Deliverable D3.2 v2

First Lab Test Setup Report

Grant agreement
No 951725

5GRAIL

5G for future RAILway mobile communication system

D3.2 v2 First Lab Test Setup Report

Due date of deliverable: 31/12/2021

Actual submission date Rv2: 30/06/2022

Leader/Responsible of this Deliverable: Nokia

Reviewed: Y

Document status		
Revision	**Date**	**Description**
0.1	21/02/2022	Draft D3.2 V1 Version for consortium review
1.0	28/02/2022	Consolidation of the first deliverable version
1.1	14/06/2022	Additional updates and consolidation of the first deliverable version Draft for consortium review
2.0	30/06/2022	Consolidation of the first deliverable version Version submitted

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 "D3.2 - First Lab Test Setup Report" is to describe the 5G reference lab in Hungary setup, including the integration and verification of radio compatibility of 5G radio modules and other public band modules depending on spectrum.

The 5G reference lab in Hungary will validate the main FRMCS functionalities related to specific applications prototypes, such as ETCS, Voice, TCMS and CCTV/Video pre-integrated within the FRMCS-On Board Gateway (a.k.a TOBA) and Trackside GW during WP2. Based on WP1 definition, also the network functionality for GSM-R – FRMCS interworking will be tested – thus emulating a cross technology/cross domain use case.

The test case scenarios described in WP1 and executed in WP3 aim at demonstrating the end-to-end integration of existing or newly developed critical and performance communications railway applications and main FRMCS functionalities and features over the 5G FRMCS architecture.

The report includes the description of the following tasks: the integration activities to set the targeted FRMCS ecosystem, and the planned activities required to execute the test cases as defined by WP1.

Details on the network integration of the various components provided by WP3 participants are also given. The test environment includes 5G radio, 5G core, GSM-R network and application servers to demonstrate Voice, TCMS, ETCS and CCTV/video.

Nokia-DE was coordinating the activities, while Nokia-HU was in charge of the lab set-up and integration for the complete telecommunication network, including the network elements supplied by Kontron, Siemens, CAF and Teleste, interconnected to the 5G core and 5G radio from Nokia. By the early delivery of the Modem by Thales the compatibility with the 5G infrastructure could be verified before integrating the OB Gateway.

Finally, having explained the integration of these various elements, a perspective on foreseen tests setup and time plan will be given.

Due to COVID19 restrictions at the Lab in Budapest (from November till Mid-February site visits by partners were not possible, and local team recommended to work from Home), the integration tasks and the document D3.2 were delivered with delays (D3.2 rev2).

The next phase will focus on the execution of the test plan for each application to verify and validate the system behaviour with reference to the user & system requirements as well as to the FRMCS specification – refer to document D1.1 [S21].

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
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
MGW	Media Gateway
MIMO	Multiple Input Multiple Output
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 Center
OTA	Over The Air
OTT	Over The Top

PCB	Printed Circuit Board
PCF	Policy Control Function
PCU	Packet Control Unit
PDN	Packet Data Network
PIS	Passenger Information Service
PSS	Process Safety System
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
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
VoNR	Voice over NR (New Radio)
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

The main objective of the 5GRAIL is to validate the first set of FRMCS specifications, known as FRMCS V1, by developing and testing prototypes of the FRMCS ecosystem, for both on-board and trackside infrastructure. The outcome of 5GRAIL will provide feedback to the FRMCS standardization based on 5G technology to demonstrate the capabilities for the deployment by railway sector in Europe.

The 5GRail grant agreement [S20] defines the objective of the D3.2 delivery as follows:

"This report outlines the lab setup, integration and verification of radio compatibility of 5G radio modules and other public band modules depending on spectrum. Based on WP1 definition, network functionality for GSM-R – FRMCS interworking will be simulated. "

Work Package 3 provides the first 5G reference lab environment situated at Nokia premises in Hungary. The activities of this lab are focused on voice applications, ETCS, TCMCS, CCTV and Video. Lab activities performed in the second 5G reference lab situated at Kontron premises in France (WP4) are complementary for the whole 5GRail project and experiences are exchanged between the two labs.
Furthermore, WP3 and WP4 constitute a valuable experience for the field activities of WP5 in Germany and France respectively, since almost all test cases will be prior realized in these labs.

The focus of the first 5G reference lab test is to combine FRMCS 5G infrastructure and On-board GW prototypes with the related application prototypes, namely Voice, Video/CCTV, ETCS and TCMS in a unique environment for testing.
This document provides a full description of the achieved integration of the various elements provide by Nokia and partners detailing all sub-systems. Partner products from Siemens, CAF, Kontron, Thales and Teleste, followed by a list of the tools – where integrated into Nokia 5G and GSM-R network setup.

GSM-R infrastructure is available to cover 5G-GSM-R interworking scenarios as defined in WP1.
The lab configuration will be used to de-risk field tests in the scope of WP5, leaded by DBN in Germany and connect 5G core, MCX server and GSM-R infrastructure remotely for field test execution.

WP1 has defined the use cases to be performed by WP3 in relation with the assigned tasks, refer to chapter 7.1. and on the details described in D1.1 document [S21].

2 Network elements integration

This chapter describes the integration of the telecommunication services of WP3 lab.

All the elements which appear in blue in Figure 1: Functional View of the WP3 Lab are provided by Nokia and are located in the Nokia labs in Budapest (Hungary). The partner products are integrated as shown: dark blue elements are provided by Kontron, light blue by Teleste, red by CAF and petrol coloured CAB radio by Siemens.

The following figure shows a functional overview of the Lab including VPN access. VPN connections to allow for remote support are setup using Nokia LAB VPN capabilities (refer to the chapter 3 for the remote access description for each partner):

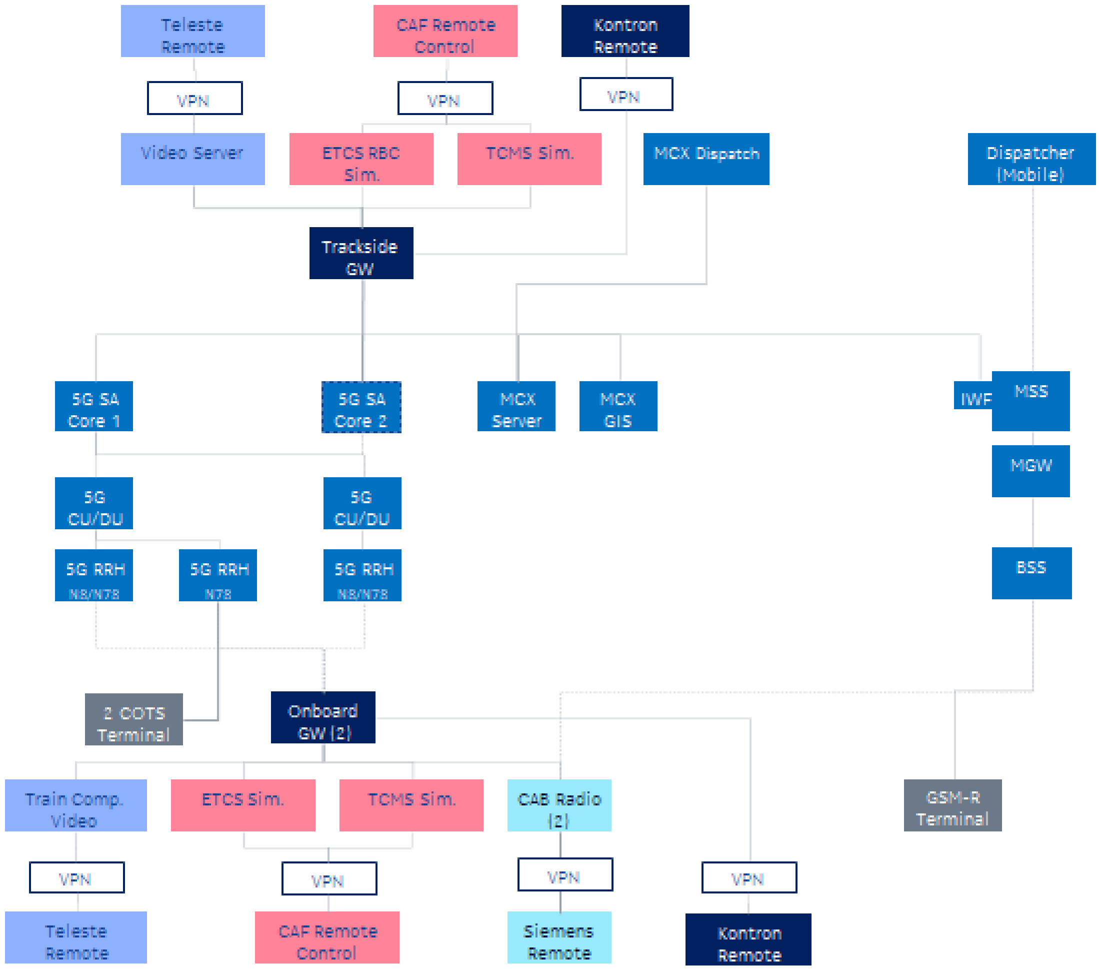

Figure 1: Functional View of the WP3 Lab

Note: the second 5G SA Core is not yet integrated as required for cross border uses cases planned as Task 3.4. The use of shared or dedicated radio for the second SA core is under evaluation.

Note: According current assumptions Wi-Fi will not be used to demonstrate Bearer Flexibility, but as defined in the WP3 Assumption tested using two 5G sub-bands as Multi Access – refer to chapter 4.5.

2.1 5G Network setting up

2.1.1 Introduction

The 5G network (in standalone mode – 5GSA) is the main component of the WP3 lab and most of the test cases will use such infrastructure.

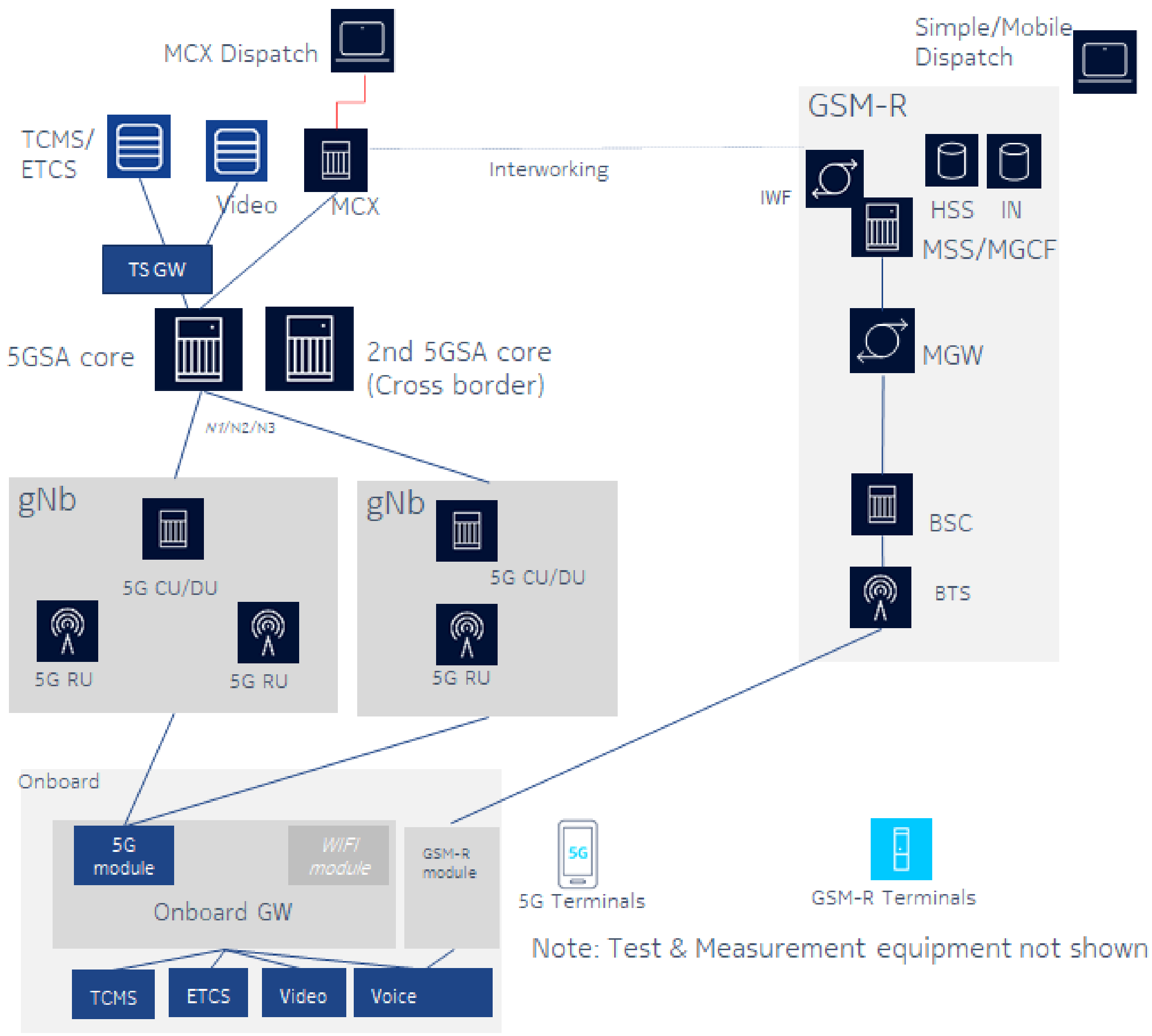

Figure 2: LAB Configuration

The gNB configuration with respect to select RRH (Band n8, Band n78) is flexible to allow the use cases to be tested and to be defined in WP1.

2.1.2 5G RAN

The following picture shows the FRMCS 5G Radio configuration integrated in the lab.

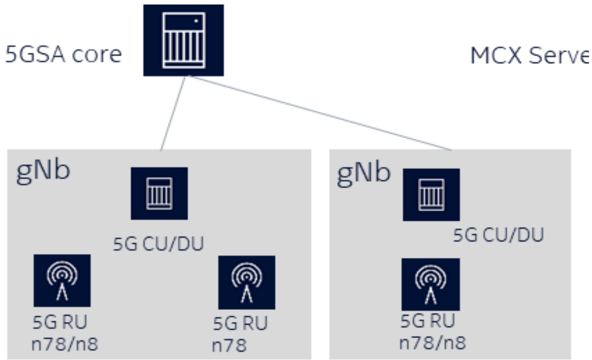

Figure 3: Radio Configuration

The Radio System consist of

- 2 gNB CU/DU: Nokia AirScale ASIK/ABIL
- 5G RU:
  - 3 Units AZQJ Band n78: 3480 -3800 MHz, 8T8R, 320 W (40W per TRX)
  - 2 Units AHDB Band n8: UL: 889 – 915 MHz/DL: 934 – 960, 2T4R, 2*80 W

The concrete configuration with RRH supporting band n8 or n78 depend on the use cases defined in WP1. Band n8 is planned to be used for functional e2e tests only.

2.1.2.1 Frequencies to be used and number of RRUs available

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

- N8 band, 900 MHz FDD (UL: 880 – 915 MHz, DL: 925 – 960 MHz)
- N78 band, 3300 – 3800 MHz TDD

WP3 ordered 3 RRUs for N78 band and 2 RUs for N8 band. Globally 5 RRUs have then been installed in WP3 lab, in Budapest Hungary.

- N78 band RRU: AZQJ
- N8 band RRU: AHDB

Datasheets of the RRUs are found in D3.1 document [S19]

2.1.2.2 Nokia AirScale 5G Baseband (CU/DU) gNB function and its engineering

RRU is managed by a 5G Baseband (CU/DU) gNB unit hosted in Nokia AirScale product. We have two gNBs in WP3 lab, in Budapest Hungary.

It should be noted that a gNB can be connected to several RRUs at the same time.

It is interesting to mention here it is possible to install both types of RRHs to one system module, so hybrid radio bands are feasible. In this case an extra ABIL unit (capacity unit for Nokia AirScale 5G gNB system module) should be placed to the gNB.

eCPRI is in use between BBU and RRU.

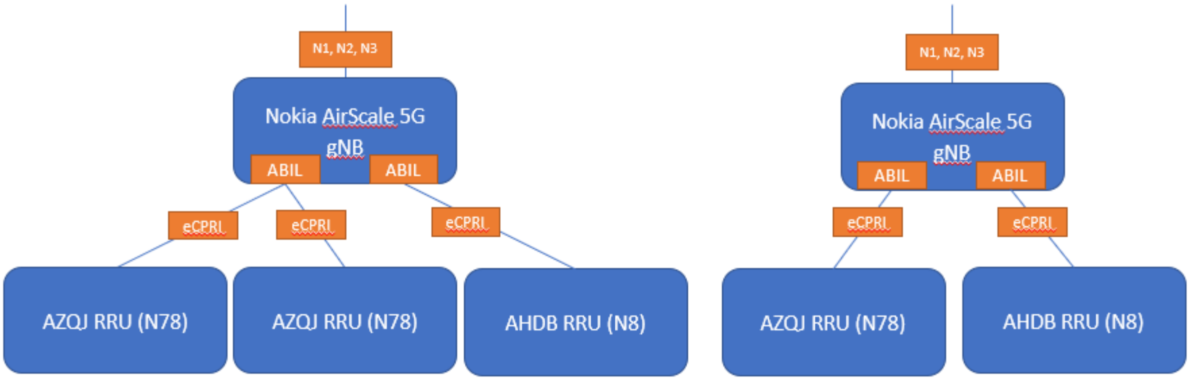

Figure 4: 5G radio configuration

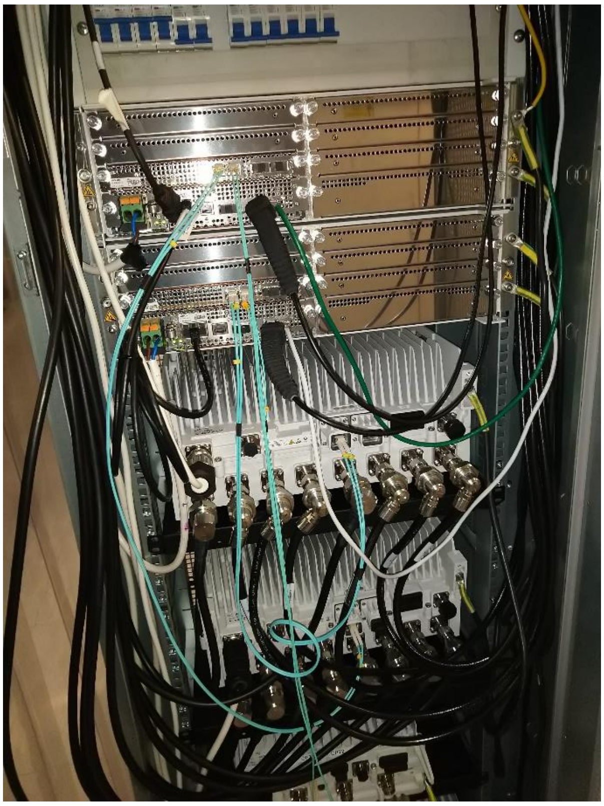

Figure 5: Picture of the 5G Radio HW

2.1.2.3 Radio link: direct cabling and Faraday cage

To avoid from interferences with public 5G operators WP3 is using direct RF cabling between network elements and Faraday cage for 5G terminals.

RF cabling can be seen in the picture below:

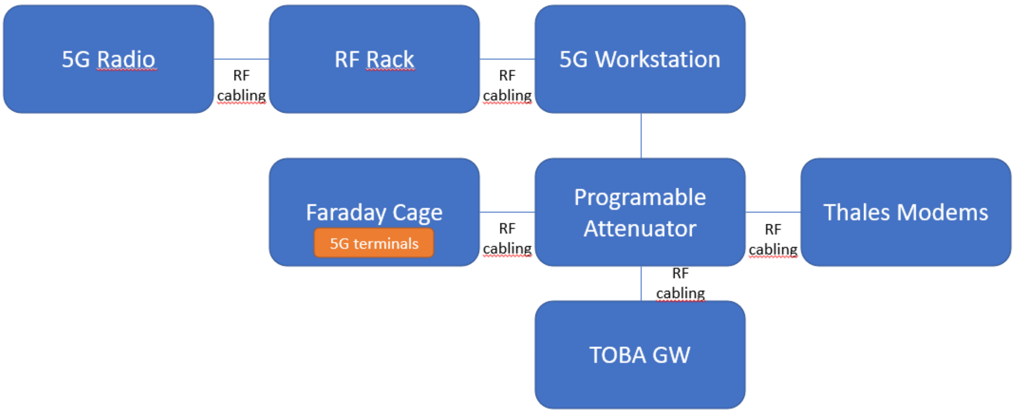

Figure 6: RF cabling configuration

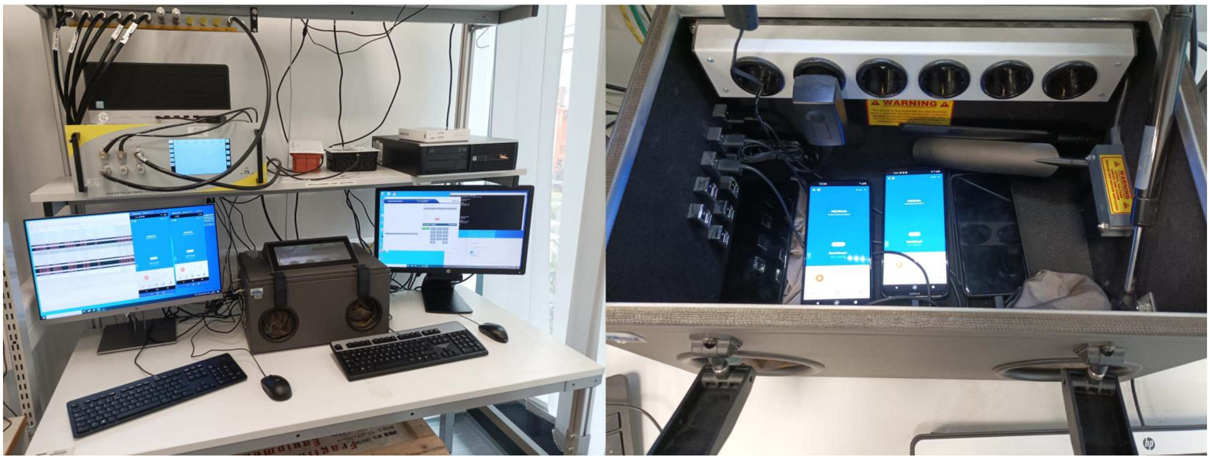

Figure 7: Picture from 5G Workstation

2.1.3 5G Core Networks

2.1.3.1 Functional view

The Nokia CMU (Compact Mobility Unit) provides a 3GPP compliant 5G SA Core network and is realised on a redundant server system with following functionality integrated:

Figure 8: Nokia 5G SA Core: Functional Units

Following functions according to 5G 3GPP standards are provided:

- UPF User Plane Function
- SMF Session Management Function
- AMF Access and Mobility Management Function
- AUSF Authentication server function
- UDM Unified Data Management

The following reference points are supported:

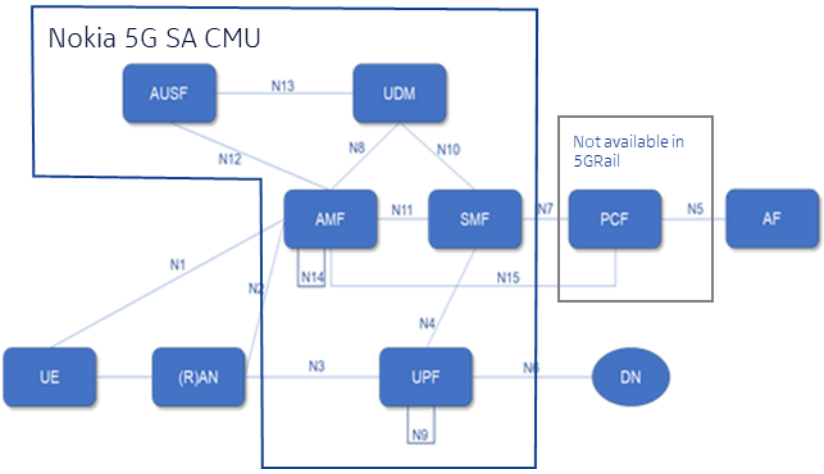

Figure 9: Nokia 5G SA core: Interfaces

Note: As the PCF is not included in CMU Static QoS settings shall be used (refer to chapter 4.4).

2.1.3.2 Possible setups with 5G RAN

Figure 10 shows the planned 5G radio configuration. There is one BBU with two n78 band RRHs and other BBU with one n78 band RRH. In addition, there is possibility to use n8 band RRH as well. In that case one BBU/one RRH is the configuration.

Note: mixed configuration is not planned (n8 and n78 band RRH on the same BBU)

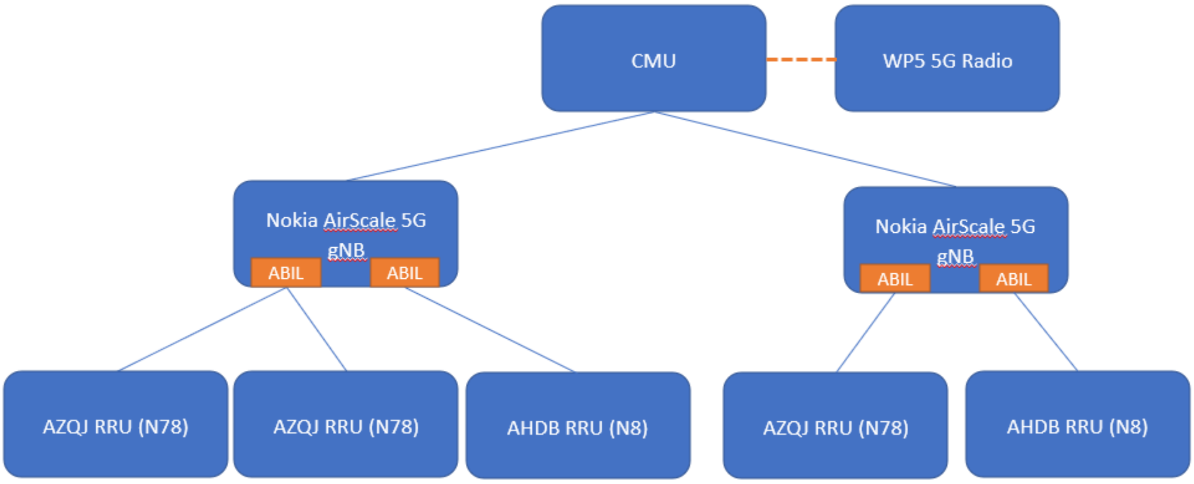

Figure 10: Picture about 5G radio configuration

2.1.4 5G network integration tests

5G radio is integrated to 5G SA core via N1/N2, N3 interfaces. Signalling is up and running. Thales modems and COST terminals can reach and attach to 5G network. Data communication (PDU session) is verified.

FTP upload and download (to/from a server) is working.

2.1.4.1 Thales modem

Thales modems were built into plastic assembly boxes with their power supplies to avoid damage.

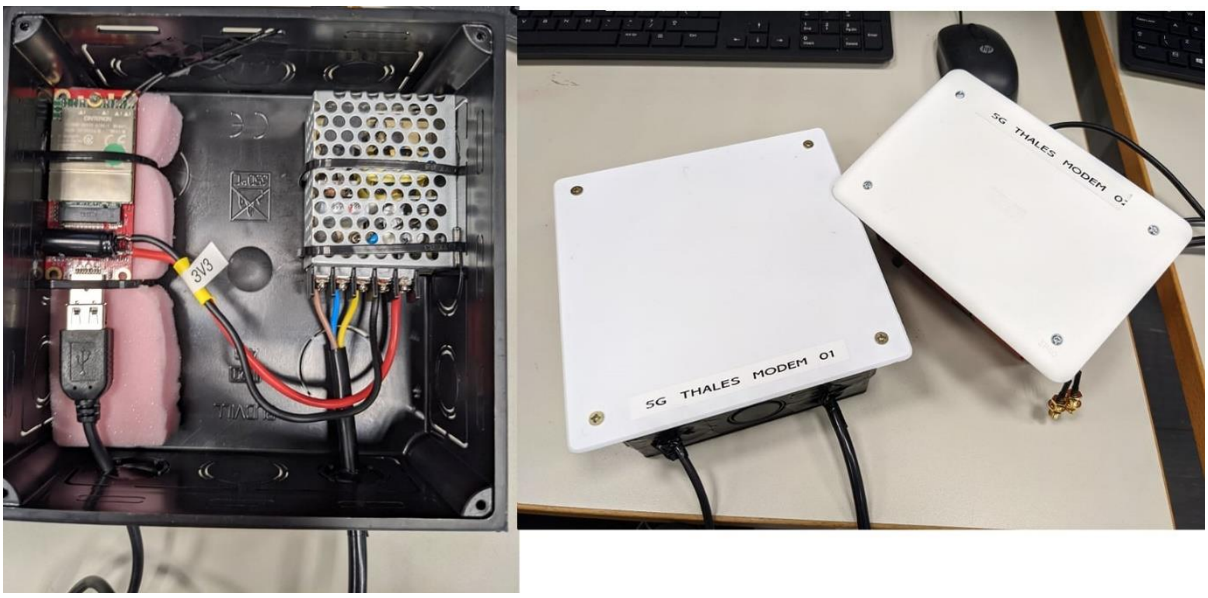

Figure 11: Picture from Thales modem

Thales modem is connected to the RRH with direct RF cabling, see Figure 6.

2.1.4.2 COTS terminals

The following COTS terminals are in use:

- Nokia 8.3 5G with special firmware
- Oneplus9 pro
- Nokia X20

To avoid from interference with public 5G networks terminals are in a Faraday cage.

2.2 MCx and dispatcher network integration

MCX is integrated to CMU via N6 interface:

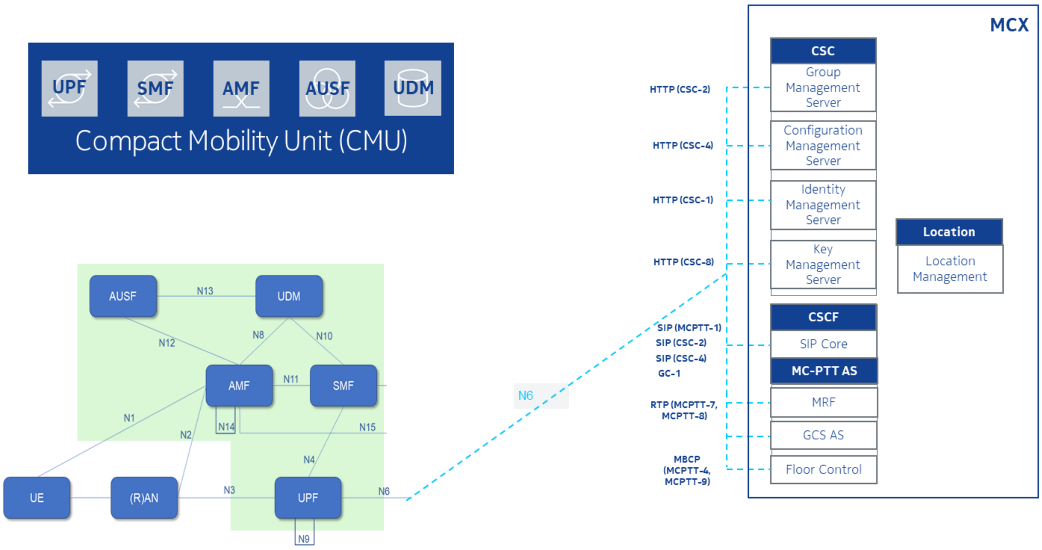

Figure 12: CMU – MCX integration

The configuration of the various identifier of the MCX System is aligned between the Work Packages and are described in detail in D2.2. The MCX server is configured as follows:

SIP core	
Name or IP address	10.88.89.178
MCx server	
SIP IMPU	mcx-service@mcptt.nokia.com
Name or IP address of IdMS	10.88.89.178

Configuration of the MCX server is achieved by an Administration Terminals integrated on the dispatcher PC. D3.1). The Graphical User Interface is also realized on dedicated PC. Both are directly connected to the MCX Server:

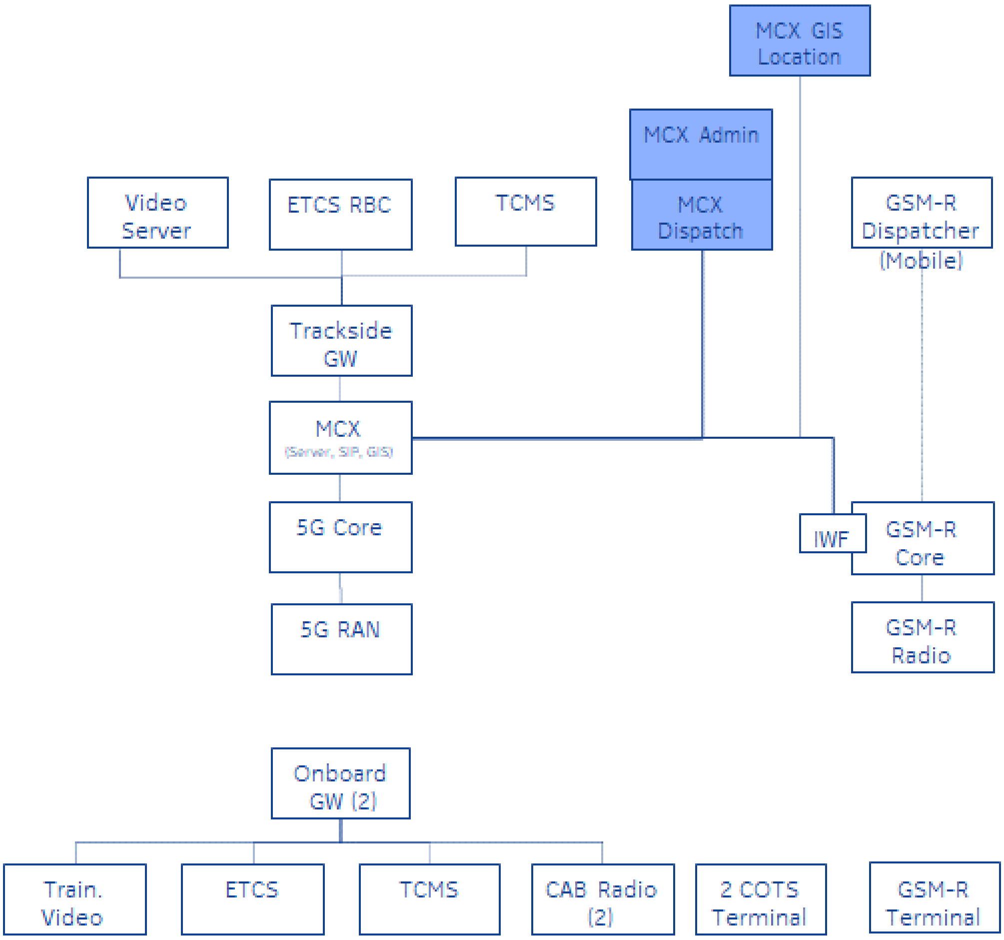

Figure 13 Connectivity Overview MCX Server

MCX UE client is an android application, installed on the COTS terminals, MCX dispatcher is an WIN10 application, installed on a WIN10 PC.

Installation procedures both for MCX and applications are well described in the MCX customer documentation set.

For verifying MCX integration some basic calls were done (voice calls: UE-UE, Dispatcher-UE, UE-Dispatcher, Push-to-talk and Push-to-video).

2.3 GSM-R network integration

The following overview depicts the components integrated for GSM-R – MCX interworking test cases:

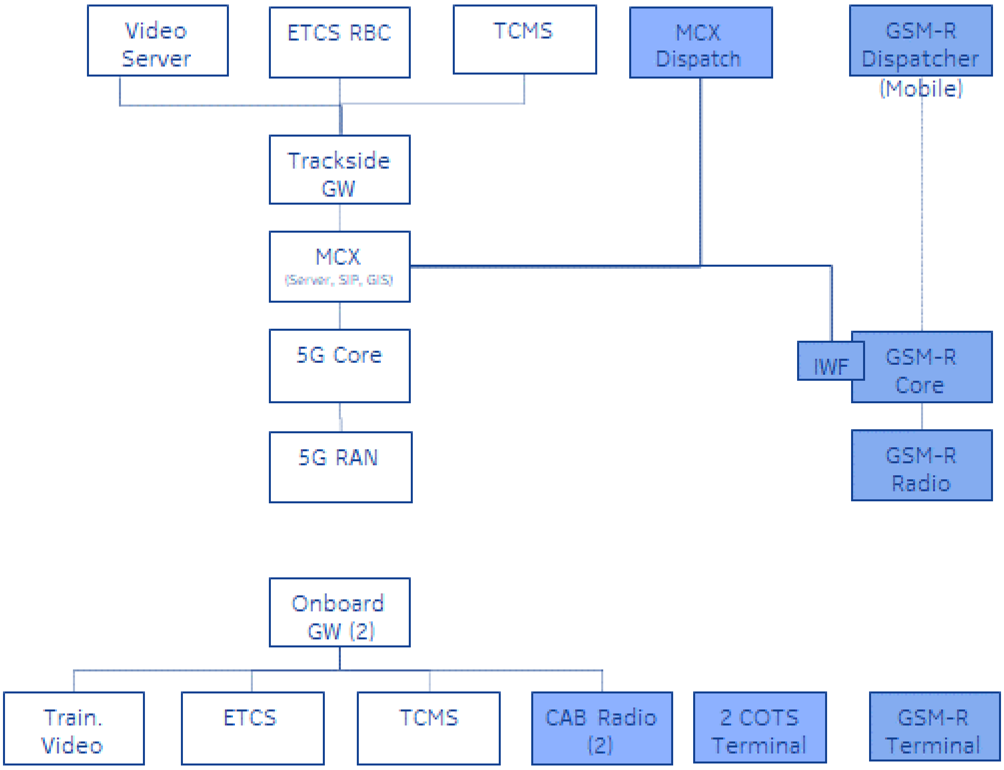

Figure 14 Connectivity Overview GSM-R Interworking

GSM-R network contains the following network elements, detailed information can be found in D3.1 document [S19]:

- Open Mobile Softswitch for Railways
- Open Multimedia Gateway
- NT-HLR/HSS + One-NDS
- IN/Service Control Point (SCP)
- Flexi BSC GSM-R
- Flexi Multiradio 10 GSM-R BTS EDGE
- Flexi EDGE GSM-R BTS

The following GSM-R terminals are in use:

- Sagem TiGR155R
- Sagem TiGR350R
- Funkwerk shuntfocX
- Triorail TTS-5 USB Ext
- Triorail TRM-5T USB Ext

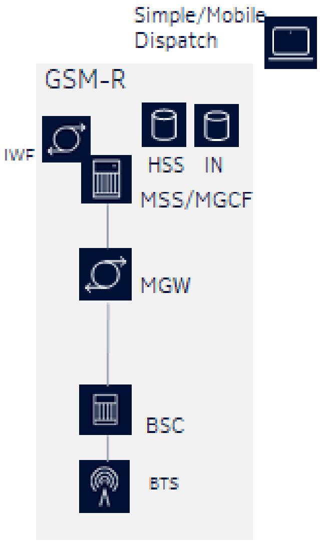

Figure 15: GSM-R configuration

GSM-R Network is integrated to MCX via a newly developed interface called GSM-R IWF to MCX-Server. This is a pre standard solution aligned with the current drafting of the ETSI study on GSM-R FRMCS Interworking (TR 103 768) defining IWFg-x :

Figure 16: GSM-R and FRMCS Interworking

It provides the interworking for Group Call communication, where a group call established in the FRMCS system triggers a Group Call establishment in GSM-R (e.g. Railway Emergency Group Call). By this inter system interworking a border cross situation can be emulated where FRMCS is provided in one network, and GSM-R in the neighbour network , refer to chapter Border Crossing4.5.

It provides an integrated mapping of Addressing schemes.

Floor Control interworking mapping is not supported. IPSecurity is not supported on the interfaces thus to be switched of in the MCX server.

Verifying MCX – GSM-R integration is still on-going (initiating basic group call in MCX and establishing in MCX and also in GSM-R system).

3 WP3 Partners product integration

WP3 as part of the 5GRAIL, provides the first 5G reference lab environment situated at Nokia premises in Hungary. The focus of the first 5G reference lab test is to leverage the FRMCS 5G infrastructure and integrate it with different vendors' products, like the On-board GW and the Trackside GW prototypes and as well as the related application prototypes, namely Voice, Video/CCTV, ETCS and TCMS in a unique environment for testing.

The On-board GW, the Trackside GW and as well as the OM server are provided by Kontron. The cab radio for voice testing is delivered by Siemens, ETCS and TCMS are from CAF, and Video/CCTV is from Teleste.

The integration activities are scheduled in Q1 2022 timeframe. The timeline planned at the time of writing this document is shown in Figure below.

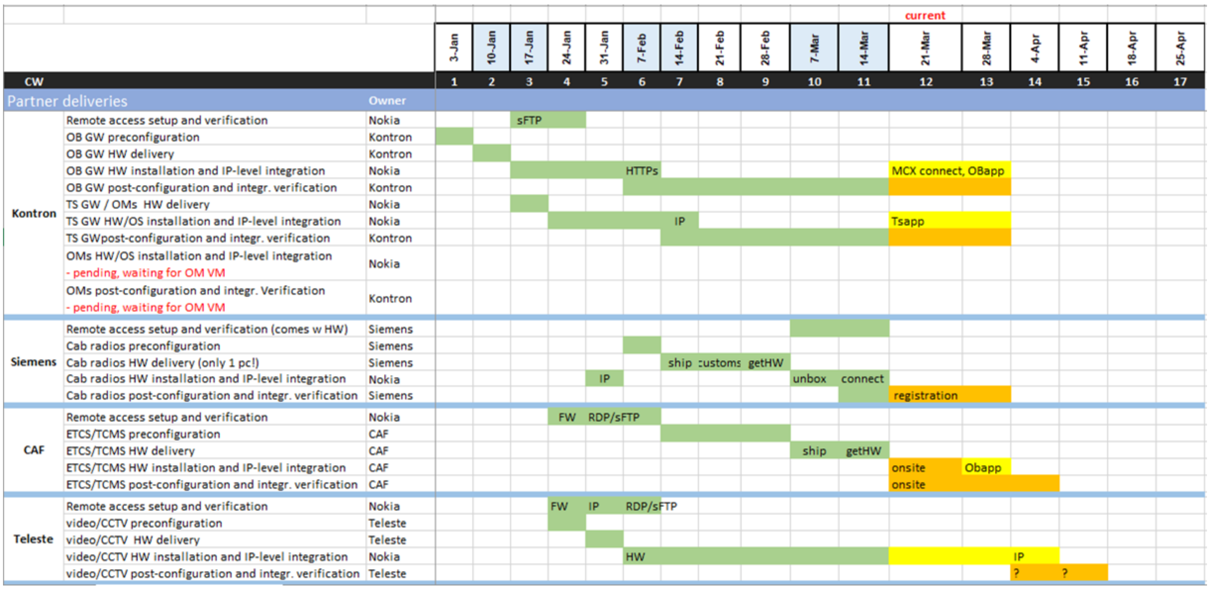

Figure 17: Timeline of the WP3 partners' product integration activities

The following figure presents the IP connectivity of the WP3 laboratory. Onboard and Trackside are separated from IP point of view. Those can reach each other only via 5G radio interface.

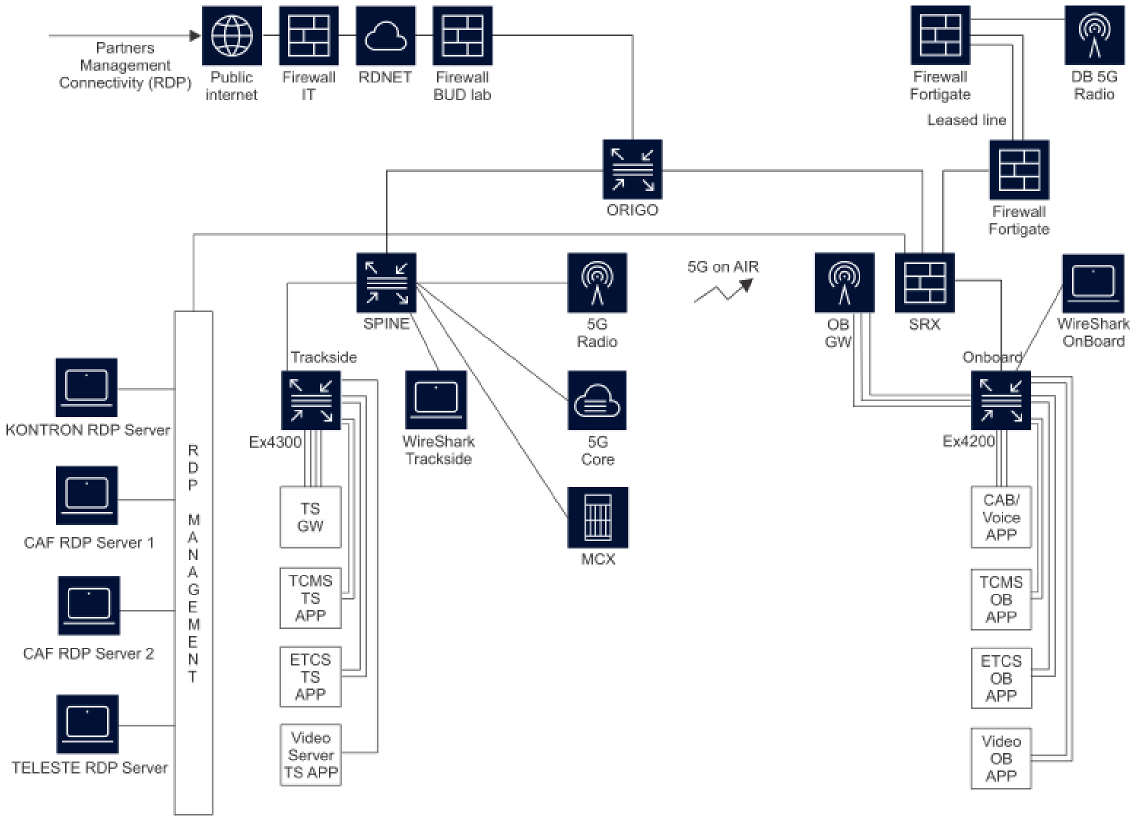

Figure 18: WP3 IP connectivity

3.1 Gateways

3.1.1 High level description

The following overview depicts the Gateways (on board and trackside) provided by Kontron and integrated in the 5G Networks. The application integration is in responsibility of WP2.

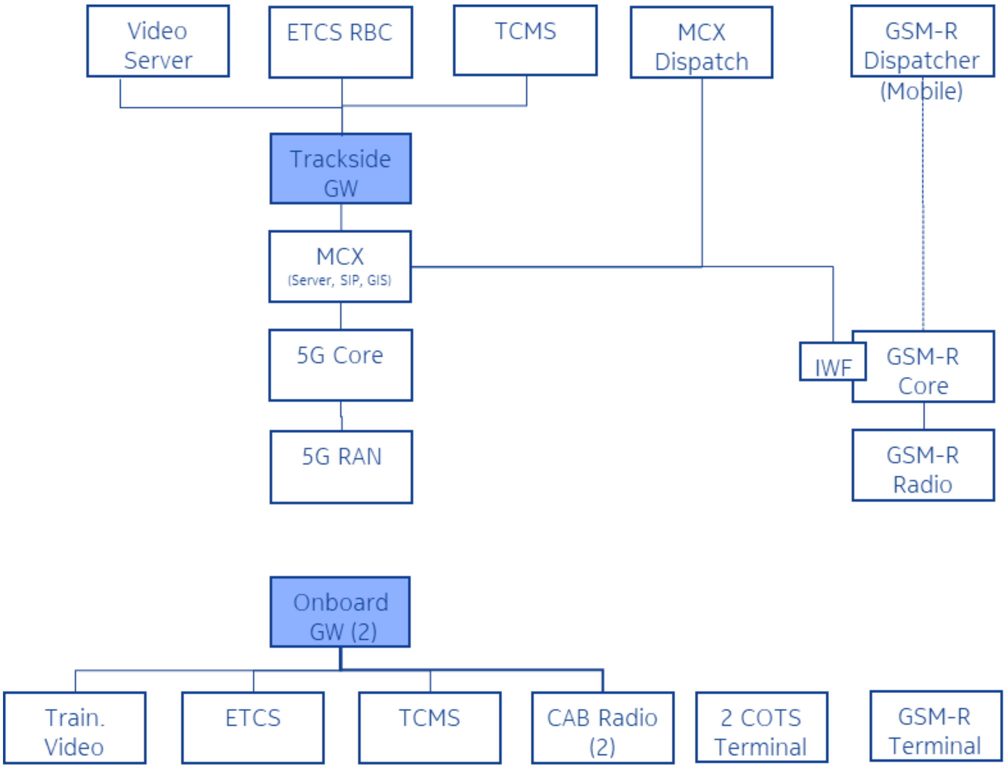

Figure 19: Connectivity Overview Gateways

3.1.2 Pre-configuration

Kontron WP2 team delivered an OB Gateway and a TS Gateway to WP3, these modules being dedicated to WP3 activities only.

Before being used by WP3, 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 [S22].

Integration testing of the gateways consisted in checking the basic behaviour of the Gateways while inserted into the WP3 lab.

3.1.2.1 OB

OB Gateway has been installed physically in a rack of the WP3 laboratory area (see Figure 21 and Figure 22).

3.1.2.2 TS

TS Gateway VM is hosted on a dedicated PC connected to Trackside and N6 LANs. Dedicated PC has been installed physically in a rack in WP3 laboratory area (see Figure 21 and Figure 22).

3.1.3 Remote connection setup

A remote PC hosting RDP Server and sFTP server is located in an isolated network area (DMZ), behind firewalls, as a first hop for the remote access. The partner, Kontron, may access only this remote PC first, and only through a dedicated IP connection, using RDP and/or sFTP protocol only. From this remote PC, Kontron may access the Onboard GW, the Trackside GW and the OM server through 5GRail firewall in the Nokia WP3 lab. The firewalls control and filter the traffic accordingly. The above-described remote connection setup is shown in Figure 20: Remote access setup for Kontron.

Security arrangements

- DMZ (demilitarized zone) to separate 5GRail partner connections and devices from the rest of the Nokia labs
- Three level of Firewalls to protect 5GRail lab against cyber attacks
- The remote PC runs the cyber security SW to protect against malware/virus attacks
- Highly complex and frequently changing passwords for RDP and sFTP access
- Encrypted RDP and sFTP connections

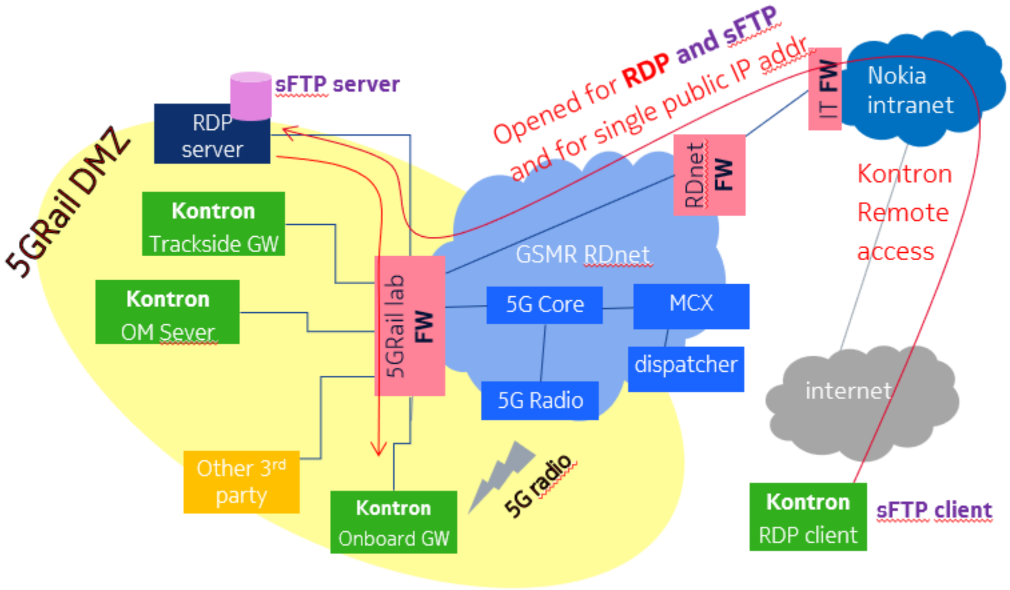

Figure 20: Remote access setup for Kontron

3.1.4 Test Bench installation

Onboard and Trackside GW were put to a rack in WP3 laboratory. An RDP server and Firewall to allow for remote access is placed in the rack as well. The Firewall is an IP switch with 1 Gbps ports that connects all partner products to the 5G infrastructure.

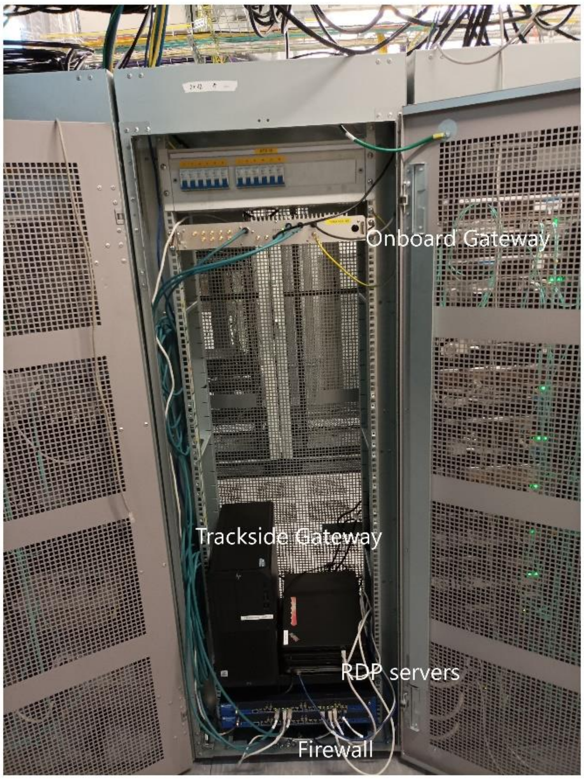

Figure 21: Hardware installation of gateways

Figure 22: Onboard and Trackside gateways

Cabling of OB and TS done by Nokia according to Kontron guideline (as Annex 7.4.1)

3.1.5 Network integration

The Kontron devices, such as the On-board GW, the Trackside GW and as well as the OM server are integrated at IP level in the WP3 lab. There two IP subnets defined: one for the onboard side (/29 subnet) and another one for the trackside (/28 subnet). These subnets are configured as separate vlans, too. Table 1 shows the IP plan structure, without indicating the exact IP addresses used in the setup.

IP	IPv4 SUBNET	VLAN_NAME	VLAN_ID	USE
IPaddr1				
IPaddr2	29	Kontron_internal1_temp	2000	Default GW
IPaddr3	29	Kontron_internal1_temp	2000	OnboardGW_app
IPaddr4	29	Kontron_internal1_temp	2000	OnboardGW_adm
IPaddr5	29	Kontron_internal1_temp	2000	OnboardGW_om
IPaddr6	29	Kontron_internal1_temp	2000	
IPaddr7	29	Kontron_internal1_temp	2000	
IPaddr8				
IPaddr1				
IPaddr2	28	Kontron_internal2_temp	2001	Default GW
IPaddr3	28	Kontron_internal2_temp	2001	TracksideGW_app
IPaddr4	28	Kontron_internal2_temp	2001	TracksideGW_adm
IPaddr5	28	Kontron_internal2_temp	2001	TracksideGW_om
IPaddr6	28	Kontron_internal2_temp	2001	TracksideGW_infra
IPaddr7	28	Kontron_internal2_temp	2001	OM_Server_adm
IPaddr8	28	Kontron_internal2_temp	2001	OM_Server_om
IPaddr9	28	Kontron_internal2_temp	2001	
IPaddr10	28	Kontron_internal2_temp	2001	
IPaddr11	28	Kontron_internal2_temp	2001	
IPaddr12	28	Kontron_internal2_temp	2001	
IPaddr13	28	Kontron_internal2_temp	2001	
IPaddr14	28	Kontron_internal2_temp	2001	
IPaddr15	28	Kontron_internal2_temp	2001	
IPaddr16				

Table 1: IP plan for integrating Kontron devices- in WP3 lab

3.1.6 Integration verification test

Integration is verified in steps

- Network attach of OB GW

- IP connectivity check between OB GW and TS GW (ping)

3.2 Voice

3.2.1 High level description

The following overview shows the Voice application integrated onboard and on trackside:

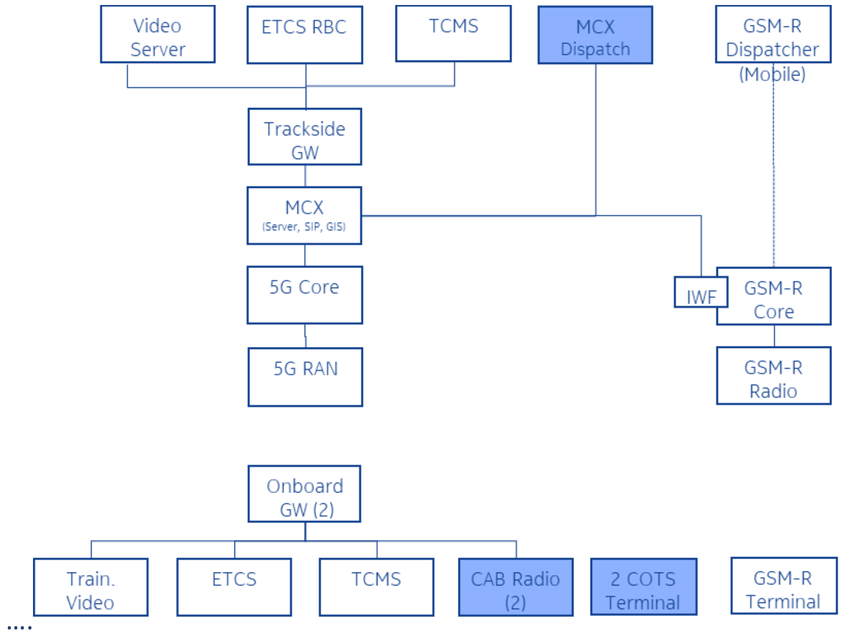

Figure 23: Connectivity Overview Voice Application

Siemens will provide the CAB radios, where Dispatching Terminal as well as COTS Terminals will be provided by Nokia. The initial integration was done using 1 Onboard GW and 1 CAB Radio.

3.2.2 Pre-configuration

Equipment was delivered with pre-configured IP plan which was agreed previously between Siemens and Nokia.

Nokia Dispatcher is connected directly to the MCX Server and is used for all voice related test cases. COTS terminals including a Nokia client based on Android are available for integration test activities, and can be used for test cases for lab and field depending on final definition of WP1 test cases.

3.2.3 Remote connection setup

Remote access for Siemens is realized through a VPN connection established via the 4G/LTE public radio network. The setup is shown in Figure 24

Siemens rents Amazon Web Service (AWC), where Siemens runs its own OpenVPN server on an AWS EC2 instance. There is an OpenVPN client running on the CAB radio. A secure VPN connection is set up between the OpenVPN server and the OpenVPN client, using private shared keys and encryption. The VPN connection, so the communication between OpenVPN server and client, is established via 4G/LTE public radio network. The CAB radio is connected to 4G/LTE network by a 4G modem and 4G sim card, which are provided by Siemens.

Through the VPN connection Siemens uses SSH protocol to access the CAB radio directly. The CAB radio is located in an isolated network area (DMZ), behind firewalls, separated from the rest of the Nokia labs. The CAB radio is able to send traffic only to permitted directions e.g. to Onboard GW and MCX, as the 5GRail lab firewall controls and filters the traffic accordingly.

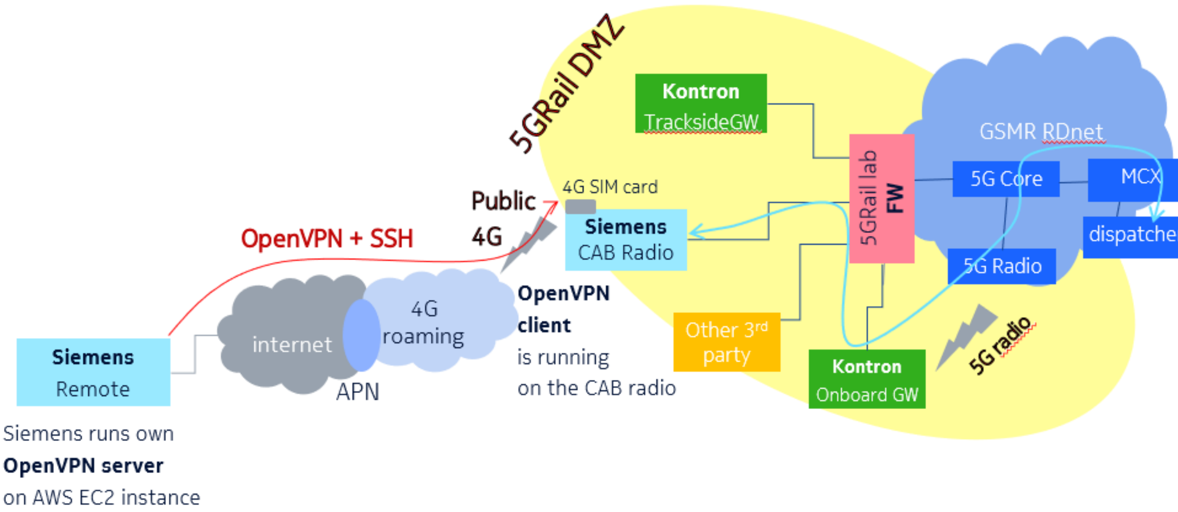

Figure 24: Remote access setup for Siemens

3.2.4 Test Bench installation

Siemens CAB radio was put to a workstation in the WP3 control room. Physical IP connectivity was set according to the installation guide provided by Siemens. All IP port were connected to onboard switch.

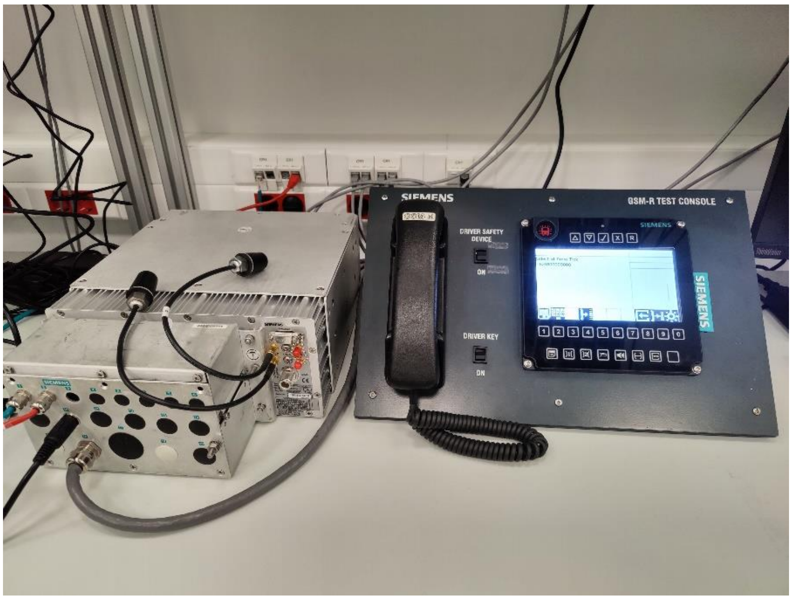

Figure 25: Siemens CAB radio in WP3 control room

Cabling of Siemens equipment is done by Nokia according to Siemens guideline (as Annex 7.4.2)

3.2.5 Network integration

The Siemens devices, such as the Cab radio and the connecting HMI console are integrated at IP level in the WP3 lab. There two IP subnets defined: one for the onboard side (/29 subnet) and another one for the trackside (/29 subnet). These subnets are configured as separate VLANs, too. Table 2: IP plan for integrating Siemens CAB Radio in WP3 lab shows the IP plan structure, without indicating the exact IP addresses used in the setup.

IP	IPv4 SUBNET	VLAN_NAME	VLAN_ID	USE
IPaddr1				
IPaddr2	29	Siemens_internal_temp1	2007	DefaultGW
IPaddr3	29	Siemens_internal_temp1	2007	Cab_Radio_OBapp
IPaddr4	29	Siemens_internal_temp1	2007	
IPaddr5	29	Siemens_internal_temp1	2007	
IPaddr6	29	Siemens_internal_temp1	2007	
IPaddr7	29	Siemens_internal_temp1	2007	
IPaddr8				
IPaddr1				
IPaddr2	29	Siemens_internal_temp2	2002	Default GW
IPaddr3	29	Siemens_internal_temp2	2002	Cab_Radio_MNGMT
IPaddr4	29	Siemens_internal_temp2	2002	HMI_MNGMT
IPaddr5	29	Siemens_internal_temp2	2002	
IPaddr6	29	Siemens_internal_temp2	2002	
IPaddr7	29	Siemens_internal_temp2	2002	
IPaddr8				

Table 2: IP plan for integrating Siemens CAB Radio in WP3 lab

3.2.6 Integration verification test

Firstly, we connect Siemens CAB radio directly to Nokia MCX to verify that IDMS authentication, REGISTER and calls are working well.

Secondly, Siemens CAB radio is connected to Onboard GW to check that the interworking between the CAB and Kontron OB is perfect.

3.3 ETCS/TCMS

3.3.1 High level description

The following overview shows the ETCS & TCMS applications integarted onboard and on trackside:

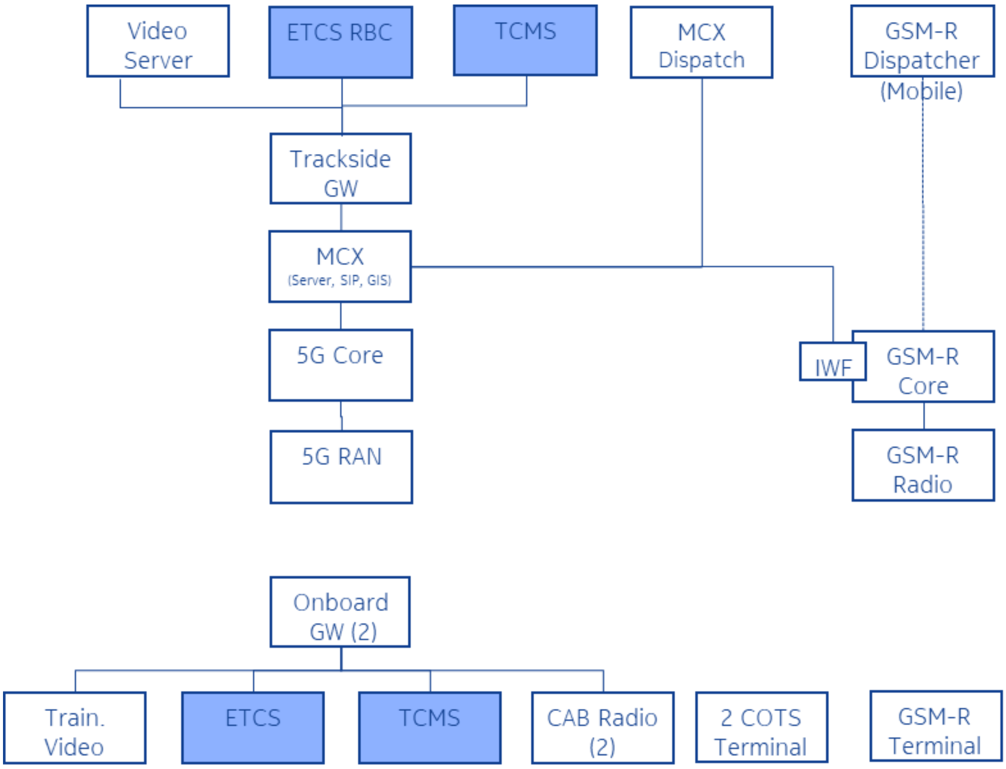

Figure 26: Connectivity Overview ETCS / TCMS Application

3.3.2 Pre-configuration

Equipment were delivered with pre-configured IP plan which was agreed previously between CAF and Nokia.

3.3.3 Remote connection setup

A remote PC hosting RDP Server and sFTP server is located in an isolated network area (DMZ), behind firewalls, as a first hop for the remote access. The partner, CAF, may access only this remote PC first, and only through a dedicated IP connection, using RDP and/or sFTP protocol only. From this remote PC, CAF may access the Onboard ETCS/TCMS servers and the Trackside ETCS/TCMS servers through 5GRail firewall in the Nokia WP3 lab. The firewalls control and filter the traffic accordingly. The above-described remote connection setup is shown in Figure 27.

Security arrangements

- DMZ (demilitarized zone) to separate 5GRail partner connections and devices from the rest of the Nokia labs
- Three level of Firewalls to protect 5GRail lab against cyber attacks
- The remote PC runs the cyber security SW to protect against malware/virus attacks
- Highly complex and frequently changing passwords for RDP and sFTP access

- Encrypted RDP and sFTP connections

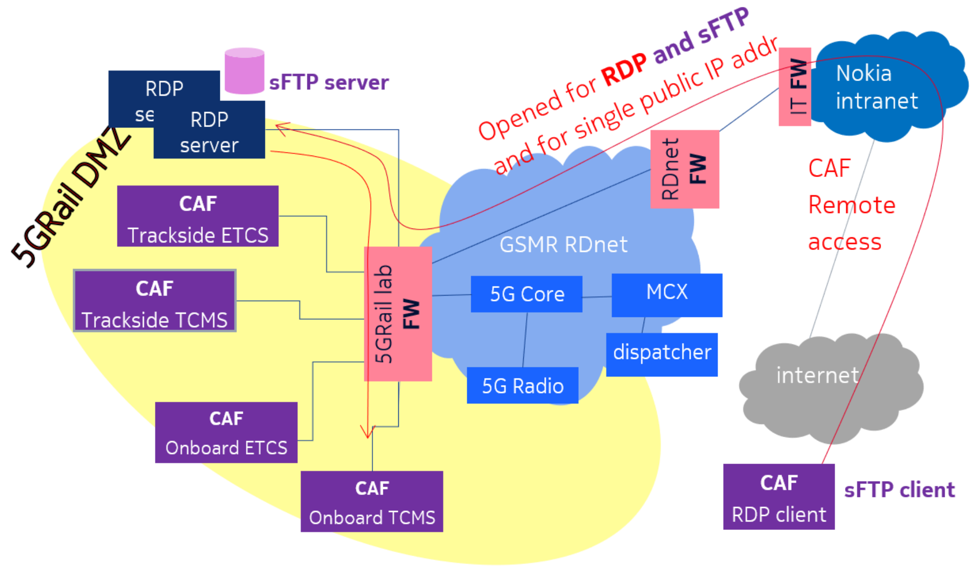

Figure 27: Remote access setup for CAF

3.3.4 Test Bench installation

ETCS/TCMS servers were installed locally by CAF engineers in WP3 control room. Onboard equipment plugged into the Onboard IP switch, Trackside equipment plugged into the Trackside switch.

Figure 28: CAF ETCS/TCMS Servers in WP3 control room

3.3.5 Network integration

Basic ping and traceroute tests were done by CAF engineers locally during the test bench installation.

3.3.6 Integration verification test

Integration will be part of functional testing.

3.4 Video/ CCTV

3.4.1 High level description

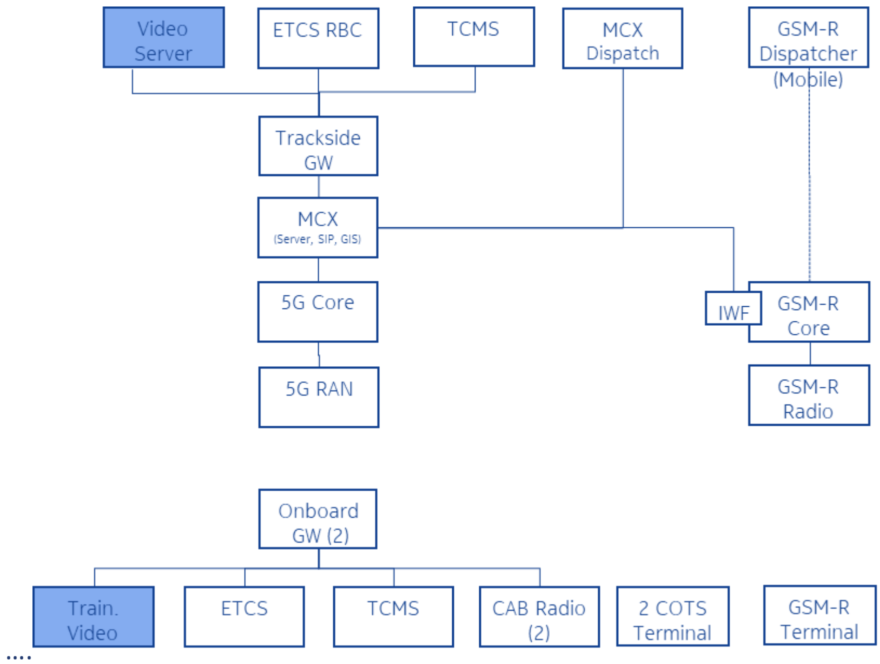

Figure 29: Connectivity Overview Video Application

3.4.2 Pre-configuration

Equipment is delivered with pre-configured IP plan which was agreed previously between Teleste and Nokia.

3.4.3 Remote connection setup

A remote PC hosting RDP Server and sFTP server is located in an isolated network area (DMZ), behind firewalls, as a first hop for the remote access. The partner, Teleste, may access only this remote PC first, and only through a dedicated IP connection, using RDP and/or sFTP protocol only. From this remote PC, Teleste may access the Train Equipment, the CCTV camera and the Video Server through 5GRail firewall in the Nokia WP3 lab. The firewalls control and filter the traffic accordingly. The above-described remote connection setup is shown in Figure30.

Security arrangements

- DMZ (demilitarized zone) to separate 5GRail partner connections and devices from the rest of the Nokia labs
- Three level of Firewalls to protect 5GRail lab against cyber attacks
- The remote PC runs the cyber security SW to protect against malware/virus attacks
- Highly complex and frequently changing passwords for RDP and sFTP access
- Encrypted RDP and sFTP connections

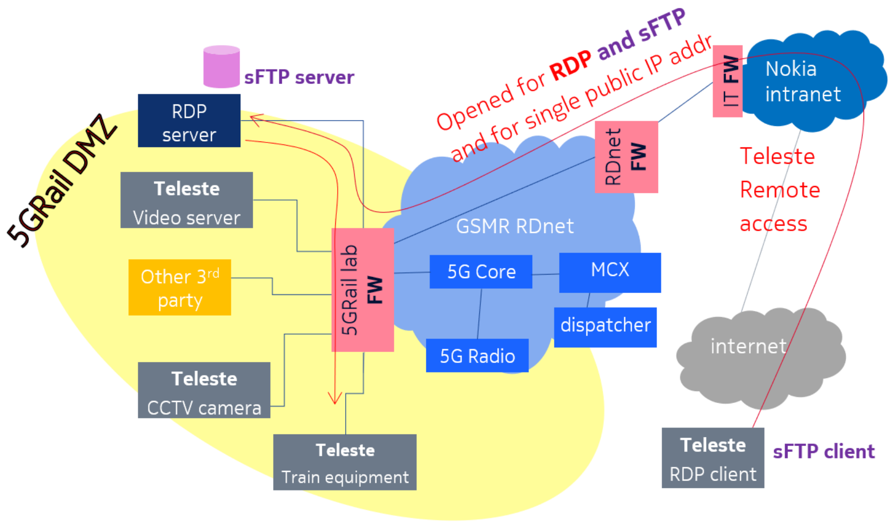

Figure 30: Remote access setup for Teleste

3.4.4 Test Bench installation

Video devices are installed in WP3 control room. Onboard equipment plugged into the Onboard IP switch, Trackside equipment plugged into the Trackside switch.

Figure 31: Teleste devices in WP3 control room

3.4.5 Network integration

Basic ping and traceroute tests were done by Teleste engineers via remote connection after the test bench installation.

3.4.6 Integration verification test

Integration will be part of functional testing.

4 Network configurations and tools to be used during test phase

4.1 Overview with all tools

Desktop PCs were installed by WP3 with WireShark network protocol analyser tool both on onboard and trackside (see Figure 18) to check what is happening on IP level.

Is should be noted the HTTPS messages are encrypted by TLSv1.2 algorithm so it can not be seen in the WireShark capture only SIP messages are visible by default.

There is a possibility to check also HTTPS messages, for it we have to enable SSLCipherSuite AES256-GCM-SHA384:AES128-GCM-SHA256 and disable SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4 algorithm in MCX. Also local host.key file is needed from MCX.

With the above settings and files we can configure Wireshark to decrypt HTTPS messages.

Details can be found in the APPENDICES 7.4.3

4.2 Handover

For 5G handover testing HYTEM 6x6 FULL FAN OUT Attenuation Matrix (6x6 - 93/110 dB - 3 to 6 GHz) on n78 band is used by WP3. Attenuator matrix can be controlled locally and remotely as well. Configuration can be seen the figure below where RRUs represent separate 5G cells.

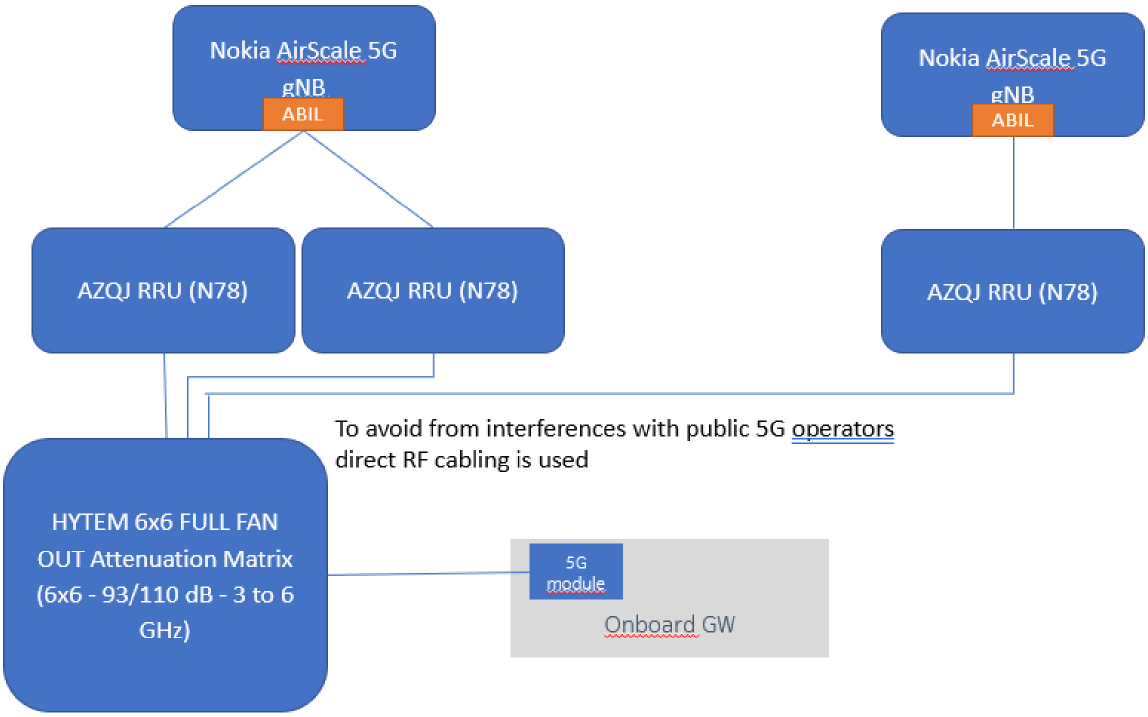

Figure 32: 5G Handover RF configuration

4.3 High Speed

To test high speed handovers and degraded radio condition situations RF emulator tool is used, namely Spirent Vertex Channel Emulator. This 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.

The Spirent Vertex Channel Emulator supports speeds up to 500 km/h, but the tests are only planned to be done with speeds up to 350 km/h. The device also supports up to 8 antennae on each side of the link.

Supporting multiple Demodulation Reference Signals (DMRS) for more than one layer isn't mandatory for the UEs, therefore the achievable results depend on the network and UE capabilities. The link level parameters are aligned with the link level parameters preceding the ETSI TC RT 103.554-2 simulation campaign.

During the tests different speed and propagation conditions will be used, based on [S23] document. Some parameters will need to be modified in order to align with the current project goals.

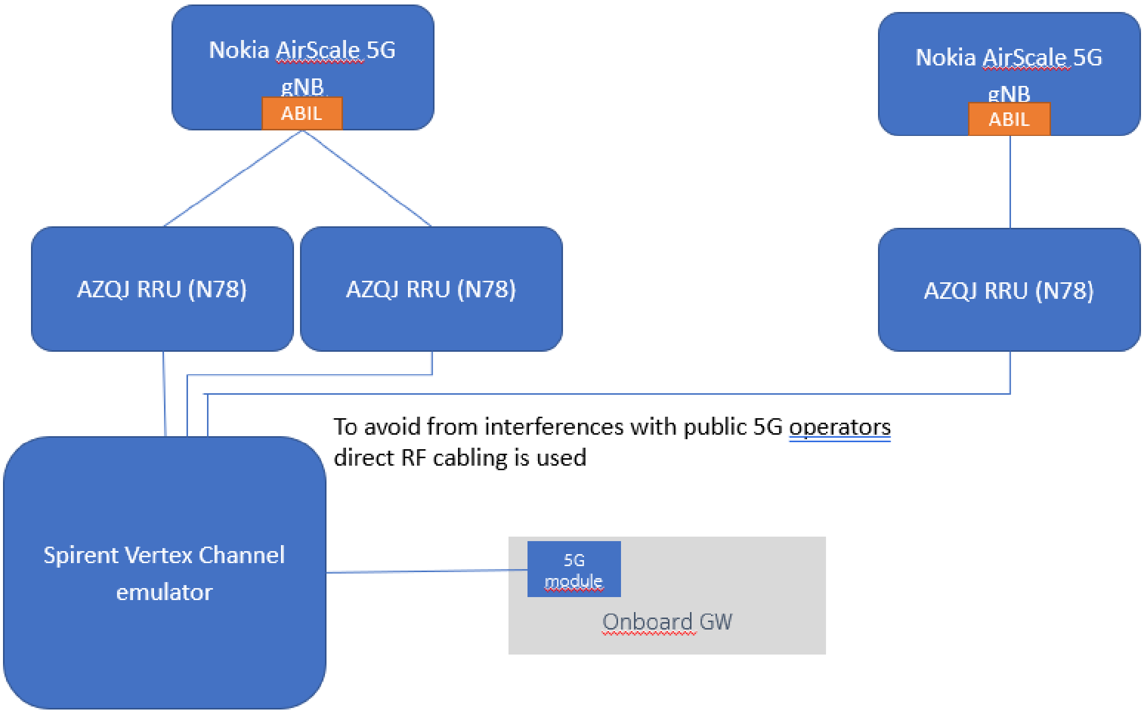

Figure 33: RF configuration setup with Spirent Vertex Channel Emulator

4.4 Priority QoS

The WP3 Lab does not include a PCF which is normally used to achieve Application specific end to end QoS setting in core and radio The following figure marks the concept noting that PCF (and it's interworking with the Application / MCX Server) is not supported in 5GRail:

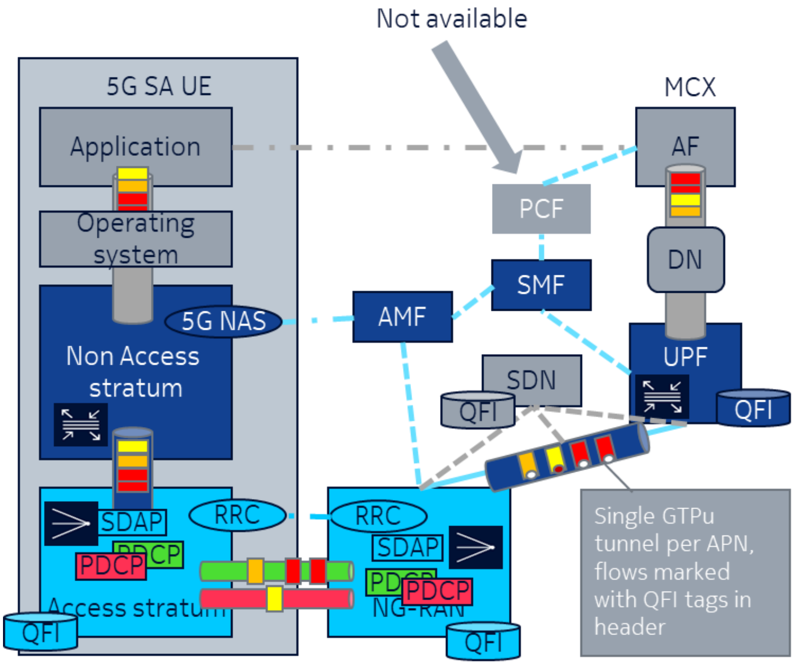

Figure 34: QoS Architecture

Whereas it is generally assumed (by 3GPP) that these functions require dynamic PCC using a Policy Control Function (PCF), in 5Grail - as the agreed workaround - advanced filter mechanisms in the core network allow to differentiate traffic demands by statically assigning the required QoS with prioritization and differentiated end-to-end QoS, including on the air interface, often the scarcest resource. The services consist of a control plane (i.e. SIP\SDP signalling) establishing user plane Service Data Flows (SDFs), usually identified by 5-tuple (Source/destination IP address, Protocol and Source/destination Port). In general a SDF is defined as the set of packets matching a single Policy & Charging Control (PCC) rule in the Policy Control & Enforcement Function (PCEF in SMF+UPF)

The 5GC SMF/UPF (PCEF) needs to

- Map SDFs to 5G QoS flows (as there's only one N3 GTP-U tunnel per PDU session in the 5GS) identified by N25 QI and N3 QFI
- Bind one or multiple SDFs to that 5G QoS flow
- Inform the UE of the QoS rules governing the mapping of uplink traffic to the correct 5G QoS Flow (although the 5GS UE may also apply reflective QoS : deriving uplink QoS rules from the received downlink traffic)
- Verify that the UE respects the SMF-imposed or Reflective QoS rules for uplink traffic

The used 5QI class is still under further evaluation, as Nokia supports today 5QI-1(*) and 5QI-2(*) for Voice/Video capable devices, means capable to support VoNR, which is not available in selected Chipset (final commitment outstanding).

For that reason, Non GBR mode will be considered for voice and as video is anyway running over MC Data as streaming type of service, not conversational, as normally used for MC Video, this should run on Non GBR as well. Appropriate priority to ensure proper handling 5QI-5 or 7 could be proposed.

Note (*): 5QI-1 and 5QI-2, are GBR modes used for conversational voice and conversational Video (live streaming).

The use of 5QI (5G QoS Identifier) GBR values 2,3,4 is under further evaluation-

The following table shows the current proposal

Application	OB_GTW		Infrastructure static configuration
comm_profile transmitted by the application	DSCP value (bit)	DSCP value (decimal)	QoS parameters used for WP3 - *Proposal*
1- Voice	101 101	43	5QI : TBD ARP: 7 GBR/MBR : TBD
2- Operational Voice	101 010	42	5QI : TBD ARP: 4 GBR/MBR : TBD
3- Emergency voice	101 001	41	5QI : TBD ARP: 1 GBR/MBR : TBD
4- Video	100 001	33	*not used for 5GRAIL*
5- Low latency Video	100 000	32	*not used for 5GRAIL*
6- Non harmonized Data	001 000	8	5QI : 9 ARP: 8 GBR/MBR : NA
7- Operational Data	010 011	19	5QI : 7 ARP: 4 GBR/MBR : NA
8- Emergency Data	010 111	23	5QI : 5 ARP: 1 GBR/MBR : NA
9- Low latency Data	010 110	22	5QI : 5 ARP: 3 GBR/MBR : NA
10 - ETCS	010 101	21	5QI : 5 ARP: 2 GBR/MBR : NA

Table 3 QoS and DSCP Marking

4.5 Border Crossing

Two border crossing use cases are planned to be tested :

1. Voice: Transition from GSM-R to FRMCS where a Group/Emergency call is setup originated by the FRMCS side as described in chapter 2.3. For this use case CAB radio will switch from GSM-R to FRMCS during border crossing (manual switch).
2. Data/TCMS: TCMS onboard connects from visited to home network. For this use case a seconds 5GCore connected to separate second Radio RRH is needed. The need for IMS in the visited PLM is an open topic.

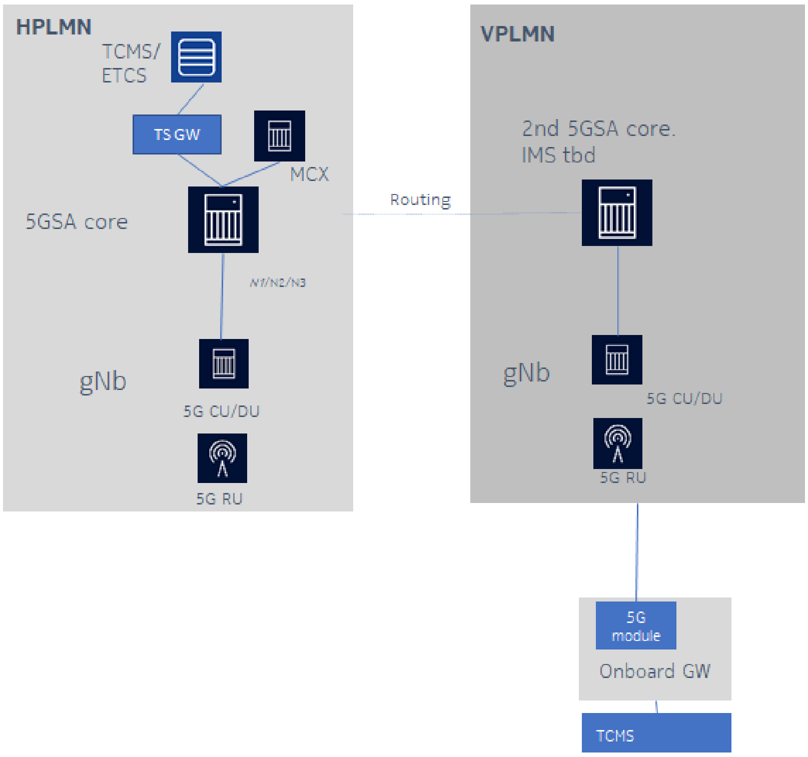

Figure 35: TCMS Border Crossing

4.6 MCX KPIs

3GPP TS 22.179 defines the following key performance indicators (KPIs) for the MCPTT service:

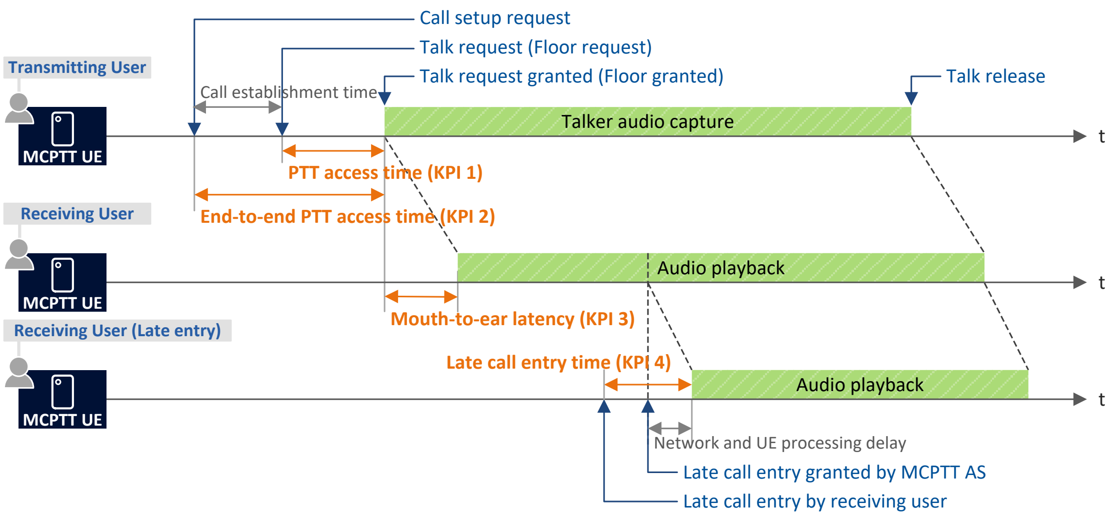

Figure 36 MCX KPI Overview

In 5G Rail : the following KPI will be measured depending on the test case:

MCPTT Access time (KPI 1)

- The time between when an MCPTT User request to speak (normally by pressing the PTT butt on) and when this user gets a signal to start speaking. This time does not include confirmatio ns from receiving users.
- MCPTT Access time (KPI 1) is less than 300ms for 95% of all MCPTT requests, for MCPTT Eme rgency Group Calls and Imminent Peril Calls, the KPI 1 is less than 300ms for 99% of all MCPT T requests

End-to-end MCPTT Access time (KPI 2)

- The time between when an MCPTT User requests to speak and when this user gets a signal t o start speaking, including MCPTT call establishment (if applicable) and acknowledgement (if used) from first receiving user before voice can be transmitted. A typical case for the End-to-end MCPTT Access time including acknowledgement is an MCPTT Private Call (with Floor con trol) request where the receiving user's client accepts the call automatically.
- The MCPTT Service shall provide an End-to-end MCPTT Access time (KPI 2) less than 1000 ms for users under coverage of the same network when the MCPTT Group call has not been est ablished prior to the initiation of the MCPTT Request.

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

Late call entry performance (KPI 4) measurement depends on the WP1 definition for Railway Emergency Call and might be skipped.

For the measurement logging of SIP messages in the UE and Server will be used (alternatively the dedicate Wireshark monitoring PC attached to Onboard and Trackside (refer to Figure 18: WP3 IP connectivity).

Both CAB Radio as well as Nokia UE will support detailed logging capabilities. In the following the measurement task are described based on Nokia UE for KPI 1:

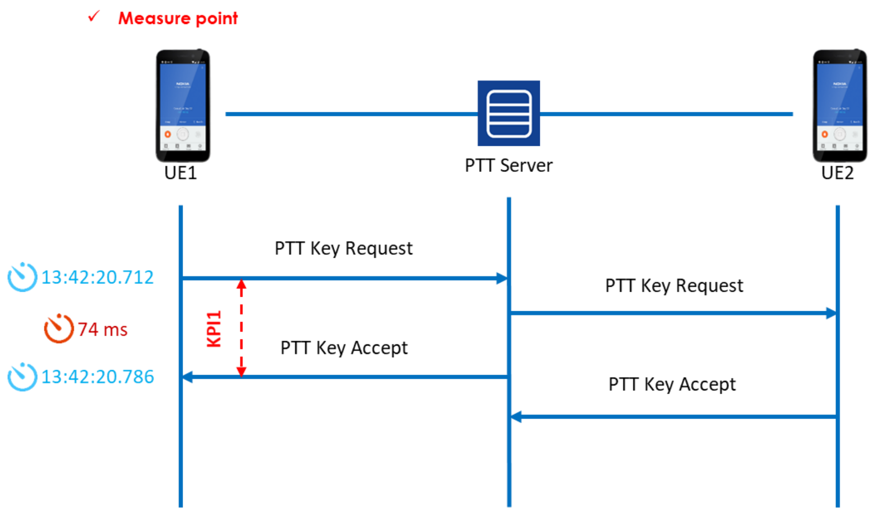

Figure 37: MCX KPI 1 Measurement Configuration

The procedure will log the RTCP messages for Key Request and Accept by timestamps allowing to derive KPI 1.

A similar setup is installed for KPI 2 measurement:

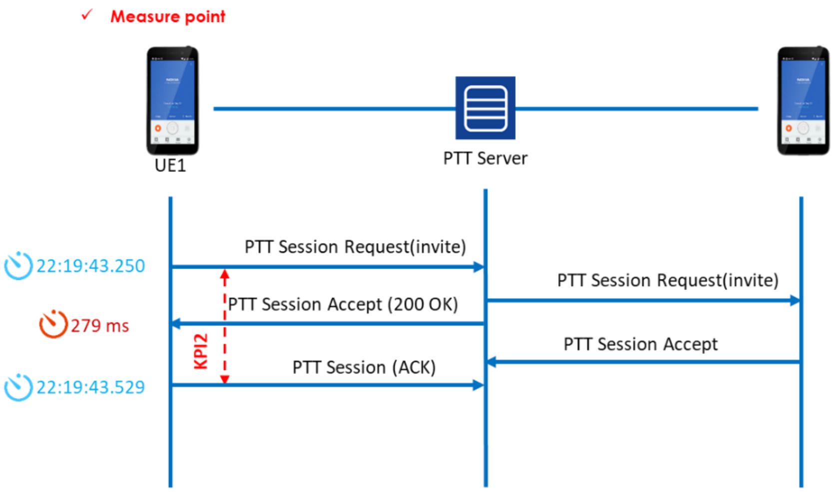

Figure 38: MCX KPI 2 Measurement Configuration

The procedure will log the SIP Invite and acknowledgement messages by timestamps allowing to derive KPI 1.

In case KPI 4 will be measured the following call flow is to be considered:

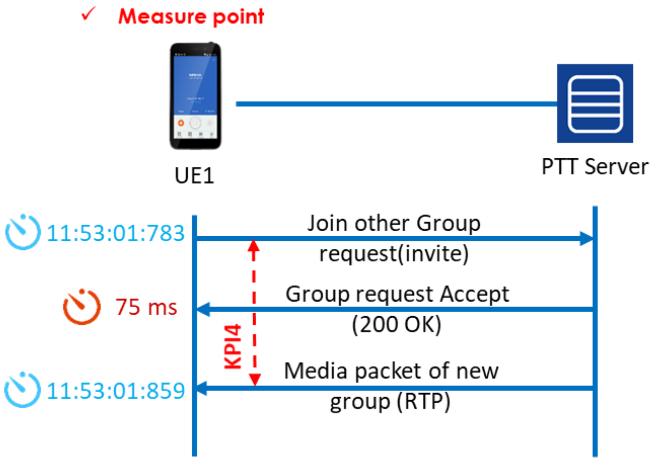

Figure 39: MCX KPI 4 Measurement Configuration

5 CONCLUSIONS

This report outlines the lab setup, integration and verification of radio compatibility of 5G radio modules.

The network functionality for the GSM-R/FRMCS interworking is also simulated.

This document describes also the network elements from the WP3 5Grail partners and their interconnection in order to build the WP3 lab.

It provides a planning of the test cases to be executed with the partners.

The WP3 lab structure was checked against the requirements related to the objectives of WP3 and WP5 and described in the Grant Agreements, in order to ensure the fulfilment of such requirements. The related information given in chapter 2 shows that the lab setup appears to be in line to address the execution of the tests that will be specified by WP1.

The next WP3 delivery (D3.3 - First Lab Test Report) will describe the different lab test phases executed for each application, documenting the work done and detailing the achieved results and the validation of the communication capabilities in the lab environment, in line with the lab test strategy document elaborated in WP1. It covers Voice, TCMS, ETCS, CCTV/Video test results, as well as cross-border testing and will include the test case execution.

6 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

Document Title	Reference, version
[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] First Lab Integration and Architecture Description	D3.1
[S20] Grant Agreement number: 951725 — 5GRAIL — H2020-ICT-2018-20 / H2020-ICT-2019-3	
[S21] Test Plan	D1.1

[S22]	System pre-integration	D2.2
[S23]	Nokia proposal for calibration of FRMCS link level simulations	ETSI TC RT(20)076043r1

7 APPENDICES

7.1 WP1 test cases definitions

The Table 4 from WP1 indicates the test cases to be executed in WP3 lab in Hungary.

The lab in Hungary deals essentially with voice test cases but some data applications will also be tested. All applications will be integrated with FRMCS -On board Gateway, provided by Kontron (a.k.a TOBA-K). Finally, the use cases to be addressed in this lab environment, according to the GA are:

Voice over FRMCS 5G (5G radio, 5G core) using MCX/MCPTT servers as well as GSM-R network for interworking, applying 3GPP Release 16 and pre-Release 17 functionalities (e.g., location and functional alias). Consequently, the agreed in WP1 test cases are:

- Railway Emergency Group calls involving FRMCS-On-Board-Gateway, voice application and COTS terminals
- Driver to controller and vice-versa communication, involving voice application, FRMCS-On-Board Gateway and MCPTT dispatcher and COTS terminals.
- Voice Group calls establishing in both FRMCS 5G network and GSM-R network.

FRMCS 5G QoS: The purpose of these test cases is to apply 5G end-to-end QoS concepts to differentiate critical and non-critical data over FRMCS-On Board Gateway + FRMCS 5G infrastructure and evaluate impact on QoS while degrading radio transmission, emulating speed. This will be supported by the below test cases:

- **ETCS (critical) and TCMS (non-critical) over FRMCS 5G**: Different radio conditions emulating different network conditions (perfect radio conditions, degraded radio conditions)
- **CCTV/Video (both non-critical) over FRMCS 5G**: Different radio conditions emulating different network conditions (perfect radio conditions, degraded radio conditions)

ETCS (critical)/TCMS (non-critical) are the applications, to be tested in the context of prioritization between applications. This feature ensures resources availability, based on FRMCS priority of the applications.

Cross-border scenarios in the scope of WP3 are foreseen for TCMS application using two 5G cores and voice implemented as service continuation between two networks (FRMCS and GSM-R). These scenarios are also planned for field tests with DB in Germany, in the scope of WP5, using the GSM-R facilities of the WP3 lab (due to missing GSM-R coverage however a service continuity cannot be demonstrated.

Voice applications	WP3 Lab Nokia Hungary
On-train outgoing voice communication from the train driver towards the controller(s) of the train	X
On-train incoming voice communication from the controller towards a train driver	X
Multi-Train voice communication for drivers including ground user(s)	X
Railway Emergency Communication (voice and data (*) application)	X
Data applications	
Automatic Train Protection communication	X
Automatic Train Operation communication (limited to GoA2 ATO)	
TCMS: ❑ On-Train Telemetry communications ❑ On-Train remote equipment control	X
Non-critical real time video	X
Transfer of CCTV archives	X
PIS	
Remote control of engines	

(*): Data, as part of the Railway Emergency Communication, will not be tested in 5GRail.

Table 4: List of use cases for 5Grail (under discussion in WP1)

							Relevant Communication Applications								Relevant Support Applications											
URS Ref	Applications	5GRAIL	LAB WP3	LAB WP4	FIELD DB WP5	FIELD SNCF WP5	5.9 Automatic Train Protection communication	5.10 Automatic Train Operation communication	5.19 Voice recording and access	5.20 Data recording and Access	5.27 Critical real time video	6.19 Messaging Services	6.20 Transfer of data	6.23 Real time video call	8.1 Assured voice communication	8.2 Multi user talker control	8.3 Role management and presence	8.4 Location services	8.5 Authorisation of communication	8.7 Authorisation of application	8.8 QoS class	8.9 Safety application key management communication	8.10 Assured data communication	8.11 Inviting-a-user messaging	8.12 Arbitration	10.1 Billing information
5	Critical Communication Applications																									
5.1	On-train outgoing voice communication from the train driver towards the controller(s) of the train*	X	X	O	X	O										X	X	X	X	X	X			X	X	
5.2	On-train incoming voice communication from the controller towards a train driver*	X	X	O	X	O										X	X	X	X	X	X			X	X	
5.3	Multi-Train voice communication for drivers including ground user(s)	X	X	O	X	O										X	X	X	X	X	X			X	X	
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	
5.13	Remote control of Engines	O		O		O							X				X	X	X	X	X		O		X	
5.15	Railway Emergency Communication*	X	X	O	X	O							X			X	X	X	X	X	X				X	
6	Performance Communication Applications																									
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	
6.11	On-train remote equipment control (TCMS includes 6.9 + 6.11 + 6.20)	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	
6.20	Transfer of data (TCMS includes 6.9 + 6.11 + 6.20)	X	X		X												X		X	X	X				X	
6.22	Transfer of CCTV archives (Wi-Fi related?)	X	X	O	TBC												X		X	X	X				X	

Table 5: current status of test cases to be executed (column LabWP3) (1/2)

URS Ref	Applications	5GRAIL	LAB WP3	LAB WP4	FIELD DB WP5	FIELD SNCF WP5	FRMCS System principles related use cases (source: TR 22.889)																					
							12.2 Area Broadcast Group Communication interworking between GSM-R and FRMCS	12.3 Location Service interworking between GSM-R and FRMCS Users	12.4 Presence interworking between GSM-R and FRMCS	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	12.1 QoS in a railway environment	12.1 Provide broadband and mission critical services with seamless connectivity	12.1 Offer railway services high-quality control functions with real-time train status monitoring	12.1 Provide call priority during interworking with LMR	12.1 FRMCS Positioning Accuracy	12.1 FRMCS System security framework	12.1 Interworking to external networks	12.1 FRMCS On-network/Off-network communication	12.1 Call restriction service	12.1 Allocation and isolation of FRMCS communication resources	12.2 FRMCS Equipment capabilities for multiple FRMCS Users	12.2 FRMCS System/FRMCS User roaming capabilities	12.2 Availability – increasing measures	12.2 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
5	Critical Communication Applications																											
5.1	On-train outgoing voice communication from the train driver towards the controller(s) of the train*	X	X	O	X	O		O		X			X	X	X					O			O	O	X	X		
5.2	On-train incoming voice communication from the controller towards a train driver*	X	X	O	X	O		O		X		O	X	X	X					O			O	O	O	X		
5.3	Multi-Train voice communication for drivers including ground user(s)	X	X	O	X	O	X	X					X	X	X					X				O	O	X		
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		
5.13	Remote control of Engines	O		O		O									O				O	X					X			
5.15	Railway Emergency Communication*	X	X	O	X	O	X	X				O	X	X	X				O	O				X	X	X		
6	Performance Communication Applications																											
6.9	On-Train Telemetry communications (TCMS includes 6.9 + 6.11 + 6.20), including PIS	X	X	X	X	X								O	X					X								
6.11	On-train remote equipment control (TCMS includes 6.9 + 6.11 + 6.20)	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		
6.20	Transfer of data (TCMS includes 6.9 + 6.11 + 6.20)	X	X		X							O		O	X					O								
6.22	Transfer of CCTV archives (Wi-Fi related?)	X	X	O	TBC									X	X													

Table 6: current status of test cases to be executed in WP3 (column LabWP3) (2/2)

7.2 WP3 assumptions

For information, the following table depicts the current assumptions (agreed by WP3 members) and open points to be taken by WP3 for the execution of the planned test:

ID	Technical Architecture Open Items and Assumptions to support WP3 execution
1	5G public Band Modem (2.7 GHz TDD/ Band n78.) Band n8 for some dedicated use cases
2	Remote access to equipment for maintenance
3	No MCVIDEO, use MCData instead. Loose Coupling for Video as a data bearer
4	Separate dispatcher (GSM-R- FRMCS). Simple dispatcher (mobile dispatcher phone) for GSM-R
5	Numbering Plan: MC User ID : 11 digit. Functional Alias: 128 byte including domain name.
6	No MCX - MCX Interworking (3GPP Rel. 18)
7	Bearer Flex vs. Multiconnectivity use case : bearer Flex (multi access, one core) : No integration of WiFi in 5GCore (missing functionality e.g. no N3IWF in Rel. 15 Modem) -> no Multi Access/ bearer flex possible. Alternative for Multi Access: : two 3GPP bands / one modem (n78 sub bands, preferred by Field test / DB). Applications: no ETCS, no TCMS. Video offload archive. . Use Cae: CCTV offload: open how to trigger . No Multi Connectivity in WP3
8	Trackside GW provided by WP2 (OB App equivalent) -> TSApp for tight coupling/Voice not needed (direct connection to server). TS GW for Loose Coupling needed
9	Location: MCX support: Voice. GPS emulated available for LAB (eCGI emulation option not considered). No GMLC for 5G. Simulation in lab for Loose Coupled is tbd
10	GSM-R Interworking: Voice only. Group call only (REC)
11	Group Communication Interworking: FRMCS initiated group call only
12	Group Communication Interworking: no floor control / talker change (not specified yet for between system)
13	No PCF functionality, No MCX related 5GQI (66,67,..) supported. 5QI for MC Data -> non GBR (aligned with Rel. 17 MC Data 5QI 70 definition). Flexible assignment of 5QI/QFlowIdentifer in ToBa needed during test
14	Group Communication Interworking: no security/encryption for IWF (Note Two options. A) "Stop at IWF (as not in GSM-R)" B) no security for security in FRMCS)
15	Group Communication Interworking: no eMLPP mapping /interworking. Not defined in ETSI yet
16	MC Data / IP CONN : no functional alias required (3GPP Rel. 17)
17	Cross Border Use case: Re - registration needed (e.g. no inter plmn handover). Trigger by application tbd (no information on network registration info known on application layer)
18	Cross Border Use Case: Voice related: No FRMCS - FRMCS use case (WP5 open) . FRMCS - GSM-R Interworking scenario can be seen as roaming scenario
19	Cross Border Use Case: No ETCS use case. TCMS use case (home routed) Full functionality in Rel. 18 (automatic) . Proposal with one MCX Server
20	Emergency Alert: base on MCPTT , 3GPP Rel. 16 capabilities. Automatic Voice call setup
21	Multi Talker Control use case: only for Multi Train /Group call
22	MCData IPCon : Client to Client routing of user plane, MCX Server only in Control Plane
23	Private call for Train to Controller and controller to train
24	Floor request and GDCP for multi talker control: solved
25	MCData IPCon : Open: border crossing
26	Group Communication Interworking: no Functional Alias mapping. Not defined in ETSI yet
27	Location: MCX support for Loose: GPS emulated available for LAB
28	Dynamic QoS to be realized by static configuration in network, (DSCP/TOS) (as described in 3GPP 23.501.) Modem evaluation . Alignment with modem capabilities for voice:: 5QI-1 GBR supported by Nokia only for Voice (VoNR) capable devices. Proposed alterative is non-GBR for Voice (Ongoing plan for GBR capabilities in Nokia for non voice)

Table 7: WP3 Assumption and open topic list

Note: this table include the agreed assumptions (green) and open assumptions not yet finalized due to ongoing discussions in WP1 and WP3 marked in Yellow.

7.3 Planning of WP3 test phase

The activity 3.1 on Prototype and Lab Infrastructure preparation is finalized with MS5 (exceptions are the installation and integration related to 2nd OB GW, 2nd CAB Radio and 2nd second Core network which will be integrated before the specific testing phase started) .Note: the task 3.1 is enhanced with the partner integration as planned in the Tasks 3.2 and 3.3.

The activities consisted in the finalization of integration of the equipment deliveries and functions of all partners for the preparation of the tests. The following figure gives the current overview of the planned further test case executions which is still under final discussion with the partner depending on availability:

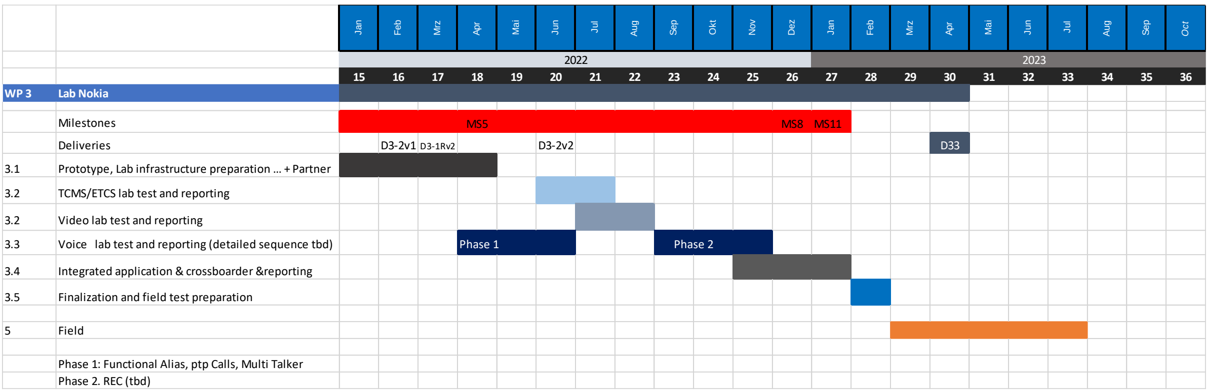

Figure 40: WP3 Planning

Due to the delivery schedule of functionality by WP2 the activities:

- 3.2 TCMS, ETCS as well as Video test cases are scheduled to be executed beginning in June
- 3.3 Voice tests will be realized in two phases, where phase 1 will cover test cases related to CAB radio to/from Dispatcher calls, Group calls, and Phase2 test related to Railway Emergency Call and GSM-R Interworking
- 3.4 This phase will focus on the test cases related to QoS related testcases with parallel applications executed as well as cross border cases and multi access.

Document D3-2 v1 focussed on the first achievements on the preparation phase, this version D3-2 v2 includes the final description of the preparation phases.

The end of this phase marks MS8 when main test activities will be finalized for tasks 3.2 and 3.3. Execution of task 3.4 is planned to last until January 2023 (MS11).

Task 3.5 is the finalization and preparation of the WP5 field test, including preparation of equipment in field and setting up the remote connection from Budapest lab with core network to the radio network in Germany.

Delivery D3.3, that will report all results of this test phase will be submitted in April 2023.

7.4 Installation guideline

The following chapter includes the installation guidelines of the partner deliveries for the Lab. This was required to be supported & executed by the Nokia team due to the access restrictions of the Budapest site due to the Covid-19 situation (restriction still in place in February 2022).

7.4.1 Installation guidelines for Gateways

7.4.1.1 OnBoard Gateway hardware installation manual (provided by Kontron):

The following pictures shows the integration aspects of the Onboard GW. First figure below shows the HW overview:

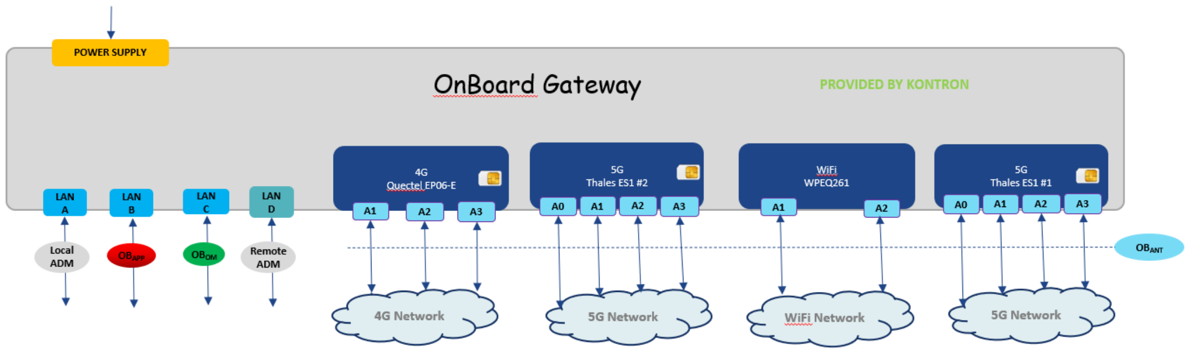

Figure 41: OnBoard Gateway Hardware overview

Power connections are shown in the following figure:

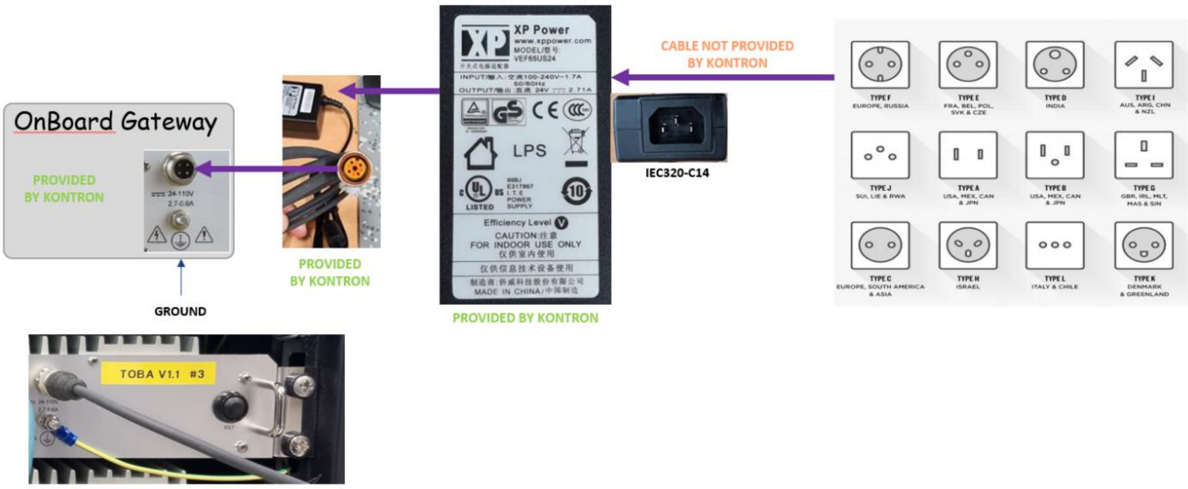

Figure 42: OnBoard Gateway Power connector

On the communication interfaces the integration considers following

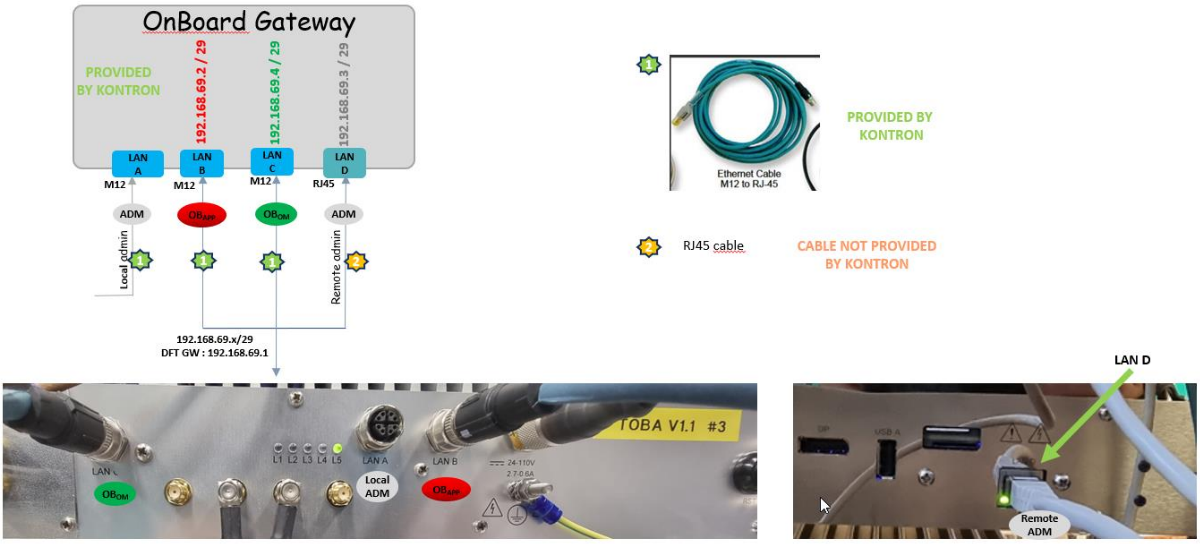

Figure 43: OnBoard Gateway Network interfaces

On the Antenna connectivity please check the following picture:

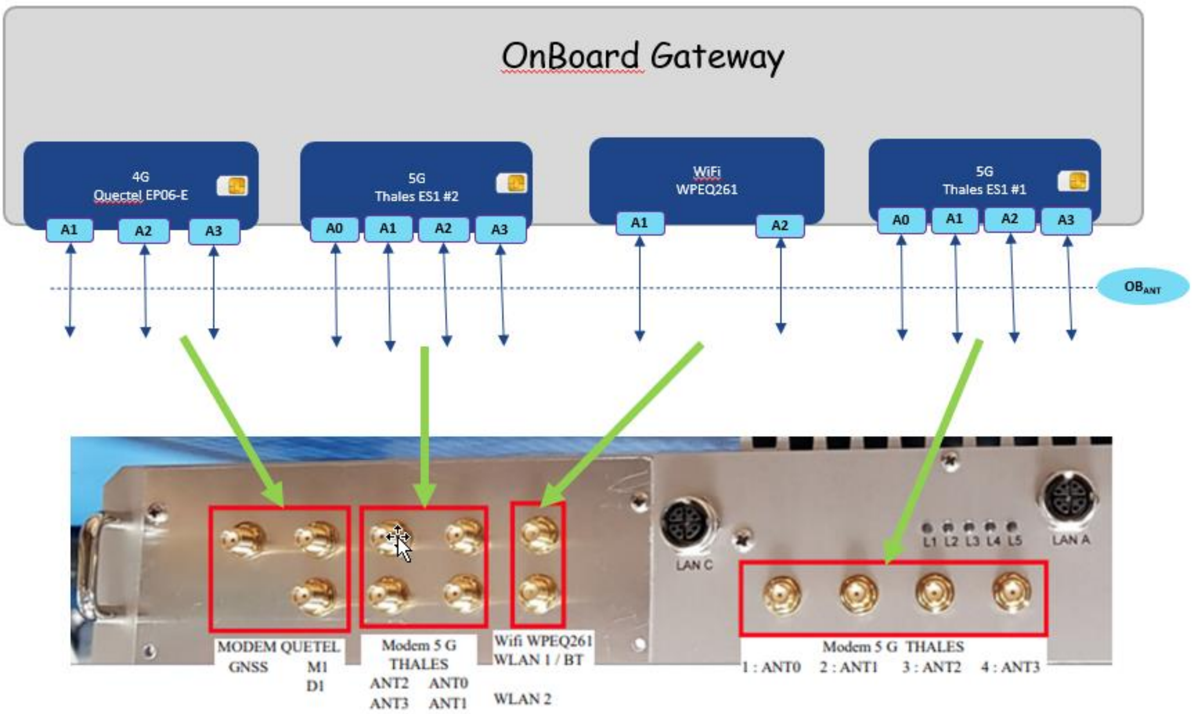

Figure 44: OnBoard Gateway Modem (antenna) interfaces

On the SIM cards integration in the Onboard GW see last figure of this chapter:

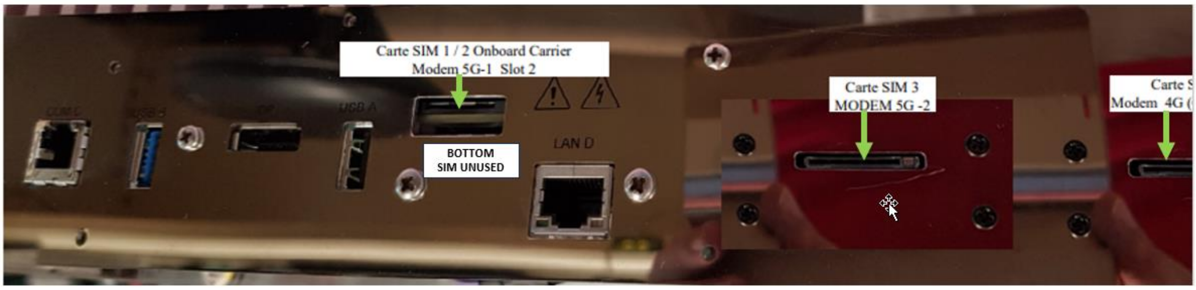

Figure 45: OnBoard Gateway SIM card locations

For modem 5G Thales ES-1 #1, upper SIM slot shall be used.

For modem 5G Thales ES-1 #1 (n78), ANT2 is used for Rx/TX and ANT0, ANT1, ANT3 can be used for Rx, based on the below figure.

Table 14: Antenna interfaces

Antenna port	TX.	RX.
ANT0	LTE: LB:B5,8,12,13,14,17,18,19,20,26,28,71 MHB:B1,2,3,4,7,25,30,34,38,39,40,41,66 5G Sub6G: LB:n5,8,12,20,28,71 MHB:n2,66	LTE: LB:B5,8,12,13,14,17,18,19,20,26,28,29,71 MHB:B1,2,3,4,7,25,30,32,34,38,39,40,41,66 UHB:B42,48; LAA: B46 5G Sub6G: LB:n5,8,12,20,28,71 MHB:n1,2,3,7,38,41,66 UHB:n77,78,79
ANT1		LTE: MHB:B1,2,3,4,7,30,38,41,66 UHB:B42,48 5G Sub6G: MHB:n1,2,3,7,38,41,66 UHB:n77,78,79
ANT2	LTE: MHB:B1,2,3,7,66 UHB:B42,48 5G Sub6G: MHB:n1,2,3,7,38,41,66 UHB:n77,78,79	LTE: MHB:B1,2,3,4,7,30,38,41,66 UHB:B42,48 5G Sub6G: MHB:n1,2,3,7,38,41,66 UHB:n77,78,79
ANT3		LTE: LB:B5,8,12,13,14,17,18,19,20,26,28,29,71 MHB:B1,2,3,4,7,25,30,32,34,38,39,40,41,66 UHB:B42,48; LAA: B46 5G Sub6G: LB:n5,8,12,20,28,71 MHB:n1,2,3,7,38,41,66 UHB:n77,78,79

Figure 46: OnBoard Gateway antenna locations

7.4.1.2 Trackside GW Operating system installation manual (provided by Kontron):

For TS GW, you can download ISO DVD "Ubuntu Server 20.04.3 LTS" from https://ubuntu.com/download/server#downloads (Downloaded file "ubuntu-20.04.3-live-server-amd64", ~1,17GB).

You can use Rufus Media Writer Software (https://rufus.ie/en/) to create the USB stick (Select GPT on:

To set the admin port, select "Network connections" and:

- Select the first ethernet device available
- Press on Edit IPv4
- Choose Manual on IPv4 Method list
- Fill in the following fields: Subnet, Address, Gateway, Name servers
- Press Save
- Press Done

For storage configuration (HDD or SSD according to your HW configuration) and mounting points:

- Ensure that the SSD disk are selected in the list
- Select "Custom storage layout" by pressing space key
- Press Done

  => Storage configuration window displayed
- Go to the AVAILABLE DEVICES
- Press Enter on the SSD disk
- Select Use As Boot Device and press Enter
- Press Enter one time more on the SSD disk

  => Create one Standard partition for boot
- Select Add GPT Partition
- Set partition size of /boot partition to 2GB
- Change partition format from ext4 to xfs
- Select /boot in the Mount list
- Press Create

  => Create a logical groupe
- Press Enter one time more on the SSD disk
- Select Add GPT Partition
- Leave empty the size line
- Select Leave unformatted on the Format list
- Press Create
- Press on Create volume group (LVM)
- Change volume group name by vg_system
- Select the SSD disk in Devices line by pressing space key
- Press Create

  => Create logical volume
- Press on the volume groupe created on the AVAILABLE SECTION device
- Press Create Logical Volume

  => Create the logical volumes using the following information

lv_root	/	LVM, xfs,	80G
lv_swap	SWAP	LVM, xfs,	16G
lv_var	/var	LVM, xfs,	10G
lv_var_log	/var/log	LVM, xfs,	8G
lv_home	/home	LVM, xfs,	50G

lv_iso /iso LVM, xfs, 20G => for iso image to install VM

lv_vm /vm LVM, xfs, 745G => for VM disk image

- Press Done
- Confirm the choices by pressing continue

7.4.2 Installation guidelines for Voice

Hungary 5G Siemens 5G Radio Setup Instructions

Hardware Setup

The 5G Radio consists of the following hardware components:

- 1x Siemens 5G Radio
- 1x ARINC Gland Box (Providing the GDCP and OBapp Ethernet leads, GDCP 25 way-D Power and Audio Male Lead and Female Din Power socket)
- 1x Power Supply with UK 3 pin plug and male Din Plug
- 1x GDCP Console (providing 25 way D for Power and Audio Female socket and RJ45 Ethernet for data)
- 2x LTE Antennas

To Set up the hardware:

- Connect the Gland Box to the Cab Radio, using the ARINC Connectors.
- Connect the 25way connector from gland box to the back of the GDCP Console, ensure it is secure.
- Screw the 2 LTE antennas into the 2 gold LTE ports on the front of the radio, labelled LTE1M and LTE1D.
- Plug the power supply DIN plug into the DIN socket on the Gland Box. Do not plug in the power supply at this point.

Set up the network hardware (a Network diagram is shown below for clarity).

- Using a Nortel supplied ethernet switch, connect the Red GDCP Ethernet cable coming from the Gland box to it. Then connect the Black ethernet cable coming from the GDCP Console to the same switch. Also connect the Management terminal to switch.
- Connect the blue OBapp Ethernet cable coming from the Gland box to the OBapp Ethernet Switch.

Setup the Management Terminal:

- In order for the Management terminal to ssh into the Siemens radio it will require a set of ssh keys to be installed. These will be provided separately.

At this point the power supply can be plugged into the mains. The Fan of the cab radio should be heard for a brief time and the GDCP should light up and eventually show the default screen.

Power on and startup of the Siemens FRMCS applications.

1. If the radio has not already been powered on, then apply power to the power supply connected to the Cab Radio.
2. Using the Management terminal, which should have an IP address of 192.168.69.22, using a dos/Cygwin/linux cmd/terminal, ssh into the Siemens Cab Radio, i.e.
   "$ssh root@192.168.69.18".
   - This will default to a /home/root directory.
3. Start the essential services, i.e.
   "$./5G_Start.sh".
4. Run the obapp client, connect and register to OBapp, i.e.
   - `$python3 obapp_client.py`
   - `connect ws://<OBAPP-Server IP Address>:8765/v0`
   - `register 1 my_id loose auto_accept`
5. `Create a new ssh session to the Siemens Cab Radio (as in 2 above) and`
   - Start the Siemens FRMCS applications, by typing:
   - $cd /mnt/part3/frmcs-prod
   - $./frmcs.sh GDCP 5grail_111 5grail
6. The GDCP will display the default FRMCS identity. Press the tick key to select the default identity.
7. At this point the GDCP should show the text "No identity".
8. Go into the Main Menu and select the 2nd option "Register identity". MCX-App should proceed to register the client id with the server.
9. More needs to be added here, depending on what is required of the radio….

Power down

To perform an ordered shutdown of the Siemens Cab Radio..

1. Using the Management terminal, which should have an IP address of 192.168.69.22, ssh into the Siemens Cab Radio, i.e."$ssh root@192.168.69.18". This will default to a /home/root directory.
2. Type "$shutdown now; exit"
3. It is then safe to remove the power from the Cab Radio.

Network Configuration

The network configuration of the Siemens 5G Cab Radio is as below.

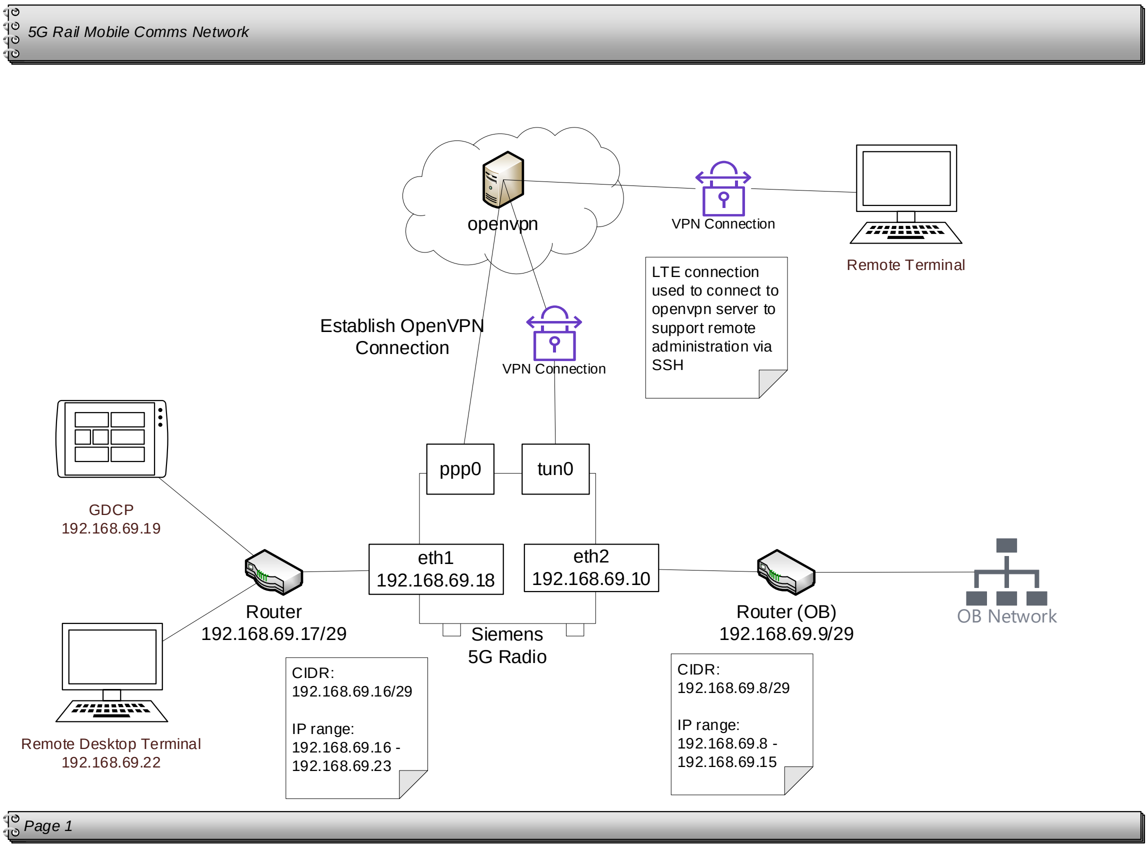

Figure 47: Network configuration of Siemens 5G CAB Radio

7.4.3 Decrypting HTTPS messages in Wireshark

MCPTT Server Setting

Step 1 : Connect to the MCPTT server.

Step 2 : Go to the path below and open the "ssl.conf" file.

- /etc/httpd/conf.d/

Step 3 : Modify the contents as follows. (See image below)

- SSLCipherSuite AES256-GCM-SHA384:AES128-GCM-SHA256 → **Delete '#'**

  #SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4→ **Insert '#'**

```
</VirtualHost>

<VirtualHost *:2359 *:2250>

  SSLEngine on
  SSLProtocol -All +TLSv1.1 +TLSv1.2
  SSLHonorCipherOrder on
  SSLCipherSuite AES256-GCM-SHA384:AES128-GCM-SHA256
  #SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
  SSLCertificateFile /etc/pki/tls/certs/localhost.crt
  SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
  #SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
  #SSLVerifyClient require
  #SSLVerifyDepth  10

  ServerSignature Off
  Timeout 300
  KeepAlive On
  KeepAliveTimeout 5
  MaxKeepAliveRequests 500
  HostnameLookups Off

  LogLevel info
  ErrorLog /var/log/httpd/error_csc.log
  CustomLog /var/log/httpd/access_csc.log combined
```

Figure 48: SSL.CONF file editing on MCX

Step 4 : Restart the httpd service with the following command.

- systemctl restart httpd

Step 5 : Download and save the "localhost.key" file in the path below to my PC.

- /etc/pki/tls/private

Only packets captured after server setup can be checked for http messages.

Wireshark Setting

Step 1 : Run wireshark

Step 2 : Click "Edit -> Preferences..." at the top of the Wireshark screen

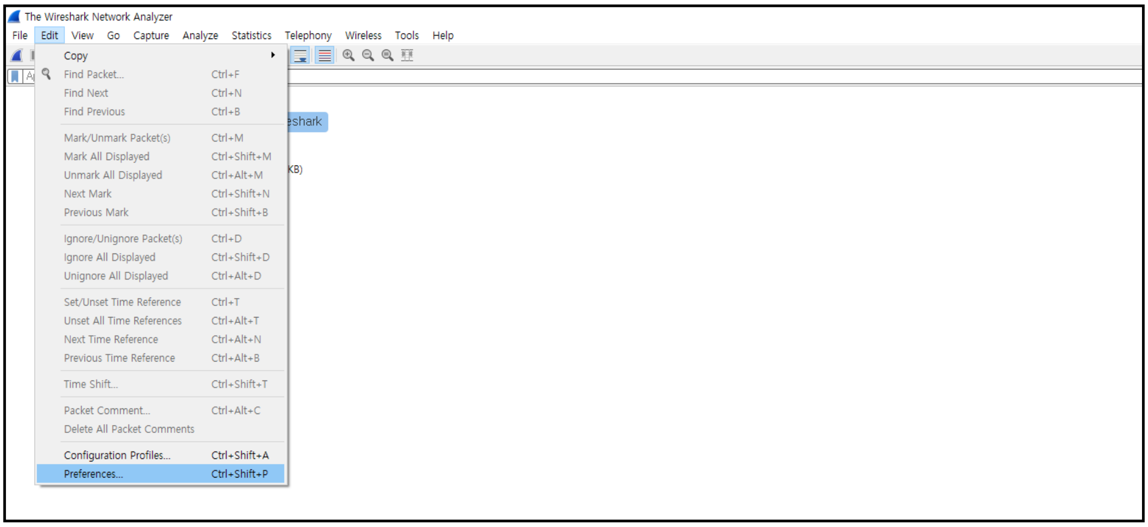

Figure 49: Preferences menu in Wireshark

Step 3 : Select TLS from "Protocols" from the left list.

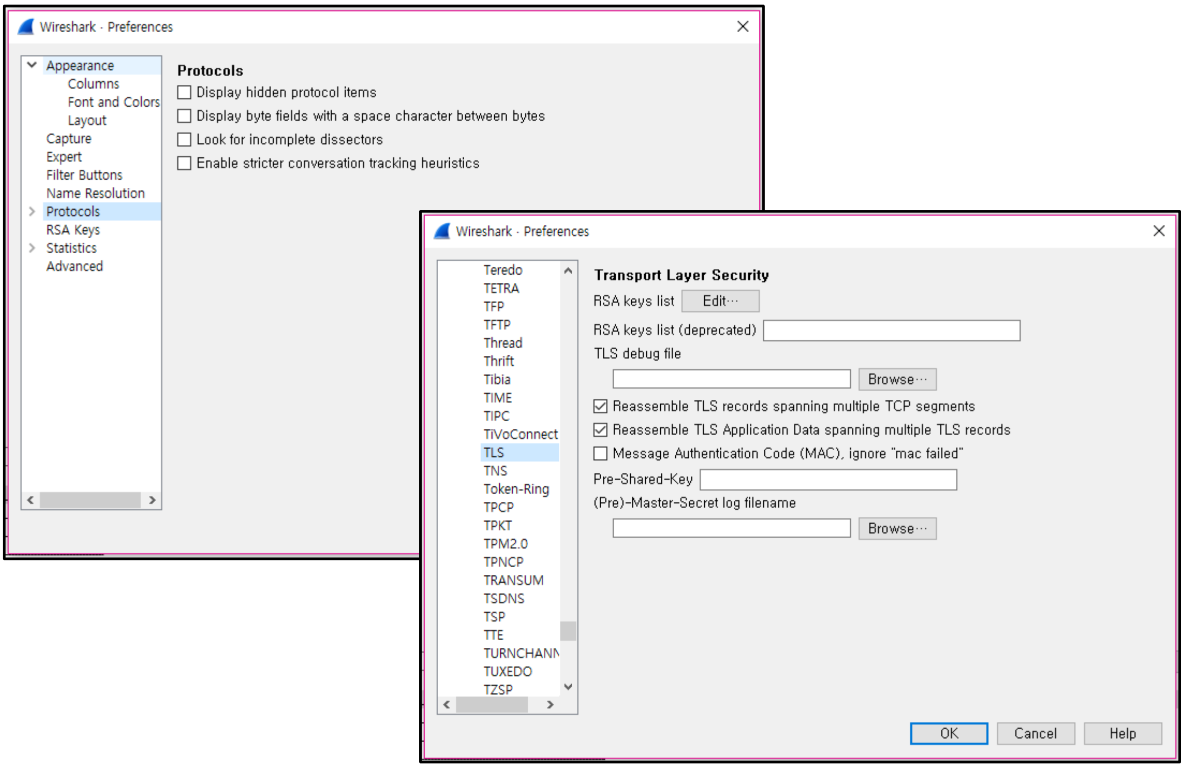

Figure 50: TLS protocol menu in Wireshark

Step 4 : Click the "Edit" button next to the RSA keys list.

Step 5 : Use the "+" button at the bottom of the TLS Decrypt screen to add the following information.

- IP address : **Enter MCPTT IP address**
- Port : **2359**
- Protocol : **http**
- Key File : **Key file path downloaded when setting up the MCPTT server.**

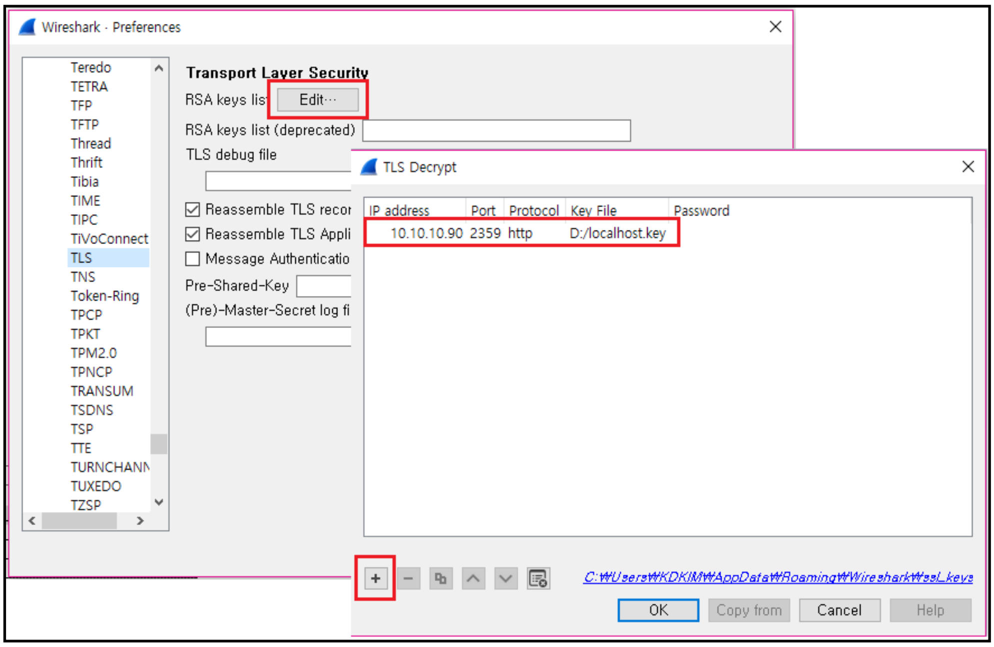

Figure 51: Adding RSA key to Wireshark for TLS decryption

Step6 : Check messages by filtering http.

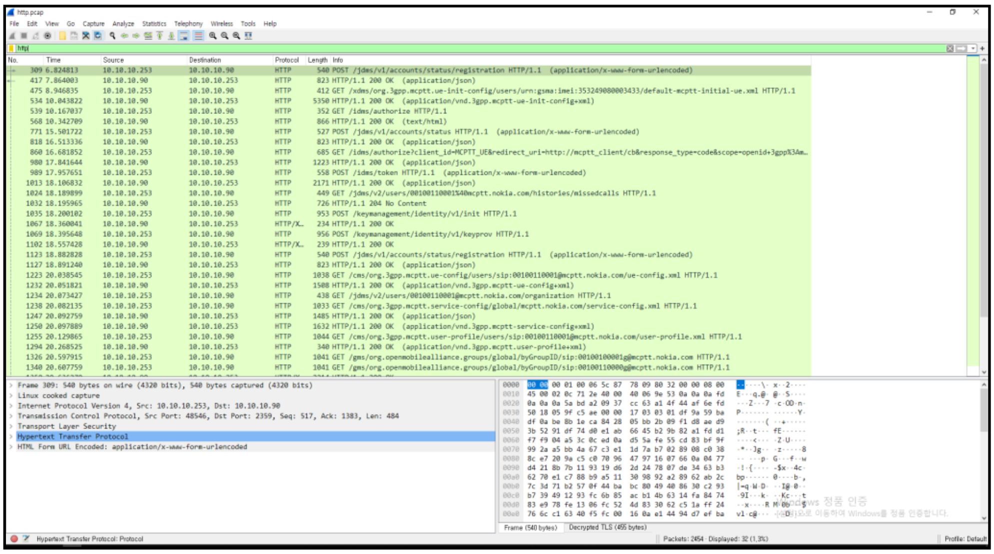

Figure 52: Decrypted HTTPS messages in Wireshark

7.4.4 Documentation of integration results

A common Teams collaborator place is created to store the integration and test results. All partners have rights to upload their results to this folder.

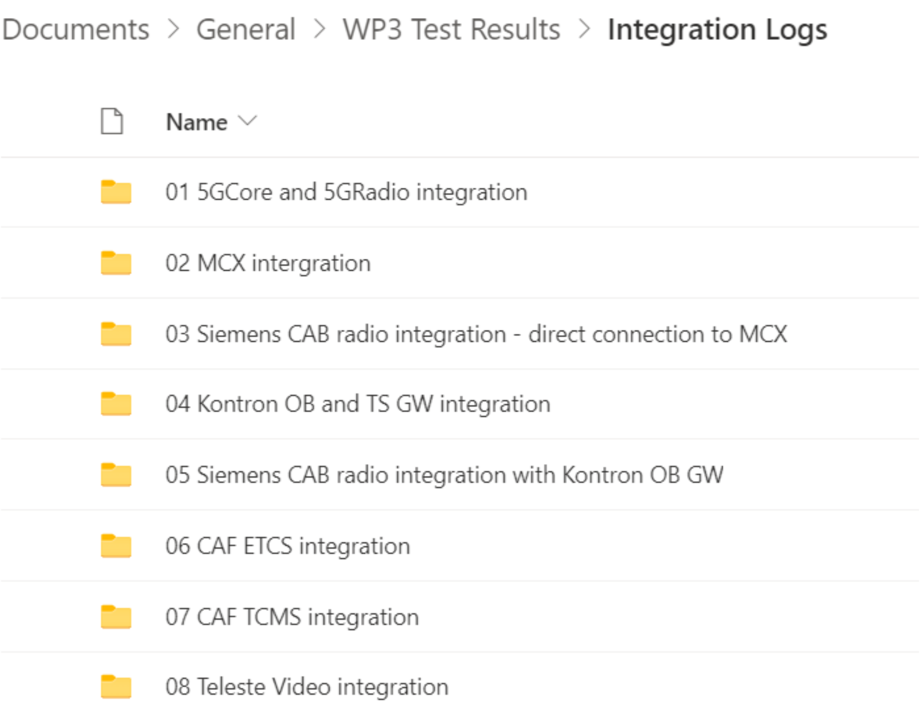

Figure 53: Folder structure of integration logs

7.4.4.1 Reference logs from 01 5GCore and 5GRadio integration

Nokia_Attach_detach_from_5G_network_phone_20211215.pcap

Nokia_Attach_detach_from_5G_network_Thales_modem_20211215.pcap

7.4.4.2 Reference logs from 02 MCX integration

Nokia_Private_call_with_talkerchange_dispatch_and_phone_20220316.pcap

Nokia_Private_call_with_talkerchange_two_phones_20220316.pcap

Nokia_PTX_call_FTP_file_transfer_on_5g_20220131.pcap

Nokia_Register_deregister_with_MCX_server_phone_20220316.pcap

Nokia_Register_deregister_with_MCX_server_Thales_modem_20220316.pcap

Nokia_Registration_to_MCX_server_with_two_phones_20220316.pcap

7.4.4.3 Reference logs from 03 Siemens CAB radio integration - direct connection to MCX

Nokia_CAB_REGISTER_to_MCX_20220510.pcap

Nokia_UE_CAB_private_call_20220510.pcap

7.4.4.4 Reference logs from 04 Kontron OB and TS GW integration

Nokia_OBGW_attach_to_5G_20220524.pcap

7.4.4.5 Reference logs from 05 Siemens CAB radio integration with Kontron OB GW

7.4.4.6 Reference logs from 06 CAF ETCS integration

7.4.4.7 Reference logs from 07 CAF TCMS integration

7.4.4.8 Reference logs from 08 Teleste Video integration

7.5 WP3 open points

For information, the following table depicts the open points to be taken into account by WP3 for the execution of the planned test:

execution of the planned test:

Ref. chapter	Topic description	Comment
2.3	Related to the integration for the end-to-end functionality including CAB Radio. A basic group call was done to verify MCX – GSM-R integration (initiated in MCX and established in MCX and also in GSM-R system).	

3	The final connectivity of the leased line is under final approval	
3.3.6.	ETCS/TCMS Integration tests will be part of functional testing.	
4.4	QoS values need to be further defined	
4.5	TCMS onboard connects from visited to home network. For this use case a second 5GCore connected to separate second Radio RRH is needed. The need for IMS in the visited PLM is an open topic.	