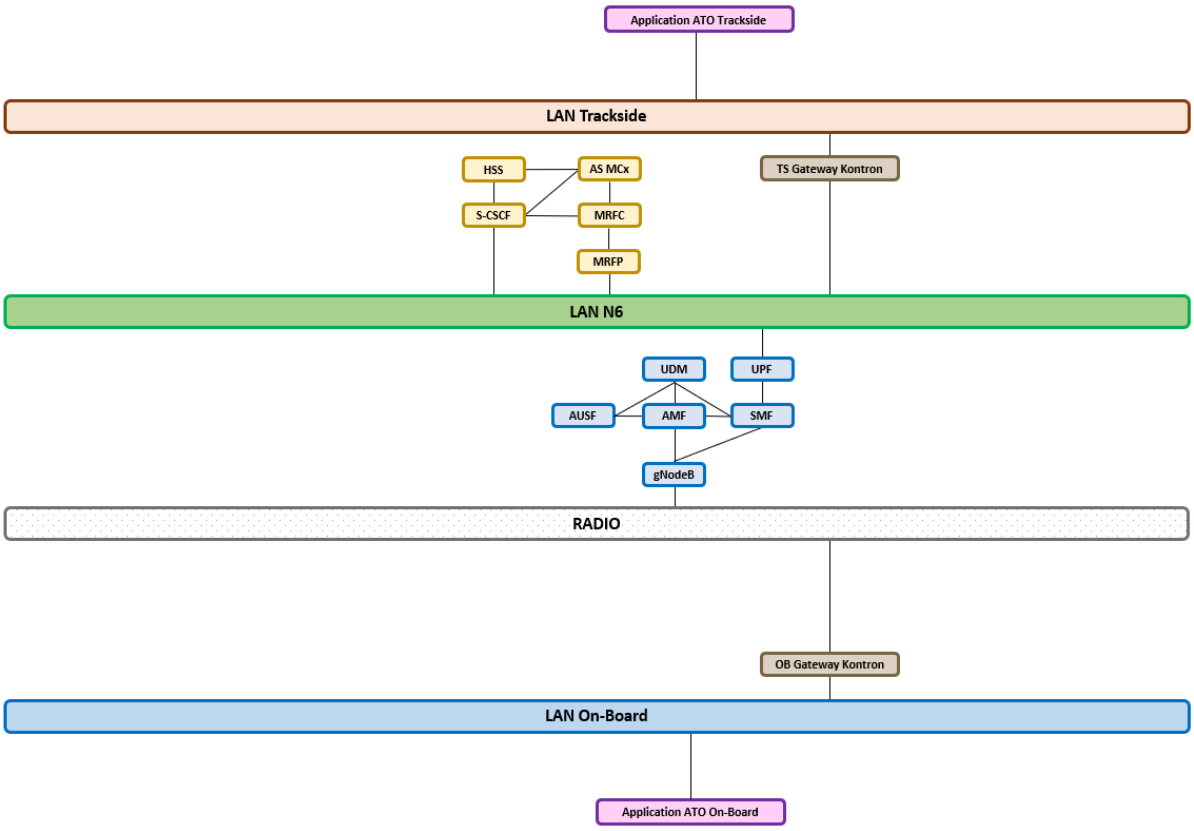


Figure 74: End to end ATO call with FRMCS Gateways over 5G

Using OBapp/TSapp interface, ATO Applications established an MCx communication between the OB and TS Gateways Kontron. Then an IPConn data connection was established between them and ATO applications were able to exchange data. Traces were saved in the repository under 5Grail_WP4_Kontron_D4.2_ATO E2E call.zip

This was the very first achievement of a FRMCS kind of call with all FRMCS bricks being in place: Applications communicating with OBapp/TSapp messages to FRMCS Gateways linked to a 5G SA network.

6 Network configurations and tools to be used during test phase

6.1 Tools used in WP4 lab

6.1.1 Protocol analysers

Protocol analysers able to record pcap traces have been set up in the platform as shown on Figure 75:

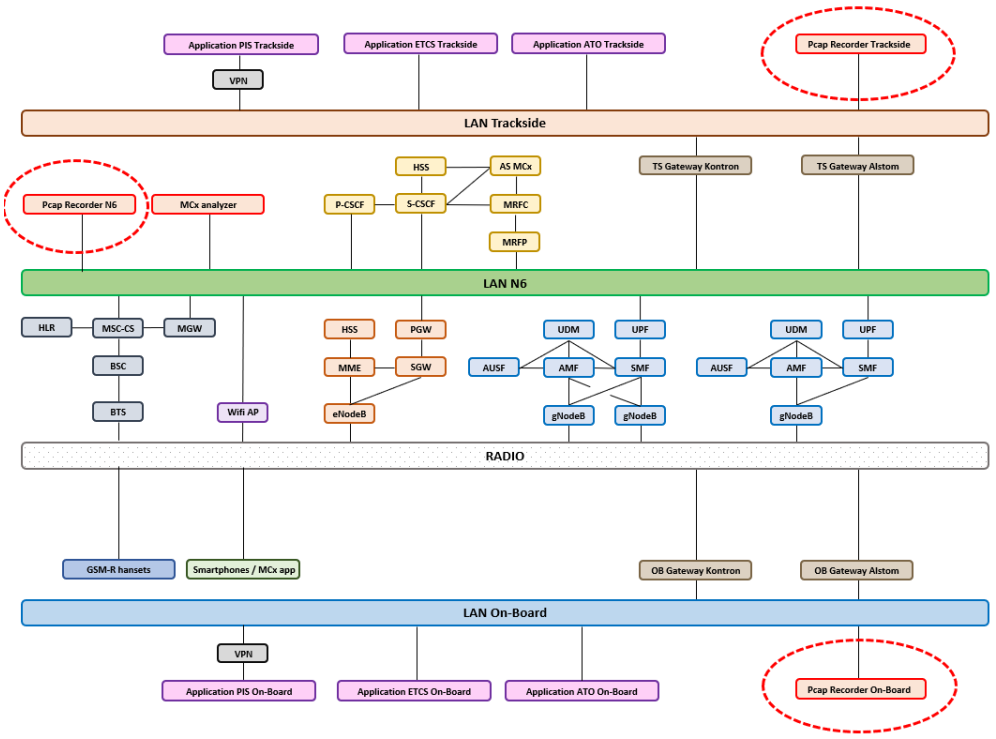


Figure 75: Wireshark protocol analysers used in WP4 lab

All these analysers are synchronized via NTP by the same clock, thus enabling to have merged traces.

It should also be mentioned that 4G and 5G solutions are able to record pcap traces on S1 and NG interfaces.

6.1.2 MCx flow analyser and KPI measurement

MCx call flow might be difficult to decode manually and the need for a specific tool was identified at the beginning of WP4 project. After some talks with a provider, it has been agreed that one of their tool would be installed in the platform. It runs on a virtual machine that we have installed on a dedicated HP Gen-10 server.

As the tool should record all IMS/MCx traffic, it has been connected onto the N6 LAN so that it can spy whatever enter or exit P-CSCF as shown on Figure 76.

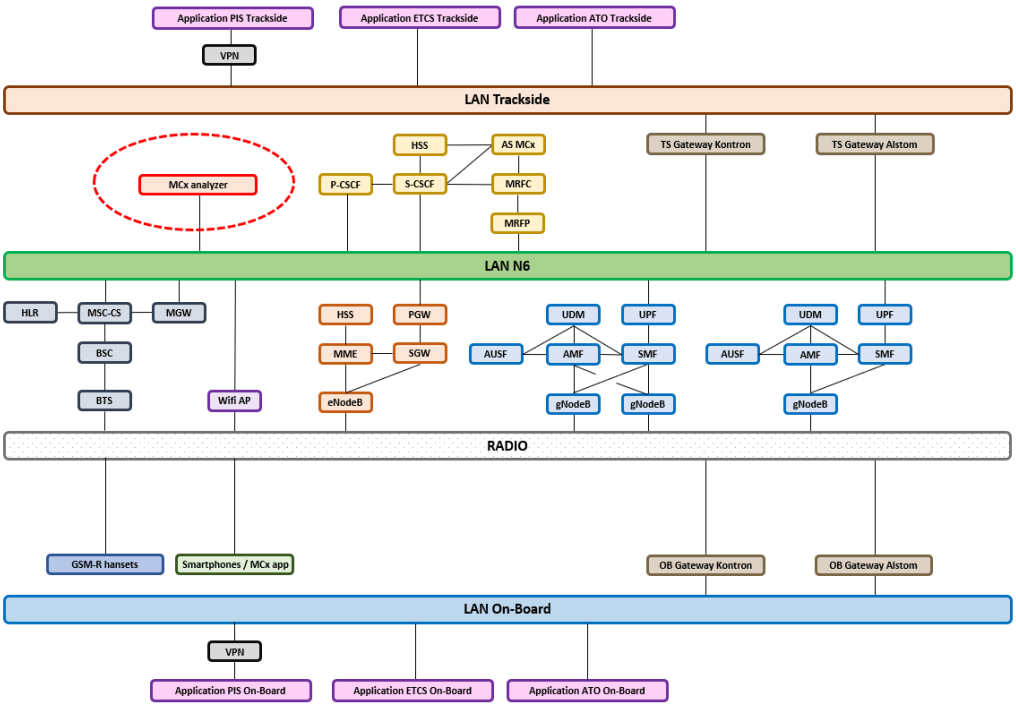


Figure 76: MCx analyser tool

The tool should help us a lot in troubleshooting activities of WP4 test phase as it enables to quickly see SIP messages and contents (as on Figure 77), apply filters and get a graphical view of messages exchanged during a specific session (see Figure 78).

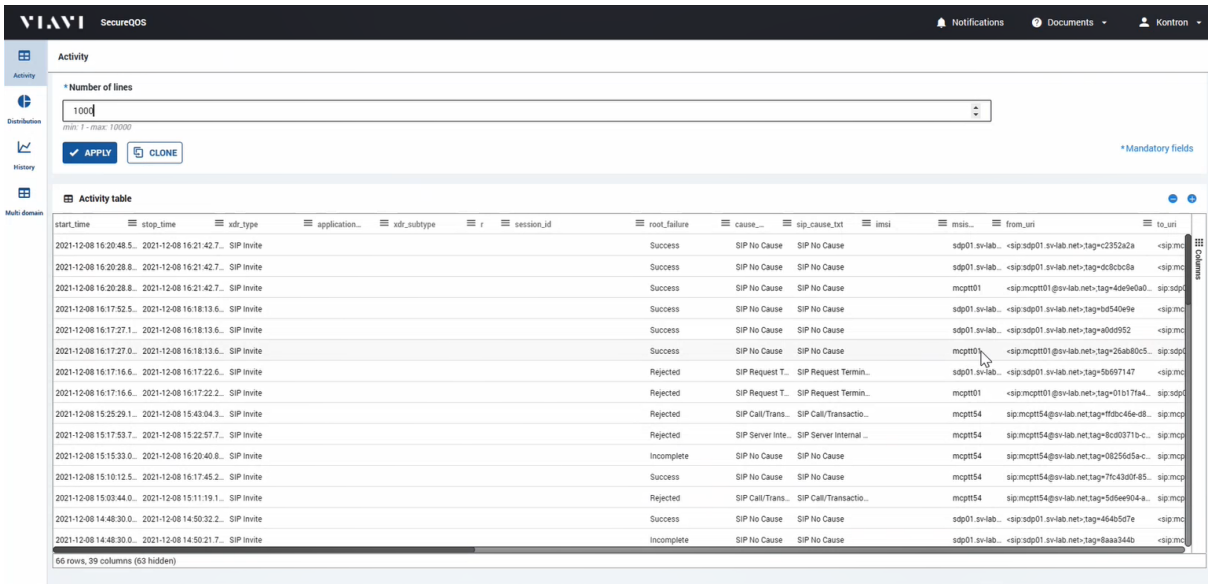


Figure 77: SIP and MCx messages viewer

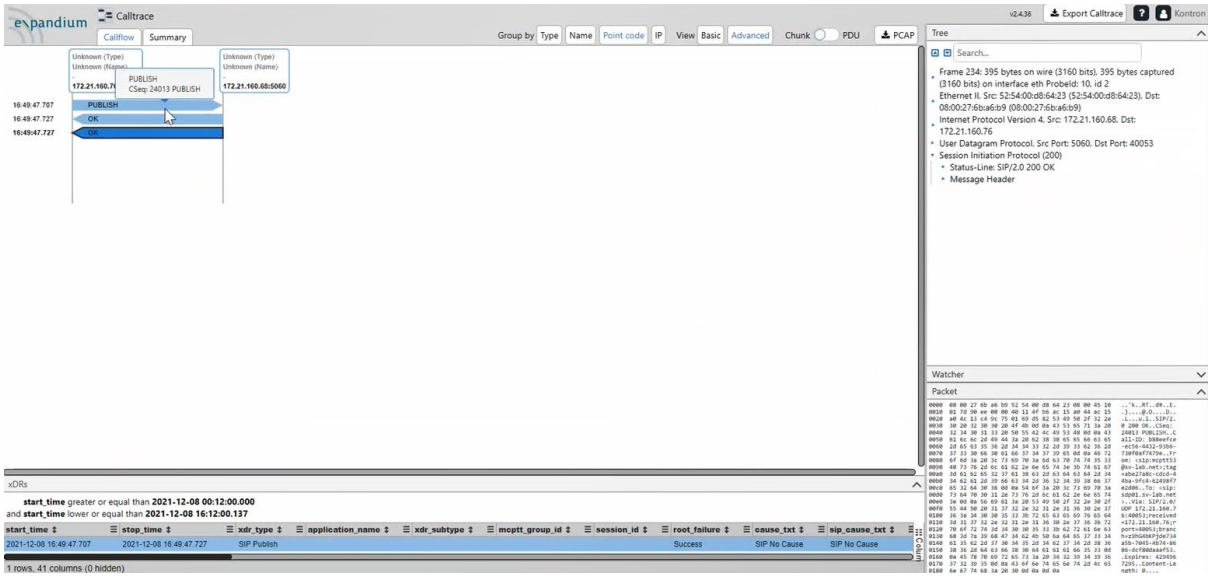


Figure 78: View of SIP/MCx call flow

Another part of the tool can compute MCx KPIs as shown on Figure 79:

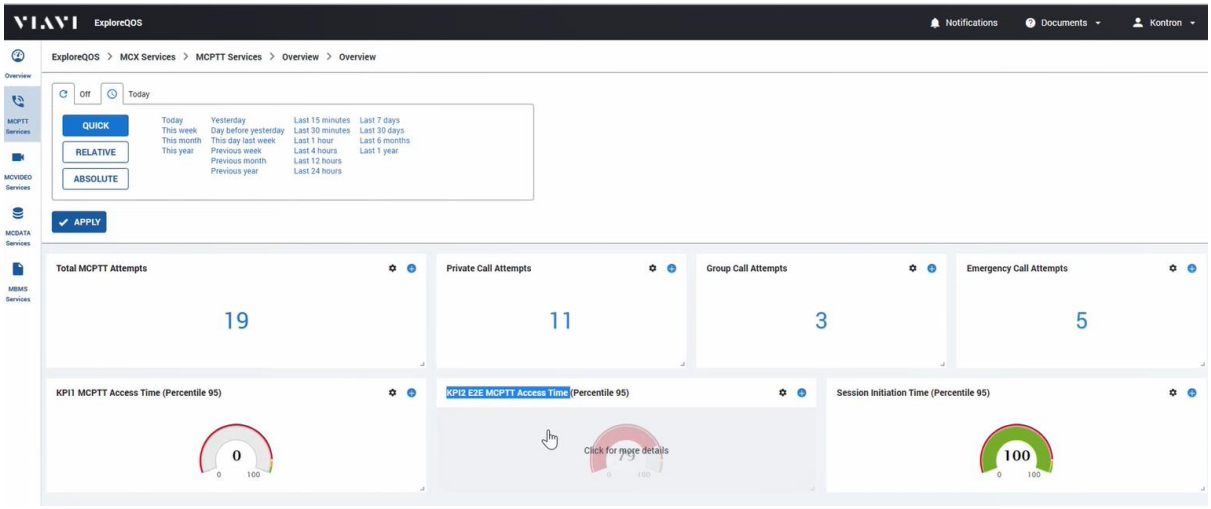


Figure 79: MCx KPI measurement tool

6.1.3 Vertex tool for degraded radio condition tests

When tests in degraded radio condition should be done in WP4, the use of a RF emulator tool is needed. In Kontron, Spirent Vertex Channel Emulator is the tool used for these type of tests. Spirent's Vertex Channel Emulator is an advanced test and measurement system that accurately simulates the complex effects of signal fading on wireless transmissions. As The Vertex channel emulator provides integrated, bi-directional RF channels, it simplifies tests in MIMO 2x2 RF configuration as described below.

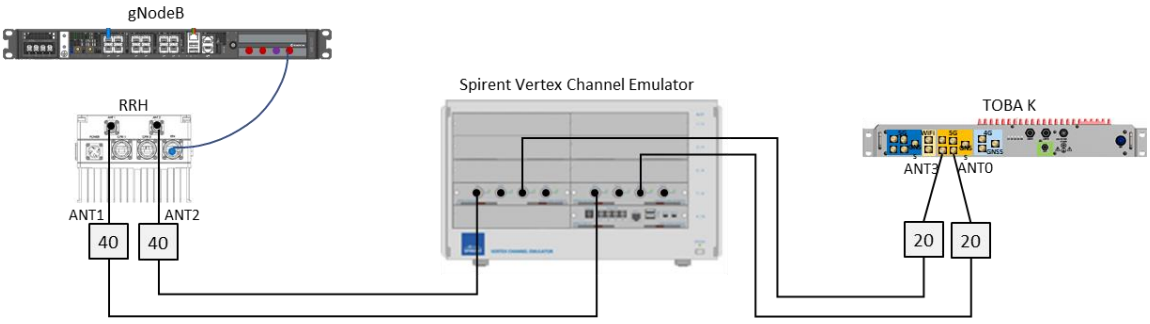


Figure 80: Degraded radio conditions RF setup

Vertex setting could be updated simply following FDD or TDD configuration is under test, knowing that n8 is FDD and n39 and n78 are TDD.

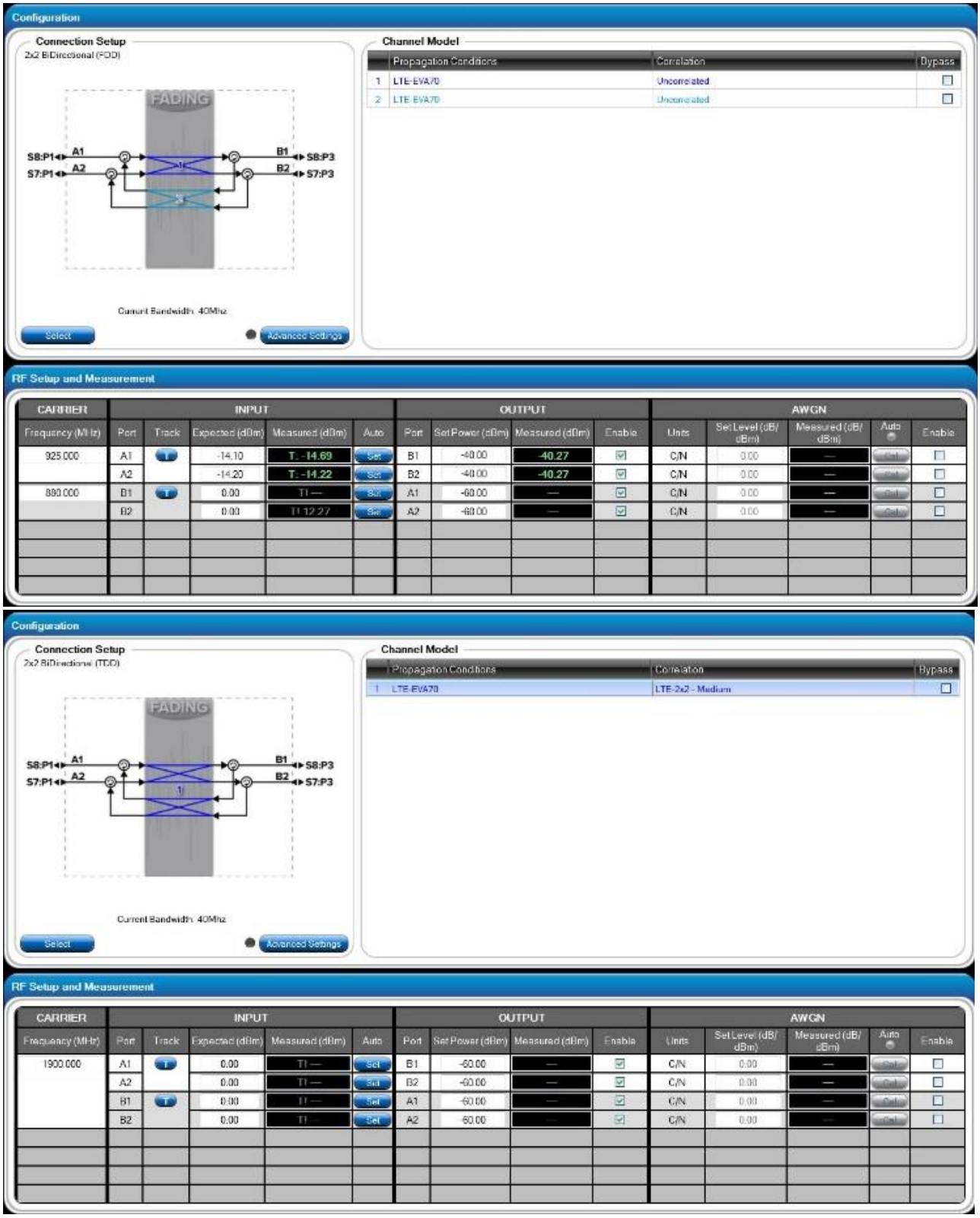


Figure 81: Vertex connection setting

When Vertex is introduced in a wired RF setup, Vertex could be set in bypass mode, static mode or dynamic mode when multipath fading propagation conditions are requested for a test.

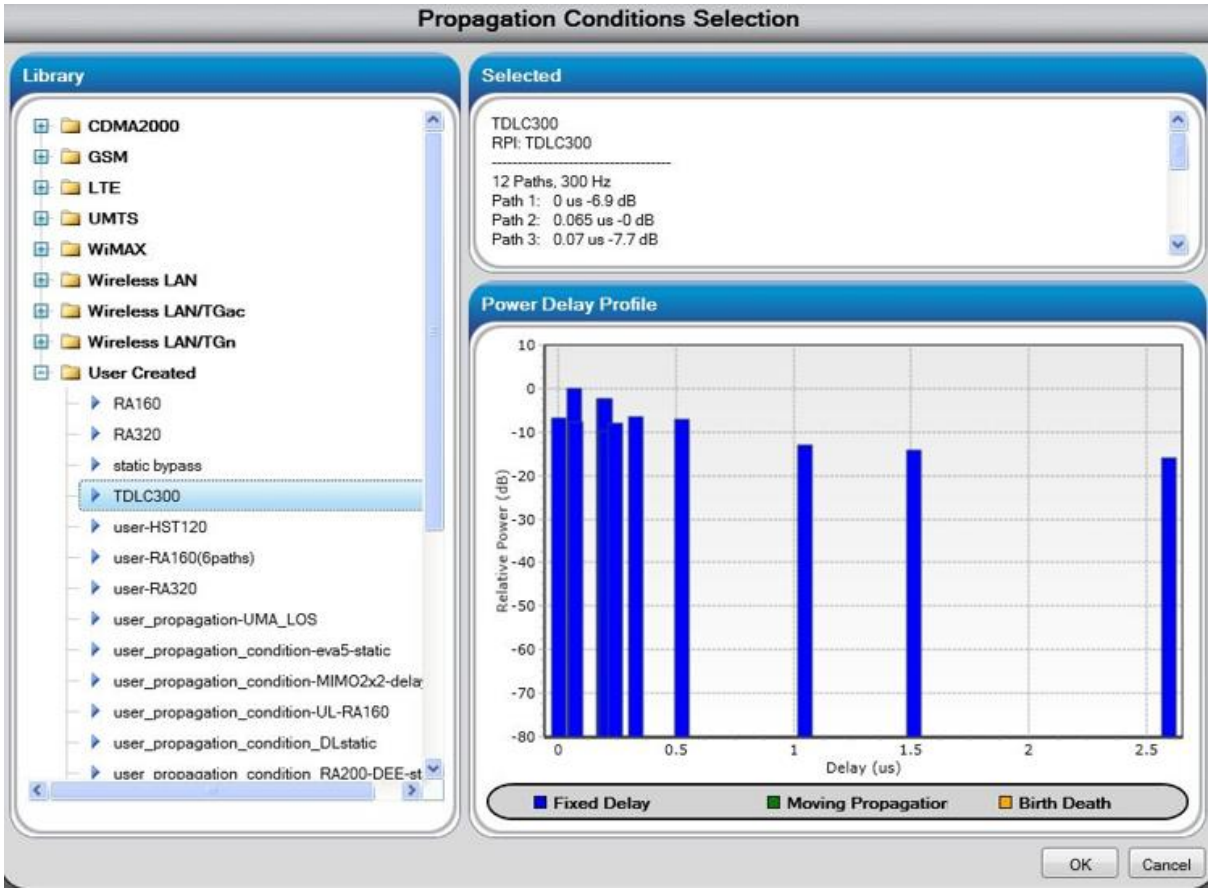
Vertex offers to use various predefined radio propagation conditions as defined in 3GPP documents but radio propagation conditions could also be defined manually if not part of the Vertex library. Currently this is the case with new FR1 5G TDL models (TDLA30, TDLB100 and TDLC300) as defined in 3GPP TS38.521.

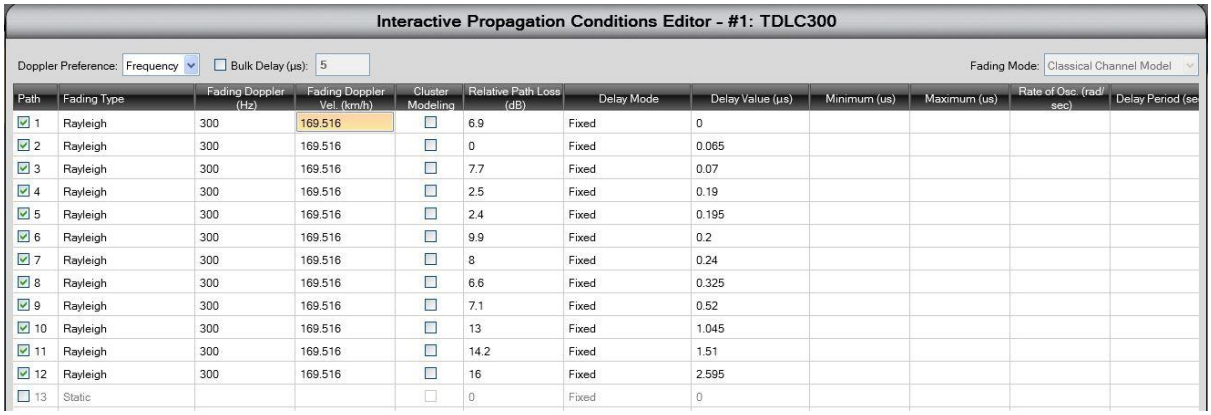
For each of these profiles, a frequency doppler should also be defined (see Table 41: Delay TDLB100) allowing to simulate UE velocity. Here is the formula linking UE velocity, doppler frequency and carrier frequency (i.e. 5G band). Vertex automatically compute velocity in function of frequency doppler.

$$Freq_{Doppler} = \frac{Velocity_{ue} \times Freq_{carrier}}{c}$$

with C ≅ Speed of Light (3x10^8 m/s)

Please find below, as an example, the Vertex MMI allowing to define this models





Path	Fading Type	Fading Doppler (Hz)	Fading Doppler Vel. (km/h)	Cluster Modeling	Relative Path Loss (dB)	Delay Mode	Delay Value (µs)	Minimum (us)	Maximum (us)	Rate of Osc. (rad/sec)	Delay Period (se
1	Rayleigh	300	169.516		6.9	Fixed	0				
2	Rayleigh	300	169.516		0	Fixed	0.065				
3	Rayleigh	300	169.516		7.7	Fixed	0.07				
4	Rayleigh	300	169.516		2.5	Fixed	0.19				
5	Rayleigh	300	169.516		2.4	Fixed	0.195				
6	Rayleigh	300	169.516		9.9	Fixed	0.2				
7	Rayleigh	300	169.516		8	Fixed	0.24				
8	Rayleigh	300	169.516		6.6	Fixed	0.325				
9	Rayleigh	300	169.516		7.1	Fixed	0.52				
10	Rayleigh	300	169.516		13	Fixed	1.045				
11	Rayleigh	300	169.516		14.2	Fixed	1.51				
12	Rayleigh	300	169.516		16	Fixed	2.595				
13	Static				0	Fixed	0				

Figure 82: Vertex MMI of propagation conditions editor (TDLC300-300)

In Figure 82 with a frequency doppler set to 300Hz, it means that for a carrier equal to 1910MHz (band 39), UE velocity is 169 km/h.

Here are parameters to set in Vertex for the 3 FR1 delay profiles for FR1:

Tap #	Delay [ns]	Power [dB]	Fading distribution
1	0	-15.5	Rayleigh
2	10	0	Rayleigh
3	15	-5.1	Rayleigh
4	20	-5.1	Rayleigh
5	25	-9.6	Rayleigh
6	50	-8.2	Rayleigh
7	65	-13.1	Rayleigh
8	75	-11.5	Rayleigh
9	105	-11.0	Rayleigh
10	135	-16.2	Rayleigh
11	150	-16.6	Rayleigh
12	290	-26.2	Rayleigh

Table 40: Delay TDLA30

Tap #	Delay [ns]	Power [dB]	Fading distribution
1	0	0	Rayleigh
2	10	-2.2	Rayleigh
3	20	-0.6	Rayleigh
4	30	-0.6	Rayleigh
5	35	-0.3	Rayleigh
6	45	-1.2	Rayleigh
7	55	-5.9	Rayleigh
8	120	-2.2	Rayleigh
9	170	-0.8	Rayleigh
10	245	-6.3	Rayleigh
11	330	-7.5	Rayleigh
12	480	-7.1	Rayleigh

Table 41: Delay TDLB100

Tap #	Delay [ns]	Power [dB]	Fading distribution
1	0	-6.9	Rayleigh
2	65	0	Rayleigh
3	70	-7.7	Rayleigh
4	190	-2.5	Rayleigh
5	195	-2.4	Rayleigh
6	200	-9.9	Rayleigh
7	240	-8.0	Rayleigh
8	325	-6.6	Rayleigh
9	520	-7.1	Rayleigh
10	1045	-13.0	Rayleigh
11	1510	-14.2	Rayleigh
12	2595	-16.0	Rayleigh

Table 42: Delay TDLC300

Combination name	Model	Maximum Doppler frequency
TDLA30-5	TDLA30	5 Hz
TDLA30-10	TDLA30	10 Hz
TDLB100-400	TDLB100	400 Hz
TDLC300-100	TDLC300	100 Hz
TDLC300-600	TDLC300	600 Hz
TDLC300-1200	TDLC300	1200 Hz

Table 43: Channel model FR1

In addition of radio propagation setting, channel correlation matrix should be defined for MIMO 2x2 tests. There are 3 type of MIMO correlation matrices: low / medium / high.

Low correlation	
α	β
0	0

2x2 case	$R_{medium} = \begin{pmatrix} 1 & 0.9 & 0.3 & 0.27 \\ 0.9 & 1 & 0.27 & 0.3 \\ 0.3 & 0.27 & 1 & 0.9 \\ 0.27 & 0.3 & 0.9 & 1 \end{pmatrix}$

Table 44: MIMO correlation matrices for medium correlation

2x2 case	$R_{high} = \begin{pmatrix} 1 & 0.9 & 0.9 & 0.81 \\ 0.9 & 1 & 0.81 & 0.9 \\ 0.9 & 0.81 & 1 & 0.9 \\ 0.81 & 0.9 & 0.9 & 1 \end{pmatrix}$

Table 45: MIMO correlation matrices for high correlation

This MIMO correlation matrices are predefined in VERTEX library.

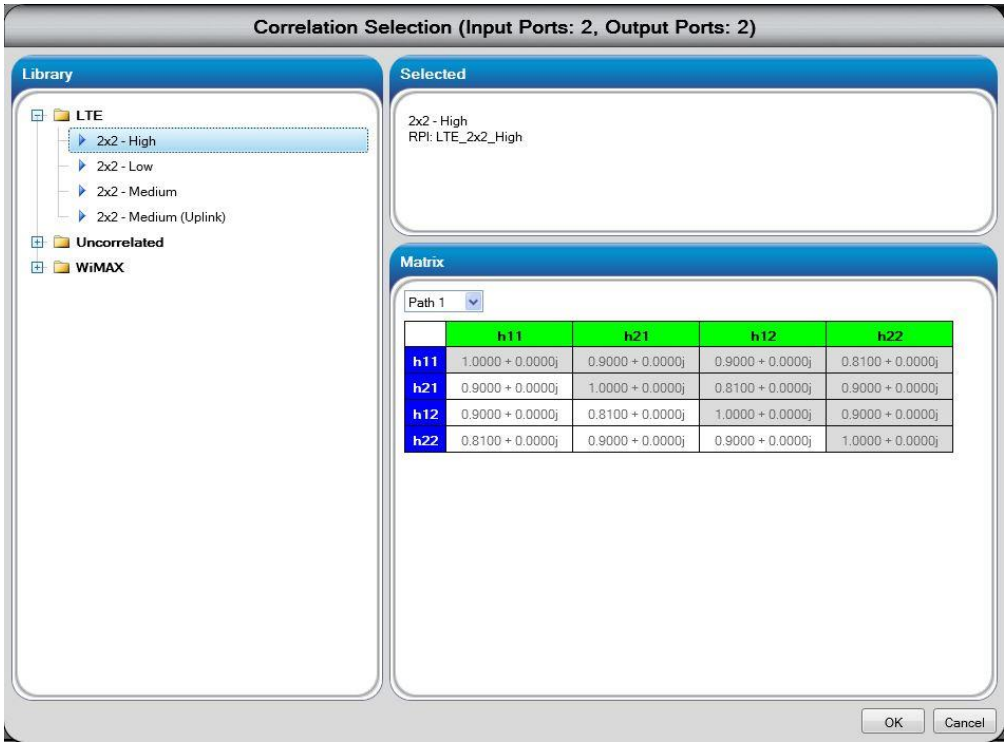


Figure 83: Vertex MMI of MIMO correlation selection

6.2 Network configurations

Network configurations to be used during test phase are detailed in document D1.1, test case per test case. Yet, in the current document, it is important to underline how the different setups are foreseen for each kind of test cases. Indeed, we can already identify several kind of tests:

- *Normal conditions test cases*: Corresponds to tests where the application is tested end to end in the most simple way and without any side action
- *Tests cases with 5G HO*: During these tests, the OB GW will move from one 5G cell to another
- *Radio degraded tests cases*: During these tests, the radio signal is modified by a tool in order to reflect a specific situation (speed, fading, radio multipath)
- *Cross border tests cases*: During these tests, the OB GW will move from one 5G PLMN to another one
- *Bearer Flex test cases:* During these tests, redundancy and aggregation use cases will be tested with 5G and 4G networks.

For each category listed above, a network configuration diagram is given in this section in order to understand how the test will be executed.

6.2.1 Normal conditions tests cases

Configuration of Figure 84 gives an example (with ETCS application and OB GW-K) of the setup for a *normal conditions* kind of test case.

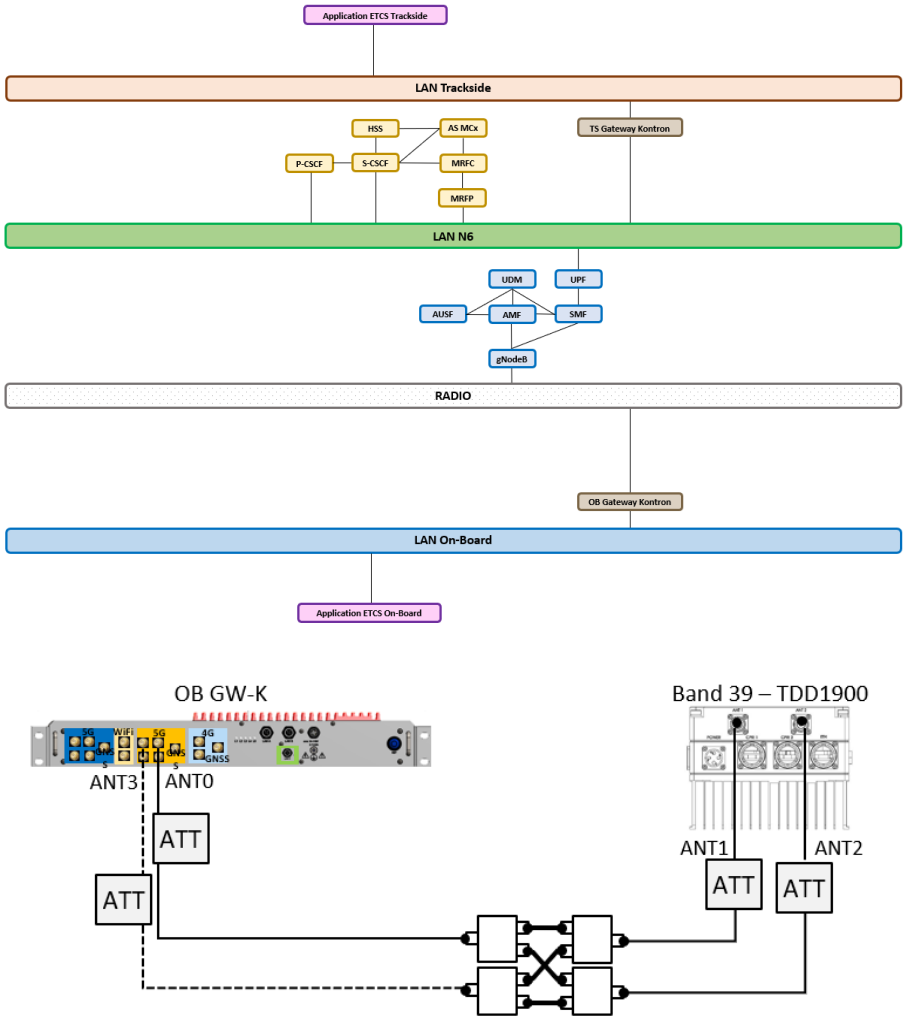


Figure 84: Setup for ETCS end to end FRMCS call in normal conditions

6.2.2 Test cases with 5G HO

Configuration of Figure 85: Setup for end to end ETCS FRMCS call with 5G HO gives an example (with ETCS application and OB GW-K) of the setup for a *5G HO* kind of test case.

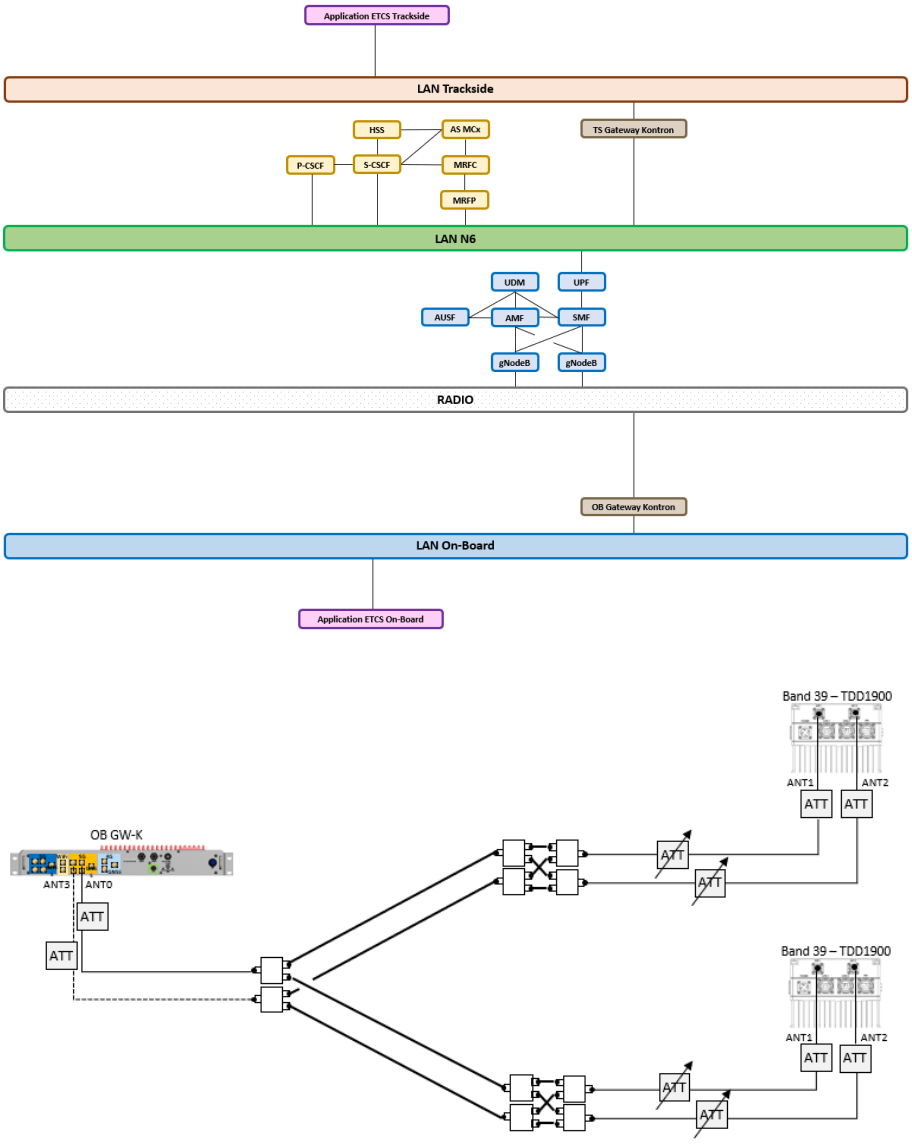


Figure 85: Setup for end to end ETCS FRMCS call with 5G HO

6.2.3 Radio degraded test cases

Configuration of Figure 86 gives an example (with ETCS application and OB GW-K) of the setup for a *Radio degraded* kind of test case.

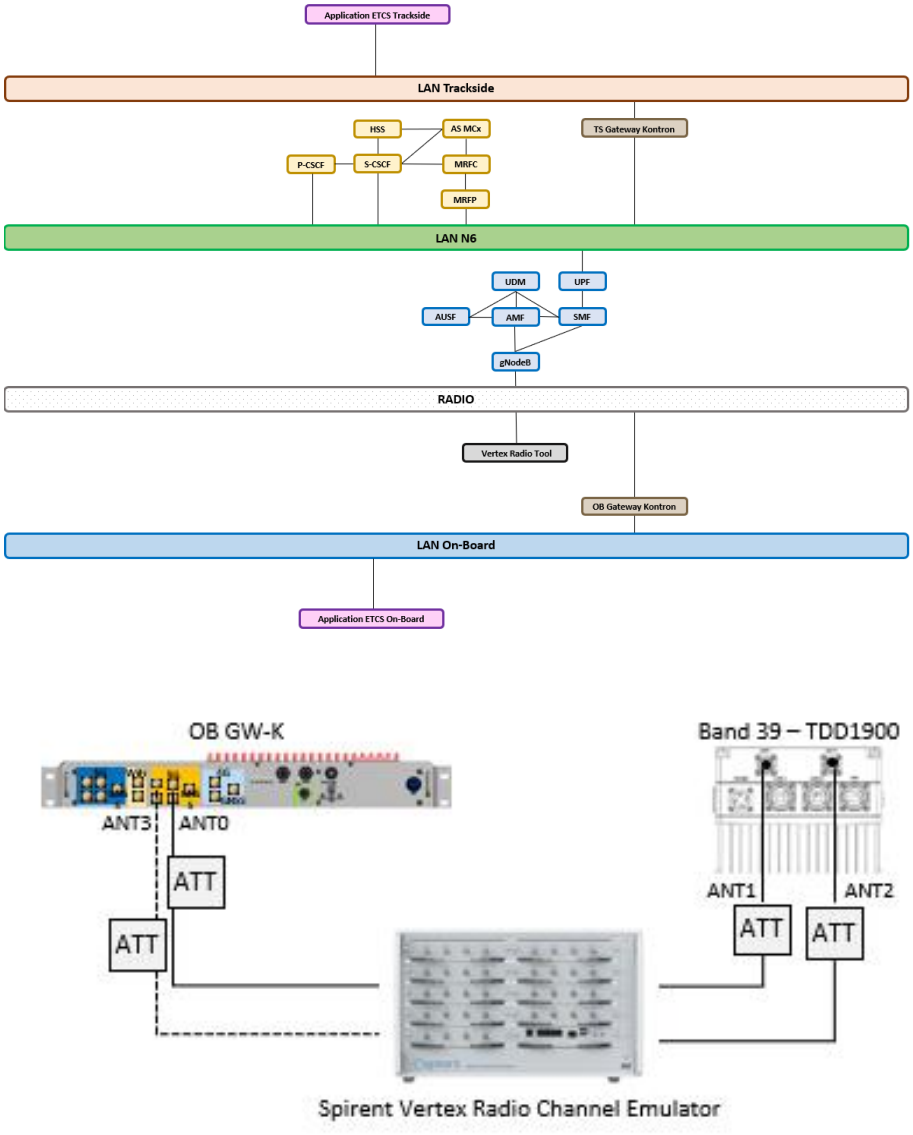


Figure 86: Setup for end to end ETCS FRMCS call with radio degraded conditions

6.2.4 Cross-border tests cases

Configuration of Figure 87Figure 85: Setup for end to end ETCS FRMCS call with 5G HO gives an example (with ETCS application and OB GW-K) of the setup for a *Cross Border* kind of test case. In 5GRail, crossborder can be achieved using one or two UEs in the FRMCS OB Gateway. Test report 132[S21] gives all the details on how crossborder scenarios have been achieved.

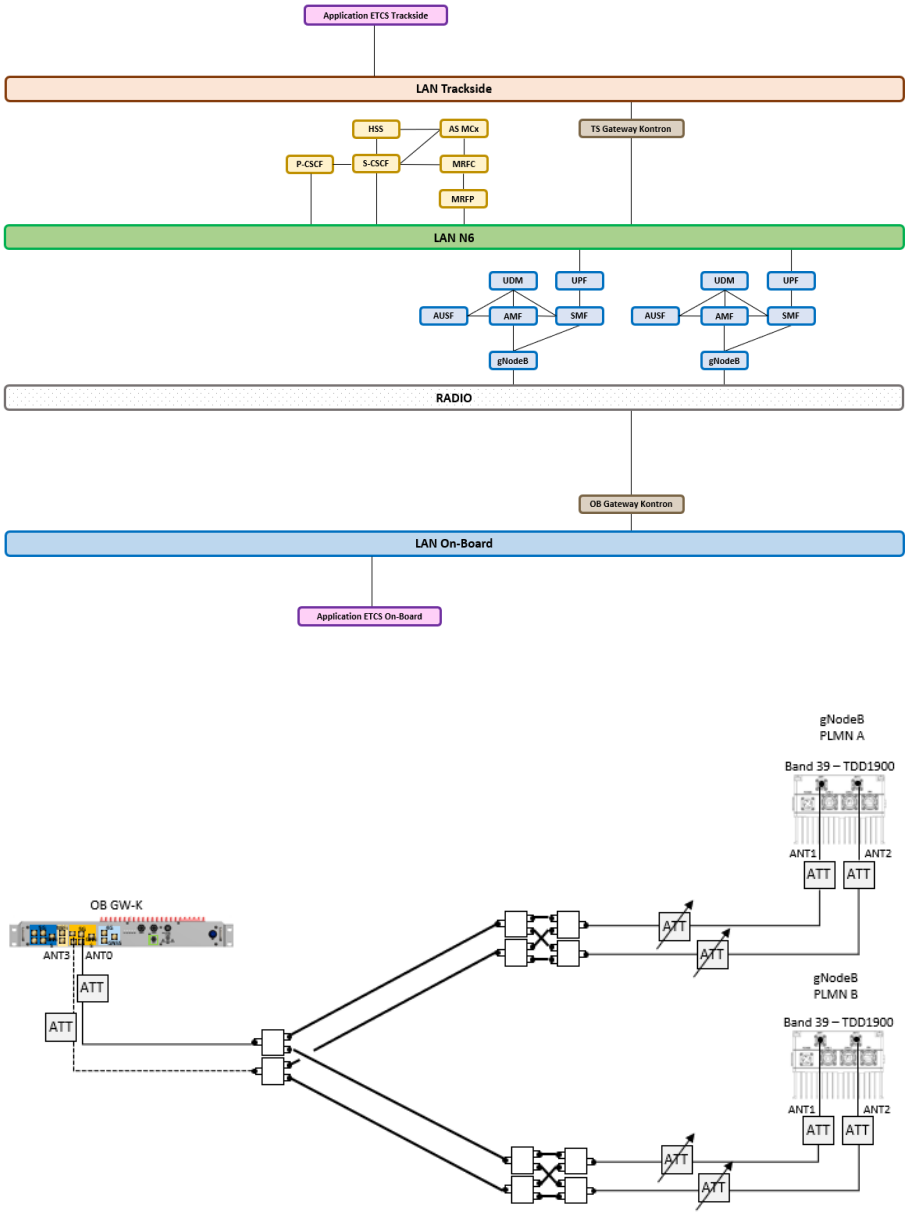


Figure 87: Setup for end to end ETCS FRMCS call with cross border

6.2.5 Bearer flex tests cases

Bearer flex deals with two scenarios:

- Redundant use case where a train goes from 5G only coverage to 4G only coverage and vice versa
- Aggregation use case where a train goes from 5G only coverage to 4G and 5G coverage, and vice versa

In order to test these scenarios, the setup of Figure 88 is used:

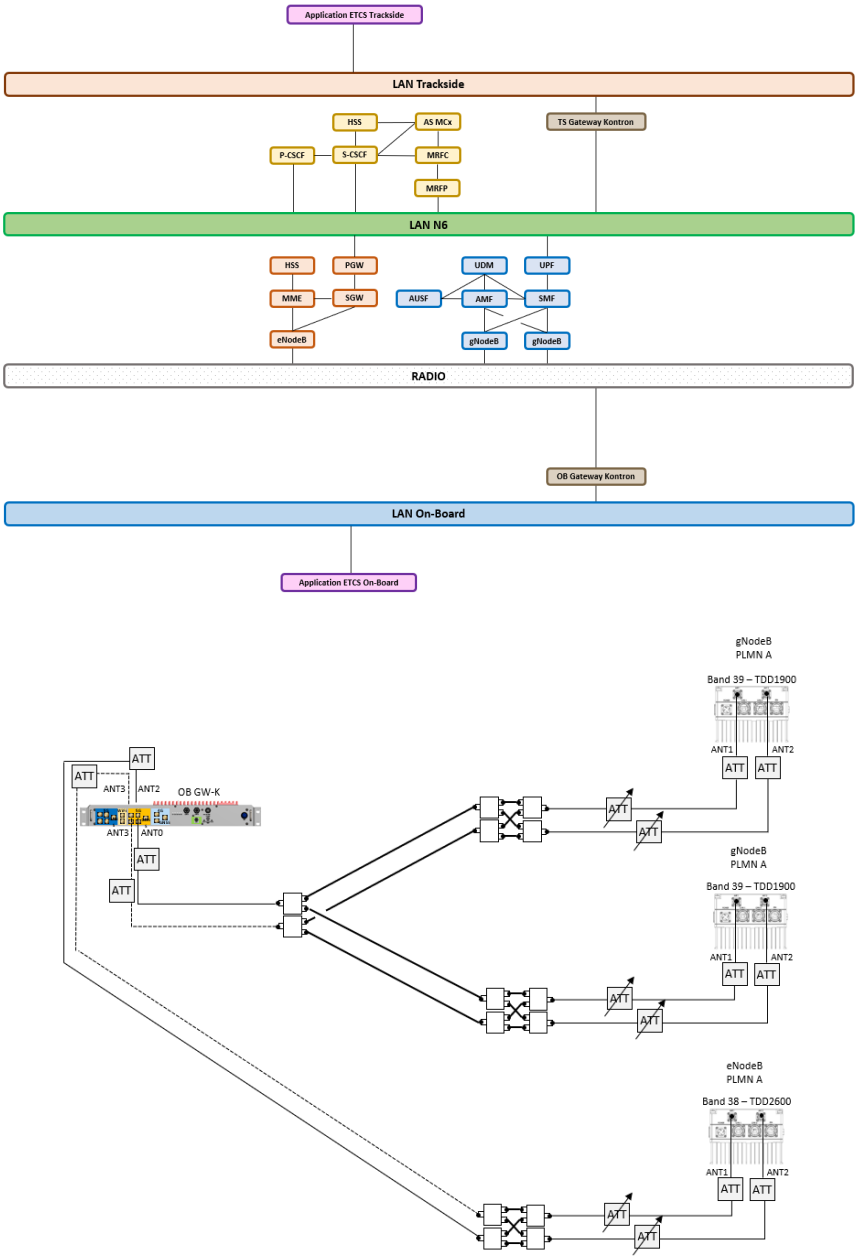


Figure 88: Setup for end to end ETCS FRMCS call for bearer flex

7 CONCLUSION

This D4.2 document reflects all the work that has been done by WP4 team in order to setup the second 5Grail lab. As described, after many efforts integrating all network pieces together, the whole lab was ready for tests phase of WP4, which corresponds to Task 4.4 :

- all interfaces with Wi-Fi, 4G and 5G networks have been checked with Thales ES1 and ES3 modems,

- IMS/MCx functions have been checked so that MCx call between FRMCS Gateways could be guaranteed,

- QoS management using DSCP to trigger a specific 5QI has been validated,

- FRMCS Gateways delivered by WP2 have been inserted in the lab successfully, even in band 39,

- FRMCS applications ATO, ETCS and PIS have passed the integration tests that demonstrated their ability to communicate with FRMCS Gateways using standard Obapp and Tsapp interfaces.

All these efforts lead to the very first FRMCS ATO end to end call using FRMCS Gateways over 5G SA network in March 2022, a major achievement quickly disseminated to the FRMCS community. With an operational WP4 lab available around the end of Q3 2022, test phase could start according to WP1 D1.1 recommandations. This phase lasted for about 5 months and is reported in deliverable D4.3 [S21].

8 REFERENCES

Document Title	Reference, version
[S1] Radio-frequency connectors –Part 16: Sectional specification – RF coaxial connectors with inner diameter of outer conductor 7 mm (0,276 in) with screw coupling – Characteristics impedance 50 Ω (75 Ω) (type N)	IEC 61169-16
[S2] Management Information Base for Network Management of TCP/IP-based internet: MIB-II	RFC 1213
[S3] MC Services Security aspects (useful to understand MCx authentication and authorization)	3GPP TS33.180
[S4] Mission Critical Data (MCData) signalling control; Protocol specification	3GPP TS 24.282
[S5] Mission Critical Data (MCData) media plane control; Protocol specification	3GPP TS 24.582
[S6] UIC – FRMCS Use cases	UIC MG-7900, Version 2.0.0
[S7] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Future Railway Mobile Communication System	3GPP TR 22.889
[S8] UIC – FRMCS Principle Architecture	UIC MG-7904 Version 0.3.0 (Draft)
[S9] UIC – FRMCS – Telecom On-board system – Functional Requirement Specification	UIC TOBA FRS-7510 Version 0.2.0
[S10] Common functional architecture and information flows to support mission critical communication services	3GPP TS 23.280 Stage 2

[S11]	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support Mission Critical Data (MCData)	3GPP TS 23.282 V17.6.0, Stage 2 (Release 17) – 04/2021
[S12]	Rail Telecommunications (RT); Future Rail Mobile Communication System (FRMCS); Study on system architecture	ETSI TR 103.459 V1.2.1, 08/2020
[S13]	UIC – FRMCS – User Requirements Specification	FU-7100 Version 5.0.0
[S14]	UIC – FRMCS – Functional Requirements Specification	FU-7120 Version 0.3.0
[S15]	UIC FRMCS On-Board System Requirements Specification (TOBA SRS)	TOBA-7530
[S16]	UIC FRMCS Functional Interface Specification (FRMCS FIS)	
[S17]	UIC FRMCS Form-Fit Functional Interfaces (FRMCS FFFIS)	
[S18]	UIC FRMCS System Requirements Specification (FRMCS SRS)	AT-7800
[S19]	TOBA Architecture Report	D2.1
[S20]	Second Lab Integration and Architecture Report	D4.1
[S21]	Second Lab Test Report	D4.3
[S22]	WP1 D1.1 Test Plan	D1.1 v2
[S23]	TOBA Integration Report	D2.2

9 APPENDICES

9.1 WP1 test cases definitions

The 2 following tables from WP1 reflects the current status of test cases to be executed in WP4.

							Relevant Communication Applications							Relevant Support Applications												
		5GRAIL	LAB WP3 LAB WP4 FIELD DB WP5 FIELD SNCF WP5				5.9	5.10	5.19	5.20	5.27	6.19	6.20	6.23	8.1	8.2	8.3	8.4	8.5	8.7	8.8	8.9	8.10	8.11	8.12	10.1
							Automatic Train Protection communication	Automatic Train Operation communication	Voice recording and access	Data recording and Access	Critical real time video	Messaging Services	Transfer of data	Real time video call	Assured voice communication	Multi user talker control	Role management and presence	Location services	Authorisation of communication	Authorisation of application	QoS class negotiation	Safety application key management communication	Assured data communication	Inviting-a-user messaging	Arbitration	Billing information
URS Ref	Applications																									
5.9	Automatic Train Protection communication*	X	X	X	X	X		X					X				X	X	X	X	X				X	
5.10	Automatic Train Operation communication (limited to GoA2 ATO)*	X		X		X	X						X				X	X	X	X	X				X	
6.9	On-Train Telemetry communications (TCMS includes 6.9 + 6.11 + 6.20), including PIS	X	X	X	X	X							X				X	X	X	X	X				X	
6.13	Non-critical real time video (see clause 5.27) - MCVideo, MCData related?	X	X	X	X	X							X				X	X	X	X	X				X	

Table 46: WP1 view of test cases to be executed in WP4 (1/2)

							FRMCS System principles related use cases (source: TR 22.889)																						
		5GRAIL	LAB WP3 LAB WP4 FIELD DB WP5 FIELD SNCF WP5				12.2 Area Broadcast Group Communication interworking between GSM-R and FRMCS Users	12.3 Location Service interworking between GSM-R and FRMCS Users	12.4 Presence interworking between GSM-R and FRMCS Users	12.5 Point to Point communication between GSM-R and FRMCS Users	12.6 Interworking with legacy systems including LMR	12.7 Builds stable positioning framework for FRMCS services and devices including trainborne and handheld devices	12.8 Interworking between GSM-R and FRMCS	12.9 Bearer flexibility	12.10 QoS in a railway environment	12.11 Provide broadband and mission critical services with seamless connectivity	12.12 Offer railway services high-quality control functions with real-time train status monitoring	12.13 Provide call priority during interworking with LMR	12.14 FRMCS Positioning Accuracy	12.15 FRMCS System security framework	12.16 Interworking to external networks	12.17 FRMCS On-network/Off-network communication	12.18 Call restriction service	12.19 Allocation and isolation of FRMCS communication resources	12.20 FRMCS Equipment capabilities for multiple FRMCS Users	12.21 FRMCS System/FRMCS User roaming capabilities	12.22 Availability – increasing measures	12.23 Flexible use of available contiguous spectrum blocks(s) and related bandwidth(s)
							Yes	Yes	N/A	TBC	N/A	Option	Yes	Yes	Yes	N/A	N/A	N/A	Yes	TBC	N/A	N/A	Option	Yes	Yes	Yes	Option	N/A
URS Ref	Applications																												
5.9	Automatic Train Protection communication*	X	X	X	X	X						O	X	X	X				X					X	X	X	O	
5.10	Automatic Train Operation communication (limited to GoA2 ATO)*	X		X		X						O		X	X				X					X	O	O		
6.9	On-Train Telemetry communications (TCMS includes 6.9 + 6.11 + 6.20), including PIS	X	X	X	X	X								O	X				X									
6.13	Non-critical real time video (see clause 5.27) - MCVideo, MCData related?	X	X	X	X	X						O		X	X			O	X					X	X	O		

Table 47: WP1 view of test cases to be executed in WP4 (2/2)

All the supported applications and features to be tested per application (ETCS-ATP/ATO) are listed in the 2 tables above.

9.2 WP4 assumptions

For information, the following updated assumptions reflect what has been agreed by WP4 members:

ID	Technical Architecture Assumptions to support WP4 execution
1	Multiconnectivity foreseen induces the need for Trackside GW to be planned in WP4 setup (WP2 deliverable)
2	TOBA prototype integrates 1900MHz FRMCS 5G modem
3	QoS managed using DSCP
4	WP4 cybersecurity assets -if any- to be provided by partner involved (potential impact on architecture and schedule)
5	For the moment WP4 plan little activity with N78 (3.7 GHz) ; main focus being N39 FRMCS band
6	Remote access to equipments for all partners
7	Some partners equipments (Alstom so far) will be installed in Montigny WP4 lab
8	No MCVIDEO, use MCData instead
9	No MCX - MCX Interworking
10	4G SIMs are suitable for 5G Rail test cases
11	ETCS on GSM-R will be based on GPRS connection
12	O&M streams should be separated for some cyber tests
13	Kontron will install a server to host DNS applications
14	Track data not linked with real one used in WP5
15	Train and Track simu separated ETCS/ATO
16	Train and Track simu and radio link simu not correlated
17	The ATO version will be the one tested in S2R and not necesseray the one currently udapted in the 2022TSI
18	RF combiner to be use in WP4 lab
19	Remote vision app will be tested in WP4 if loose coupling chosen
20	Wifi test should be run in WP4 before WP5 if agreed to be done in WP5
21	4G test should be run in WP4 before WP5 if agreed to be done in WP5
22	PIS will not use GSM-R
23	PIS application trackside must be time synchronized by NTP (master clock trackside)
24	PIS application is no longer to be considered as the demonstrator for cyber security test cases

9.3 Planning of WP4

WP4 planning of activities is shown on Figure 89:

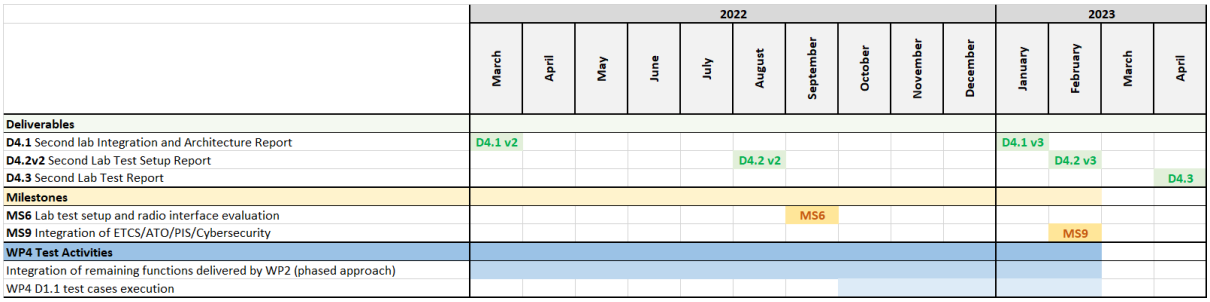


Figure 89: WP4 planning

After having installed all WP4 lab and tested all interfaces, including N39 radio, MS6 was achieved. At that moment WP4 was be ready for execution of all tests cases specified in D1.1 delivery, according to the available possibilities because WP2 deliveries lasted several months after that date.

Test execution period extended till end of February 2023, when MS9 marks end of lab activities. Delivery D4.3, that reports all results of this Task 4.4 phase will be submitted in April 2023.

9.4 Some WP4 IMS/MCx default parameters

		parameter	value	unit
S-CSCF	tm	fr_timer	4000	ms
S-CSCF	tm	fr_inv_timer	120000	ms
S-CSCF	ims_auth	name	URI	
S-CSCF	ims_auth	auth_used_vector_timeout	300	s
S-CSCF	registrar	default_expires	3600	s
S-CSCF	registrar	min_expires	60	s
S-CSCF	registrar	max_expires	5400	s
S-CSCF	registrar	support_wildcardPSI	1	
S-CSCF	registrar	dereg_in_progress_window	30	s
P-CSCF	rtimer	timer interval	15	10s
P-CSCF	rtimer	timer mode	1	
P-CSCF	tm	failure_reply_mode	3	
P-CSCF	tm	fr_timer	5000	ms
P-CSCF	tm	fr_inv_timer	120000	ms
P-CSCF	tm	auto_inv_100	0	
P-CSCF	registar	is_registered_fallback2ip	1	
P-CSCF	registar	ignore_contact_rxport_check	1	
P-CSCF	registar	pending_reg_expires	15	
P-CSCF	registar	subscribe_to_reginfo	1	
P-CSCF	registar	publish_reginfo	1	
P-CSCF	registar	subscribe_to_reginfo	0	
P-CSCF	registar	publish_reginfo	0	

Grant agreement
No 951725