Ref. Ares(2022)3701967 - 16/05/2022

Project funded by the Horizon 2020 Framework Programme of the European Union,

Grant agreement Nº: ***951947.***

Start date: **01/09/2020**

Duration: **36 months**

D3.2: 5GMED ICT architecture and initial design

WP	WP3
WP Leader	RETE
Responsible Author	RETE
Contributors	RETE, NBC, VEDE, VALEO, AXBRYD, I2CAT, ATOS, COMSA, IRT, CNXFR, CTTC
Dissemination Level	PU
Nature	RE

Dissemination Level:	
PU	Public

Nature	
RE	Report

Synopsis	Deliverable D3.2 represents the baseline of the 5GMED network design, deployment and test activities that are carried out within WP3. It describes the cross-border 5G network architecture designed to support the automotive and railways use cases. This deliverable contains the details of the initial design of the multi-connectivity infrastructure components required to integrate several Radio Access Network (RAN) technologies (e.g., IEEE 802.11ad, satellite) with 5G, cross-border network management and service orchestration mechanisms, network slicing, roaming optimization techniques, and network security mechanisms. In the final section, the deployment planning of the infrastructure in small-scale and large-scale testbeds is reported.
List of Keywords	5G, Architecture, Multi Connectivity, Orchestration, Roaming, Network Slicing.

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the 5GMED Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the 5GMED Consortium.

Funded by the Horizon 2020 Framework Programme of the European Union

DOCUMENT HISTORY

Version	Status[1]	Date	Comments	Author
0.1	Draft	08/02/2022	Draft ToC	Giovanni Rigazzi
0.2	Draft	15/02/2022	ToC revised by I2CAT	Daniel Camps
0.3	Draft	13/03/2022	Integrated contributions from VEDE, NBC and security for 5GMED infrastructure	Giovanni Rigazzi
0.4	Draft	19/03/2022	Integrated AXBRYD contribution (not final)	Giovanni Rigazzi
0.5	Draft	31/03/2022	Integrated AXBRYD final section, integrated COMSA subsection on 70GHz train-to-ground	Giovanni Rigazzi
0.6	Draft	19/04/2022	Integrated the latest versions of UC analysis for slice design. Started restructuring section 2 based on comments	Giovanni Rigazzi
0.7	Under review	28/04/2022	Draft ready for internal review (TM + main editor)	Giovanni Rigazzi
1.0	Under review	02/05/2022	Draft reviewed by editor and TM	Giovanni Rigazzi
1.1	Draft	04/05/2022	Integrated comments from WP3L	Giovanni Rigazzi
1.2	Draft	06/05/2022	Integrated comments from TM	Giovanni Rigazzi
1.3	Draft	13/05/2022	Addressed comments – integrated input from COMSA, VEDE, I2CAT, HSP, AXB, NBC	Giovanni Rigazzi
1.4	Issued	16/05/2022	Final version submitted to EC	Giovanni Rigazzi

[1] Status (a status is associated to each step of the document life cycle)
Draft. This version is under development by one or several partner(s)
Under review. This version has been sent for review
Issued. This version of the document has been submitted to EC

TABLE OF CONTENTS

Funded by the Horizon 2020 Framework Programme of the European Union

LIST OF TABLES

LIST OF FIGURES

Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
5GAA	5G Automotive Association
5GCN	5G Core Network
ACS-GW	Adaptive Communication System Gateway
AF-NEF	Application Function – Network Exposure Function
AI	Artificial Intelligence
AMF	Access and Mobility management Function
BBU	Base-Band Unit
BGP	Border Gateway Protocol
BTP	Basic Transport Protocol
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CAS	Cooperative Awareness Service
CAV	Connected and Automated Vehicle
CCAM	Cooperative and Connected Automated Mobility
CDN	Content Delivery Network
C-ITS	Cooperative Intelligent Transport Systems
CNF	Cloud-native Network Function
CPE	Customer Premises Equipment
CPM	Collective Perception Message
CPRI	Common Public Radio Interface
CPS	Collective Perception Service
C-V2X	Cellular Vehicle to Everything
DENM	Decentralised Environmental Notification Message
DENS	Decentralised Environmental Notification Service
DHCP	Dynamic Host Configuration Protocol
DN	Data Network
DO	Domain Orchestrator
DPDK	Data Plane Development Kit
eBPF/XDP	extended Berkeley Packet Filter - eXpress Data Path
eMBB	Enhanced Mobile Broadband
EPLA	Enhanced Physical Layer Aggregation
HMI	Human Machine Interface
HO	Handover
HR	Home Routed
IP	Internet Protocol
IPSec	Internet Protocol Security
ISC	Internet Services Consortium
GN	GeoNetworking
gNB	gNodeB
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
KPI	Key Performances Indicator
LBO	Local Break-Out

MAPEM	MAP Extended Message
MCS	Manoeuvre Coordination Service
MEC	Multi-access Edge Computing
mmWaves	Millimetre Waves
MNO	Mobile Network Operator
MPLS	Multi-Protocol Label Switching
MPTCP	Multi-Path Transmission Control Protocol
MRI	Maximum Information Rate
MTU	Maximum Transmission Unit
NAS	Non-Access Stratum
NAT	Network Address Translation
NR	New Radio
PCF	Policy Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PMF	Performance Measurement Function
PMFP	PMF Protocol
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RRU	Remote Radio Unit
RS	Remote Station
RSU	Road-Side Unit
RTT	Round Trip Time
RU	Remote Unit
RV	Remote Vehicle
SBA	Service-based architecture
SDF	Service Data Flow
SIM	Subscriber Identity Module
SMF	Session Management Function
SOME/IP	Scalable service-Oriented MiddlewarE over IP
SRIOV	Single-root input/output virtualization
STAMP	Simple Two-way Active Measurement Protocol
TCN	Train Communication Network
TNG	Trusted Network Gateway
TCP	Transmission Control Protocol
TCU	Telematic Control Unit
TMC	Traffic Management Centre
ToD	Tele-operated Driving
UC	Use Case
UE	User Equipment
UPF	User Plane Functions
UPMT	Universal Per-Application Mobility Management Using Tunnels
USIM	Universal Subscriber Identity Module
V2I	Vehicle-to-Infrastructure
V2V	Vehicle to vehicle
V2X	Vehicle to Everything

Funded by the Horizon 2020 Framework Programme of the European Union

VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal

Executive Summary

The present document is the second deliverable of Work Package 3 entitled “5GMED ICT architecture and initial design” and represents the main output of T3.3, T3.4, T3.5 and T3.6. The objectives of this deliverable are to provide an initial design of the 5G network architecture by taking into account the technical challenges and geographical constraints of the 5GMED cross-border corridor as well as by introducing multi-connectivity solutions to integrate additional non-5G radio technologies, cross-border network management and service orchestration, and network slicing mechanisms. The network requirements captured in D3.1 are accounted in order to investigate the technological enhancements needed for building a scalable and multi-tenant 5G infrastructure, including low-latency roaming, security, and MEC support.

The design of the 5G architecture is initially split into two regions of the corridor, i.e., the French side and the Spanish side, as each section presents fairly different conditions in terms of radio access nodes, backhauling and MEC availability. A set of multi-connectivity solutions for the highway and railway use cases is also described. Such mechanisms will allow to take advantage of short-range communication systems, i.e., C-V2X on the highway and IEEE 802.11ad on the railway, and satellite connectivity, thus extending coverage and capacity beyond 5G. Cross-border orchestration, i.e., how to manage and provide computing and connectivity resources across the border, is also covered in this deliverable, and an initial discussion of network slicing is addressed. Lastly, an updated deployment planning for the small-scale and the large-scale testbed is reported.

The findings and activities described in this deliverable will serve as a basis for future architecture enhancements and developments that will be reported in D3.3 and D3.4.

1. Introduction

D3.2 reports on the initial design of the 5G network architecture of 5GMED taking into account the analysis and assessment of the network requirements introduced by the use cases as well as the challenges and constraints characterizing the cross-border corridor, as discussed in D3.1 [1]. In the following, more details on the scope and the structure of this document are given.

1.1. Scope of the document

D3.2 takes into account four technical challenges identified in D3.1 and proposes appropriate solutions that will make an impact in the architecture design. The technical challenges and solutions are summarised below.

MEC and network slicing support in 5GC

MEC and network slicing are two fundamental features for meeting the diverse service KPIs characterizing the UCs proposed in 5GMED. On one hand, the deployment of computing machines next to the 5G nodes or at specific traffic aggregation point is expected to reduce the end-to-end latency and to alleviate possible congestions affecting the transport network. In D3.2, a detailed description of the MEC servers and of the deployment options is provided. On the other hand, network slicing will help to classify and prioritize the traffic acting on the RAN, the transport network and the core network. This is an essential feature of the 5GC, although 5GMED aims to extend the concept of resource isolation and reservation to other non-3GPP radio access technologies considered in this project.

Low latency and Secured 5G roaming at cross-border

As 5GMED focuses on cross-border roaming between France and Spain, major effort will be devoted towards introducing novel mechanisms to enhance the signaling exchange between the two 5GC networks and reduce the latency experienced by a user when crossing the border. D3.1 reports all the 3GPP features necessary to achieve this goal as well as the mechanisms to ensure a secure roaming process. In particular, in D3.2 the list of key features consists of the N14 interface and the Local Break-out. The implementation of the former connecting AMFs (Access and Mobility management Function) will advance the signaling procedures involving inter-PLMN mobility, whereas the latter will heavily reduce the user traffic packet latency by preventing the data from being routed to the home PLMN while visiting another country.

Secure Inter-MEC federation and connectivity

To ensure inter-MEC federation, a multi-access edge orchestrator will be developed and validated in 5GMED. This component will be part of the network management and orchestrator stratum representing the top layer of the 5GMED architecture. Moreover, inter-MEC federation is a key enabler for the Follow-me infotainment use case (UC4) given that the synchronization of multiple MEC instances distributed across the corridor must be guaranteed as the video content consumers move.

Multi-Connectivity and integration of heterogeneous access networks

Multi-connectivity is one of the key elements in 5GMED and is addressed by introducing specific network components. On the one hand, vehicular communications can rely on cellular 5G connectivity and short-range ITS-G5/C-V2X connections, and the cooperation and coordination between these two technologies is performed by integrating the V2X gateway into the 5GMED infrastructure, as explained in Section 3.2.On the other hand, train-to-track communications are supported by 5G and other two non-3GPP radio access technologies, i.e., 70 GHz IEEE 802.11ad and satellite links, which may or not be available at the same time along the corridor. For this reason, 5GMED will feature a novel network component called Adaptive Communication System gateway (ACS-GW), capable of selecting the most appropriate connection at any time, thus satisfying the requirements of each application and service related to the railways use cases. More details on the proposed solution will be provided in Section 3.

1.2. Structure of the document

This deliverable is organized as follows. Section 2 gives an in-depth overview of all the building blocks of the 5GMED architecture. Three different strata are identified and discussed, starting from the infrastructure, which is composed of the Spanish side and the French side, and then describing the network slicing stratum and the network management and service orchestration stratum.

Section 3 describes in more details the proposed multi-connectivity approach, making a distinction between the railway communications, where the ACS-GW is introduced, and the vehicular communications, where the V2X gateway is employed.

Section 4 discusses the architecture for cross-border roaming and explains the solution adopted to ensure low-latency signaling interchange between two 5GC networks, relying on specific 3GPP features.

Section 5 provides a security assessment of the 5GMED infrastructure, not only considering the 5G system but also the physical security policies and recommendations for ensuring protection against physical threats.

Section 6 describes the onboard TCUs to enable multi-connectivity for automotive use cases.

Section 7 presents the plan for the network infrastructure deployment in the small-scale and large-scale testbeds of 5GMED.

Finally, Section 8 concludes the deliverable and illustrates the future work.

2. 5GMED Architecture Definition

The 5GMED network architecture is composed of the following strata depicted in Figure 1 and briefly described below.

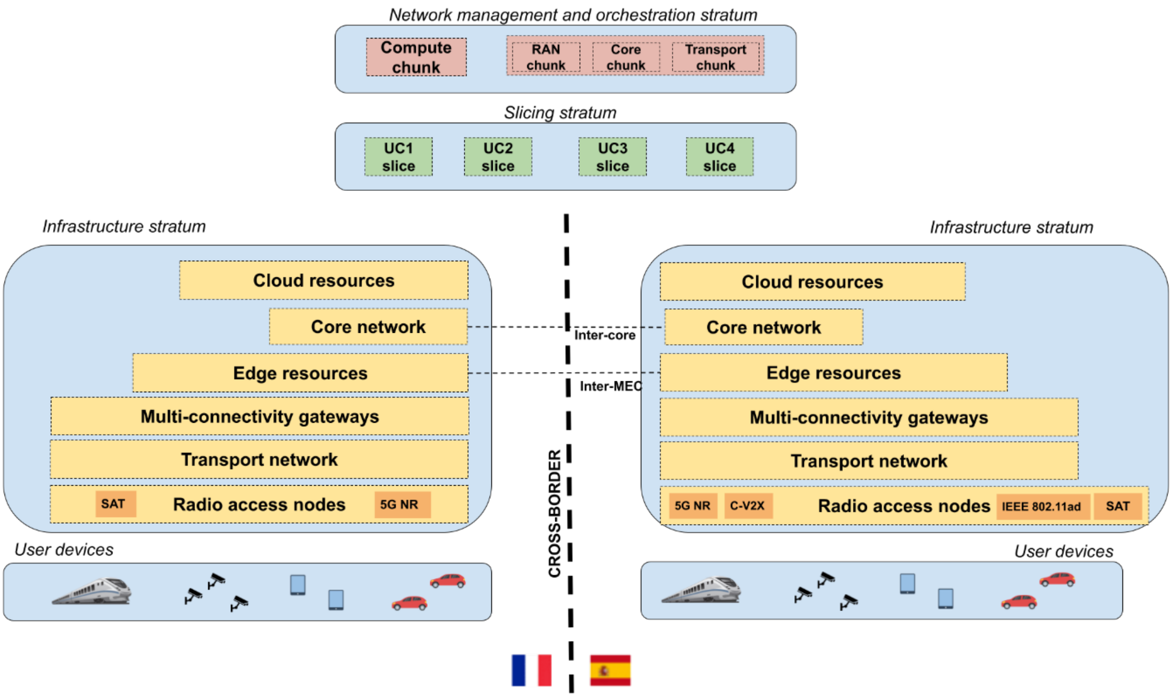


Figure 1: The 5GMED multi-stratum architecture.

Infrastructure stratum

The infrastructure stratum contains all the essential hardware and software resources for ensuring end-to-end connectivity between user devices or between a user device and a service located on the edge or cloud. Moreover, the infrastructure also includes novel solutions such as the multi-connectivity gateways, which enable the dynamic selection of a radio access technology (RAT) based on traffic conditions and QoS. As shown in the figure above, the infrastructure stratum consists of two separate instances, i.e., in the French side and the Spanish side, featuring different deployment conditions in terms of RAT options, MEC availability and transport networks. Finally, the interconnection between the two sides will be needed to allow the interchange of 5GC signaling for roaming (inter-core) as well as the user data exchange between MEC nodes located in the two countries (inter-MEC). Moreover, although it is not shown in the figure, some of the applications will require Internet access to reach remote servers (backend).

Network Slicing stratum

The network slicing stratum is instrumental in ensuring the appropriate Quality of Service (QoS) and in meeting the requirements of each of the 5GMED use cases. In 5GMED, network slicing will take into account the 3GPP 5G approaches and will extend the concept of resource isolation and reservation to other non-3GPP access technologies, including 70 GHz IEEE 802.11ad and satellite.

Funded by the Horizon 2020 Framework Programme of the European Union

Network Management and Service Orchestration stratum

The network management and service orchestration stratum includes all the functions responsible for managing the networks and orchestrating computing and networking resources.

In the following subsections, a more in-depth analysis of each stratum will be provided.

2.1. Infrastructure stratum

As mentioned before, the infrastructure stratum represents the collection of physical resources available in 5GMED to provide end-to-end connectivity. illustrates the overall architecture of the 5GMED infrastructure and denotes the difference between the French side and the Spanish side. Through the following subsections of this deliverable, the presented architecture will be dissected and each key element will be illustrated in a specific subsection.

Funded by the Horizon 2020 Framework Programme of the European Union

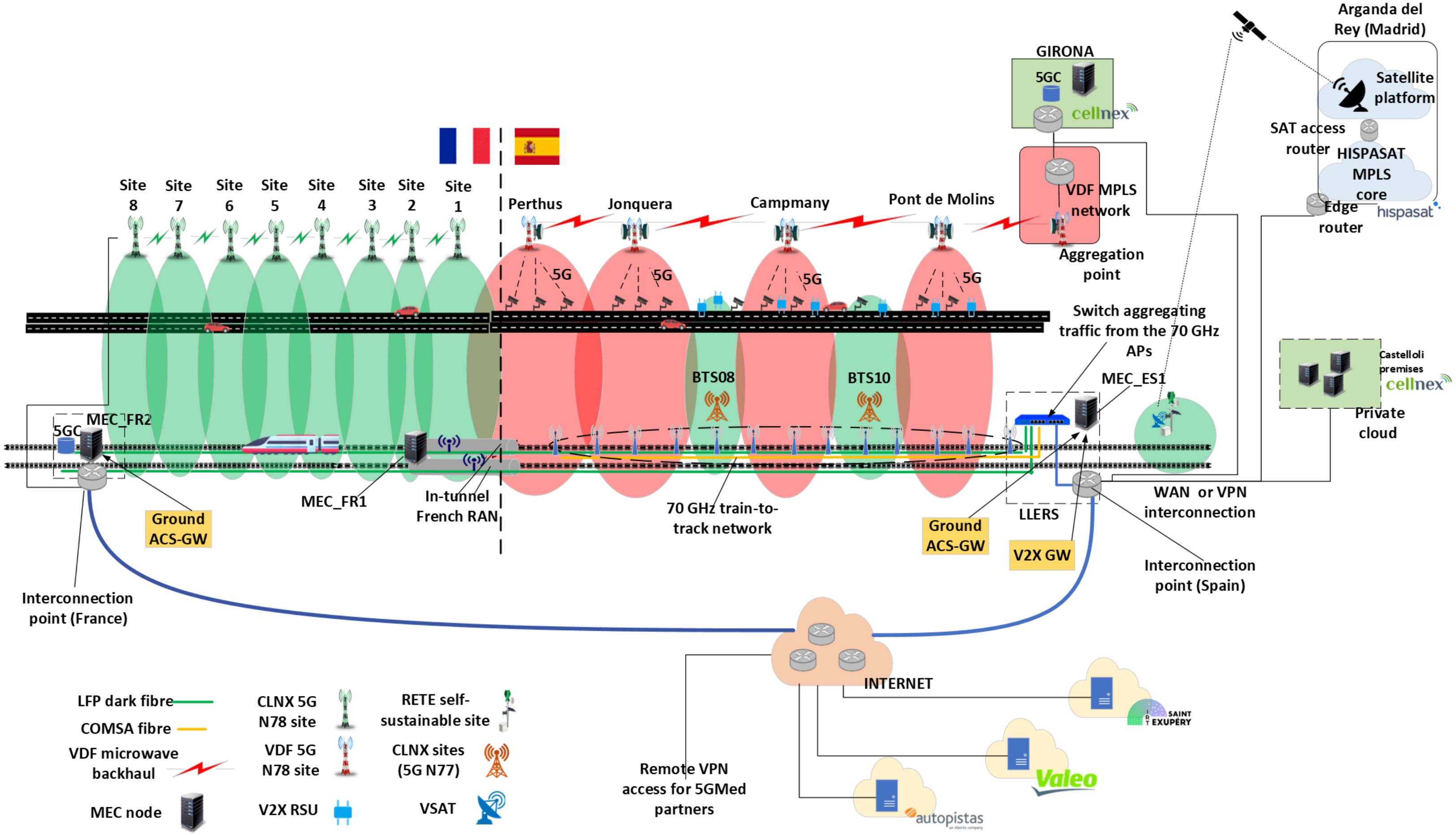


Figure 2: The 5GMED infrastructure architecture.

Funded by the Horizon 2020 Framework Programme of the European Union

The infrastructure stratum of 5GMED is composed of the following parts:

- **Radio access nodes** such as 5G NR gNBs, 70 GHz IEEE 802.11ad access points, V2X Roadside Units (RSUs), i.e., ITS-G5 and C-V2X, and VSATs (Very Small Aperture Terminals), whose role is to provide terminals with wireless access. Unlike the 5G gNBs, the 70 GHz APs, the V2X RSUs and the VSAT can be considered as stand-alone wireless solutions due to the fact that they do not need a core network to operate and manage the terminal sessions.
- **Transport network**, including microwave point-to-point connectivity, fibre optics and satellite backhaul, which is relevant to cellular technologies and typically enables the communication between the access nodes and the core network.
- **Core network,** 5GMED will employ two different 5GCs, one in France and one in Spain, and will validate enhanced roaming mechanisms to reduce the signaling latency experienced by terminals crossing the border.
- **Multi-connectivity gateways**, increasing service reliability and availability by allowing a user device to dynamically select alternative wireless access technologies to support 5G, based on network conditions and on the specific QoS requirements dictated by the application. In 5GMED two different solutions will be developed and validated, namely, the ACS-GW and the V2X gateway. The former will be adopted for train-to-track communications and will manage 5G NR, 70 GHz IEEE 802.11ad and VSAT, whereas the latter will be employed for vehicular communications and will handle 5G NR and ITS-G5/C-V2X connections.
- **Edge resources**, representing the collection of servers and computing machines deployed in the proximity of the terminals with the goal of minimizing the latency experienced by the end users as well as offloading the transport network, since the data packets do not need to reach remote servers or the Internet.
- **Cloud resources**, representing more computing, memory and storage capacity located far away from the end users. In 5GMED, the cloud will be private as in the case of the computing resource located in the Cellnex lab in Castelloli, and public, as with UC1 where VALEO relies on AWS (Amazon Web Services).

For the sake of claritiy, the structure of the rest of this section is here summarised:

- Section 2.1.1 describes the Spanish and the French 5G network, consisting of the access network, the transport network and the core network.
- Section 2.1.2 describes the 70 GHz train-to-track wireless system that will be employed only on the Spanish railway stretch.
- Section 2.1.3 describes the satellite access for the train.
- Section 2.1.4 describes the V2X roadside units (RSU) employed only on the Spanish highway stretch.
- Section 2.1.5 presents the edge and cloude nodes and explains how the MEC nodes can be connected with the 5G gNBs.

2.1.1. 5G network

The 5G network employed in 5GMED is structured as follows:

- **Spanish 5G network**, consisting of a Spanish 5GC connected to the following radio access networks:
  - Vodafone 5G RAN, comprising four gNBs in the stretch between Figueres and the French border
  - Cellnex 5G RAN, comprising two gNBs in the stretch between Figueres and the French border, required to fill the regions not covered by the Vodafone RAN
  - Cellnex 5G small cell, deployed at a self-sustainable site to provide extra coverage in an area not served by the 5G gNBs (= macro-cells)
- **French 5G network**, consisting of a French 5GC connected to the following radio access networks:
  - Cellnex France 5G RAN, comprising eight cell sites in the stretch between the Spanish border and Perpignan
  - Cellnex France in-tunnel 5G RAN, comprising a number of sites inside the Perthus railway tunnel

In the following, a more detailed description of the employed equipment, the geographical locations and the connectivity solutions is provided.

2.1.1.1. Spanish 5G network

The Spanish 5G network is illustrated in Figure 3 and consists of three building blocks: 5G RAN, transport network and 5GC network.

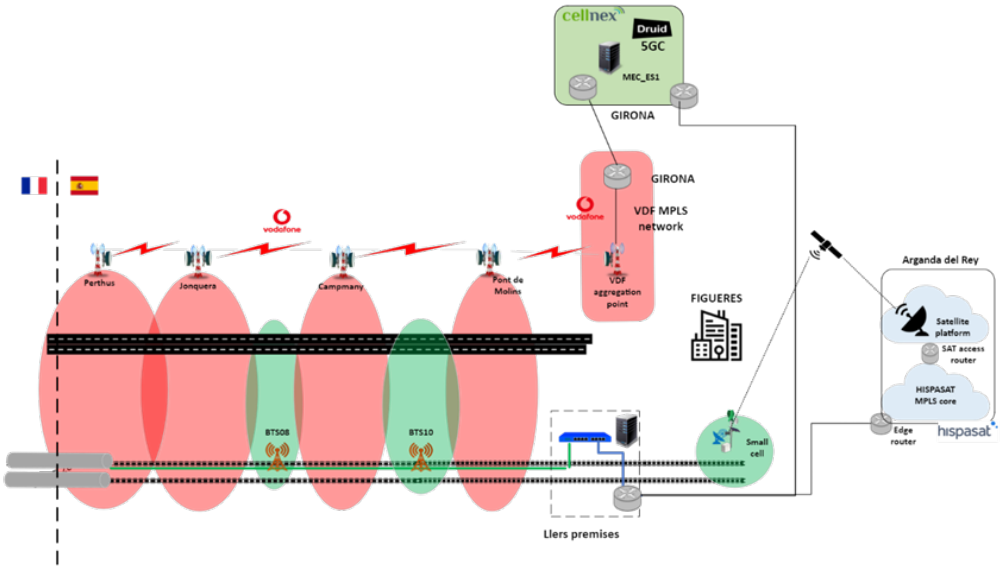


Figure 3: The Spanish 5G network consisting of different RANs.

<u>Radio Access Networks</u>

The 5G RAN is split into the section managed by Vodafone and the section managed by Cellnex. In the figure above, the red cells denote the coverage provided by the Vodafone gNBs, whereas the green cells denote the coverage provided by the Cellnex gNBs.

Vodafone is deploying four 2-sector gNBs along the last 25 kms of the AP-7 highway between Figueres and the French border, whose locations are reported in Table 1. Such 5G RAN will be specifically designed and optimized to obtain the maximum coverage along the highway, which is achieved by properly configuring the antenna azimuths. Nevertheless, further optimization will be carried out to provide coverage over the railway stretch based on the results obtained from a field measurement campaign. The 5G spectrum corresponds to the portion of the Spanish N78 band at 3.5 GHz assigned to Vodafone, spanning between 3.710 GHz and 3.8 GHz.

Table 1: List of Vodafone sites hosting 5G gNBs.

VDF Site name	Coordinates (Lat., Long.)	No. sectors	Azimuth
Pont de Molins	42.46413742118243, 2.8665932251858184	2	40º
			130º
Capmany	42.417557556543954, 2.8692692558649022	2	145º
			330º
La Jonquera	42.360310376150586, 2.902800509007647	2	0º
			160º
El Pertus	42.314868524811615, 2.9282025348743064	2	180º
			310º

Funded by the Horizon 2020 Framework Programme of the European Union

The gNBs will be supplied by Ericsson and will consist of two modules connected through a Common Public Radio Interface (CPRI) fiber optic cable:

- Ericsson BB6648, which is a Base-Band Unit (BBU),
- Ericsson AIR 6449, which is a Remote Radio Unit (RRU).

Figure 4 shows the location of both of the modules within a Vodafone site. The BBU is located inside a ground cabinet, while the RRU is installed on top of the tower.

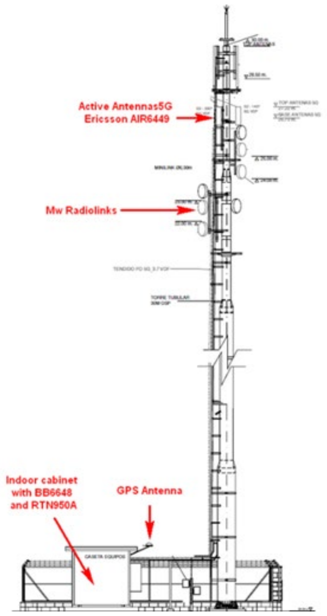


Figure 4: Structure of one of the VDF sites.

Table 2 lists the technical specifications of the Ericsson BB6648 BBU.

Table 2: Technical specifications for the Ericsson BB6648 BBU.

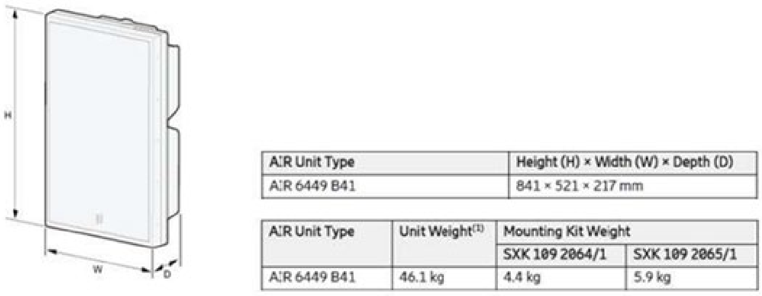
Feature	Description
Maximum throughput	Downlink: 10-15 Gbps Uplink: 3 Gbps
Interfaces	Support for CPRI and eCPRI x12 RI ports (SFP28) 3 + 1 TN and IDL optical ports 3x 25Gbps ports, 1 QSFP 4x 25 Gbps 1 electrical TN port LMT port + USB port for simplified O&M Sync port
Alarms	8 external alarms
Weight	Approx. 7.5 kg (including fans)
Size	Height = 44 mm, Width = 483 mm, Depth = 313 mm

Table 3 presents the technical specification of the Ericsson RRU.

Table 3: Technical specifications for the Ericsson AIR6449 RRU.

Feature	Description
Advanced Antenna System (AAS)	Comprising an AAS radio (integrated hardware unit with antenna array) and multi-antenna features, including adaptive beamforming and MIMO
Massive MIMO configuration	64TX/64RX with 192 antenna elements
Number of supported layers	Downlink: 16 Uplink: 8
Mechanical tilt	Set to 0º because the AIR6449 has electrical tilt and the vertical bandwith can also be remotely modified
Transmit power	Up to 320W (band-dependent) The maximum output licensed power is 180W for the 90-MHz bandwidth (2W/MHz)
Supported bandwidth	Maximum total carrier bandwidth is 200 MHz (5G NR) In 5GMED the VDF 5G spectrum consists of 90-MHz continuous bandwith (3710-3800 MHz)
Interfaces	4 x 25 Gbps eCPRI
Power voltage	48 VDC (3-wire or 2-wire)
Operating Temperature	-40 to +55°C

Figure 5 shows a picture of the active antenna unit indicating dimensions and weight.



AIR Unit Type	Height (H) × Width (W) × Depth (D)
AIR 6449 B41	841 × 521 × 217 mm

AIR Unit Type	Unit Weight(1)	Mounting Kit Weight	
		SXK 109 2064/1	SXK 109 2065/1
AIR 6449 B41	46.1 kg	4.4 kg	5.9 kg

Figure 5: Picture of the Ericsson AIR6449 active antenna.

Cellnex will deploy two gNBs to fill the coverage holes generated by the Vodafone RAN. Figure 6 (left side) illustrates a simulation coverage considering two sites owned by LFP, i.e., BTS08 and BTS10, which are located next to the Vodafone gNB Capmany. The two sites are well located to fill the coverage holes generated by the Vodafone 5G network, as shows in the right side of the same figure. The blue colour indicates the coverage threshold which is set to -115 dBm. Further assessment will be necessary to optimise the coverage and to make sure that both the highway (green line) and railway (red line) are properly served. Table 4 also provides a list of parameters used to simulate the 5G coverage. It is worth pointing out that such gNBs cannot radiate on the Vodafone N78 band due to

Funded by the Horizon 2020 Framework Programme of the European Union

operator policies which prevent other partners from using that frequency. For ths reason, the portion of the 5G spectrum will be assigned by the Spanish frequency regulator and will consist of a certain amount of bandwidth at the N77 band, which does not interfere with the Vodafone N78 band.

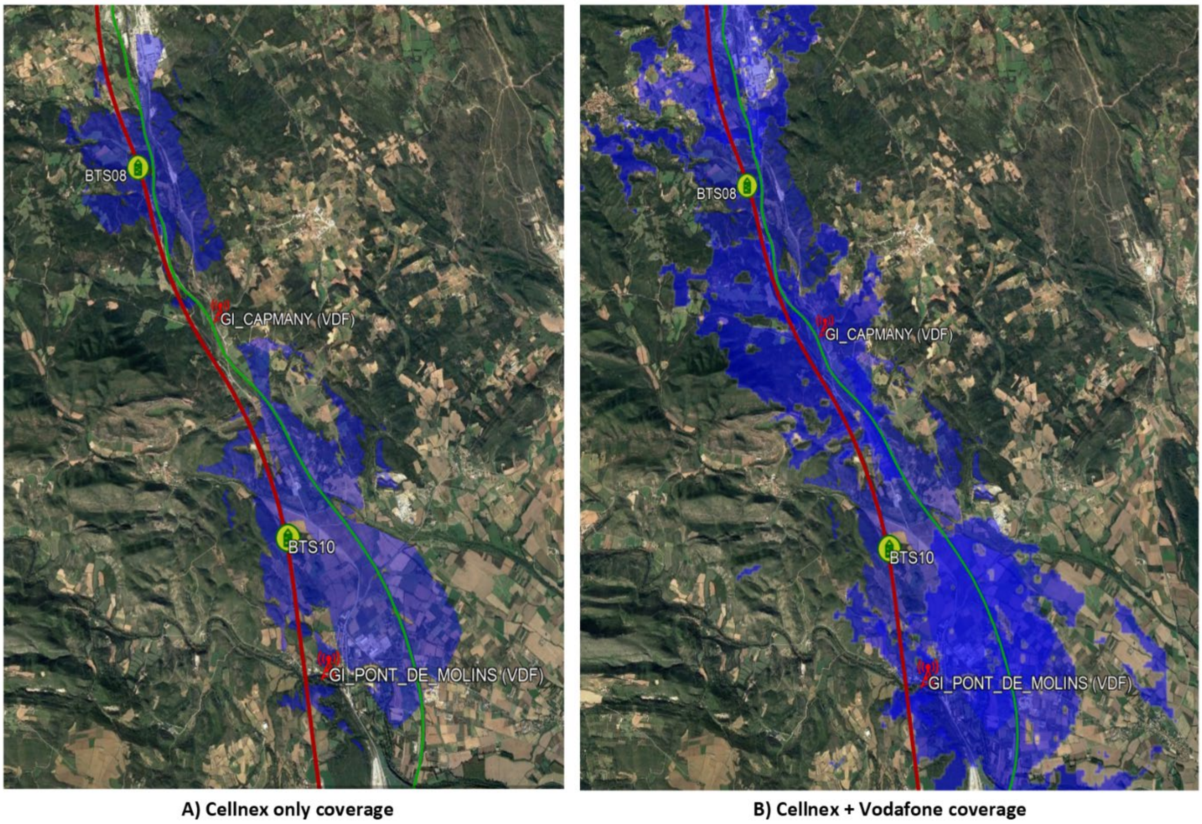


Figure 6: Simulation coverage with and without the Vodafone sites.

Table 4: Simulation parameters for the coverage provided by two gNBs deployed at the LFP sites (BTS08 and BTS10).

Parameter	Value
GPS coordinates	BTS08: lat. 42°22'50.58"N, long. 2°52'57.40"E BTS10: lat. 42°19'47.95"N, long. 2°55'9.83"E
Tower height	30 metres
Azimuths	BTS08: 116°, 152°, 348.0° BTS10: 57°, 116°, 343°
Transmit power by beam	40 W
Frequency	3.5 GHz
Antenna gain	17 dBi
Propagation model	ITU-R 1546

Cellnex will also install a 5G small cell in a self-sustainable site that will be deployed in a location next to the railway where the gNBs cannot ensure coverage. The objective of this solution is to provide alternative solutions for deploying sites in rural areas, where the conditions do not allow a quick installation of new equipment and the power grid is unavailable. Figure 7 shows the self-sustainable site with the small cell within the red box.

Figure 7: A picture of the self-sustainable featuring a 5G small cell.

Transport network

The Spanish 5G RAN will be connected to the 5GC through a transport network consisting of two different solutions: microwave links for the Vodafone sites and optical fibre for the Cellnex sites.

The equipment used for the microwave links between the four Vodafone gNBs is a Huawei RTN950A.

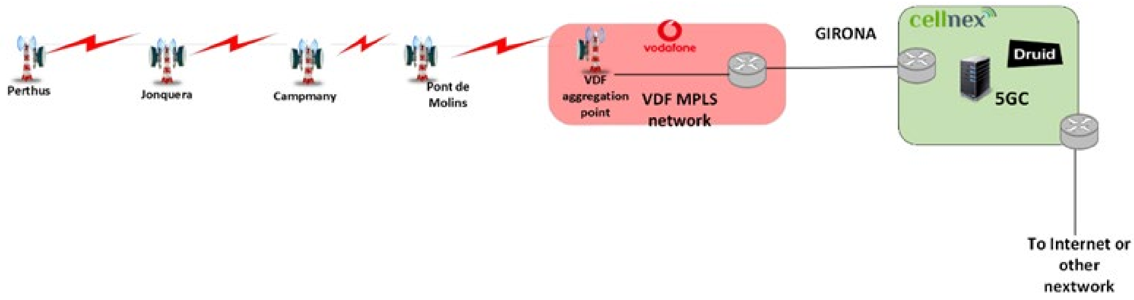


Figure 8: Transport network employed for the Vodafone RAN.

The TX configuration of each radiolink is 4+0 Cascade EPLA (Enhanced Physical Layer Aggregation) with capacities in each hop between 1 Gbps and 1.5 Gbps. EPLA is a Layer-1 link aggregation group technology capable of sharing load according to the bandwidth at physical layer. The full list of specifications of the Huawei unit is shown in Table 5.

Table 5: Technical specifications for HUAWEI RTN950A [2].

Feature	Description
Frequency carrier	6-42 GHz
Channel spacing	3.5/7/14/28/40/56/112 MHz
Modulation scheme	QPSK Strong, QPSK, 16QAM Strong, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM, 512QAM, 512QAM Light, 1024QAM, 1024QAM Light, 2048QAM, 4096QAM
Air interface capacitiy	1166 to 2500 Mbit/s per carrier
Interfaces	E1, STM-1 (e/o), FE (e/o), GE (e/o), 2.5GE (o) , 10GE (o)
Security	Provides AES-256 encryption and anti-theft to ensure high security
Header compression	Supports unique four-layer Ethernet frame header compression to provide a large throughput for IP services.
Link aggregation	Up to 8-channel enhanced physical link aggregation (EPLA) and load sharing for high-level granularity traffic.
Ethernet functions	• Ethernet ll, IEEE 802.3, and IEEE 802.1q/p service format adding or deleting, and exchange VLAN tags (IEEE 802.1q/p) • ISIS, OSPF, BGP, RSVP, LDP • Flow control (IEEE 802.3x) • Link aggregation groups (IEEE 802.3ad LAG and L1 LAG) • RMON (IETF RFC 2819)
Synchronization	Ethernet synchronization and full IEEE 1588 V2 (TC/OC/BC) provide high quality eLTE backhaul networks

As shown in Figure 8, the 5G traffic originated from or directed to the Vodafone gNBs is carried over the microwave links and aggregated in a remote Vodafone site located near the city of Figueres. This is the entry point to the Vodafone Multi-Protocol Label Switching (MPLS) network. It allows forwarding the packets to any location belonging to Vodafone. As the 5GC will be provided by Cellnex and to minimize the transport network latency, Vodafone and Cellnex agreed to interconnect their respective networks in a site of the city of Girona.

On the other hand, the two Cellnex sites (BTS08 and BTS10) can take advantage of the existing optical fibre running along the railway. As the LFP optical network is classified as critical infrastructure, the 5GMED consortium is not allowed to use the resources allocated to railways services. As a result, a new optical backbone network has to be built at the LFP premises. Such infrastructure will rely on two optical fibres running between the Llers campus in Spain and the outskirts of Perpignan in France, which were already deployed to make the LFP network more redundant. The pair of fibres will then be segmented in order to provide physical connectivity to any IT equipment, including MEC servers and base stations. The detailed network topology design will be reported in D3.3.

shows the transport network deployed for the two Cellnex gNBs, i.e., BTS08 and BTS10. The green line represents the optical fibre available for 5GMED, which connects the towers to the Llers maintenances premises. The traffic reaches an optical switch and is then forwarded to the Internet or other networks.

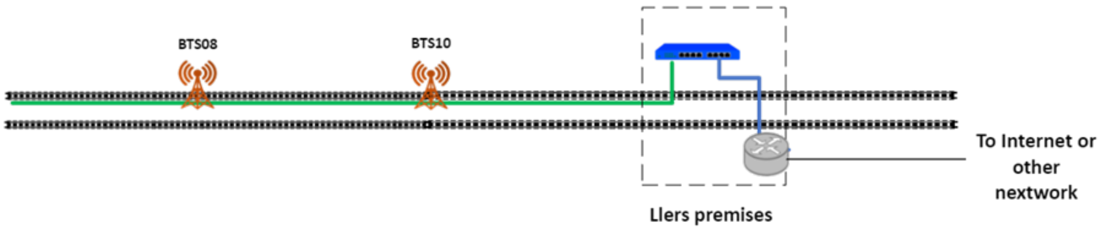


Figure 9: Transport network employed for the BTS08 and BTS10.

The optical fibre is supplied by Draka and belongs to the single-mode class. It complies with a wide range of standards, such as ITU-T Recommendation G.652.B [3] and IEC International Standard 60793-2-50 [4]. The Draka fibre presents low attenuation and dispersion and is highly efficient for the O-band (1260-1360 nm), C- and L-band (1530-1625 nm). Furthermore, the fibre is fully compatible with other fibres in terms of transmission, connections, and installation tools. It is also easy to strip through both mechanical and heating techniques. Table 6 shows the fibre technical specifications.

Table 6: Specifications of the Draka optical fibre [5].

Attenuation		
@ 1310 nm	0.33 – 0.35 dB/km	
@ 1383 nm	1 dB/km	
@ 1550 nm	0.19 – 0.22 dB/km	
@ 1625 nm	0.21 – 0.24 dB/km	
Attenuation vs wavelength (Maximum attenuation change over the window from reference)		
Wavelength range (nm)	Reference λ (nm)	(dB/km)
1285 - 1330	1310	<= 0.03
1525 - 1575	1550	<= 0.02

1550 - 1625	1550	<= 0.03	
Attenuation with bending			
Number of turns	Mandrel Radius (mm)	Wavelength (nm)	Induced Attenuation (dB)
100	25	1310	<= 0.05
100	25	1550	<= 0.05
100	30	1625	<= 0.05
Chromatic dispersion			
Wavelength (nm)		Chromatic dispersion (ps/[nm.km])	
1285 – 1330		<= 0.03	
1550		<= 18.0	
1625		<= 22.0	
Zero Dispersion Wavelength (λ0):		1300 – 1322 nm	
Slope (S0) at λ0:		<= 0.090 ps/(nm2.km)	
Geometrical specifications			
Cladding Diameter		125.0 ± 1.0 µm	
Core/Cladding Concentricity Error		<= 0.6 µm	
Cladding Non-Circularity		<= 1.0 %	
Fiber Curl (Radius)		>= 4 m	
Coating Diameter		242 ± 7 µm	
Coating/Cladding Concentricity Error		<= 12 µm	
Coating Non-Circularity		<= 5 %	
Length		Standard lengths up to 50.4 km	

As mentioned before, Cellnex will also deploy a 5G small cell on a self-sustainable site. Such gNB will be connected to the 5GC through a satellite backhaul. It should be noted that the objective of this backhaul will be to provide an alternative connectivity solution for the delay-tolerant services of railways use case (UC3) since the availability of optical fibre or radio links may not be always guaranteed in rural and isolated areas along the corridor.

The **satellite backhaul** will employ the Ka-band (27–40 GHz) through a VSAT-based system. VSAT is a dual-way ground station with a small antenna and is used to transmit and receive the data to and from the satellite [6].

Figure 10 shows an end-to-end satellite backhauling system consisting of the following blocks:

- **Small cell** – the system requesting a backhaul service. In 5GMED, a 5G small-cell will be connected to a remote 5GC through the satellite backhaul.
- The **InDoor Unit (IDU)** – it is the satellite receiver and router which may embed some networking functions, including routing, encryption, compression, acceleration and QoS (traffic shaping, VLAN tagging, etc.). The IDU contains the following components:
  - The Modulator/Demodulator (MUX/DEMUX)
  - Satellite modem

- **OutDoor Unit (ODU)** – it is the unit allowing the terminal to transmit and receive signals to and from the satellite. It usually consists of:
    - Antenna operating in the selected band, for example, Ka-band.
    - Standard L-band Low-Noise Block (LNB) for the receiving signal. The LNB converts the RF band signal received from the satellite into an L band signal (IF band).
    - Block-Up Converter (BUC).The transmitter converts the frequency (IF to RF) that is received from the modulator and passes to the power amplifier for further amplification and transmission.
    - OMT (Orthomode Transducer). It is used to combine and/or to separate the transmission and reception signal paths to the different ports. Together with the feed horn, they form the end/start part of an antenna and aid to transfer electromagnetic signals into the air.
- **InterFacility Link (IFL)** - a cable that is used to connect an ODU and an IDU. For L band, 75 Ω impedance cables with F connectors are typically used.
- **Satellite** - The satellite Konnect provides broadband internet and communications coverage to Europe and Sub-Saharan Africa. The baseline mission is to provide 75 Gbps of capacity across a network of 65 spotbeams in Ka band. The satellite will address direct-to-user consumer and enterprise broadband services using dishes from approximately 75 cm. It will also be used for community networks connected to Wi-Fi hotspots, mobile phone backhauling, and rural connectivity.
- **Teleport** – The teleport is a ground station responsible for the communication with the satellite, for route planning and tracking, and for retrieving telemetry and any relevant data. In 5GMED, HSP will employ the teleport of Arganda del Rey (Madrid, Spain), which can be considered the gateway of all the incoming and outgoing traffic transferred via the satellite backhaul.

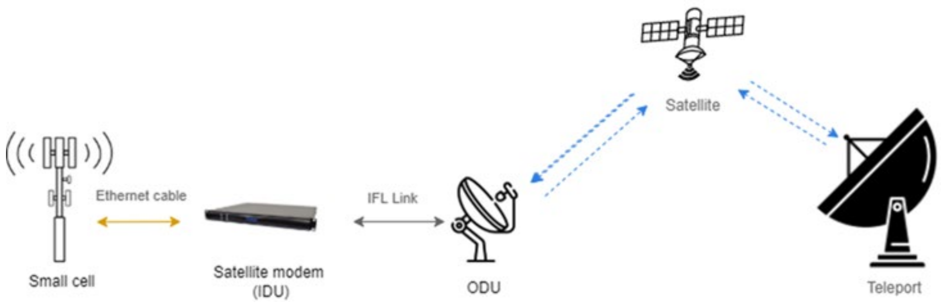


Figure 10: Satellite modem and related components.

The IDU selected for 5GMED is a Hughes HT2524, which is a powerful satellite router designed for Cellular Backhaul applications for 2G, 3G, 4G/LTE, and 5G networks. It is designed to accelerate 4G/ LTE traffic and to support high bandwidth applications, such as IP-trunking [7]. The HT2524 features integrated GTP acceleration, which can handle as many as 16,000 TCP sessions between an eNodeB and the 4G/LTE core and provide better network utilization due to the higher efficiency with typical CAPEX savings of 60%. Thanks to the hardware developments and improved efficiencies, this system supports the most demanding enterprise applications, such as data trunking, VoIP, SIP, VPN, Remote Database Administration, or IoT. The HT2524 satellite modem provides Internet service by connecting a computer to a Ka-band bent-pipe satellite network. The modem features a small desktop chassis with 4 GigE LAN port and two cable IFL for interface to the ODU.

The specifications for the HT2524 modem are listed in Table 2.

Table 7: HT2524 modem specifications.

Item	Specifications
Weight	3.72 Kg
Height	4.5 cm (1RU)
Width	48.26 cm (1RU)
Depth	38.74 cm (1RU)
Operating temperature range	0 °C to 50 °C Above 1524 m altitude, the maximum temperature is reduced by 1 °C per 305 m.
Operating humidity range	5% to 77% (non-condensing)
Altitude	Up to 4572 m
Protocol support	TCP/IP (Transmission Control Protocol / Internet Protocol) protocol suite
Supported frequency ranges	Ka-band
L -Band	TX: 950–2400 MHz RX: 950–2150 MHz
Network interface ports	4 GigE LAN ports
Maximum power consumption	75 W

The mechanical and environmental performance of the antenna is shown in Table 3.

Table 8: VSAT antenna performance.

Mechanical Performance	
Reflector Material	Steel
Antenna Optics	One-Piece Offset Feed Prime Focus
Mast Pipe Size	60 mm diameter
Elevation Adjustment Range	5°- 90° Continuous Fine Adjustment
Azimuth Adjustment Range	360° Continuous Course Adjustment ± 10° Fine Adjust
Environmental Performance	
Wind Loading Operational	80 Km/h
Wind Loading Survival	201 Km/h
Temperature (operational)	-40 °C to +60 °C
Relative Humidity	0 to 100% with condensation
Solar Radiation	360 BTU/h/ft^2

In order to find the best size antenna for backhaul satellite in 5GMED, a preliminary link budget analysis has been performed assuming the MIR (Maximum Information Rate) as a requirement, with 10.92 Mbps of uplink channel as target. Figure 11 shows simulations of the terrestrial coverage that the satellite would have for a 10.92 Mbps uplink channel with different antenna sizes, concluding that the configuration A), i.e., a 120 cm antenna and a 3W user terminal is the optimal which ensures the total coverage of Spain and specifically the 5GMED corridor with the required performance.

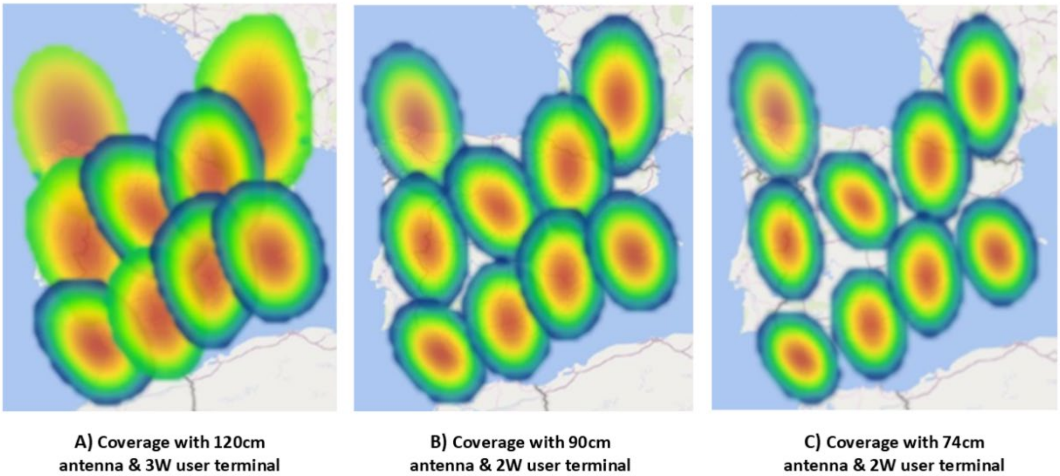


Figure 11: Spanish coverage simulation for three different VSAT configurations.

5GC Network

The Spanish 5G network will feature a 5GC supplied by Druid, a software development company specialized in 4G/5G private network solutions. More details of the 5GC features are provided in D3.1 Section 4.2 [1]. The 5GC will be hosted in a server located in a Cellnex site of the city of Girona. Figure 12 gives a high-level overview of how the Spanish 5G access network can be broken down into three elements, including the Vodafone gNBs, the Cellnex gNBs and the Cellnex 5G small cell installed on the self-sustainable site. Such network segments will be connected through different backhaul solutions to the 5GC hosted in a Cellnex building in Girona.

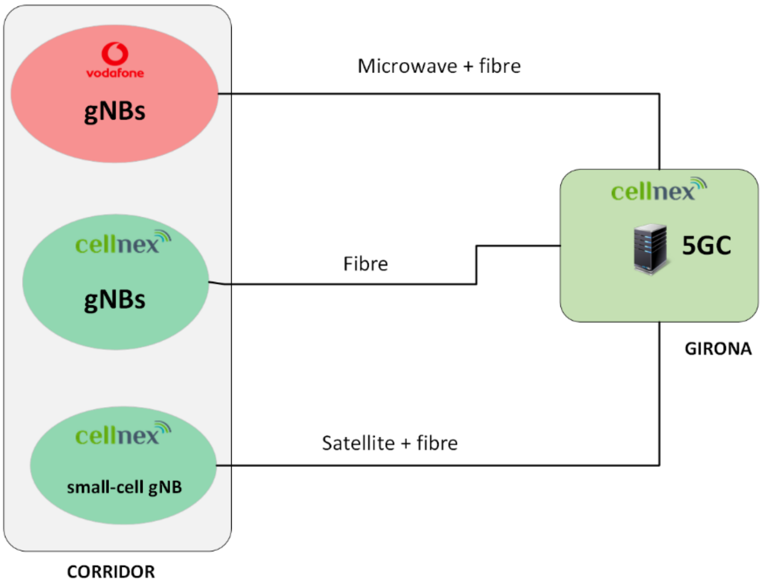


Figure 12: High-level overview of the connections between Spanish RANs and 5GC.

2.1.1.2. French 5G network

In the French side of the corridor, Cellnex France will deploy a 5G RAN at 3.5 GHz with the support of a French MNO. Table 9 reports the candidate sites for the deployment of the 5G RAN in France. Each row specifies the GPS coordinates of the site (in latitude and longitude) and gives a preliminary estimation of the required hardware, such as the number of base-band units and the number of radio units. Such estimation has been made by taking into account the preliminary results of a simulation coverage performed by Cellnex France. Further adjustments will be made based on the analysis of the vendor selected for the deployment[2].

Table 9: Details of the candidate French sites.

5GMED site ID	Internal site ID	Latitude	Longitude	Azimuth (in degrees)	No. BBU	No. radios
FR-gNB-1	660289	42.640	2.8572	9 & 180	1	2
FR-gNB-2	FR-66-900050	42.687	2.8139	75	1	1
FR-gNB-3	1667825	42.627	2.8309	150 & 330	1	2
FR-gNB-4	BTS02	42.594	2.8491	0 & 175	1	2
FR-gNB-5	BTS03	42.491	2.8352	305 & 130	1	2

[2] At the time of writing, NOKIA is the candidate vendor for the French RAN deployment.

FR-gNB-6	BTS04	42.646	2.8209	346 & 160	1	2
FR-gNB-7	517648	42.559	2.8513	0 & 175	1	2
FR-gNB-8	FR-66-900034	42.476	2.8658	280 & 180	1	2

A first coverage simulation conducted by Cellnex France is shown in Figure 13, where the red line denotes the railway and the green line the highway. The simulation parameters are presented in Table 11. Note that the colours employed indicate the signal strength threshold as reported in Table 10.

Table 10: Colours and meaning for the 5G simulation coverage.

Colour	Signal strength range and meaning
Green	[-85, -108] dBm (good coverage)
Yellow	[-109, -118] dBm (sufficient coverage)
Red	[-119, -123] dBm (bad coverage)
Blue	[-124, -143] dBm (very bad coverage)

It is worth noting that:

- The north-centre area presents an overall good coverage although the signal strength is not uniform due to the impact of the orography. There is no perfect overlap of the green zones, while a coverage hole affects the highway in the south suburbs of the city of Perpignan.
- The south-west area has no coverage due to the lack of a site nearby the village of Le Boulou. This issue will need to be further assessed since it would heavily affect users travelling along the highway.
- The area next to the Spanish border (bottom) presents extremely irregular coverage due to the orography and the vegetation impacting on the signal strength received by highway users. Specifically, the site number 8 is located on top of a hill surrounded by trees which heavily hamper the connectivity. As a result, an alternative solution will have to be investigated with the help of a 5G equipment vendor.

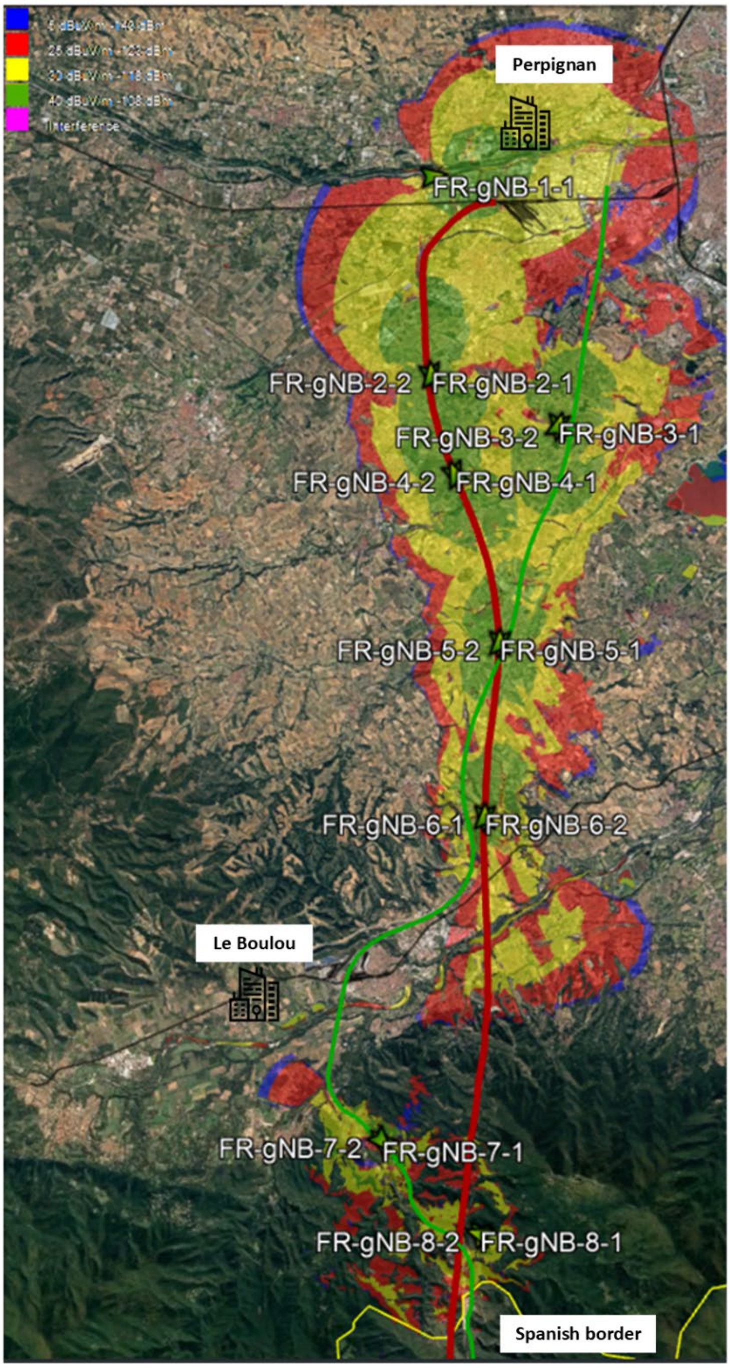


Figure 13: Simulation coverage for the French 5G RAN between Perpignan (top) and the Spanish border (bottom).

Table 11: Simulation parameters employed.

Parameter	Value
Tower height	18 metres
Transmit power by beam	40 W
Frequency	3.8 GHz (bandwidth: 70 MHz)
Antenna gain	17 dBi
Propagation model	ITU-R 1546

As for the transport network between 5G RAN and core network, Cellnex France is also investigating the best solution to provide backhauling. Being this area mostly rural, a transport network based on microwave links appears to be the most suitable solution. Nevertheless, this will require further analysis.

The Perthus tunnel 5G RAN

As the railway crosses the border through an 8-km tunnel below the Perthus mountain, an ad-hoc indoor solution for providing connectivity to the train will be required. Figure 14 shows the geographic location of the tunnel denoted by the north entrance (French side) and the south entrance (Spanish side). It is worth pointing out that the majority of the tunnel sits on the French soil as it can be seen in the figure, where the yellow line denotes the country border. As a result, the indoor spectrum usage will be subject to the French regulation given that the radio signal spill-over effect is unavoidable and will likely be able to cover the small Spanish section of the tunnel. Further evaluation and assessment will be necessary to analyse the impact of the spill-over effect.

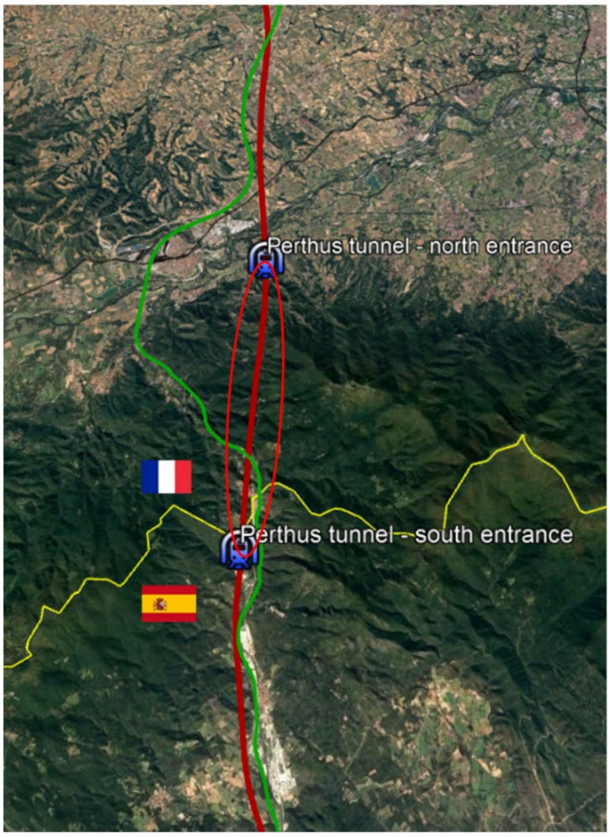


Figure 14: Geographical area of the railway tunnel crossing the two countries.

Cellnex France and Cellnex Spain are currently seeking the best solution to provide 5G connectivity at 3.5 GHz inside the tunnel for high-speed trains travelling at 300 Km/h. Given the big technical challenges of such deployment, the partners will be supported by a leading 5G vendor. Specifically, a technical discussion is in place with NOKIA which has the technical know-how and the relevant experience in this field.

5GC Network

As with the Spanish side, the French 5G network will feature a 5GC supplied by Druid. The 5GC will be hosted in a server located in one of the LFP facilities along the railtrack. Figure 15 gives a high-level overview of the French 5G system, highlighting the connections between the 5GC and the 5G RAN. As mentioned before, the tunnel features fibre that will connect the indoor 5G base stations to the 5GC. On the other hand, the outdoor gNBs may need microwave or fibre backhaul depending on the site availability.

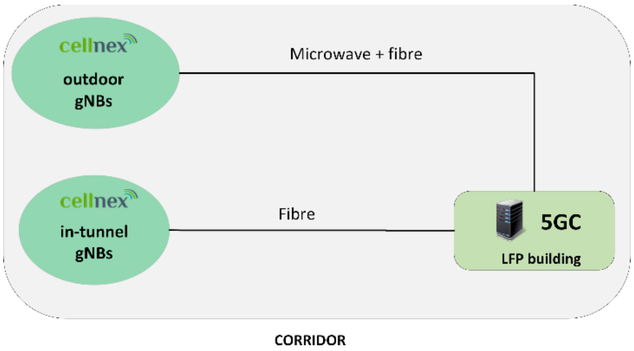


Figure 15: High-level connections between the French 5GC and RANs.

2.1.2. 70-GHz train-to-track

The 70 GHz train-to-track network is a communication system specifically designed for railway environments. The general concept for a mmWave train-to-track system is shown in Figure 16. It consists of a set of trackside units or access points (APs) deployed on trackside poles. These APs will establish a radio connection with two radio units on-board the train. As a result, the train will be able to access multiple radio connections for improved throughput and reliability. These units will operate on the unlicenced 57-71 GHz millimetre wave band.

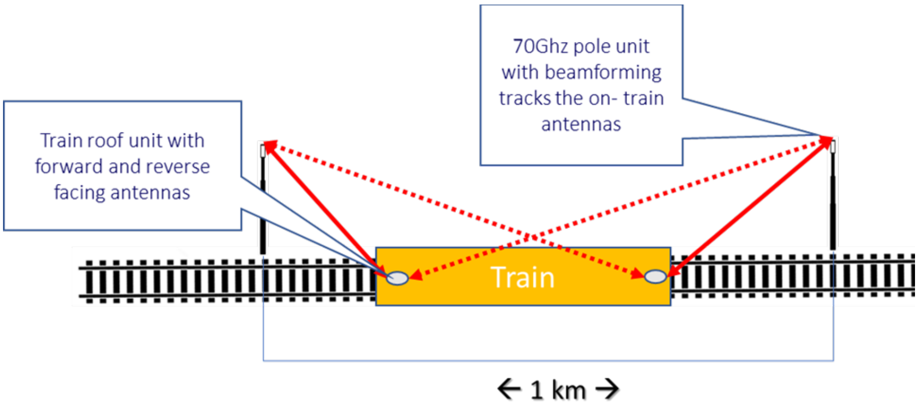


Figure 16: 70 GHz IEEE 802.11ad train-to-track system concept (pole-to-pole distance is 1 km).

It should be noted that active beamforming is needed to maintain direct line of sight connections from the trackside units to the on-board radios. The air interface is based on extended IEEE 802.11ad protocol for mobility and extended services set [8].

<u>Trackside radio units:</u>

The track radio units will be deployed on poles attached to railway stanchions along the track side. Two types of stanchion posts are available in the corridor: lattice and solid post.

On the opposite side of the pole stanchion mounting, a cabinet will house an AC to DC converter and a 16-way Fibre ODF (Optical Distribution Frame) to terminating the fibre.

Table 12 summarizes the trackside units' technical specifications.

Table 12: Specifications of the 70 GHz APs.

Characteristics	Details
Radio	- Dual 57-71GHz mmWave radio (180º separation) - IEEE 802.11ad with infrastructure extensions MCS0 to MCS12.5 (64QAM) modulation - Supports all six IEEE 802.11ad channels (lower attenu-ation in channel 5 and 6)
Networking	- Internal SPF+ receptacles providing flexible support for fibre backhaul and pass-through. - Network fibre port 10G Ethernet
Applications processor	- Quad-core 1800 MHz ARMv8 CPU - Linux OS with user-space networking
Environmental	- Ambient temperature -25°C to +45°C - IP66 Protection
Power & Power consumption	- 20V to 48V DC (internally isolated) - Nominal: 42 Watts - Maximum: 55 Watts
Mechanical	- Height 296 mm; Length 170 mm; Width 83 mm - Weight 3.9 Kg

Train radio units:

The radio equipment needed in the train is described in deliverable D5.1 section 2 [9].

Locations and coverage:

The deployment will provide approximately 17.5 Km of high-bandwidth coverage from the entrance/exit of Le Perthus tunnel towards the LFP Maintenance Depot (LFP Le Perthus Base de Mantenimiento) in Llers, close to Figueres. The trackside radio units are labelled from AP-1 to AP-15, where AP-1 the closest unit to Le Perthus Tunnel.

Figure 17 shows the track segment that will be covered by the on-track units. This information is compiled after a first site survey, in order to obtain the information needed to prepare the corridor to locate the poles, assess the required power and determine the fibre needed to compose the backhaul. This is the optimum location to ensure that multiple mmWave associations are maintained for peak throughput and resilience.

Figure 17: Map of the 15 trackside radio APs.

The backhaul will consist of a 16-core single-mode fibre bundle running between the pole locations and one central switch located in the LFP maintenance building in Llers. Each AP will connect directly to the central switch at Llers, while a single strand of fibre will be dropped at each pole for AP connectivity, and all remaining fibres will be spliced through for further connection.

The 70 GHz network equipment in the LFP maintenance building in Llers consists of the following components:

- **Fiber optic distributor**. Terminals trackside fibre network and local connection to the 10 Gbps Fibre Switch
- **10 Gbps Fibre Switch**, combining the multiple data-streams from the different APs in a single data-stream received from one train unit
- **Aggregation Server**:
    - It recombines the multiple flows from the different train units in a single data-stream.
    - Traffic from/to train is encrypted/de-encrypted in the aggregation units (on-track and in-train)
    - Interfaces at 10 Gbps with a firewall.

- **Firewall**:
  - It provides a secure gateway and remote access termination to the 70 GHz mmWave network
  - It connects the 70 GHz network to the 5GMED aggregation switch node at 10 Gbps (the same point of interconnection of the other technologies will use for this purpose).

Figure 18 presents the section between AP-10 and AP-11 with the mounting stanchion and expected up/down line view.

Figure 18: Section between AP-10 and AP-11.

2.1.3. Train satellite access

Besides the 5G small-cell backhaul, satellite connectivity will also be employed as onboard radio access technology for the train. The end-to-end architecture is similar to the backhaul use case presented in Section 2.1.1.1, except for two differences:

- The VSAT is installed on top of the train roof and is capable of tracking the satellite beam as the train travels along the railtrack (more details on this solution can be found in D5.1 [9]).
- The satellite modem will be configured as a terminal device, thus any parameters related to the backhaul support, including GTP acceleration and header compression, will be disabled.

Figure 19 shows the the high-level architecture of the train satellite access solution.

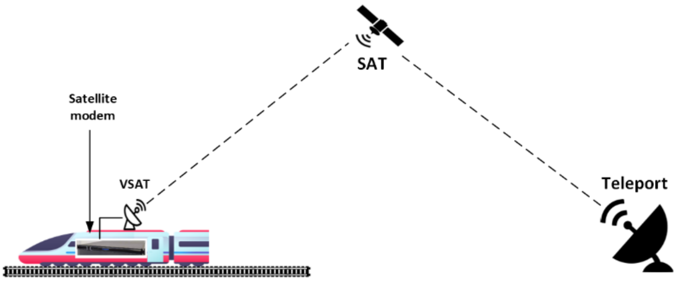


Figure 19: End-to-end architecture for the train satellite access.

2.1.4. Roadside infrastructure

A certain stretch of the Spanish highway running between the city of Figueres and the French border will be equipped with V2X roadside units (RSUs) providing connectivity to vehicles through short-range wireless technology, i.e., ETSI ITS-G5 [10] and 3GPP C-V2X [11].

The product selected for the 5GMED infrastructure is the Neavia V2I outdoor RSU manufactured by Lacroix City, which is shown in Figure 20.

Figure 20: A Lacroix Neavia V2X outdoor RSU.

Figure 21 shows the connectivity options available on the RSU, namely, two N-type antenna connectors for the 5.9 GHz band, an SMA-type antenna connector for WiFi, an SMA-type antenna connector for Bluetooth, and a connector for Ethernet and PoE.

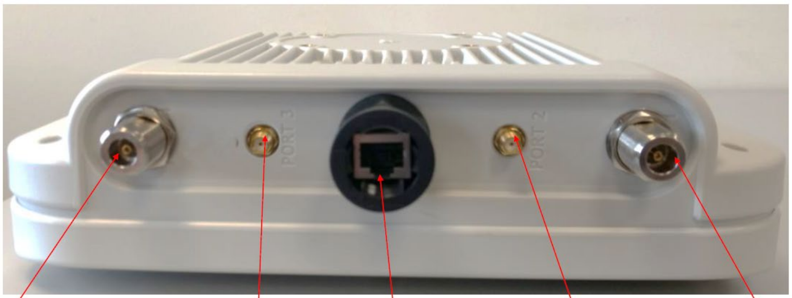


Figure 21: View of the physical connectors available.

A list of technical specifications of the RSU is reported in Table 13.

Table 13: Technical specs of the Lacroix RSU.

Radio	Protocol	TX Power	RX sensitivity	Channels	Supported bands
V2X	IEEE 802.11p	+23 dBm	-98 dBm	CCH + SCH	5.8 / 5.9 GHz
C-V2X	3GPP Rel-14 PC5	+23 dBm	-93 dBm	B47	5.8 / 5.9 GHz
GNSS	GPS, Glonass , Galileo, Beidou	N/A	-161 dBm	L1, E1, B1	1.575 GHz
Cellular	GSM/UMTS/LTE	+23 dBm	-110 dBm	B2, B3, B5, B8	850 / 900 / 1800 / 1900 / 2100 MHz
Wi-Fi	IEEE 802.11 b/g/n	+17 dBm	-96 dBm	1-13	2.4 GHz
Bluetooth	EDR 2.1 class 1	+17 dBm	-94 dBm	0-78	2.4 GHz

Furthermore, Table 14 lists all the European standards supported by the RSU.

Table 14: EU standards supported by the Lacroix RSU.

Common architecture	
Communications Architecture	ETSI EN 302 665 v1.1.1
Access layer	
Wireless Access in Vehicle Environment (ITS G5)	IEEE 802.11p ETSI EN 302 571 v2.1.1, ETSI EN 302 663 v1.2.1, ETSI TS 102 724 v1.1.1
DCC	ETSI TS 102 687 v1.2.1
Network & Transport layers	
Geonetworking	ETSI EN 302 636 4 1 v1.2.1
BTP	ETSI EN 302 636 5 1 v1.2.1
Facilities layer	

CAM	ETSI EN 302 637-2 v1.3.2 ETSI TS 102894-2 v1.2.1
DENM	ETSI EN 302 637-3 v1.2.2 ETSI TS 102894-2 v1.2.1
MAPEM	ETSI TS 103 301 v1.1.1 SAE J2735-2016 03
SPaTEM	ETSI TS 103 301 v1.1.1 SAE J2735-2016 03
IVIM	ETSI TS 103 301 v1.1.1 ISO TS 19321-2015 04 ISO TS 17425-2016 05
CPM	ETSI TR 103 562 v0.0.8
LDM	ETSI EN 302 895 v1.1.1
Security layer	
Security Architecture	ETSI TS 102 940 v1.3.1
Secured message and certificate formats	ETSI TS 103 097 v1.2.1
Privacy	ETSI TS 102 941 v1.1.1
PKI	ISE PKI
Applications layer	
I2I Communications Datex II (for RSU)	ESC/TS 16 157-1 2011 10 ESC/TS 16 157-2 2011 10 ESC/TS 16 157-3 2011 10 ESC/TS 16 157-4 2014 04 ESC/TS 16 157-5 2014 04 ESC/TS 16 157-6 2015 10

Figure 22 shows how the V2X RSUs will be connected to applications running on MEC servers or cloud premises. Specifically, each RSU will communicate with a 5G CPE (customer premises equipment) through Ethernet connectivity. The CPE is equipped with a 5G SIM card to access the 5G network at the Spanish side of the corridor and forward the V2X packets to external networks through 5G. This solution will allow to interconnect all the RSUs by providing end-to-end connectivity with V2X services at the edge or in the cloud, including the V2X gateway. It is worth pointing out that although 5G connectivity is meant to be available across the whole corridor, C-V2X will be employed to ensure that any potential 5G coverage hole will be filled and no service outage will be experienced by the user.

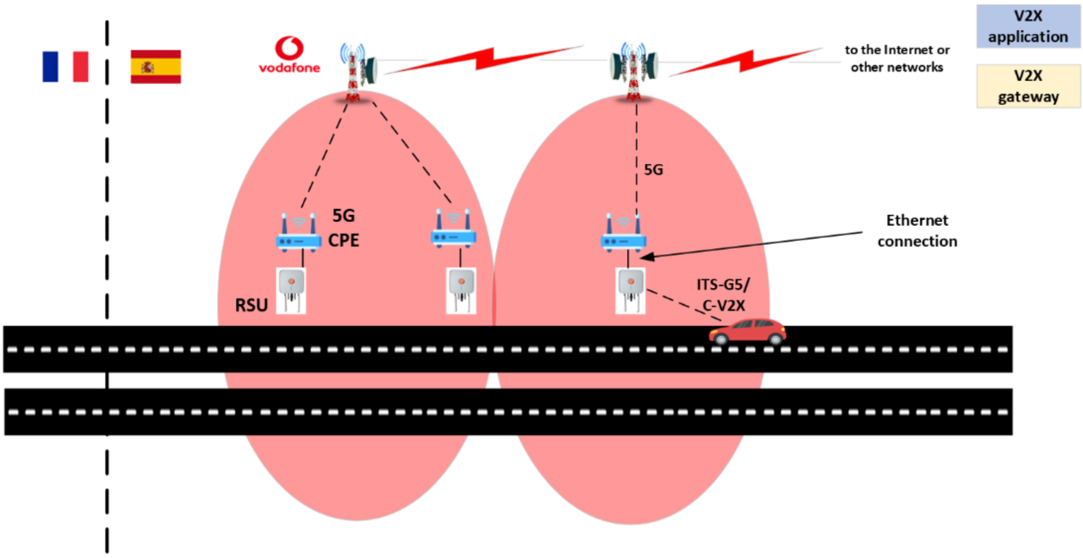


Figure 22: Overview of the connection of the RSUs with V2X services running in the edge/cloud.

2.1.5. Edge/Cloud nodes

The MEC layer represents the set of local resources, i.e., computing and storage capabilities, made available by edge servers located within a multi-stakeholder network with the characteristics that 5GMED project promotes. Originally, MEC refers to an ETSI standard [12] for mobile networks that later covered fixed and convergent networks. Unlike a centralized cloud computing architecture, MEC unlocks real-time information processing, reduces the application latency and increases reliability. Some examples of MEC services in 5GMED are:

- the V2X gateway, which processes and forwards V2X packets to other geographic regions.
- The obstacle detection function, which employs AI capabilities to interpret images and to identify potential obstacles,
- the local Traffic Management Control (TMC), which generates and disseminates appropriate traffic strategies in case of an accident, and
- the Follow-Me feature, reducing the distance between the Infotainment Edge Server and the end-user by moving the applications running on the edge servers, thus following the user movements.

Due to the stringent requirements of the use cases set out in 5GMED, the MEC layer plays a pivotal role in achieving adequate performance and fulfilling the Quality of Experience (QoE). Considering the very demanding latency requirement, a number of edge nodes will be deployed in the proximity of the cell sites, where sufficient space, power and connectivity can be guaranteed.

Figure 23 and Figure 24 show a possible MEC deployment for the Spanish side and the French side of the corridor, respectively, in line with latest ETSI's guidelines [13]:

1. **MEC at traffic aggregation point**: This is the case with the Vodafone 5G RAN since security concern prevents from installing MEC servers next to the cell sites. As a result, the 5G traffic has to be delivered to the Cellnex aggregation point and then reach the MEC server where a specific UPF will be running.
2. **MEC at the cell site**: This is only possible at cell sites owned by Cellnex. In this configuration, a MEC server will be installed next to the radio equipment and a dedicated UPF will process the 5G traffic and forward it to the MEC applications running on the same machine.

It is worth pointing out that such deployment flexibility can only be ensured by a specific 5GC feature called UPF distribution or UPF chaining, which allows to distribute multiple instances of the UPF, each one connected to the same core network.

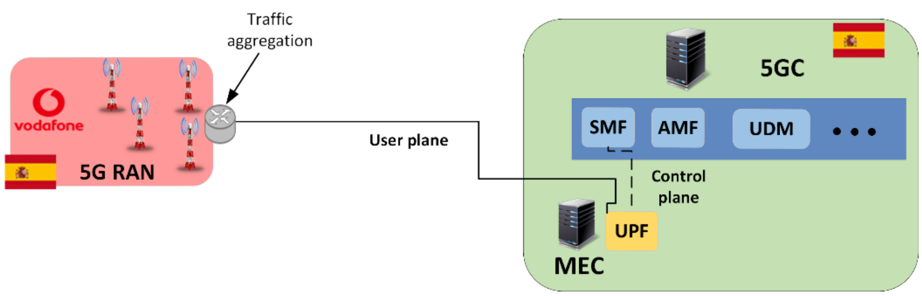


Figure 23: MEC deployment example for the Spanish 5G network.

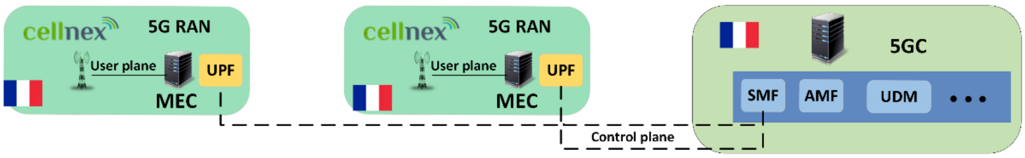


Figure 24: MEC deployment example for the French 5G network.

In 5GMED, three different models of Lenovo edge servers will be considered for deployment based on space and energy constraints as well as on the requirements dictated by the use cases. These machines are already under evaluation at the Castelloli small-scale testbed and will be employed for testing and validating the service KPIs.

Lenovo ThinkSystem SE350

The SE350 model is a very compact server designed for bringing the computer power, storage and networking closer to the edge. Table Table 15 lists the technical specifications.

Table 15: technical specification of Lenovo SE350.

Feature	Lenovo ThinkSystem SE350
Form factor	Edge server, 40mm x 215mm, 1U high
Processor	One Intel Xeon D-2100 Series processor (formerly codenamed "Skylake D"). Supports processors up to 16 cores, core speeds of up to 2.2 GHz
Memory	Up to 256 GB with 4x 64 GB LRDIMMs
Storage	NVMe drives: 16 TB using 8x 2TB NVMe drives SATA & NVMe drives: 15.68 TB using 4x 1.92 TB SATA drives + 4x 2TB NVMe drives
Network interface	• Wireless network module (Wireless enabled LOM package): 802.11ac Wi-Fi and LTE, 2x 10GbE SFP+, 2x 1GbE SFP, 2x 1GbE RJ45 (support 10/100 Mbps), dedicated port for remote management • Wired SFP+ network module (10G SFP+ LOM package): 2x 10GbE SFP+, 2x 1GbE RJ45 (support 10/100 Mbps), 2x dedicated ports for remote management • Wired BASE-T network module (10GBASE-T LOM package): 2x 10GBASE-T RJ45, 2x 1GbE RJ45 (support 10/100 Mbps), 2x dedicated ports for remote management
Cooling	Three non-hot-swap 40 mm fans (all 3 standard), N+1 redundant in most configurations
Video	G200 graphics with 16 MB memory with 2D hardware accelerator, integrated into XClarity Controller. Maximum resolution is 1920×1200 32bpp at 60Hz
Security	ThinkShield Key Vault Portal web site for security management. Trusted Platform Module, supporting TPM 2.0. Kensington cable slot with intelligent lock position switch, G-sensor trigger for motion detection, intrusion detection, self-encrypting drive (SED) support, power-on password, administrator's password.
Power consumption	Idle: 119 W 100% Load: 201 W Maximum Recorded: 238 W
Weight	Maximum: 3.75 kg

The SE350 is typically employed in edge/IoT use cases, such as autonomous vehicles (V2X), video analytics, CDNs (Content Delivery Networks), and a wide range of smart city applications. In 5GMED, the SE350 will be adopted to support the Follow-Me concept of UC4 as well as to host the V2X gateway.

Lenovo ThinkEdge SE450

The SE450 features edge capabilities with AI-ready technology in a 2U rack form-factor and is purposely designed to accelerate real-time decision making at the edge. Table 16 reports the technical specifications.

Funded by the Horizon 2020 Framework Programme of the European Union

Table 16: technical specification of Lenovo SE450.

Feature	Lenovo ThinkEdge SE450
Form factor	2U rack server
Processor	Up to 1x 3rd gen Intel Xeon Platinum processor, up to 36 cores
Memory	10x DDR4 memory slots; maximum 1TB using 8x 128GB 3DS RDIMMs
Storage	Up to 6x 2.5-inch 7mm drives
Network interface	PCIe 4.0 x16
Cooling	Three non-hot-swap 40 mm fans (all 3 standard)
Video	Up to 4x single-width GPUs
Security	ThinkShield activation, security bezel, tamper protection, encrypted SSD, system lockdown, silicon root of trust, TPM 2.0
Power consumption	N/A
Weight	N/A

According to Lenovo, the SE450 is extremely optimized for AI computation and includes all flash storage for executing analytics at the edge and optimized for delivering intelligence. In 5GMED, the SE450 represents a good candidate for UC2, where video streams coming from multiple cameras need to be processed at the edge with the goal of detecting and classifying relevant events on the highway.

Lenovo ThinkSystem SR650

The SR650 is one of the Lenovo top computing machines that can fill many roles and meet many requirements, being extremely flexible in terms of hardware configuration and settings. The technical specifications are listed in Table 17.

Table 17: technical specification of Lenovo SR650.

Feature	Lenovo ThinkSystem SR650
Form factor	2U rack server
Processor	Up to two 205 W Intel Xeon Scalable family processors, Bronze, Silver, Gold, or Platinum. Up to 28 cores at 2.5 GHz, up to 3.6 GHz with 4 cores. Two processors are connected with two UPI (Ultra Path Interconnect) links up to 10.4 GT/s
Memory	Up to 7.5TB in 24 DIMM sockets using DIMM modules of 128 GB and Intel® Optane™ DC Persistent Memory; TruDDR4 at 2666 MHz / 2933 MHz
Storage	Up to 14x 3.5-inch or 24x 2.5-inch 7mm drives
Network interface	2/4-port 1GbE LOM; 2/4-port 10GbE LOM (Base-T or SFP+); 1x dedicated 1GbE management port
Cooling	Three non-hot-swap 40 mm fans (all 3 standard)
Video	Integrated Matrox G200 in XClarity Controller
Security	Five fans (4+1) for single processor model, six fans (5+1) for dual processor model

Power consumption	2x hot swap/redundant: 550W/750W/1100W/1600W 80 PLUS Platinum; or 750W 80 PLUS Titanium; or 48V DC 80 PLUS Platinum
Weight	Maximum configuration: 70.54 lb (32 kg)

Two units of the SR650 are currently deployed in the Castelloli testbed to host the NearbyOne orchestrator and the Druid 5GC. Based on the experience and testing done in the past two years, the SR650 represents the right choice for meeting the huge capacity demand of such applications. Moreover, the SR650 will host backend services related to UC3, which are considered cloud applications due to the large distance between Castelloli and the 5GMED corridor (approx. 120 km in line of sight).

2.2. Network slicing stratum

This section explains the view of the 5GMED consortium on how to implement 5G network slicing. It first presents in Section 2.2.1 the overall idea of network slicing in 5G, including the guidelines and standards that are followed and adopted to demonstrate such technology in 5GMED. Then, we discuss in Section 2.2.2 the plan of the 5GMED consortium on how to implement 5G network slicing. Finally, we present the use case requirements that will be used to create the mapping between use cases' services and slices.

2.2.1. 3GPP Network Slicing

Network slicing is a key enabling feature for 5G and mobile communication systems. It enables the creation of logical networks under a common shared physical network infrastructure, guaranteeing proper isolation, dedicated resources, and optimized topology to support a specific service, application, or service type.

A *network slice* is a self-contained, isolated end-to-end *logical network* created on a shared physical infrastructure that meets the defined service quality. The network slice can span across multiple parts of the network from the access, transport, and compute resources up to the core network, and may also be deployed across multiple operators. When a network slice is deployed, the set of network function instances and the required resources (i.e., compute, storage, networking) will form a Network Slice Instance (NSI).

Each network slice is uniquely identified by a Single – Network Slice Selection Assistance Information (S-NSSAI). An S-NSSAI is composed of:

- Slice/service type (SST), which specifies the slice/service type and its profile, and
- Slice Differentiator (SD), which is an optional information that complements the SST to differentiate among multiple network slices of the same SST.

Figure 25 illustrates an example of three different communication service instances provided by multiple Network Slice Instances (NSIs). The other parts of a given NSI are grouped as Network Slice Subnets (e.g., RAN, 5GC, and Transport), allowing the independent lifecycle management of a Network Slice Subnet Instance (NSSI). Each NSSI will contain different Network Function (NF) instances or will require specific configurations on a Physical Network Function (PNF) that is shared across NSSIs, to serve specific requirements.

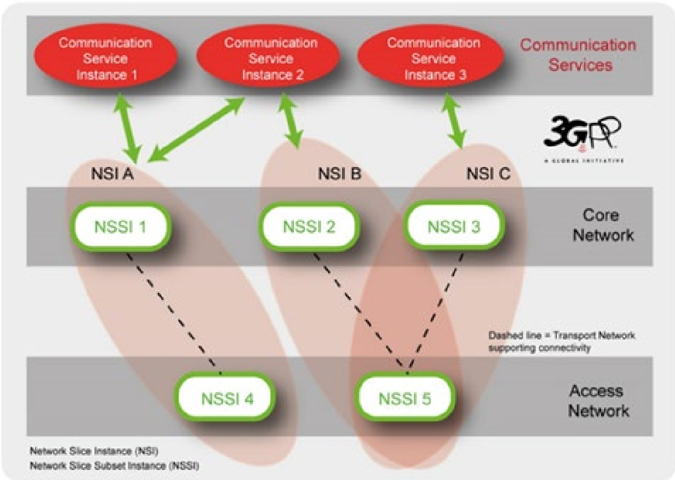


Figure 25: Different communication service instances provided by multiple NSIs [14].

In Figure 25, Communication Service Instance 1 is supported by NSI A, and Communication Service Instance 2 could be supported by either NSI A or NSI B. In contrast, the Communication Service Instance 3 is supported by NSI C. Furthermore, NSI A comprises NSSI 1 in the core network and NSSI 4 in the RAN, which is different from the NSSIs used by NSI B and NSI C. The latter share the same RAN NSSI 5 but have different NSSI in the core.

The management of an NSI is shown in Figure 26 and includes the following four phases:

1) Preparation: The slice template is defined at this stage, containing the necessary user requirements and the resources to be deployed.

2) Commissioning: This phase covers the NSI creation. All the required resources are assigned and configured to satisfy the network slice requirements. The NSI creation may include the creation and/or modification of the NSI components.

3) Operation: This phase comprises the activation, supervision, performance monitoring, resource capacity planning, reconfiguration, and de-activation of an NSI.

4) Decommissioning: this phase is responsible for the decommissioning of non-shared constituents if required, and for removing the NSI-specific configuration from the shared components. After the decommissioning phase, the NSI is terminated.

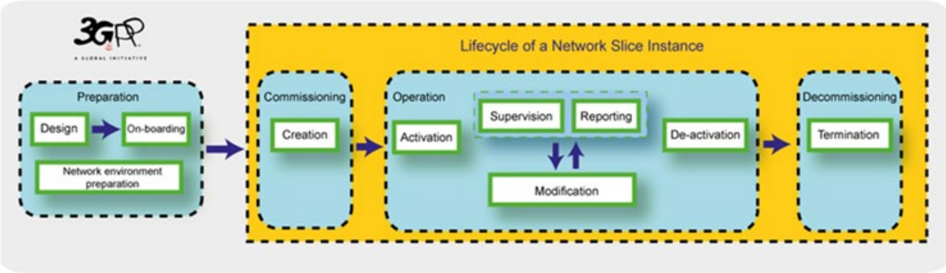


Figure 26: NSI lifecycle management [14].

It is envisioned that operators can deploy a single network slice type that satisfies the requirements of multiple services, as well as multiple slices of different types that serve diversified requirements of a business customer.

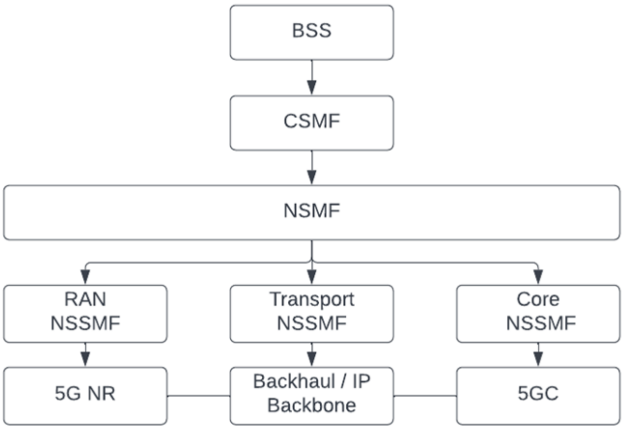


Figure 27: End-to-end network slicing architecture [15].

The 3GPP has designed an architecture to manage and orchestrate the 5G network slices through different network management functions, as shown in Figure 27 [15]. These functions are:

- The Business Support Systems (BSS), which is the entity facing the customer, exposing the products or services available. The BSS is connected to the Communication Service Management Function (CSMF).
- The CSMF, which is part of the management and orchestration domain. This entity is the translator of the communication service-related requirements to network slice-related requirements. This includes the number of allowed users, the uplink (UL) and downlink (DL) transmission rates, latency, and jitter. The CSMF is the one that communicates with the Network Slice Management Function (NSMF).
- The NSMF, which is also part of the management functions according to 3GPP. It is the function that handles the management and orchestration of the NSIs. The NSMF communicates with both the CSMF and Network Slice Subnet Management Functions (NSSMF) through its Northbound Interface (NBI) and Southbound Interface (SBI), respectively.

- The NSSMF, which is the function that manages one or more NSSIs. In fact, the network slice requirements sent by the CSMF are further decomposed into network slice subnet requirements. Each subnet, i.e., the access network (AN), transport network (TN), and core network (CN), has its own NSSMF that manages and orchestrates its respective slice subnets. Each NSSMF decomposes these slice subnet instances on its network domain into Virtual Network Functions (VNF) instances. For instance, the core NSSMF is responsible for creating a new network slice subnet instance based on the slice profile in the core domain. When creating the new core network slice subnet instance, the corresponding VNF or Cloud Native Network Functions (CNF) must be instantiated if necessary. The reason is that some Network Functions (NF) may be reused while some of them are currently not in place. Hence, instantiation is needed. Moreover, the Core NSSMF is responsible for defining the NSSIs in the 5GC NFs.

2.2.2. 5GMED approach to network slicing

In this stage of 5GMED, we have two steps to implement the 5G network slicing. The first step (described in Section 2.2.2.1) is related to the network slice service provisioning and management that follows the 3GPP network slicing architecture. This is implemented to design and create the end-to-end network slices with their specified Service Level Agreements (SLA). Moreover, this is where the instantiation and activation of network slice subnets and virtual network resource allocation and instantiation will occur. On top of that, the connectivity between the network functions and data centers through the transport network is established.

The second step of the implementation (described in Section 2.2.2.2) is the actual network slice selection, enabling the deployment of different services associated with that specific network slice.

The implementation of network slicing in the RAN will require (i) the ability to configure the Single-Network Slice Selection Assistance Information (S-NSSAI), and the support for different S-NSSAI types, (ii) S-NSSAI resource allocation, and (iii) the link of S-NSSAIs to a transport endpoint. The consortium is holding ongoing tasks with gNB providers and their proprietary MNOs to investigate whether the required configurations are supported.

2.2.2.1. Slicing preparation and commissioning stream

In this stream, the network slice is configured with the PLMNID/S-NSSAI, VLANs, and IP addresses, among other network parameters, to connect the radio nodes to the appropriate core instances providing the required resources for each service or use case. In 5GMED, the NearbyOne end-to-end orchestrator by NBC, the slice manager and RAN controller by i2CAT, and the transport SDN controller by CTTC will be made available for the project. Different options on how to map these components to the slicing architecture are under discussion in the project. One of the approach, shown in Figure 28, is that the slice manager and slice manager will take the role of the Access Network (AN) NSSMF, the transport SDN controller will take the role of the Transport Network (TN) NSSMF, and the NearbyOne orchestrator takes the role of the NSMF and the Core Network (CN) NSSMF.

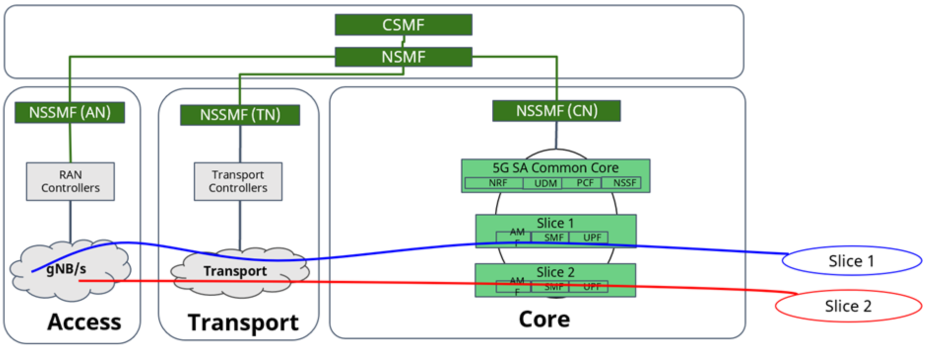


Figure 28: 5GMED end-to-end network slicing architecture.

The user generally requests a network slice through the CSMF, and the CSMF will send the service requirements to NSMF. With this request, a new network slice instance will support the demand for the slice. The NSMF will also determine the slice profiles for RAN, Transport, and core subnets. To this end, the NSMF communicates with the domain NSSMFs, i.e., the RAN NSSMF, Transport NSMMF, and the Core NSSMF, to coordinate the sub-slice management for each part. The domain NSSMFs are responsible for allocating the network slice subnet instance in their respective domains based on the slice profile.

In this stream, the full slicing lifecycle management will be deployed and tested. In particular, the procedure of moving the slicing context of users moving from one MNO to another will be implemented and evaluated. This stream will be mainly tested in Castelloli testbed and can be extended to the large scale testbed if the conditions explained in the previous section are met. The final architecture and test results will be be reported in WP3 and WP6 deliverables.

2.2.2.2. Slicing operation stream

We consider that use cases/services will be statically mapped to network slices. The slices will be manually configured to support the requirements of the use cases and their services as they were defined in Deliverables D2.1 and D3.1.

An example of the proposed architecture is shown in Figure 29. In this example, one UPF instance will serve each slice. Furthermore, each service inside the use case will be associated with a Data Network Name (DNN). It should be noted that different services having the exact QoS requirements can be related to the same DNN.

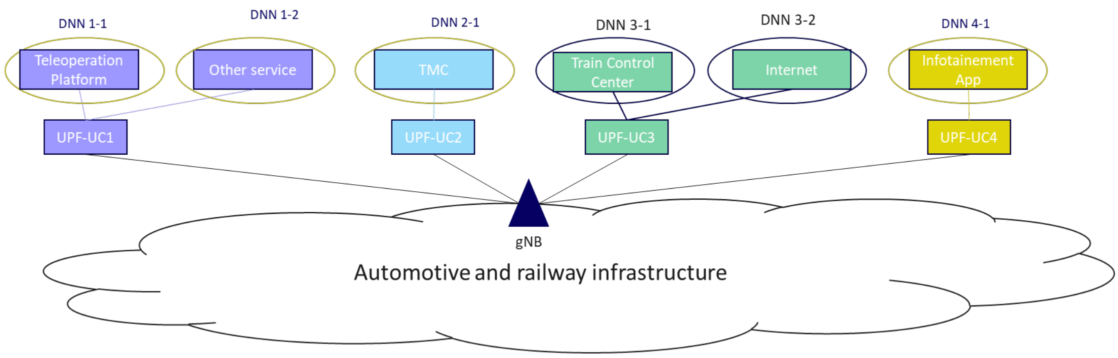


Figure 29: Mapping use cases to DNNs and UPFs.

In this scenario, each UE will be configured with the DNN corresponding to the service that it is executing. This setup will force the traffic of the UEs to go through the UPF that serves its service. To differentiate these services' QoS requirements, each service (DNN) will be configured with a 5G QoS Identifier (5QI) that specifies other QoS parameters, including priority. In addition, the Aggregate Maximum Bit Rate (AMBR) will be set for each service so that services with high priority will not consume the whole bandwidth.The 5QI and AMBR will be used by core, Transport, and radio access networks to reserve the resources corresponding to the requested services. In the table below, we show an example of mapping some 5GMED services to slices following this approach and usin the KPIs used in Deliverables D2.1 and D3.1.

Table 18: Example of mapping services to slices.

5GMED slice	Affected UC	Affected Service	Identifier (S-NSSAI)	DNNs	5QI	AMBR-DL	AMBR-UL
Slice 1	UC1	Teleoperation Maneuver	SST=V2X, SD=0	Teeloperation	85	2 Mbps	11 Mbps
Slice 2	UC2	Relay of emergency messages	SST=V2X, SD=1	Traffic Management Center	69	52 Kbps	8 Kbps
Slice 3	UC3	Railway Track Safety – Obstacle Detection	SST=mMTC, SD=0	Train Control Center	70	70 Mbps	10 Mbps
Slice 4	UC3	Multi-tenant Mobile Service	SST=eMBB, SD=1	Small Cell	3	5 Mbps	2 Mbps
Slice 5	UC4	EMT livestreaming 360	SST=eMBB, SD=2	CDN	80	600 Mbps	600 Mbps

This approach is enabled by the already existing features provided by the 5G core and radio networks deployed in the large scale testbed. In particular, the DRUID core allows the configuration of S-NSSAI, deploying dedicated DNNs per S-NSSAI, where each DNN has different 5QI and AMBR parameters.

2.2.2.3. Network Slicing in non-3GPP access technologies

As it was explained in Section 2.1, the use case services will use, in addition to the 5G network, other radio access technologies. Therefore, there is a need to define how slicing will be done in these technologies. The 5GMED consortium is investigating the possible approaches to integrate slicing in these technologies:

- **For C-V2X**: A possible solution is to create an instance of V2X Gateway for each DNN, which is the destination of a slice traffic.
- **For satellite network**: IRT has already developed an equipment (named "slicing manager") to insure 5G slicing continuity when the satellite link is used, based on the requested QoS. A scheme illustrating all the entities involved is reported in Figure 30. The satellite link will be used for backhauling the onboard gNB. The continuity of the 5G slices on the satellite link is

implemented with the help of five components deployed at different functional levels: an altered SMF (Session Management Function) in the 5GC, a 5G QoF (Quality Of service Function) at control plane level, a NTN QOF (Non Terrestrial Networks Quality Of Service Function) at control plane level and two Slice Classifiers at user plane (one on track, one on board the train). The altered SMF can hook at PDU Management level. The 5G QOF converts the PDU Session Info into a unique 5G Flow and send it to the NTN QOF. The NTN QOF maps the 5G Flows to the NTN Flows and program the Slice Classifiers. Finally, the two Slice Classifiers interconnect Satellite and 5G Networks (Flow translation), enforce Slice Policy, enforce QoS policy.

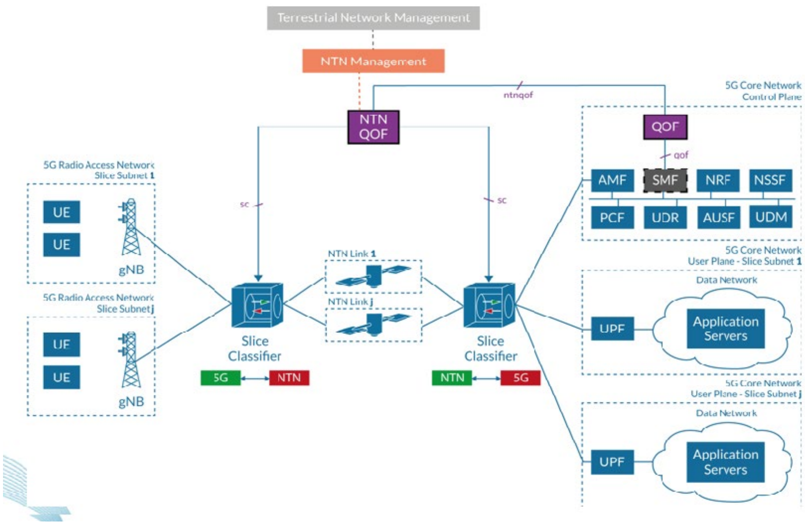


Figure 30: Overview of the satellite slicing manager developed by IRT.

- **For 70 GHz network**: Slices can be mapped to QoS priority,e.g., through VLAN Priority Code Point (PCP)/ DiffServ Code Point (DSCP).

More details about the approach adopted by the 5GMED consortium will be provided in Deliverables D3.3 and D3.4.

2.2.3. Use case analysis

This subsection provides for each UC an analysis of the computing and networking resources required. Besides the application building blocks, a list of networking blocks is presented for Spain and France. This analysis is meant to support the network slicing design that will be conducted in D3.3.

2.2.3.1. Use case 1

Table 19 provides the analysis of UC1, while Figure 31 shows the related data flow.

Table 19: Analysis of UC1 – remote driving.

UC1: Remote Driving	
Brief Description of the Scenario: The Valeo's Cruise4U vehicle is remotely driven by a teleoperator across the FR-SP border. It is assumed that the stretch of highway crossing the border and where Remote Driving will take place is under full 5G coverage, i.e., without any coverage gap. Figure 31 shows the data flow related to UC1.	
Service KPIs	1. E2E Latency – 20-30 ms 2. DL/UL Throughput – 10/20 Mb/s 3. Service Continuity / Interruption Time during Inter-PLMN roaming - < 5ms 4. QoS/5QI metrics
Application Building Blocks	1. Valeo Teleoperation Cloud (Internet /public cloud) 2. Remote Station (Internet) 3. QoS Prediction Module(edge) 4. ToD-enabled Vehicle
Relevant Network Parts and Requirements	
France 1. gNBs: RU + (DU/CU-UP/CU-CP-H/CU-CP-L) in 5G RAN Cloud 2. vUPF in 5G RAN Cloud 3. 5GCN Control Functions in Core Cloud	
Spain 1. gNBs: RU + (DU/CU-UP/CU-CP-H/CU-CP-L) in 5G RAN Cloud 2. vUPF in 5G RAN Cloud 3. 5GCN Control Functions in Core Cloud	

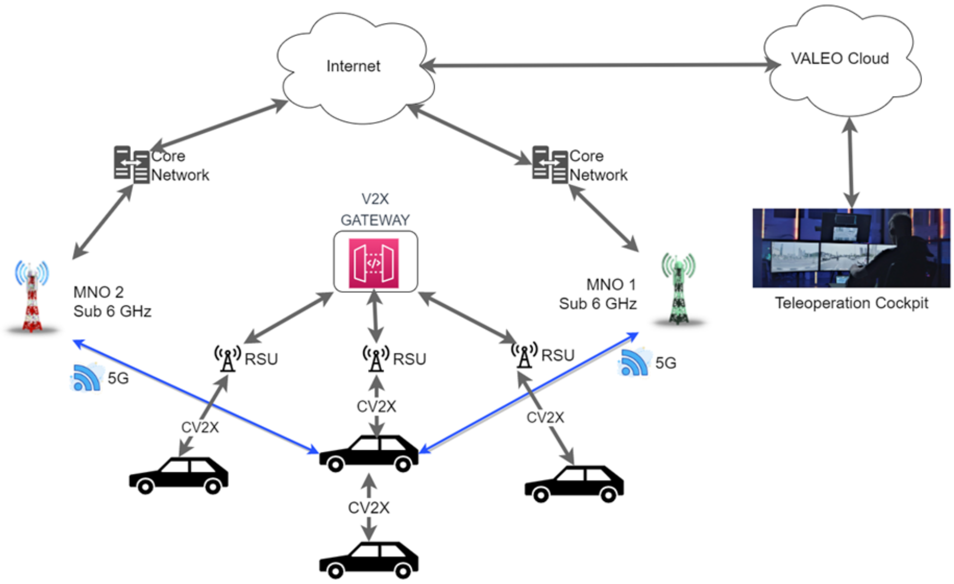


Figure 31: Data flow for UC1.

2.2.3.2. Use case 2

UC2 includes three different services for the automotive environment:

- **Relay of emergency messages (REM)**, whose analysis is shown in Table 20 and the data flow is illustrated in Figure 32.
- **Automatic incident detection (AID)**, whose analysis is shown in Table 21 and the data flow is illustrated in Figure 33.
- **Traffic Flow Regulation (TFR),** whose analysis is shown in Table 22 and the data flow is illustrated in Figure 33.

Table 20: Analysis of UC2 - service 1.

UC2 – Service 1: Relay emergency message sent by vehicle to infrastructure	
Brief Description of the Scenario: The aim of the service is to detect any dangerous situation as an obstacle by CVs and CAVs and the infrastructure, based on this information, disseminates traffic warning strategies to ensure safety on the road. The TMC edge receives and processes the data coming from the road via the V2X gateway. As output data, the TMC edge will communicate to the V2X gateway the traffic strategies and obstacles alert messages to be sent to the CVs and CAV on the road. It also communicates to the TMC Global in the cloud the traffic status, detected incidents and local strategies launched. Suppose the incident that occurred under the coverage of one MEC may affect other cars under another MEC. In that case, the TMC Global will send the alert messages and traffic strategies from the originating MEC to the next MEC.	
Service KPIs	1. Data rate < 1 Mbps. Maximum data rate: 5 Mbps 2. Round End-to-End Latency (including processing times in the Edge and Cloud) < 700 ms

	3. Service reliability: 99.9% 4. Handover success rate (roaming or InterRAT): 99.9% 5. Mobility interruption time < 80 ms
Application Building Blocks	1. In-vehicle Applications. 2. V2X Gateway located in the MEC layer. 3. TMC Edge in the MEC layer. 4. TMC Global in the Cloud layer.
Relevant Network Parts and Requirements	
France 1. TCUs 2. 5G Radio Access: 3.5GHz 3. V2X GATEWAY (5G/C-V2X/ITS-G5) 4. Local MEC at least: 225GB HD, 8 CPUs, 48GB RAM 5. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM 6. 5GC SA	
Spain 1. TCUs 2. 5G Radio Access: 3.5GHz 3. C-V2X/ITS-G5 Radio Access: RSU 4. V2X GATEWAY (5G/C-V2X/ITS-G5) 5. Local MEC at least: 225GB HD, 8 CPUs, 48GB RAM 6. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM 7. 5GC SA	

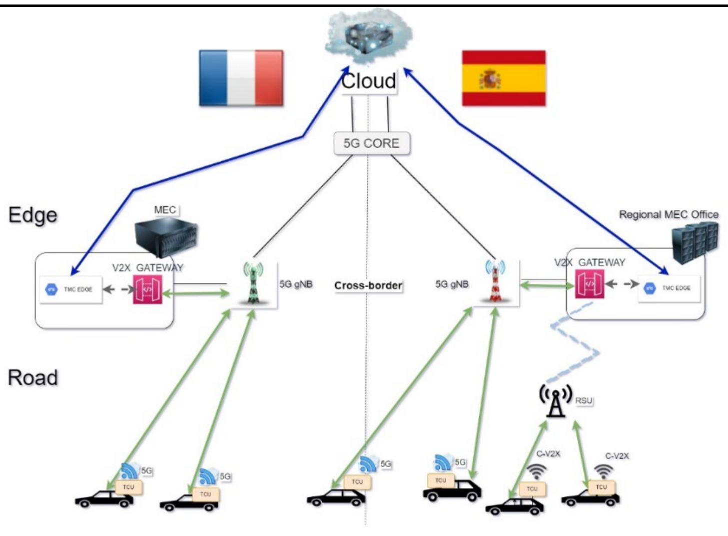


Figure 32: Data Flow UC2 - Service 1.

Table 21: Analysis of UC2 - service 2.

UC2 – Service 2: Automatic Incident Detection	
Brief Description of the Scenario: The purpose of the service is the same as service 1 but the only difference is that the hazardous situation is detected by video sensors on the road (via 5G radio access). The video stream is transformed into obstacle detection information in the TMC Edge and then the rest is as detailed in service 1.	
Service KPIs	1. Data rate cameras (6 units): 10 Mbps/camera 2. Data rate CCAM messages < 1Mbps 3. Round End-to-End Latency (including processing times in the Edge and Cloud) < 700 ms 4. Service reliability: 99.9% 5. Handover success rate: 99.9% 6. Mobility interruption time < 100 ms
Application Building Blocks	1. Road video sensors. 2. In-vehicle Applications. 3. V2X Gateway located in the MEC layer. 4. TMC Edge in the MEC layer. 5. TMC Global in the Cloud layer.
Relevant Network Parts and Requirements	
France 1. TCUs 2. 5G Radio Access: 3.5GHz 3. V2X GATEWAY (5G/C-V2X/ITS-G5) 4. Local MEC at least: 325GB HD, 16 CPUs, 56GB RAM 5. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM 6. 5GC SA	
Spain 1. TCUs 2. Cameras and 5G TCU or equivalent 3. 5G Radio Access: 3.5GHz 4. C-V2X/ITS-G5 Radio Access: RSU 5. V2X GATEWAY (5G/C-V2X/ITS-G5) 6. Local MEC at least: 325GB HD, 16 CPUs, 56GB RAM, GPU NVDIA ≥ 8 GB 7. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM 8. 5GC SA	

Table 22: Analysis of UC2 - service 3.

UC2 – Service 3: Real time traffic flow regulation
Brief Description of the Scenario: In this service, the objective is that the infrastructure regulates the traffic flow by detecting abnormal behavior (e.g., slow speed, etc.) and sends regulation orders to a group of circulating vehicles. The TMC Global assesses the real-time traffic situation along the entire corridor through video sensors deployed on the road and external traffic data

<table>
<tr><td colspan="2">analyzed from third parties. In case of abnormal behavior detected in the coverage of a MEC, the Global TMC transmits (via the corresponding TMC Edge and V2X Gateway) a traffic regulation strategy to the CVs and CAVs circulating under the coverage of the MEC.</td></tr>
<tr><td>Service KPIs</td><td>Data rate cameras (6 units): 10 Mbps/camera
Data rate CCAM messages < 1Mbps
Round End-to-End Latency (including processing times in the Edge and Cloud) < 600 ms
Service reliability: 99.9%
Handover success rate: 99.9%
Mobility interruption time < 100 ms</td></tr>
<tr><td>Application Building Blocks</td><td>1. Road video sensors.
2. In-vehicle Applications.
3. V2X Gateway located in the MEC layer.
4. TMC Edge in the MEC layer.
5. TMC Global in the Cloud layer.</td></tr>
<tr><td colspan="2">Relevant Network Parts and Requirements</td></tr>
<tr><td colspan="2">France
1. TCUs
2. 5G Radio Access: 3.5GHz
3. V2X GATEWAY (5G/C-V2X/ITS-G5)
4. Local MEC at least: 325GB HD, 16 CPUs, 56GB RAM
5. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM
6. 5GC SA</td></tr>
<tr><td colspan="2">Spain
1. TCUs
2. Cameras and 5G TCU or equivalent
3. 5G Radio Access: 3.5GHz
4. C-V2X/ITS-G5 Radio Access: RSU
5. V2X GATEWAY (5G/C-V2X/ITS-G5)
6. Local MEC at least: 325GB HD, 16 CPUs, 56GB RAM, GPU NVDIA ≥ 8 GB
7. CLOUD at least: 400GB HD, 16 CPUs, 32GB RAM
8. 5GC SA</td></tr>
</table>

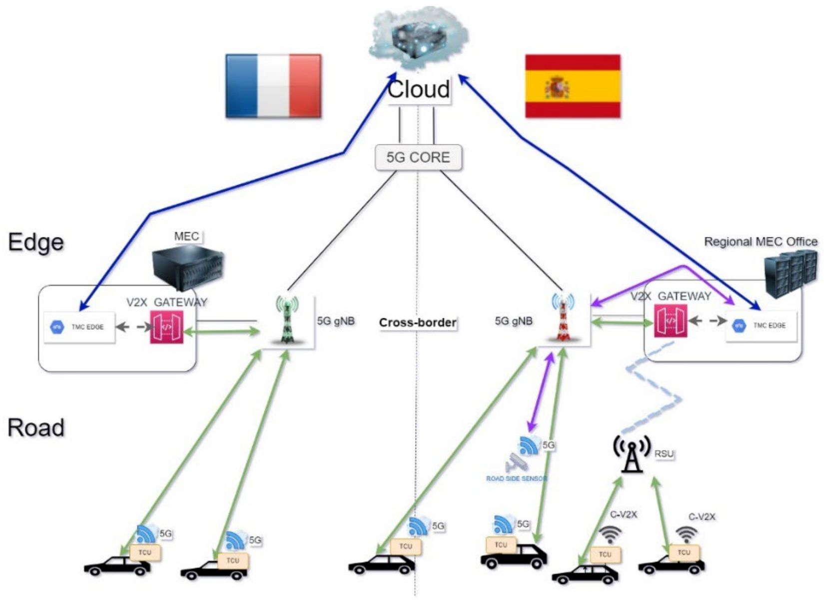


Figure 33: Data Flow in UC2 - Service 2 -3.

2.2.3.3. Use case 3

UC3 is composed by five different services to be deployed in the train will be as follow, classified as performance (P – higher priority) or business (B – lower priority):

- **FRMCS P1**: Advanced Sensor Monitoring on Board, whose analysis is shown in Table 23 and the data flow is illustrated in Figure 34.
- **FRMCS P2**: Railway Track Safety - Obstacle Detection, whose analysis is shown in Table 24 and the data flow is illustrated in Figure 35.
- **FRMCS P3**: Passenger safety and comfort, whose analysis is shown in Table 25 and the data flow is illustrated in Figure 36.
- **FRMCS B1**: High Quality Wi-Fi to passengers, whose analysis is shown in Table 26 and the data flow is illustrated in Figure 37.
- **FRMCS B2**: Multi-tenant Mobile Service, whose analysis is shown in Table 27 and the data flow is illustrated in Figure 38.

Table 23: Analysis of UC3 - FRMCS P1.

UC3 – FRMCS P1: Advanced Sensor Monitoring On-board	
Brief Description of the Scenario: Data communication between non-critical systems on-board and railway staff to monitor and control those infrastructure systems remotely. The objective is for experiencing the influence of massive IoT traffic types over 5G links. Several sensors will be simulated on-board to generate appropriate traffic	
Service KPIs	1. Data Rate: 1/1 Mb/s 2. One-way Latency (Cloud): 1 sec. 3. Reliability: 99% 4. Mobility interruption time: 1 sec.

Application Building Blocks	IoT Traffic Generator (train) IoT Data Processing Tool (Cloud) IoT Presentation Tool (train)
Relevant Network Parts and Requirements	
France and Spain: ACS-GW unit (onboard) The connection between train and Cloud Server: around 1 Mbps. Any access network (5GNR, 70GHz) is valid, including satellite connection (that will be the preferred one) ACS-GW unit (ground) Cloud Server (IoT Data Processing): • Storage: 8GB for LXC or 10GB for KVM + 1024MB for Swap storage • 2 vCores at 1.3GHz min • RAM:1024MB for a LXC or 1536MB for KVM	

Figure 34: Data flow in UC3 - service P1.

Table 24: Analysis of UC3 - FRMCS P2.

UC3 – FRMCS P2: Railway Track Safety - Obstacle Detection	
Brief Description of the Scenario: The idea is to use a LiDAR on the train cabin to monitor the adjacent rail track parallel to the track followed by the train. An AI module in the edge will be used to perform object detection. Alerts will be sent to the Cloud Train Operation Centre and/or nearby trains.	
Service KPIs	1 Data Rate: 32/10 Mb/s 2. One-way Latency: 100 ms 3. Reliability: 99% 4. Mobility interruption time: 1 sec.
Application Building Blocks	LiDAR (train cabin) AI module (edge) Alarm Management Simulator (Cloud) Alarm Presentation Tool (Train)
Relevant Network Parts and Requirements	
France and Spain: ACS-GW unit (onboard) Any access network (5GNR, 70GHz) is valid, except satellite connection ACS-GW unit (ground) Edge Server (AI Module): 100 GB storage, 4 cores, 32 GB RAM Cloud Server (Alarm Management Simulator): 100 GB, Y CPU, 32 GB RAM (module in development) shared with P3. The connection between train and Cloud Server has no specific requirements	

Funded by the Horizon 2020 Framework Programme of the European Union

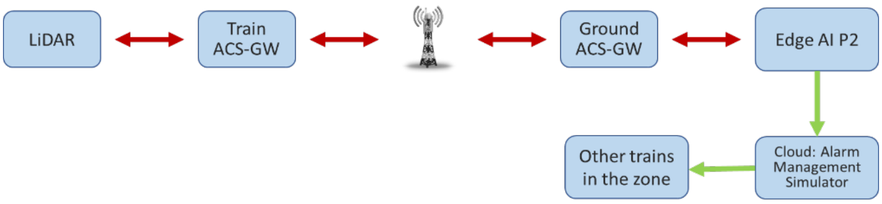


Figure 35: Data Flow in UC3 – Service FRMCS P2.

Table 25: Analysis of UC3 - FRMCS P3.

UC3 – FRMCS P3: Passenger Safety and Comfort	
Brief Description of the Scenario: A danger/tense situation happens in a train vehicle. Stage 1: Microphones in the vehicle capturing the background sound of the vehicle permanently, forwarding it to an AI module in the edge, thar will register the incident (also passengers can rise an alarm for this). An alert will be sent to the Cloud Train Operation Centre: cameras on-board will be managed remotely by the Cloud Train Operation Centre or the train staff located in another train vehicle **Stage 1**: A camera also equipped with microphones is capturing audio and video in one passenger's vehicle. A permanent flow of this video and sound is locally stored and received on AI module on edge. When a tense situation in the vehicle, a warning is sent to the Cloud Train Operation Center. Alternatively, a passenger can activate a Manual Alarm to send a similar warning to the Cloud Train Operation Center. **Stage 2**: When this message is received, the train staff will be able to manipulate the cameras inside the vehicle to obtain more information about the incident and alert other vehicles staff in the same train. Once the danger/tense situation will be analyzed, the Control Center can store images sound locally and sent a message to the train staff. The train staff can request to the Control Center to receive the stream live video.	
Service KPIs	1. Edge Data Rate: 256/64 Kb/s 2. Edge One-way Latency: 100 ms 3. Cloud Data Rate: 8/8 Mb/s 4. Cloud One-way Latency: 150 ms 5. Reliability: 99% 6. Mobility interruption time: 1 sec.
Application Building Blocks	Vehicle micros & cameras Edge AI module + Video/audio storage (edge) Video/audio management (Cloud) - similar to the edge- Alarm Management Simulator (Cloud) Alarm Presentation Tool (Train)
Relevant Network Parts and Requirements	
France and Spain: ACS-GW unit (onboard) Any access network (5GNR, 70GHz, satellite) is valid ACS-GW unit (ground) Edge Server (AI Module + Video/Audio storage): 256 GB SSD, 8 CPU 3GHz, 32 GB RAM Cloud Server (Video/Audio storage): 128 GB storage, 4 CPU cores and 16 GB RAM (modules are still under development)	

Cloud Server (Alarm Management Simulator): 100 GB, Y CPU, 32 GB RAM (module in development) shared with P1.

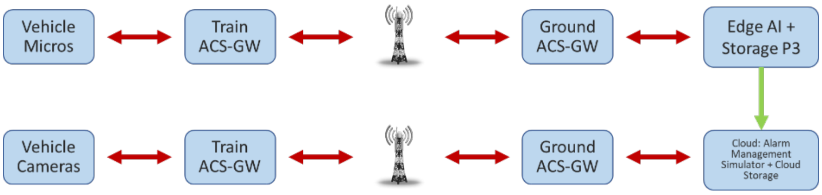


Figure 36: data flow in UC3 - FRMCS P3.

Table 26: Analysis of UC3 - FRMCS B1.

UC3 B1: High Quality Wi-Fi to passengers	
Brief Description of the Scenario: Application focused on the Gigabit Train concept: to ensure that Internet connectivity for passengers travelling at high-speed across borders is like connectivity at home or at work. Really, traffic generators will be used to simulate a train plenty of passengers	
Service KPIs	1. Data Rate: 1024 Mb/s for the whole train 2. One-way Latency [ms]: 100 3. Reliability: 99% 4. Mobility interruption time: 1 sec.
Application Building Blocks	Wi-Fi AP Traffic generator (train) Traffic generator (ground)
Relevant Network Parts and Requirements	
France and Spain: ACS-GW unit (onboard) Any access network (5GNR, tunnel, 70GHz) is valid, except satellite connection ACS-GW unit (ground)	

Figure 37: Data Flow in UC3 – Service B1.

Table 27: Analysis of UC3 - FRMCS B2.

UC3 B2: Multi-tenant Mobile Service for Passengers	
Brief Description of the Scenario: A 5GNR multi-tenant small cell used to radiate the signal of various MNOs inside the moving train, connected to a specific 5GCore supporting Home Roaming which will support dynamic instantiation of tenants, and reconfiguration of the carrier frequency when crossing the border. In this way, the multi-tenant small cell allows the train passengers to establish videoconference with other MNOs users in a cross-border scenario. (12)	
Service KPIs	1. Data Rate: 4/1 Mb/s 2. E2E Latency between UEs: 200 ms 3. Reliability: 99% 4. Mobility interruption time: 1 sec.
Application Building Blocks	Passenger UEs Train Small Cell Neutral 5GC National 5GC (specific for B2)
Relevant Network Parts and Requirements	
France and Spain: Small Cell ACS-GW unit (onboard) Any access network (5GNR, tunnel, 70GHz) is valid, except satellite connection ACS-GW unit (ground) Neutral 5GC 2 x National 5GC (specific for B2)	

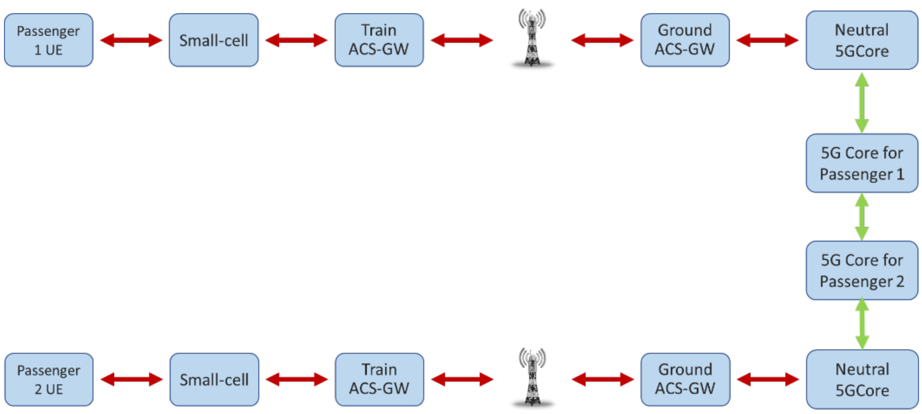


Figure 38: Service Flow in UC3 – Service B2 (Worst case: Passenger videoconference between two train users belonging to different countries).

2.2.3.4. Use case 4

UC4 includes two different infotainment services, i.e., EMT (Enjoy Media Together) and TP (Tour Planning), that will be deployed both in the automotive and railway environment.

- The analysis and the data flow of the EMT for automotive are shown in Table 28 and Figure 39, respectively.

- The analysis and the data flow of the EMT for railway are shown in Table 29 and Figure 40, respectively.
- The analysis and the data flow of the TP for automotive are shown in Table 30 and Figure 41, respectively.
- The analysis and the data flow of the TP for railway are shown in Table 31 and Figure 42, respectively.

Table 28: UC4 Follow-Me infotainment (EMT service - automotive).

<table>
<tr><th colspan="2">UC4: Follow-me Infotainment (EMT Service - Automotive)</th></tr>
<tr><td colspan="2">Brief Description of the Scenario: Different functionalities will be considered in the EMT Service. The service is split into three functionalities: EMT Video Streaming, EMT Video Conference, and EMT 360 Livestreaming. All of them are intended to offer high-quality interactive media content to the end-users, some of them, are requiring high throughput and some others low latency. Beyond the offering of the media contents themselves, the main objective of this UC4 is to demonstrate the “follow-me” concept, i.e., the migration of certain VNFs associated with the service across the MEC nodes while end-users are travelling along the 5GMed corridor.</td></tr>
<tr><td>Service KPIs (most stringent)</td><td>1. Data Rate: >100 Mbps (per user)
2. Latency: <20ms
3. Jitter: <2ms
4. Mobility Interruption time: <30ms
5. Reliability: 99,9%
6. Service Migration Time: 20-35 s</td></tr>
<tr><td>Application Building Blocks</td><td>1. The EMT Master Server, located in the cloud layer
2. The EMT Edge Server, located at the MEC layer and migrated over the MEC infrastructure
3. The EMT Client, running on the end-user UEs.</td></tr>
<tr><td colspan="2">Relevant Network Parts and Requirements</td></tr>
<tr><td colspan="2">France & Spain
5G (Radio Access):
• Data Rate: >100 Mbps (per user)
• Latency: <20ms
• Jitter: <2ms
Local and Regional MECs (EMT Edge Server): 50GB, 8 CPU, 16 GB RAM
Connection to the cloud: Data Rate: >1 Gbps
Cloud (EMT Master Server): 200GB, 12CPUs, 16 GB RAM</td></tr>
</table>

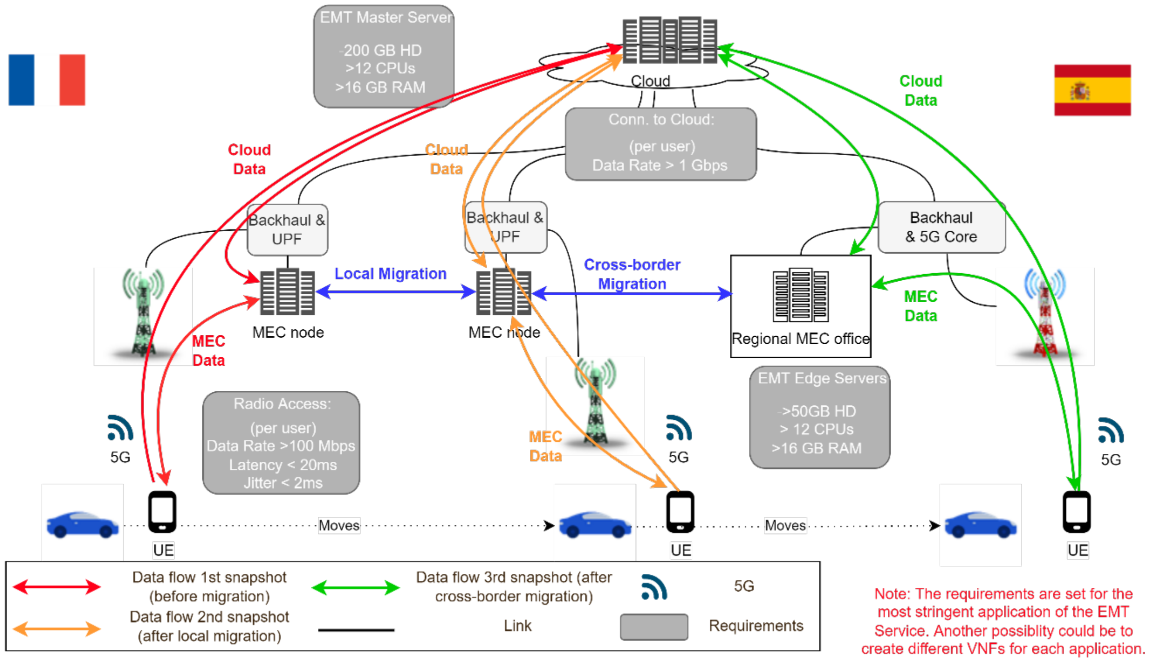


Figure 39: Data Flow UC4 (EMT – Automotive).

Table 29: UC4 Follow-Me infotainment (EMT service - railway).

UC4: Follow-me Infotainment (EMT Service - Railway)	
Brief Description of the Scenario: Different kinds of applications will be considered in the EMT Service. The service is split into three applications: EMT Video Streaming, EMT Video Conference, and EMT 360 Livestreaming. All of them are intended to offer high-quality interactive media content to the end-users, some of them are requiring high throughput and some others low latency. Beyond providing the media contents themselves, the main objective of this UC4 is to demonstrate the "follow-me" concept, i.e., the migration of certain VNFs associated with the service across the MEC nodes while end-users are travelling along the 5GMed corridor.	
Service KPIs	1. Data Rate: >100 Mbps (per user) 2. Latency: <20ms 3. Jitter: <2ms 4. Mobility Interruption time: <30ms 5. Reliability: 99,9% 6. Service Migration Time: 20-35 s
Application Building Blocks	1. The EMT Master Server, located in the cloud layer 2. The EMT Edge Server, located at the MEC layer and migrated over the MEC infrastructure 3. The EMT Client, running on the end-user UEs.
Relevant Network Parts and Requirements	
France 1. 5G (Radio Access): a. Data Rate: >100 Mbps (per user) b. Latency: <20ms	

Funded by the Horizon 2020 Framework Programme of the European Union

c. Jitter: <2ms 2. Local and Regional MECs (EMT Edge Server): 50GB, 8 CPU, 16 GB RAM 3. Connection to the cloud: Data Rate: > 1 Gbps 4. ACS-GW Onboard (Traffic not encapsulated) Cloud (EMT Master Server): 200GB, 12CPUs, 16 GB RAM
Spain 5. 5G (Radio Access): a. Data Rate: >100 Mbps (per user) b. Latency: <20ms c. Jitter: <2ms 6. Local and Regional MECs (EMT Edge Server): 50GB, 8 CPU, 16 GB RAM 7. Connection to the cloud: Data Rate: > 1 Gbps 8. ACS-GW Onboard and On-ground (For encapsulated traffic in case multiple Access technologies are used) 9. Cloud (EMT Master Server): 200GB, 12CPUs, 16 GB RAM

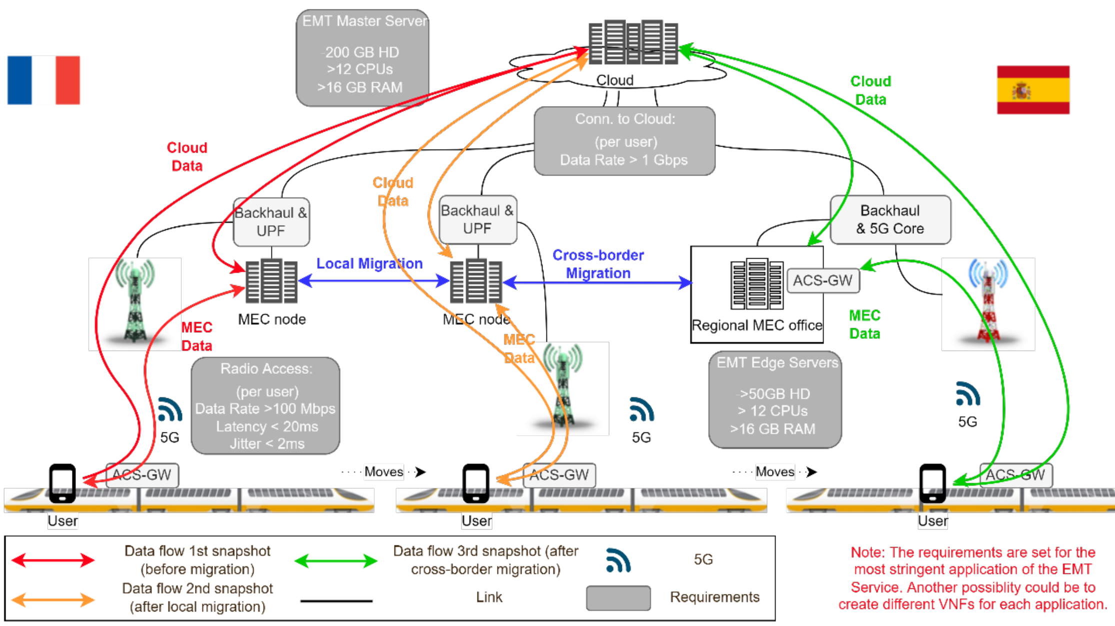


Figure 40: Data Flow UC4 (EMT – Railway).

Table 30: UC4 Follow-Me infotainment (TP service - automotive).

UC4: Follow-me Infotainment (TP Service - Automotive)	
Brief Description of the Scenario: The Tour Planning (TP) service provides high resolution and immersive media content to travellers and a full set of functionalities for planning trips, giving them enriched information regarding the surroundings, nearby points of interest along with the functionalities of TP, Tour suggestion and sharing experiences. An enhanced XR enabled experience is available to the end-user, making use of the related options to receive virtual reality content as long as she has an XR capable mobile device and a head mounted device with her.	
Service KPIs	1. E2E Latency: < 20-100 ms 2. Bandwidth: Min: 25 Mbps, Max: Greater than 100 Mbps

	3. Jitter: Min: Less than 10 ms, Max: 50 ms 4. Framerate > 30 fps 5. Packet Loss: Min: Less than 1%, Max: 5 % 6. Number of users: Up to 5 users 7. Service migration time: 20-35 sec 8. Reliability: 99.9%
Application Building Blocks	1. The TP Server, located in the cloud layer 2. The TP Edge Server, located at the MEC layer and migrated over the MEC infrastructure 3. The TP Client, running on the end-user UEs.
Relevant Network Parts and Requirements	
France 1. ACS-GW (TCU) 2. 5G – 3.5Ghz (Radio Access): >25 Mbps, <20ms 3. Local MECs (TP Edge Server): 100GB, 8 CPU, 16 GB RAM 4. Radio Link: >25Mbps 5. 5GC SA 6. Connection to cloud: >25Mbps 7. Cloud (TP Server): 200GB, 8CPUs, 16 GB RAM	
Spain 1. ACS-GW (TCU) 2. 5G - 3.5 GHz (VDF Radio Access): >25 Mbps, <20ms 3. VDF Backhaul: > 25Mbps 5. VDF Core 6. Regional MEC office (TP Edge Server): 100GB, 8 CPU, 16 GB RAM 7. 26Ghz (Radio Access): >25 Mbps, <20ms 8. Fiber Link: >25Mbps 9. Local MEC (near 26GHz antennas): 50GB, 8 CPU, 16 GB RAM 10. 5GC SA 11. Connection to the cloud: >25Mbps 12. Cloud (TP Server): 200GB, 8CPUs, 16 GB RAM	

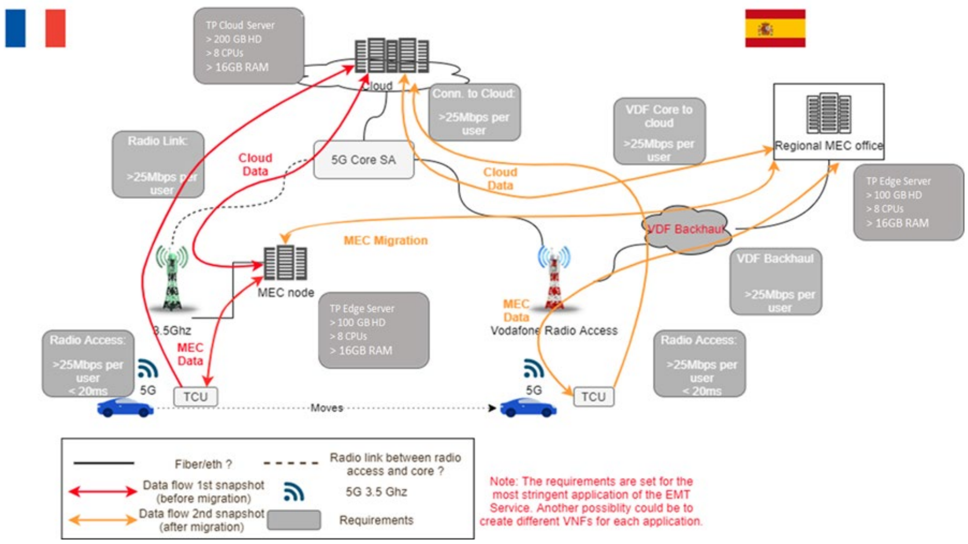


Figure 41: Data Flow UC4 (TP – Automotive).

Table 31: UC4 Follow-Me infotainment (TP service - railway).

UC4: Follow-me Infotainment (TP Service - Railway)	
Brief Description of the Scenario: The Tour Planning (TP) service provides high resolution and immersive media content to travellers and a full set of functionalities for planning trips, giving them enriched information regarding the surroundings, nearby points of interest along with the functionalities of TP, Tour suggestion and sharing experiences. An enhanced XR enabled experience is available to the end-user, making use of the related options to receive virtual reality content as long as she has an XR capable mobile device and a head mounted device with her.	
Service KPIs	1. E2E Latency: < 20 -100 ms 2. Bandwidth: Min: 25 Mbps, Max: Greater than 100 Mbps 3. Jitter: Min: Less than 10 ms, Max: 50 ms 4. Framerate > 30 fps 5. Packet Loss: Min: Less than 1%, Max: 5 % 6. Number of users: Up to 5 users 7. Service migration time: 20-35 sec 8. Reliability: 99.9%
Application Building Blocks	1. The TP Server, located in the cloud layer 2. The TP Edge Server, located at the MEC layer and migrated over the MEC infrastructure 3. The TP Client, running on the end-user UEs.
Relevant Network Parts and Requirements	
France 1. ACS-GW (TCU) 2. 60-70Ghz (Radio Access): >25 Mbps, <20ms 3. Local MECs (TP Edge Server): 100GB, 8 CPU, 16 GB RAM 4. Radio/Fiber Links: >25Mbps 5. 5GC SA 6. Connection to the cloud: >25Mbps 7. Cloud (TP Server): 200GB, 8CPUs, 16 GB RAM	
Spain 1. ACS-GW (TCU) 2. 70 GHz (Radio Access): >25 Mbps, <20ms 3. Backhaul: > 25Mbps 5. Core 6. Regional MEC office (TP Edge Server): 100GB, 8 CPU, 16 GB RAM 7. Connection to the cloud: >25Mbps 8. Cloud (TP Server): 200GB, 8CPUs, 16 GB RAM	

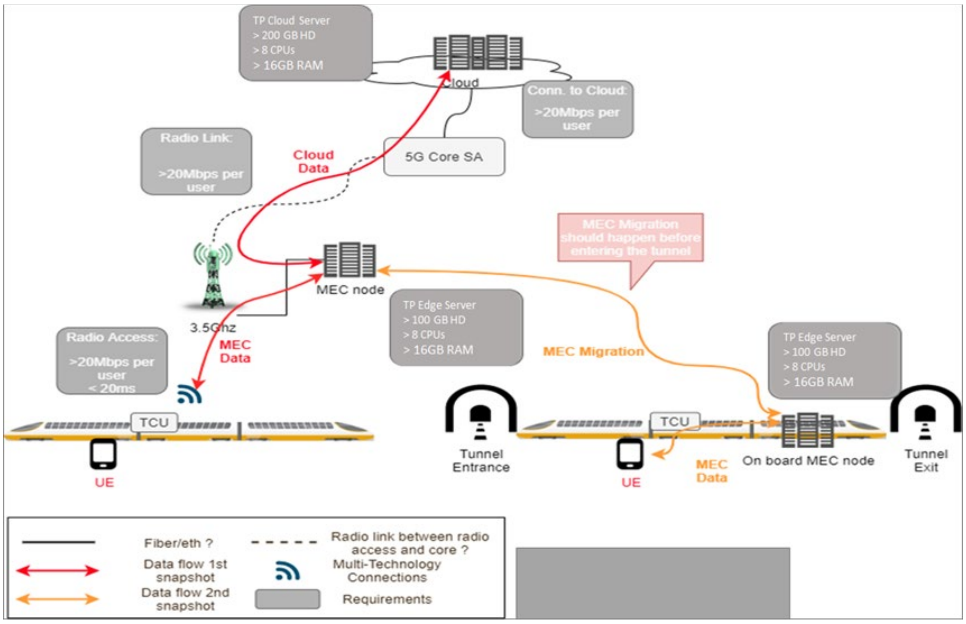


Figure 42: Data Flow UC4 (TP – Railway).

2.3. Network Management and Service Orchestration

In this section, we first describe the orchestrator solution called Nearby One. Next, we discuss the solution's components called the orchestration platform and Nearby Blocks. We then expound on the capabilities of the orchestrator platform. Then, we explain the concept of the Nearby Block and how it integrates with the orchestrator. After which, we elaborate on how the orchestrator platform monitors the Nearby Block using its telemetry tools, which allows the former to make decisions and perform actions based on the metrics being monitored. Lastly, we describe how the orchestrator will enable the cross-border scenarios.

The NearbyOne is an edge orchestrator platform that is used to deploy workloads at the edge of the network. Moreover, the platform is responsible for covering the complete lifecycle management of these distributed platforms or MEC servers where the the network components and the applications will be hosted.

The NearbyOne solution considers two aspects of end-to-end service orchestration [16]:

- **Inter-node orchestration**: the selection and management of the MEC servers to automatically decide the service placement based on intent-based parameters such as service SLA requirements.
- **Intra-node orchestration**: managing the hardware platform components inside the MEC servers to manage the lifecycle of services and applications, taking advantage of the hardware resources (i.e., cores, memory, accelerators) to optimize resource allocation.

The NearbyOne solution is composed of two main elements, also shown in Figure 43:

Funded by the Horizon 2020 Framework Programme of the European Union

- **The Nearby Orchestration Platform** is the main component of the solution, runs in a central location, and oversees the performance of all tasks related to the orchestration of applications and infrastructure.
- **The Nearby Blocks** are distributed components that encapsulate logic and code for different applications and VNF-specific functionalities. These blocks represent all the elements that the orchestration platform can manage. These may be physical nodes hosting telco functions and applications, public cloud, or even small IoT devices.

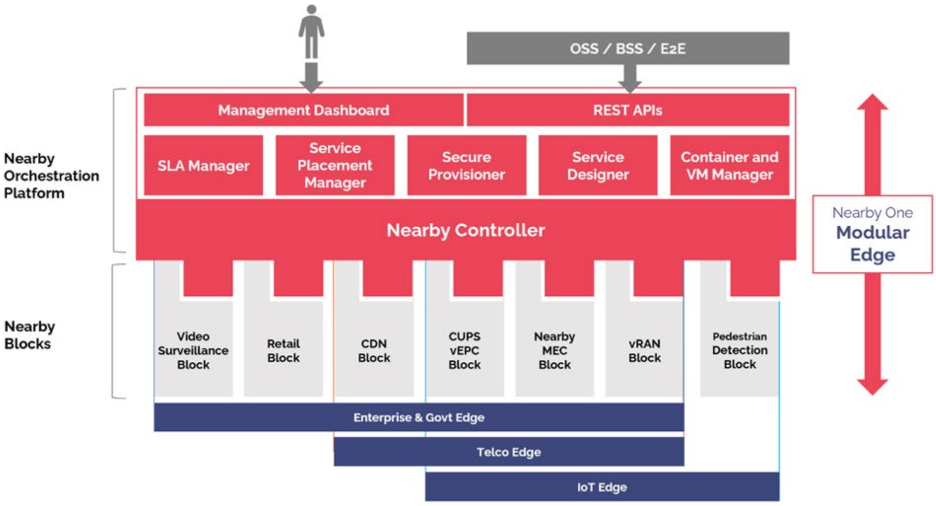


Figure 43: NearbyOne modular architecture.

In Figure 43, we see the two components of the Nearby One solution. The first component is the Orchestrator platform or the Nearby Controller. This component acts as the central component of the solution. This component is responsible for collecting information by monitoring all the events to make decisions. The second component is the Nearby Block, an abstraction representing all the elements that the orchestrator manages. These elements may be physical nodes, telco functions, and applications. The orchestrator also can manage instances running on the public and private clouds.

As the solution is modular, blocks may vary. They may be deployed based on the required network components, such as LTE or 5G, and applications such as Video Analytics, Content Delivery, or Cloud Gaming. In the context of 5GMED, the Nearby Blocks are the elements like the telco function such as 5GC from Druid and applications from autopistas, ATOS, and ATC. These blocks expose their KPIs and health statuses to the orchestrator through the blocks' NBI. The orchestrator can perform lifecycle management and reconfiguration based on these monitored metrics. This ensures that all applications are behaving as expected, ensuring that the defined QoS and KPIs are met in an automated way.

2.3.1. NearbyOne Modular Architecture

The NearbyOne orchestrator component continuously monitors the MEC server's performance (processors, memory, accelerators) and the VNF/application Blocks. When a new application or VNF block is deployed, the orchestration layer checks the available resources on the server such as CPU, and memory, and allocates the necessary resources to the block. All this information is made available to the orchestrator to enforce automated service placement decisions, allowing it to decide where to place the workloads based on resources and location.

In order to provide the abovementioned functionalities, the orchestrator includes the following capabilities:

- **SLA Manager** – This functionality allows the platform to continuously monitor the network parameters to dynamically activate or deactivate resources allowing the SLAs to be constantly met.
- **Service Placement Manager** – This functionality allows the platform to continuously analyze the operational status of each node in the network, enabling it to relocate computational, network, and storage resources associated with the service, especially when there is a high probability of a node failure.
- **Secure Provisioning** – This functionality allows the platform to manage the entire lifecycle of the edge network. The lifecycle covers automated provisioning, configuration, and installation of all elements in the edge stack. Moreover, dynamic upgrades, patching, and reprovisioning are done.
- **Service Designer** – The designer allows a unified dashboard to perform end-to-end deployment from the design phase to operations and maintenance. This functionality enables mechanisms to provision services through a drag and drop approach, also giving the customers access to the catalog showing the available network functions and applications.
- **Container and VM Management** – This functionality allows the orchestrator to merge the container and VM technologies transparently, so there are no constraints in deploying any VNF, CNF, or applications.

More specifically, three components (part of SLA Manager and Service Placement Manager) are responsible for enforcing placement policies:

- **SLA monitoring:** collects all telemetry generated at the infrastructure, network, and chassis levels i.e, CPU usage, fan operations, temperature and system heat that may affect the performance of the server affecting theKPIs observed at the service level such as framerate (fps), inference time, and number of objects detected, among others.
- **Policies:** description of the expected behaviors for the different components of service when some of the SLA are not met.
- **Placement Engine:** makes decisions about service location based on the inputs of the SLA monitoring component and according to the policies component.

Network Functions and applications, as deployed in the NearbyOne solution, are encapsulated into **Nearby Blocks** to address ecosystems that require inter-application communication and accurate placement decisions and usually require advanced tuning of their execution platform. Note that the blocks that appear in the figure above are sample applications; these may be even

Funded by the Horizon 2020 Framework Programme of the European Union

telecommunications components such as LTE, 5G RAN and Core network functions, and other applications such the ones from ATOS and ATC to enable the follow-me infotainment under UC4.

Each Nearby Block contains the Application/VNF logic (containers or VMs provided by a third-party vendor/partner such as ATOS and ATC), and they are encapsulated with a set of auxiliary components that provide the means for the application to be effectively managed, including:

- VNF/Application health/status KPIs for continuous lifecycle monitoring and management as well as SLA assessment such as end-to-end latency, bandwidth, and jitters.
- VNF/Application capabilities dynamically exposed at deployment time (e.g., services exposed by the application for external consumption, like an output video feed or a third-party management dashboard).
- Correlation between the application KPIs and platform (processor, accelerators, memory, storage) to perform a more effective platform management.

2.3.2. Telemetry Collection Interfaces

The monitoring of the blocks, such as the 5GC from Druid and the applications from autopistas, ATC and ATOS, is done through the **telemetry collection interfaces** shown in Figure 44**,** which allows the orchestration layer to have access to all the resources consumed by these blocks, map the available resources, and the high-level KPI metrics for each application (its actual performance as perceived by the end-user using the different applications and services). This allows the orchestrator to perform actions such as allocation of more resources, enablement of FPGA, when needed, to meet the defined KPIs. Moreover, NearbyOne integrates different open-source technologies used to aggregate logs and system telemetry, provide analysis tools for the generated data, and connect the platform to external charging and ticketing systems.

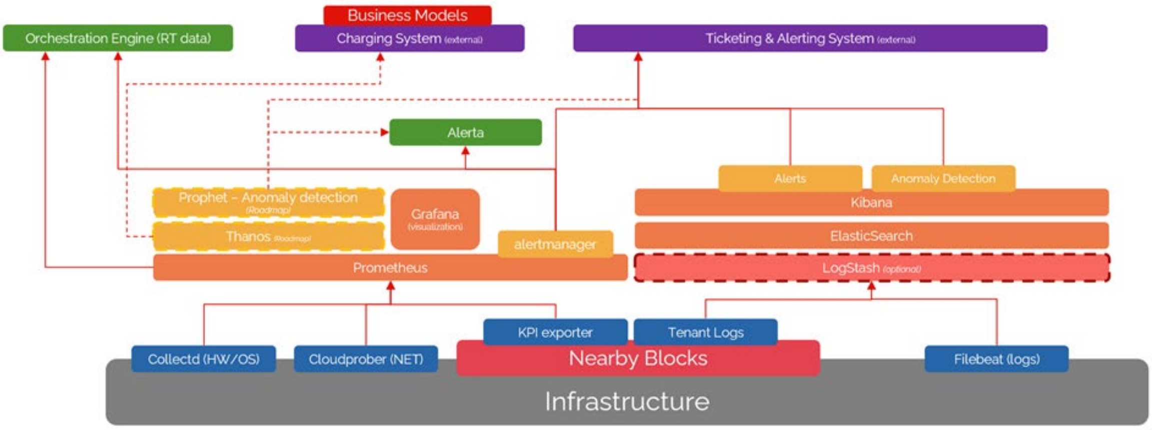


Figure 44: Telemetry collection and aggregation flows.

The ecosystem of open technologies used to consolidate system information is mainly composed of:

- **Logs**
    - OpenDistro (ElasticSearch and Kibana): used to aggregate logs from both the platform and the tenant deployments.
    - LogStash: Used to pre-process logs before being ingested by ElasticSearch.
    - Filebeat: Extracts system logs from the different software components.
- **Telemetry**
    - Collectd: Telemetry collection agent for system resource consumption information (CPU, memory, disk).
    - CloudProber: Active network monitoring mechanism to measure real-time telemetry about dynamic latency and bandwidth status.
    - Prometheus: Time series database used to aggregate all system telemetry globally. The alert-manager component of Prometheus is used to trigger alarms.
    - Grafana: To analyze tenant's application telemetry (KPIs) and node telemetry in real-time.
    - Alerta: Alarm processing system that aggregates and consolidates system alarms generated by Prometheus alert-manager.

In addition, NearbyOne provides the following telemetry services:

- **System telemetry**: Based on *collectd*, each physical and virtual node reports through Prometheus exports information about:
    - **CPU usage** (User, system, idle) to determine overcommitment situations
    - **Memory usage** to assess overcommitment situations
    - **Network and disk usage** per interface to identify bottlenecks
    - **Chassis Information**: ambient/CPU/components temperature, fan speed, and several other HW parameters that can be used to identify system malfunctions.
- **Network latency/bandwidth/jitter**: For automated Block deployment, the NearbyOne solution actively monitors network parameters for each site to understand the status of each connected element. This is used to determine if SLAs can be met and automatically choose the proper location for service placement. This monitoring infrastructure is automatically updated every time a new element is registered into the repository.

The set of metrics collected can be easily extended, as Prometheus comes with many different exporter modules that can be used to collect metrics from many external data sources.

2.3.3. Cross-border orchestration

Network management and service orchestration is an essential concept in cross-border scenarios to ensure seamless data flow and guarantee end-to-end service quality and continuity among different administrative domains. To enable cross-border orchestration, several other elements and components of the network must operate in a coordinated way. These elements are:

- 5GC control plane (one instance – at least – per country)
- 5G RAN control plane (one instance – at least – per country)
- 5GC user plane (mainly the UPF, one instance – at least – per MEC site)
- 5G RAN user plane (mainly the CU-UP and the DU, one instance – at least – per MEC site)
- The Mobile UE (onboard trains or vehicles)
- The Edge Application components (one instance – at least – per MEC site)
- The Edge Application backend components (one cloud-hosted instance – at least – per application)
- The MEC platform manager (one instance – at least – per MEC site) enables Radio Network Information Services (RNIS) interfaces at the MEC site
- The Edge Domain Orchestrator (DO) coordinates the actuations across all these components
- The physical and logical infrastructure:
  - Cloud site for hosting backend application components
  - MEC site servers and networking elements (L2)
  - Other Cloud-native Network Functions (CNF) are deployed at the MEC site.

Nearby Computing can operate different MEC platforms across MNOs. Figure 45 illustrates the relationships across all these components, as well as the flows and responsibilities associated with the handover process (of both the UE and the Application):

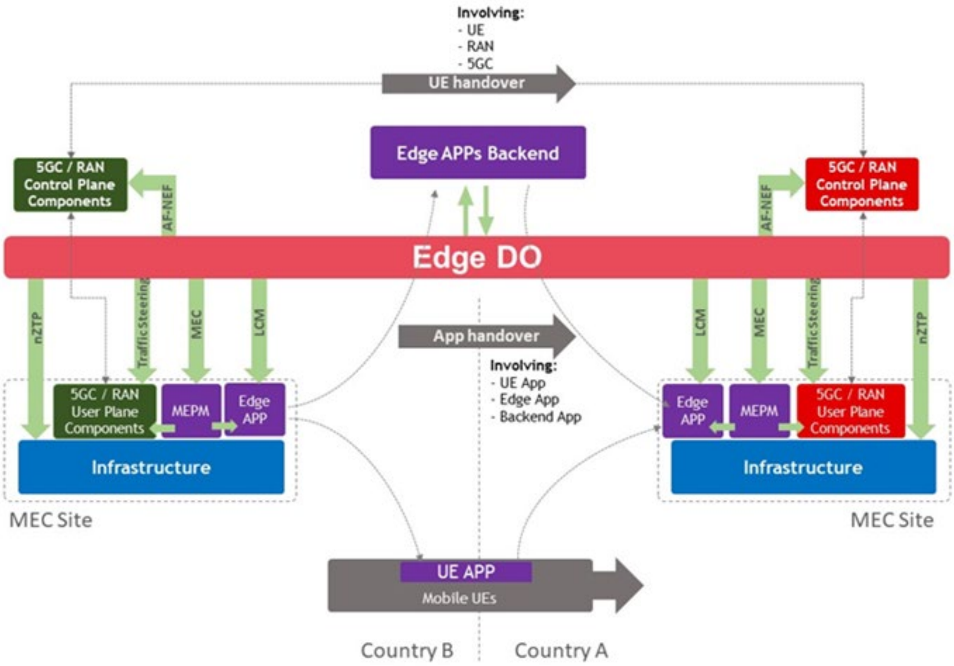


Figure 45: Proposed Architecture for Cross-border Orchestration.

According to Figure 45, the DO is responsible for interacting with the following elements and with the following responsibilities:

- **Infrastructure (Hardware, OS):**
    - Provisioning of the infrastructure (if not already available), including the OS and container/VM platform configuration.
    - Continuous monitoring of the server status, including OS resources (cores, memory, disks) and chassis telemetry.
    - Automatic upgrades and maintenance of the servers, with the corresponding workload eviction when there is a need to restart some of the IT components.
    - Integration with the virtualization and/or containerization platform in terms of authentication with the platform and enablement of the life cycle management of CNFs and Applications
- **Edge Applications (UE, MEC site, and backend):**
    - Lifecycle Management (LCM) of the applications, from their deployment to the continuous service level assurance over time.
    - KPI extraction to monitor SLAs, generate alarms (in collaboration with the analytics module), or even perform reactive actions associated with different user-defined policies.

  - Configure application parameters based on network, host, or environmental conditions. The DO needs to integrate with the existing control knobs exposed by the applications to push initial configurations or adapt them to changing conditions. This includes the edge components, sitting in the MEC sites, and the back-end components, potentially sitting in data centers owned by the operators or even in public clouds. The operation of both elements needs to be performed in a coordinated way in all cases. An example of this type of interaction is the migration of a user session (or "Follow-me" concept, as described in other deliverables) – at the application level - from one MEC site to another, that may require, for instance, the pre-population of contents in a different MEC site when it is detected that the UE session is about to be migrated to a new location.

- **5GC and RAN (control plane and user plane):**

  - The user plane components (mainly cDU, cCU-UP, cUPF) must be deployed and configured to connect to the 5GC and RAN control plane components correctly. This step is divided into the following two processes:

    - Deployment of the CNFs in the right location and proper configuration of the software stack (from resource allocation to leveraging low-level functionalities like Single-root input/output virtualization (SRIOV) and Data Plane Development Kit (DPDK) enablement) to ensure the expected service levels and throughputs to be delivered.

    - Configuration of the software parameters to enable the communication among all the involved NFs (e.g., CU-UP to CU-CP host and port mapping, and N3 and N6 interfaces of the UPF). All these configurations must be pushed according to the environment in which each component is deployed. Of course, this may change based on the location (MEC site) and the country of operation.

  - The interaction between the applications and the 5GC is driven through different interfaces. The AF-NEF (Application Function – Network Exposure Function) is recommended for enforcing group policies (instead of interacting directly with the PCF). This interface is used for traffic steering and influencing to allow the 5GC to instruct and configure the UPFs through the corresponding SMF.

  - Configure the 5GCs on each side of the border to know each other and to be prepared to hand over sessions for roaming across the border when needed. Note that **UE handover is an exclusive responsibility of the 5GC** that must be interconnected to allow roaming between countries at the UE session-level. PLMN IDs need to be correctly registered and authorized in both 5GCs, and the roaming interfaces between the cores must be in place to enable UE sessions to be migrated across countries.

- **Enabling the MEC interfaces** (e.g., Radio Network Information Service – (RNIS)) in the MEC platform to allow UEs to obtain information about their attachment status and extract information can be valuable for the application backend to determine how to manage contents, for instance, across different MEC sites.

Funded by the Horizon 2020 Framework Programme of the European Union

In this context, cross-border orchestration operation is responsible for sensing applications' state, including the analytics module to estimate the presence of UEs in different locations and react to the request's issues either by App Backends, App Edge instances, or even App Backends UE components. The orchestration layer will be responsible for obtaining these requests, associating to them actuation policies (e.g., if a UE is expected to be soon transitioning to a new MEC site, interact with the app backend to register and deploy a new app edge instance in that MEC so that contents can be prepopulated in advance of the arrival of the UE). Of course, by enabling this migration and actuation on the infrastructure, the orchestration layer is also responsible for registering components into the 5GC, performing the necessary traffic steering, and influencing requests to enable service continuity.

It is worth noting that, while in the project, a single instance of the orchestration layer will be used to coordinate activities across the border, an extension of this model could be achieved following an East/West federation between different instances of orchestrators as shown in the figure below. According to the Operator Platform Telco Edge Proposal [17] from the GSMA, this E/W interface is the critical enabler for app roaming across different DOs. Figure 46 illustrates how the proposed architecture would be modified to introduce this concept. All NBI (North-bound interfaces) and SBI (South-bound interfaces) would remain as in the initial architecture proposal.

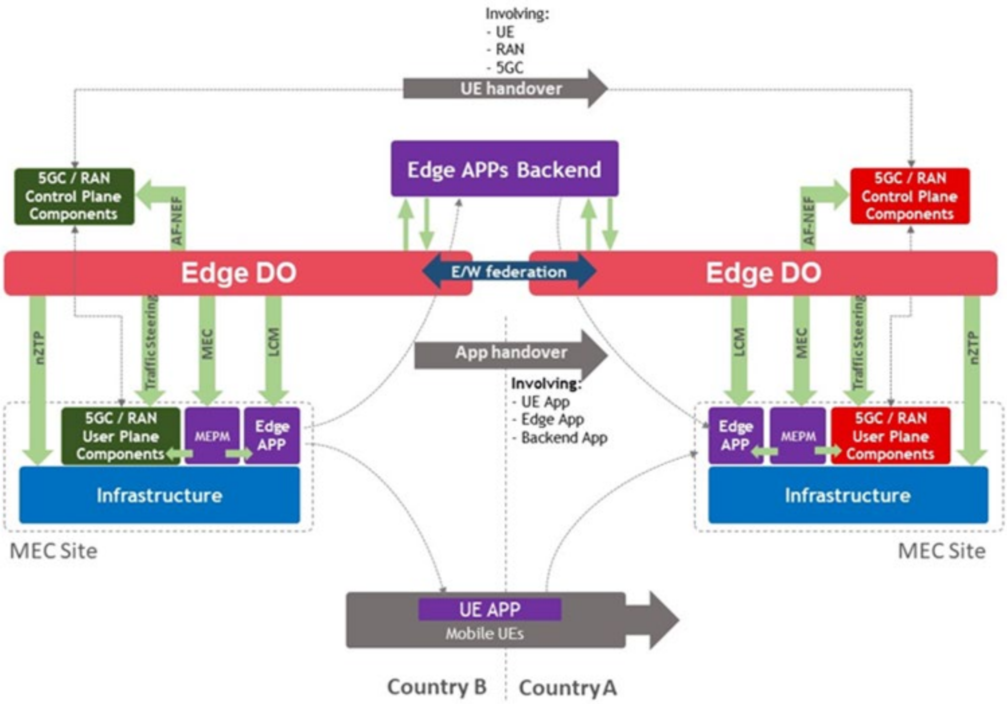


Figure 46: Extension of the Architecture to enable E/W federation across DOs.

3. 5GMED Multi-connectivity approach

This section presents the 5GMED approach to take advantage of multiple connectivity solutions simultaneously available in addition to 5G. The first mechanism is called Adaptive Communication System Gateway (ACS-GW) and is specifically designed to support communications in the railway scenario. The second solution is the V2X gateway, which is employed in vehicular communications.

3.1. ACS Gateway

This section describes the 5GMED ACS-GW, a key component required by the 5GMED project to realize an adaptive multi-connectivity packet forwarding strategy providing IP mobility and session continuity through different Radio Access Network (RAN) technologies, both 3GPP and non-3GPP. Figure 47 gives an overview of the network architecture, where two instances of the ACS-GW, i.e., train or onboard ACS-GW and ground ACS-GW play the role of middleware box between the routers and the RATs.

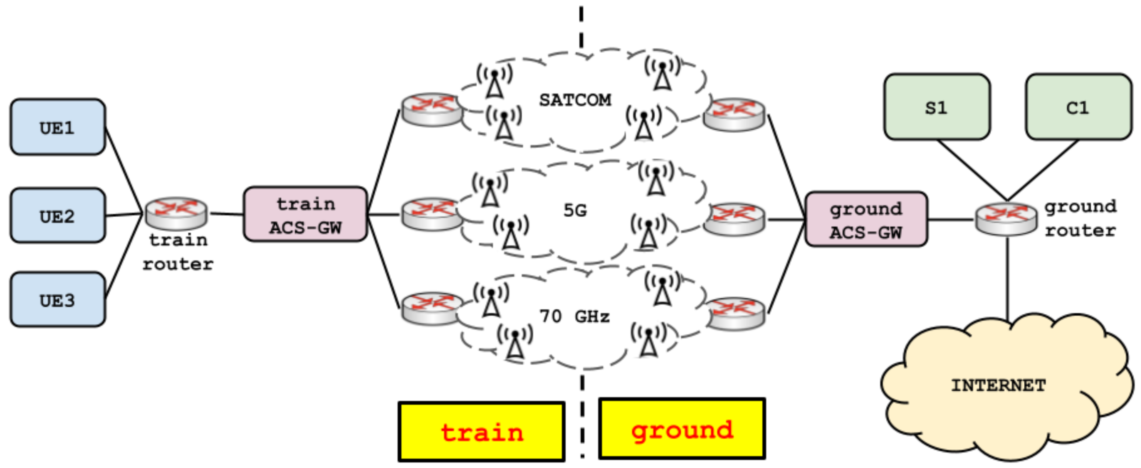


Figure 47 High level network diagram

The main goal of the ACS-GW is to realize transparent per-application independent forwarding of IP packets exchanged between the train network and the ground network over an overlay network consisting of several IP/UDP tunnels associated with each of the RANs. The basic mechanism implemented by the ACS-GW can be summarized as follows:

- Packets sent by end devices (both on ground and on board) are classified according to a set of user configurable matching rules and the relative application ID is retrieved.
- Each application is associated with a forwarding policy that specifies a list of RANs ordered by preference. The forwarding policy may also consider the location of the train.
- For each RAN the ACS-GW establishes an IP/UDP tunnel and periodically verifies its availability by exchanging keep alives and keep alive acknowledgments. The goal of this function is also to refresh the NAT binding for masqueraded RANs (when needed).
- Packets are encapsulated within the proper tunnel according to the current tunnel status and the forwarding policy of each application. The tunnel can be seamlessly changed if packets

cannot be delivered through any of the available RAN. In this case the external header is changed according to the specific tunnel endpoints while the inner application packets are left unchanged. This provides seamless IP mobility.

- The current 5GMED architecture considers multiple instances of the ACS-GW. One instance is deployed on board the train, and it acts as the default gateway for the train network. Multiple instances (at least one per country along the 5GMED corridor) are deployed on ground.
- The role of the ACS-GW depends on the flow direction. For flows initiated on board, the train ACS-GW acts as the classification and encapsulation endpoint, while the ground ACS-GW acts as the decapsulation endpoint. For flows initiated on ground the role is swapped: the ground ACS-GW performs classification and encapsulation and the train ACS-GW performs decapsulation.

3.1.1. On-board ACS-GW

The 5GMED ACS-GW acts as a middlebox between the end user devices on the train (mobile phones, laptops, servers, etc.) and the radio access units installed on the train (5G NR, 70GHz and SatCom), in the next sections the main functionalities of the ACS-GW will be explained.

3.1.1.1. Functional overview

The main function of the ACS-GW is to intercept the traffic sent by the end user devices and to choose the best radio access technology to send the packets toward ground according to a set of per-application forwarding policies.

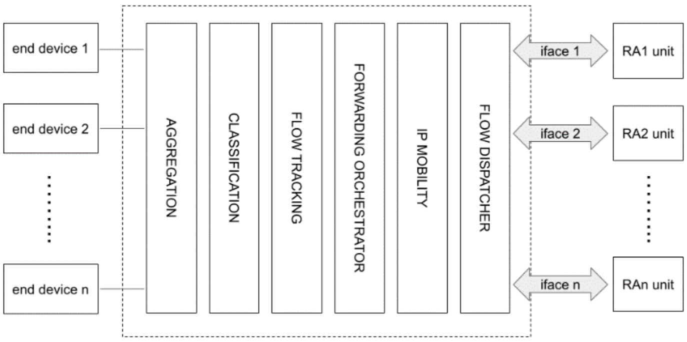


Figure 48: ACS-GW high level function breakdown.

As shown in Figure 48, the ACS-GW high level function breakdown consists of the following six distinct layers:

1. Aggregation
2. Classification
3. Flow Tracking

4. Forwarding Orchestration
5. IP Mobility
6. Flow Dispatching

In the remainder of this subsection, a detailed description of each of the ACS-GW functions is provided.

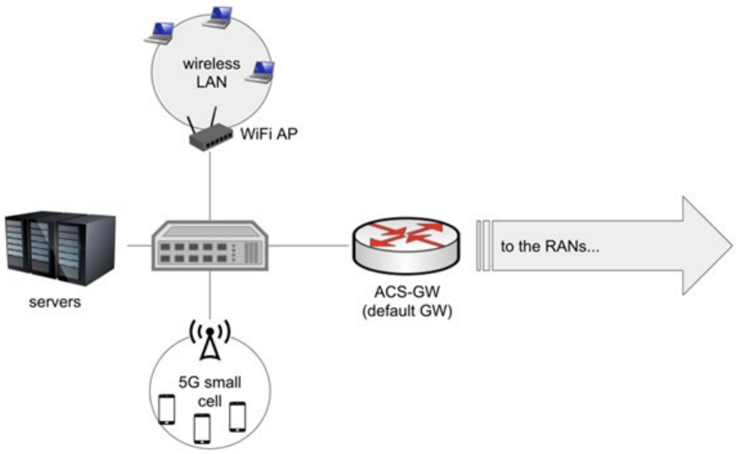


Figure 49: Onboard high-level Network Topology.

3.1.1.2. End User Traffic Aggregation

The first goal is to intercept the packets sent by the end user devices on the train. The Train Communication Network (TCN) topology support the communication with the following devices as shown in Figure 49:

1. laptops and mobile phones connected to the 802.11 WiFi access points,
2. mobile phones connected to the neutral host cell on the train.
3. servers directly connected to the TCN switch.

From a network topology point of view, the simplest approach for transparently interfacing the end-user devices is for the ACS-GW to act as the IP default GW of such nodes, as shown in Figure 49. The user devices are configured in order to get the dynamic IP configuration via DHCP (Dynamic Host Configuration Protocol). The ACS-GW functions will be implemented as software modules hosted by a Linux server. For this reason, it appears reasonable to implement the DHCP server in the same Linux server as the ACS-GW. In particular, the widely adopted ***ISC (Internet Systems Consortium) DHCP*** [18] implementation (supported by all Linux distros) will be deployed.

It is important to underline that in order to avoid IP fragmentation, the end-user devices are required to adjust the Maximum Transmission Unit (MTU) value in order to account for the additional overhead introduced by the IP/UDP encapsulation (20 bytes IP + 8 bytes UDP).

3.1.1.3. Application Classification

The application classification function is described in detail in Deliverable D5.1. Briefly, this function has the goal of retrieving the application ID associated to the raw IP packet. Each application ID is associated with a set of wildcard matching rules against the raw packet header fields, i.e. VLAN tags, IP addresses, L4 ports and GTP header fields. To realize such classification the ACS-GW only requires to have the list of matching rules agreed with the use case owners and to be able to parse the fields associated with such classification rules.

3.1.1.4. Flow tracking

The ACS-GW is responsible for keeping track of all the active application flows and monitoring the different tunnel availability and the train position that are required to implement a “smart” and adaptive strategy responsible for the actual forwarding of the application flows over the different available radio access units. In other words, the train ACS-GW is responsible for the following tasks:

1. Keep track of all the application flows. This will be done by individually tracking the different transport layer sessions (i.e., the traffic flows identified by the usual socket 5-tuple: source IP address, destination IP address, transport protocol, source port, destination port) along with the current RAN used to deliver the packets to the ground network.
2. Passively monitor ground reachability over the different RANs.
3. Change the current RAN associated with the active application flows if required.

Regarding the actual radio access selection intelligence, the ACS-GW can implement the following strategies:

1. Using a priority list (APPx[3] preference: 5G, 70Ghz, satellite)
2. Using a blacklist (NO satellite for APPx, NO 70Ghz for APPy, etc...)
3. Links status prediction based on the train location (see Section 3.1.1.7)

3.1.1.5. Packet Forwarding to the Radio Access Modules

As already mentioned, the ACS-GW acts as a relay between the end-user devices and the radio access networks. The ACS-GW does not embed any radio interface for the actual transmission of the packets

[3] APPx refers to Generic Application ID. Each application ID is associated to a forwarding policy that has a RAN preference list.

toward ground. All radio access networks are accessed through external modules (i.e., radio access units) responsible for the actual transmission over the radio links.

The following radio access technologies are considered:

1. 3GPP 5G
2. 70 GHz IEEE 802.11ad
3. Satellite

The ACS-GW delivers the packets to the different radio access units on board by simply changing the the destination MAC address in the packet, as with standard MAC forwarding.

It is important to note that also the radio access network selection is performed on a per-application basis. From the point of view of IP forwarding, this resembles to a policy-based routing scenario in which the routing decision is not made only according to the destination IP address, but it rather takes into account more complex policies. Even if the Linux kernel supports the policy routing paradigm, the ACS-GW will not use the standard IP networking subsystem implemented by the Linux kernel. Instead, the ACS-GW functions responsible for the actual packet forwarding will be realized at a lower layer, most likely within the eBPF/XDP (extended Berkeley Packet Filter – eXpress Data Path) framework [19]. As for the policy based routing approach, the ACS-GW will be able to:

1. take independent forwarding decision for each application flow
2. balance the traffic of a given application over different radio access networks
3. enforce a granular selection on what application flows share the same radio access network

3.1.1.6. IP Mobility

The services supported by the 5GMED project require the support for seamless mobility, meaning that the end-user applications should not be affected by handovers or cross-border roaming. Unfortunately, changing the radio access network may modify the IP source address of the packets coming from the train. This is for example the case of a handover between 5G and satellite or from the 70 GHz network to the 5G network.

In this case, all application connections are not preserved upon such handovers. Some IP mobility techniques should be enforced for applications requiring seamless mobility. The research community has widely addressed IP mobility over the last 30 years, and a plethora of solutions have been proposed, including [20].

At a very high level, the 5GMED IP mobility scenario presents the following requirements:

1. it cannot rely on the exchange of routing information among the different core networks
2. it should support a per-application forwarding approach in which the individual application flows are managed independently
3. it should consider the involvement of access networks with private addressing that require Network Address Translation processing

4. it should be transparent to the end-user devices and the application servers
5. it should be easily integrated within the ACS-GW, as it is the relay point of all traffic between the train and ground.

A possible solution to this problem may be based on a tunnelling overlay mechanism, Figure 50, as the one proposed in Universal Per-Application Mobility Management Using Tunnels (UPMT) [21].

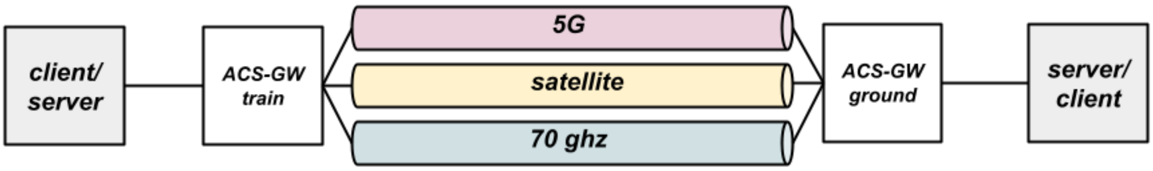


Figure 50: Overlay Tunnel Approach for seamless IP mobility.

The idea is to establish different IP/UDP tunnels between the ACS-GW unit on board and a mobility anchor on the ground (particularly with the ACS-GW unit on ground) and encapsulate the original IP packets sent by the end-user application within them. By doing so, the ACS-GW can change specific radio access networks and at the same time preserve the original IP packet.

From the network topology point of view, the only requirement is that the mobility anchor on ground should be reachable from all possible radio access networks.

From an operational point of view, this approach requires the implementation of a control agent responsible for:

1. establishing the IP/UDP tunnels before the actual packet forwarding;
2. keeping the tunnel alive by means of keepalive messages. This will ensure that *a)* the radio access links are up, and *b)* the NAT (Network Address Translation) binding in the path between the two middleboxes are kept open.

In other words, this approach requires a simple signalling protocol responsible for the above-mentioned functions.

Without entering into the details of the final mechanism implemented, and Figure 52 summarize the processing of a packet sent from a client (C) on the train to a server (S) on ground, the packet is forwarded through the ACS-GW on board, the radio access, (RA) the gateway (GW) and finally the ACS-GW ground forwards it to the server (which can be either in the MEC or in the cloud), and vice versa, from the server on ground to the client on board.

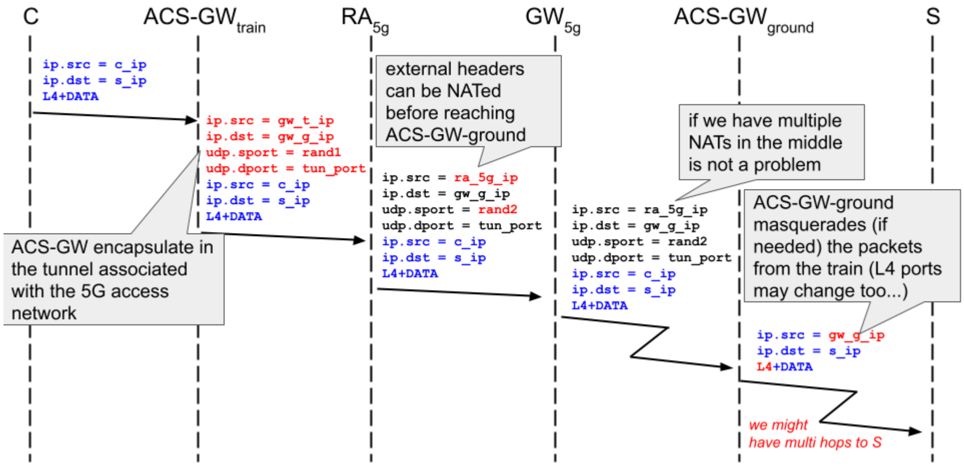


Figure 51: Packet processing from train to ground.

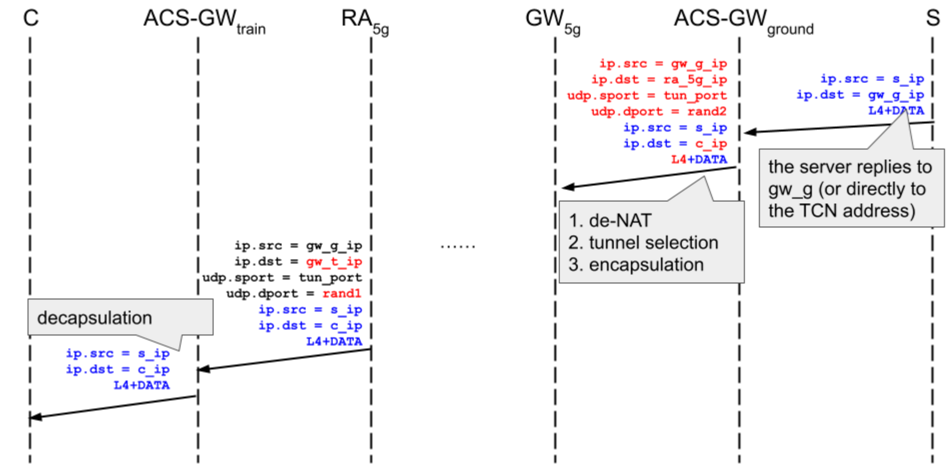


Figure 52: Packet processing from ground to train.

This approach appears to be well suited for the 5GMED scenario, for the following reasons:

1. this only requirement is the reachability of the *mobility anchor (the ground ACS-GW)*
2. it is NAT friendly
3. it can be implemented easily and efficiently
4. it supports the per-application forwarding strategy of the ACS-GW
5. the tunnel establishment/refreshment can be leveraged by the ACS-GW to understand if the *Ground ACS-GW* is reachable from the available radio access networks
6. it adds a negligible latency in case of communication with a server in the MECs

7. it could support the deployment of multiple mobility anchors on the ground (in the different MECs)
8. it can be applied only to the traffic flow that requires seamless IP mobility
9. as only IPv4/IPv6 packets are encapsulated, the tunnels can support an in-band signalling protocol that can also be used to implemented advanced mechanisms, e.g., packet duplication.
10. it provides an implicit way of reaching a server inside the train without requiring to establish other mechanisms (like a VPN, a remote port forwarding or a reverse proxy)

On the other hand, the following aspects should be carefully addressed:

1. the packet detour required may result in a non-negligible additional latency (for example, this may be the case of UC4 – FollowMe Infotainment). Nonetheless, it should be noted that the ACS-GW can also work in a hybrid mode in which a subset of the applications are simply forwarded through the available RANs without encapsulation. If on the one hand this would not preserve the IP session contiuity feature in case of masqueraded access networks, on the other hand it removes the necessity of terminating the IP/UDP tunnel on the ground units.
2. it requires to change the MTU on the end-user device to avoid the necessary IP fragmentation that would be performed by the ACS-GW. This can be transparently solved by configuring the MTU with the specific DHCP option. The Linux ISC DHCP server supports this option (clients' support should be verified).
3. it clearly introduces a bottleneck. In any case, given the aggregated throughput target, this should be not a problem
4. it introduces latency in case of handovers (i.e. the tunnel should be established before the actual packet forwarding). In any case, even without tunnels, the ACS-GW needs to detect that a given radio access network is up

3.1.1.7. Links status prediction based on the train position

The forwarding intelligence implemented by the ACS-GW can leverage the knowledge of the current train position. Assuming that a mapping between the radio coverage and the train position is provided, this could be exploited to predict the status of the different access links. To achieve the necessary information for the intelligent forwarding the ACS-GW can implement different interfaces to external modules. These include an interface to receive the real-time train position.

3.1.2. Ground ACS-GW

The ground ACS-GW is a module that is functionally equivalent to the ACS-GW unit on board the train from a high-level point of view. More specifically, the ground ACS-GW implements the same following functions as the ones described in section 3.1.1:

1. it acts as an aggregation point of the packets sent from the ground devices toward the end-user devices on board
2. it acts as a relay toward the different gateways to the radio access networks connected to the train
3. it classifies the active application flows
4. it keeps tracks of which radio access networks can be used to reach the train with an independent per-application flow approach
5. it terminates the overlay tunnels established from the train required to provide seamless IP mobility (when required)

In the remainder of this section, we underline the differences between the ground ACS-GW and the on-board ACS-GW concerning the detailed description of the on-board ACS-GW provided in section 0.

3.1.2.1. Network Topology and ACS-GW placement

Figure 53 shows the ground network topology designed at the time of writing, consisting of two main segments associated with the two countries traversed by the 5GMED corridor, namely the French side and the Spanish side. Even if the use of multiple ACS-GWs is not technically required to support this particular topology as already mentioned, two physically distinct ACS-GWs are deployed in the 5GMED project in order to support the project business requirements and a more complex and realistic scenario consisting of multiple independent networks deployed over the entire European area: one in France (the ACSGW_FR) and one in Spain (the ACSGW_ES).

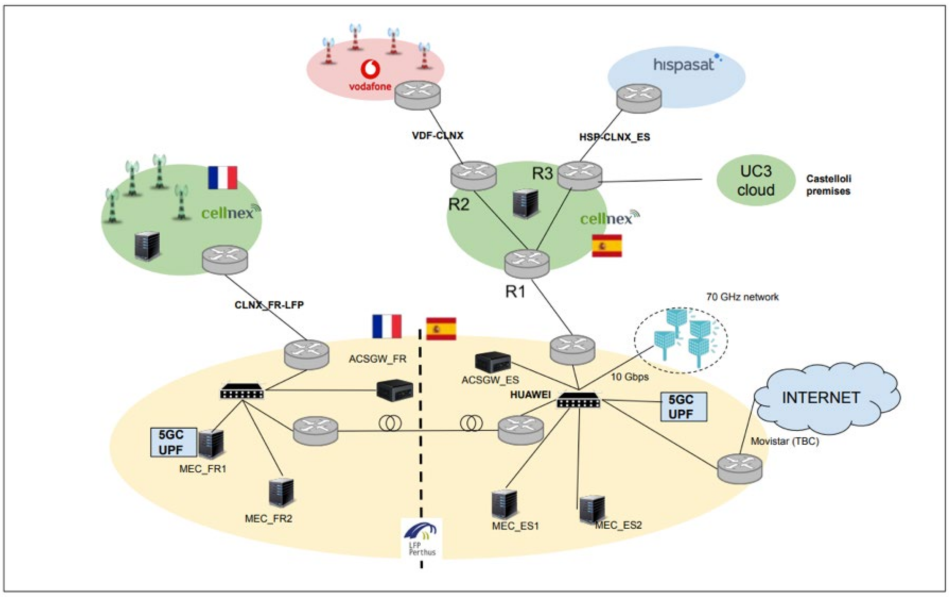


Figure 53: ACS-GW placement in the ground network topology.

The ACS-GW forwarding strategy is based on the following simple approach: when the train is in France, the traffic is forwarded through the tunnels established between the ACS-GW unit on board and the ACSGW_FR. Vice versa, when the train is in Spain, the traffic is forwarded through the tunnels established between the ACS-GW unit on board and the ACSGW_ES.

These two ACS-GW units on ground (ACSGW_FR, ACSGW_ES) have the same requirements:

1. They need to be reachable from the ACS-GW unit on board
2. They need to be considered as the gateway toward the TCN
3. They need to differentiate the traffic coming from the different RANs.
4. They need to differentiate the traffic sent back to the TCN and meant to be forwarded through the different RANs

Regarding the only integration of the ACS-GW, the 5GMED ground network has been designed according to the following principles:

1. Both ACS-GW units on-ground require to be configured with an IP address which is routable from all the different RANs. It is not mandatory that this IP address is public, provided that (i) all routers in the path between the TCN and the ground network know a route to the ACS-GW on ground; (ii) the internet access router is configured to masquerade the packets. As the two ACS-GW units on ground sit on the same network in which different 5GMED use case components are deployed, this requirement does not introduce new challenges for the overall architecture.
2. The ACSGW_FR must be seen by all servers and routers in the French side as the next hop to the TCN. Similarly the ACSGW_ES must be considered by all servers and routers in the Spanish side as the next hop to the TCN. This requirement is tackled by a proper configuration of the IP routing plane, which can be done either statically or dynamically with any routing protocol (e.g., OSPF). Clearly, a situation in which the train is in one country but the correspondent ground host/server is in the other one should be supported. In this case traffic will be encapsulated withing a bidirectional tunnel between the two ACS-GWs.
3. Both ACS-GW units on ground need to differentiate the (tunnelled) traffic coming from the different RANs. This can be done at different layers, including: (i) layer 2, i.e., traffic coming from the different RANs are distinguished according to different MAC addresses; (ii) layer 3, i.e., different IP endpoints for the tunnels received from the different RANs; (iii) layer 4, i.e., different UDP ports associated to each tunnel. The association between the tunnels and the RANs is done trough the implementation of a control message interfaced multiplexed within the same IP/UDP overlay data channels.
4. Unfortunately, the approach mentioned above is not sufficient to properly deliver the tunnelled traffic sent back to the TCN to the proper border gateway facing these RANs. This is because it is impossible (and also unrealistic) to deploy the ACS-GW units on the same L2 network containing all the RAN border gateways. As it appears clear from Figure 53, there are different "intermediate" routers in the path between the ACS-GWs and the border routers. These routers are totally unaware of the 5GMED policy routing approach (which is based on RAN availability, preference and train position) and implement their forwarding behaviour

purely on a destination IP basis. To solve these problem without requiring the border gateways to NAT the incoming packets addressed to the ACS-GWs, we leverage the current TCN architecture's support for multiple VLANs. The train ACS-GW will therefore be placed between the VLANs of the end user devices and the VLANs of the different radio access units on board. While in the past months the possibility to deploy the different on board radio access units on different VLANs was just a desirable option to support the multi stake-holder business model of the project, it now becomes mandatory. Since now the on board ACS-GW has necessarily multiple IP addresses for each of the VLAN on board, the tunnels coming from the different RANs will have different source IP addresses. All the routers in the middle between the ACS-GWs on ground and on board are thus able to configure different routes for the different VLAN subnets associated to the specific RANs. For example, traffic meant to be forwarded back to the TCN through the satellite link will have a destination IP of the satellite access unit's VLAN on board, while traffic meant to be forwarded back to the TCN through the 5G networks will have a destination IP of the 5G access unit's VLAN on board. This allows for example router R1 to differentiate the path to reach the TCN via the satellite (via router R3) and the path to reach the TCN via the 5G network (via router R2).

3.1.2.2. Packet Forwarding Strategy

In principle, the ground ACS-GW replicates the same operations as the ACS-GW unit on board. In other words:

1. It keeps track of the application flows received from the train and maintains the binding between the relative transport layer 5-tuples and the RANs from which the flows were received.
2. It decapsulates the packets sent from the train.
3. It intercepts the packets sent toward the train.
4. It identifies the applications sending the packets.
5. It forwards the packets to the gateways responsible for reaching the train via the different radio access networks, performing encapsulation when required.
6. It keeps track of the tunnel keep alives received trhoguh each of the available RANs and it performs handovers if the current RAN cannot not be used reach the train TCN.

The forwarding behaviour of the ground ACS-GW unit and train ACS-GW unit depends on the application flow direction. For flows initiated on board, the train ACS-GW unit is responsible for classifying the application and forwards packets according to the current network availability, while the ground ACS-GW unit automatically learns the association between application flows and RAN used to deliver the packets. For flows initiated on ground, the role is swapped. The ground ACS-GW unit is responsible for classifying the application and forwarding packets according to the current network availability, while the train ACS-GW unit automatically learns the association between application flows and RAN used to deliver the packets.

Nevertheless, it is worth noting what follows. The ACS-GW will always detect that a radio access network is not available before the ground unit. As soon as the train ACS-GW understands that a handover is necessary, a set of application flows are sent through a different access network, and the ground ACS-GW will understand where to forward the response packets by simply keeping track of which network the request packets are originating from. Unfortunately, this approach is useless in the case of application protocols in which a request from the client generates a “long” data flow sent from the server (e.g., UDP streaming). Anyway, it should be noted that both units are constantly checking the keep-alive exchange and thus also the ground unit is able to move all the application flows associated with an unreachable RAN as soon as the keep-alive mechanism detects such unreachability.

In conclusion, it is worth noting that also the ground ACS-GW can leverage information regarding the real-time train position. For example, when the train is in the tunnel, the ground ACS-GW will send all application flows through the in-tunnel 5G network without considering any other information.

3.2. V2X gateway

The objective of the V2X gateway is to ensure vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications by playing a role of V2X application server specified by 3GPP in TS 23.285 and TR 23.786. It is the key entity that allows the exchange of V2X messages among vehicles and infrastructure. Furthermore, V2X gateway enables interfaces to other technologies particularly ITS G5 or C-V2X for the vehicles that are beyond 5G cell coverage or those that are equipped with only such a technology. As illustrated in Figure 54 (already presented in D4.1 [22]) and Figure 55, the V2X gateway is installed at the MEC level and interfaces with different telecommunication infrastructures, mainly RSUs equipped with C-V2X and/or ITS-G5 technologies and 5G gNBs. Each V2X gateway has a service area, which is defined by the union of the coverage ranges of RSUs and gNBs, with which it has direct interfaces. In particular, ITS-G5 and C-V2X RSUs will make simple L2 or L3 forwarding of V2X message between vehicles and V2X gateway. On the other hand, the N6 interface (N6 traffic routing information) will be used between the 5G and the V2X gateway as specified in 3GPP TR 23.786.

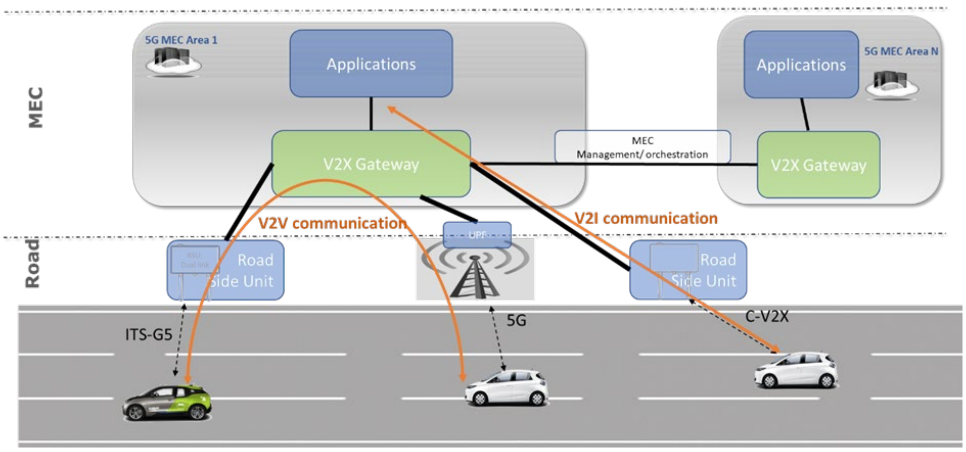


Figure 54: V2X Gateway disseminating V2X messages using multiple technologies: 5G, C-V2X, and ITS-G5.

Funded by the Horizon 2020 Framework Programme of the European Union

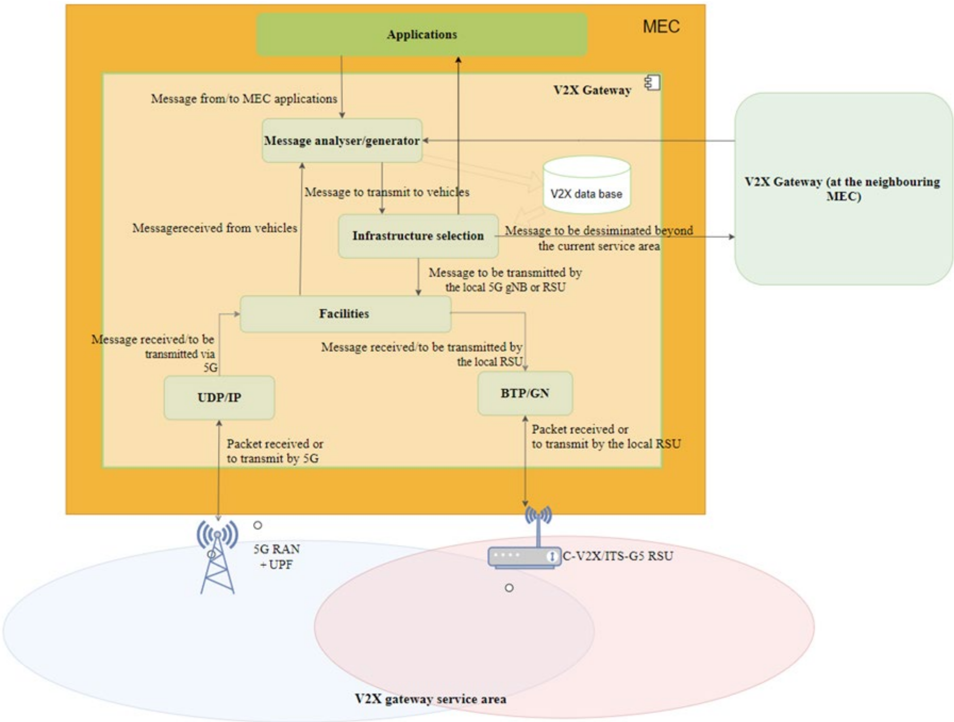


Figure 55: Architecture of a V2X gateway.

V2X gateways on different MECs will inter-operate to disseminate messages beyond the range of the service area of a given V2X Gateway. Each of 5GMED MEC node will be supplied with one instance of V2X gateway, and the V2X gateways will always be activated on the MECs, without the need for service migration between individual V2X gateways. The computational requirements of a V2X gateway are shows in Table 32.

Table 32: technical requirements for the V2X gateway.

Feature	Detail
Processor	Intel core i7-4930K CPU @ 3.40 GHz × 8
Memory	8 GB
Hard disk capacity	100 GB
Graphics	No graphic
OS type	64 bits
Operating system	Ubuntu 18.04.6 LTS
Technology	802.11p, 4G, 5G,
Physical Ethernet intefaces	TBD (e.g. 1 for RSU and 1 for 5G)
Virtuel Ethernet interfaces	TBD (min one)
Dependencies (SW)	Docker

Moreover, by exploiting multiple communication infrastructures with overlapping coverage, the V2X gateway can also provide solutions for increased bandwidth or improved reliability.

The key intelligence for the above functionalities is provided for outgoing packets (to be supplied to MEC applications and/or vehicles). Figure 56 depicts the flow chart of outgoing message processing.

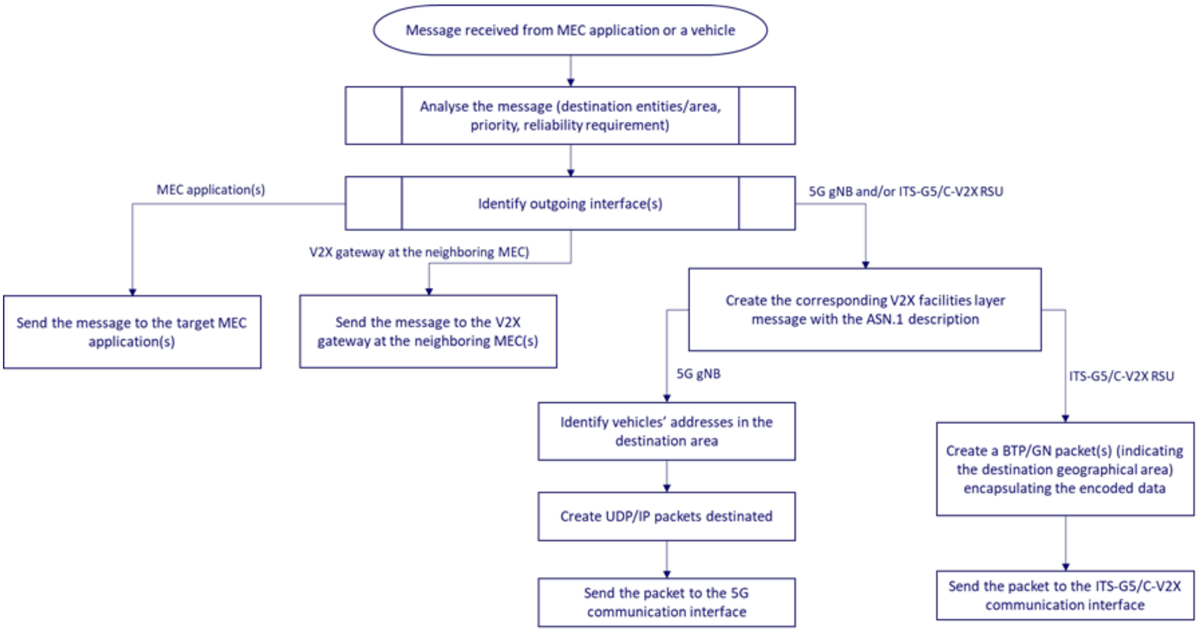


Figure 56: Processing of outgoing messages at the V2X gateway.

As shown in Figure 56, upon reception of a message (from MEC application, vehicles or neighbouring MEC), the V2X gateway analyses the message, particularly identifying the destination entities or geographical areas, priority of the message, and reliability requirement. This procedure is carried out at the message analyser module (see Figure 55). Once the message is analysed, the V2X gateway will identify the outgoing interfaces for the message. The message can be sent to a MEC application(s) and/or vehicles that are in its service area and/or vehicles beyond its service area. Such an interface identification is made by the infrastructure selection module. If the message is to sent to applications in the MEC and/or a V2X gateway at a neighbouring MEC, the message is provided directly by the infrastructure selection module. If the message needs to be transmitted over 5G and/or C-ITS/ITS-G5 interfaces, an ASN.1 encoded message is generated and encapsulated by UDP/IP or BTP/GN (GeoNetworking) headers. Facilities server, UDP/IP, BTP/GN modules are dedicated for these procedures. Specifically, if the message is to be sent by an ITS-G5/C-ITS RSU(s), the GN header indicates the destination area. If the message is to be sent by 5G, the V2X gateway identifies the vehicles in the target destination area, particularly their IP addresses. For this reason, the V2X gateway maintains the V2X database, which contains information on radio coverage of the different communication interfaces, the service coverage of neighbouring v2X gateway, vehicles' positions and addresses. Depending on the level of complexity of the 5GMED network and infrastructure deployment (e.g., RSUs and gNBs have large overlapping coverages and vehicles have multitude types of interfaces), technology selection may need a machine learning model.

Funded by the Horizon 2020 Framework Programme of the European Union

4. Roaming architecture for low-latency communications

In Deliverable D3.1 [1], we have analysed different options to reduce latency in roaming scenarios. In addition, we also discussed the two possible architectures of roaming, mainly Home Routed (HR) roaming and Local Break-Out (LBO) roaming. Based on this analysis and the available features provided by the Druid core, the following approach will be considered in the 5GMED project.

The LBO roaming will be used especially for delay-sensitive use cases such as Use cases 1 and 4. Using the LBO roaming, the user plane traffic does not need to go to the home User Plane Function (UPF) as in the case of HR roaming. This is critical especially for Use case 4, where the application server will follow the user equipment by migrating the allocated resources from one MEC to another as shown in Figure 57. Therefore, it is important that the final UPF, which is connected to the serving MEC, is very close to the new closer MEC. The LBO roaming has been added to DRUID roadmap and will be available in Quarter 2 of 2022.

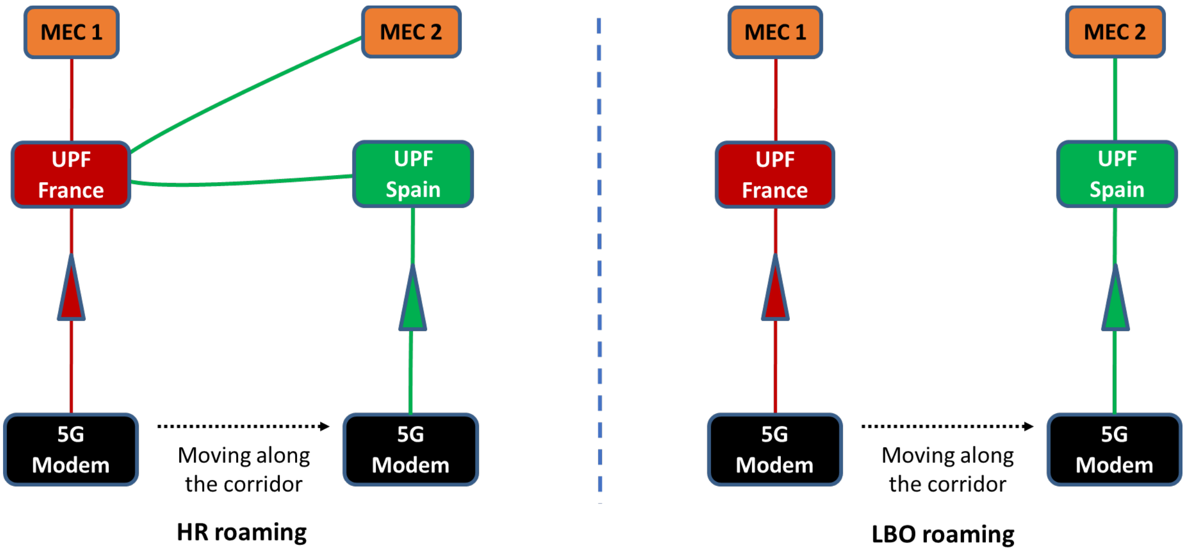


Figure 57 Comparison between LBO and HR roaming for UC4.

In addition, the approach based on the deployment of the N14 interface and proposed by the 5GAA [23] will be also adopted. In this approach, as it was discussed in Deliverable D3.1, the N14 interface between the AMF in the home network and the AMF in the visited network will be deployed. By using this interface, the interruption time can be reduced very significantly by allowing a fast establishment of UE connection. In fact, an proactive UE context transfer to the visited network will be performed when the UE is close to the border; as shown in Figure 58, the AMF in the visited network will contact the AMF in the home network to retrieve the UE context. Hence, the UE context will be available in the visited network when the UE cross the borders and attach to the visited network. The N14 interface is already in the roadmap of DRUID and will be available in the third quarter of 2022.

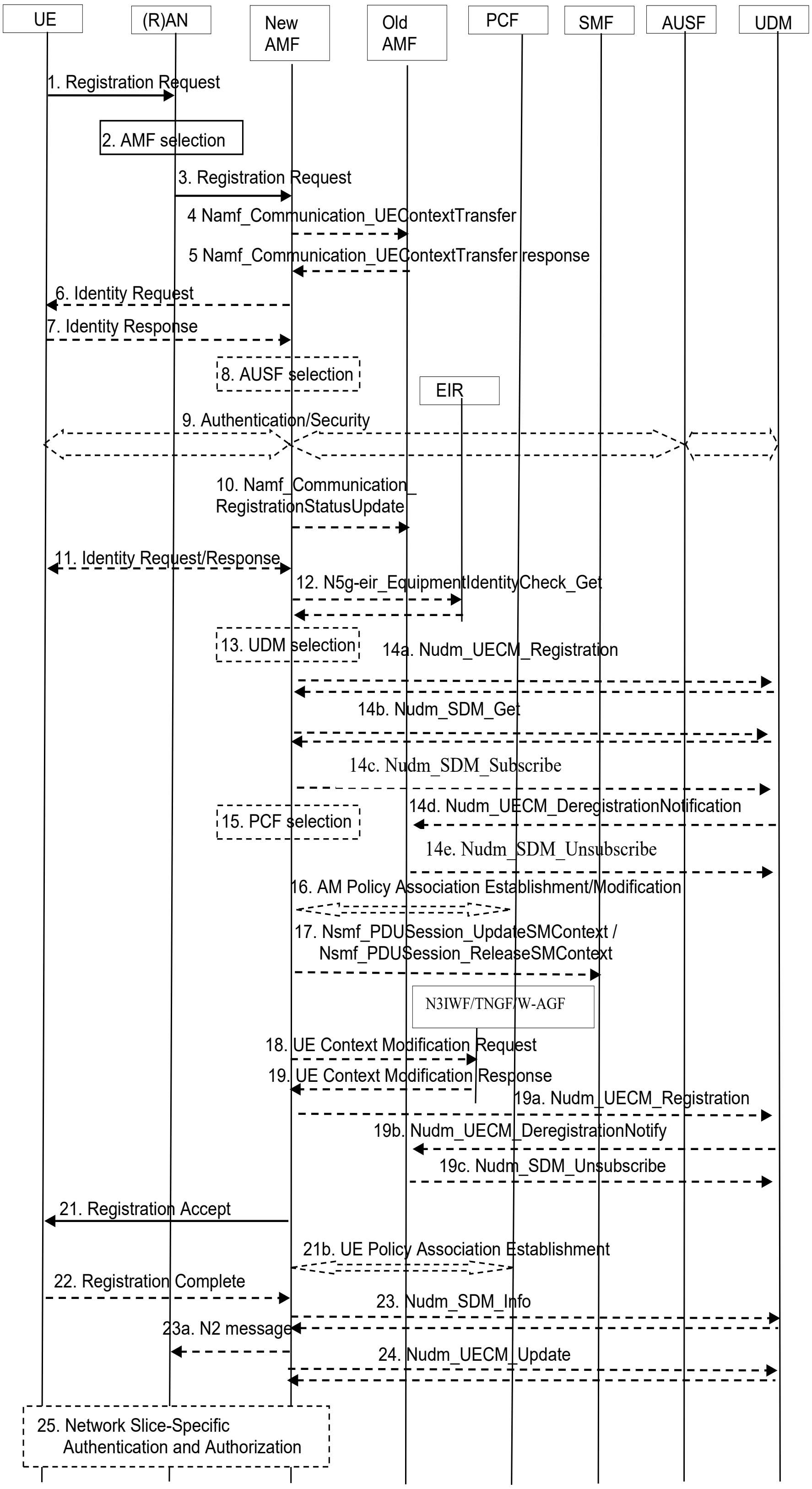


Figure 58 Registration procedure using N14 interface [24].

5GMED will be a great opportunity to test this approach together with LBO roaming, as it was not tested before.

Furthermore, and in order to reduce failed attachements, the home and the visited PLMNs will be configured as Equivalent PLMNs in the UE.

Funded by the Horizon 2020 Framework Programme of the European Union

5. Security for 5GMED infrastructure

Ensuring cybersecurity protection is crucial in the 5GMED project, particularly in UC1 of teleoperated driving and UC2 of road digitalization for hazard detection. In addition, a cybersecurity attack in UC3 or UC4 can reduce application performance and degrade the passenger experience. To provide security against cyber-attacks, 5GMED implements the standard security procedures outlined in 5G network standards[4], as detailed below.

The 3GPP committee has established six tiers of security for 5G networks [25].

Network access security (I): the collection of security characteristics that enable a UE to securely authenticate and access network services, including 3GPP access and non-3GPP access, and to guard against attacks on (radio) interfaces. Two important security elements in the 5G network access procedures are (1) mutual authentication between the UE and the network and (2) key agreement utilized to supply keying material to secure subsequent security processes.

The following are the security protocols used in the access procedure. The 3GPP committee [25]- [26] supports two Authentication and Key Agreement (AKA) protocols named 5G AKA the Extensible Authentication Protocol (EAP)-AKA protocols to execute mutual authentication and key agreement in the 5G network. To provide mutual authentication, a UE can use the 5G AKA or the EAP-AKA'.

The following security measures are included in the handover procedure. During the handover, the 3GPP committee has established the various mobility scenarios for the 5G system, including Mobility intra New Radio (NR), Mobility inter-3GPP access, and Mobility between the 3GPP and untrusted non-3GPP access [27]- [28]. A key management technique similar to that used in the 4G system has been provided to achieve a safe handover procedure in Mobility within New Radio (NR). The handover method from a non-3GPP source access to a 3GPP target access is based on the 3GPP access's Protocol Data Unit (PDU) session creation mechanism. The UE must implement the EAP-AKA' or 5G-AKA process before performing the PDU session setup procedure for 3GPP access.

Network domain security (II): include the set of security elements that allow network nodes to exchange signals and user plane data in a safe manner. The 5GC network functions use state-of-the-art security protocols such as TLS 1.2 and 1.3 at the transport layer and the Open Authorization (OAuth) 2.0 framework at the application layer to guarantee that only authorized network functions have access to a service provided by another function.

User domain security (III): the set of security elements that protect the user's access to mobile devices. On the user equipment side, it is divided into three domains: mobile equipment (ME), universal subscriber identification module (USIM), and identity management (IM). The logical functions necessary for accessing network services and utilizing user applications are contained in the

[4] Security procedures for non-3GPP access technologies will be addressed in the next deliverables, i.e., D3.3 and D3.4.

ME and USIM domains. The IM domain is a critical component of our 5G security architecture since it includes capabilities to provide alternatives to USIM-based authentication.

Application domain security (IV): the collection of security measures that allow apps in the user and provider domains to safely exchange messages. In this domain, no protocols are provided.

Service-Based Architecture (SBA) Domain security (V): the collection of security elements that allow network functions in the SBA architecture to safely connect inside the serving network domain and with other network domains. These characteristics include network function registration, discovery, and authorization security elements, as well as service-based interface protection. The primary components of SBA security include TLS-based authentication and transit protection between network operations, as well as an authorization system based on OAuth2.

Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

Finally, another important element is **physical security**. As shown in the following figure, different recommendations and policies must be enforced to ensure physical access against unauthorized personnel.

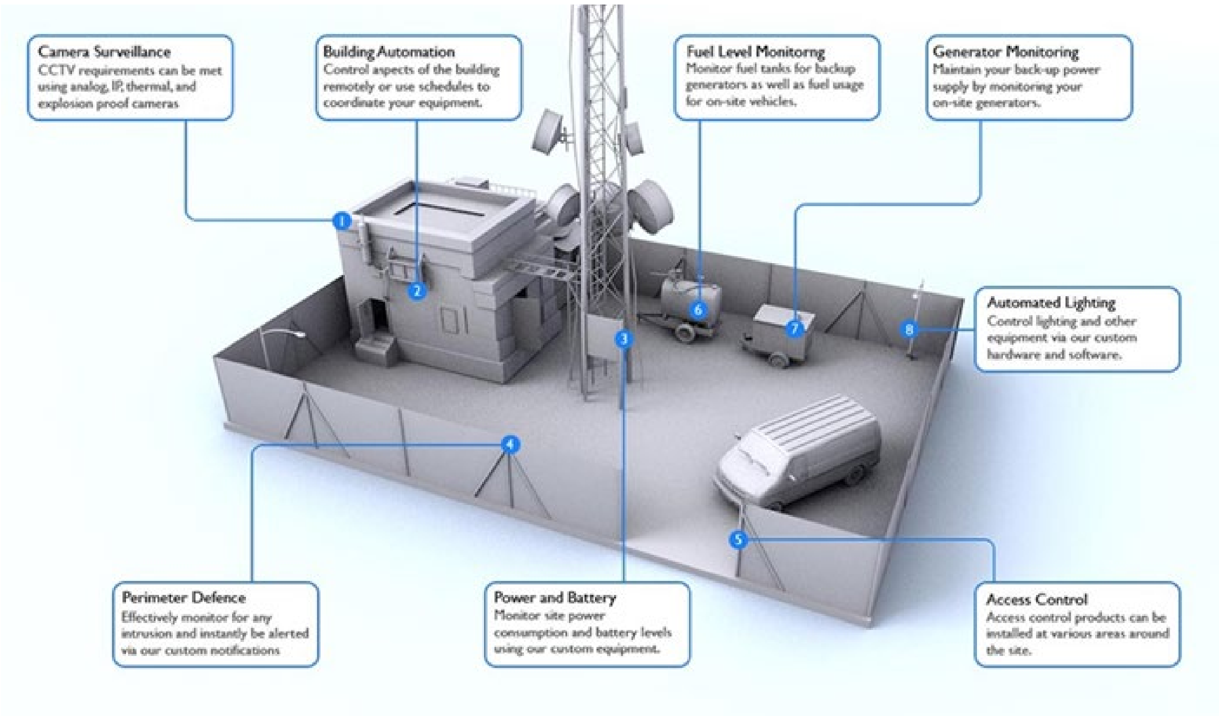


Figure 3: Recommendations for ensuring cell tower security (figure obtained from [29]*).*

Camera Surveillance: All the sites must be surveilled remotely through cameras and intelligent software and backup tools must be used.

Building Automation: Since most towers are unattended, use of building automation is mostly recommended for controlling lights and executing theft deterrent activities.

Generator and Fuel Level Monitoring: Cell sites may be not connected to the electrical grid. In such case, critical infrastructure must be equipped with a backup generator to allow the connectivity to continue during the power outages.

Power and Battery Monitoring: as already mentioned, cell towers are critical infrastructure and require battery backup in case of a blackout. Such batteries must be 24/7 monitored to guarantee continuous operation.

Perimeter Defence and Access Control: it is fundamental to including several layers of physical security to surveil and protect such important assets. A perimeter intrusion system is needed, as well as additional tools which monitor and secure the most valuable and vulnerable assets such as the batteries, fuel supplies and generators. It is also high-priority to fit a high-tech padlock solution that can add significant confidence that the most important assets are accessed only by authorized personnel, as well as enhancing the capability of tracking and reporting on such access on a long- term basis.

6. Onboard TCUs

This section presents the initial design and development of the multi-connectivity TCUs employed in 5GMED to support the automotive UCs, i.e., UC1 and UC2. More specifically, three different modules are being implemented by Valeo, CTTC and VEDECOM, and will be then validated through interoperability testing procedures being devised within WP6.

6.1. Valeo TCU

Valeo is being developing a 5G prototyping platform named "Vulcano", providing cellular connectivity, V2X connectivity, and GNSS positioning capabilities. On the one hand, Vulcano-5G v1.2 embeds a Quectel industrial-grade module, namely RG550Q-EU, based on the Qualcomm SDX55 chipset. On the other hand, Vulcano-5G v2.0 is fitted with Quectel AG551Q-EU, an automotive-grade Network Access Device (NAD) fitted with the Qualcomm SA515M chipset.

Figure 59 shows the inside of Vulcano-5G v1.2 with RF pigtail cables connecting the RF connectors on the circuit board to the connectors fixed to the plastic housing. The large module in the middle of the board is the 5G Quectel NAD.

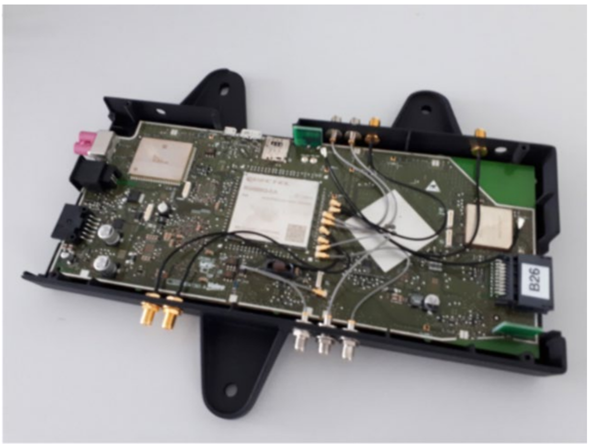


Figure 59: Internal picture of the industrial-grade Vulcano-5G TCU.

Figure 60 shows the high-level architecture of Vulcano-5G, where all the technical specifications of the system are listed.

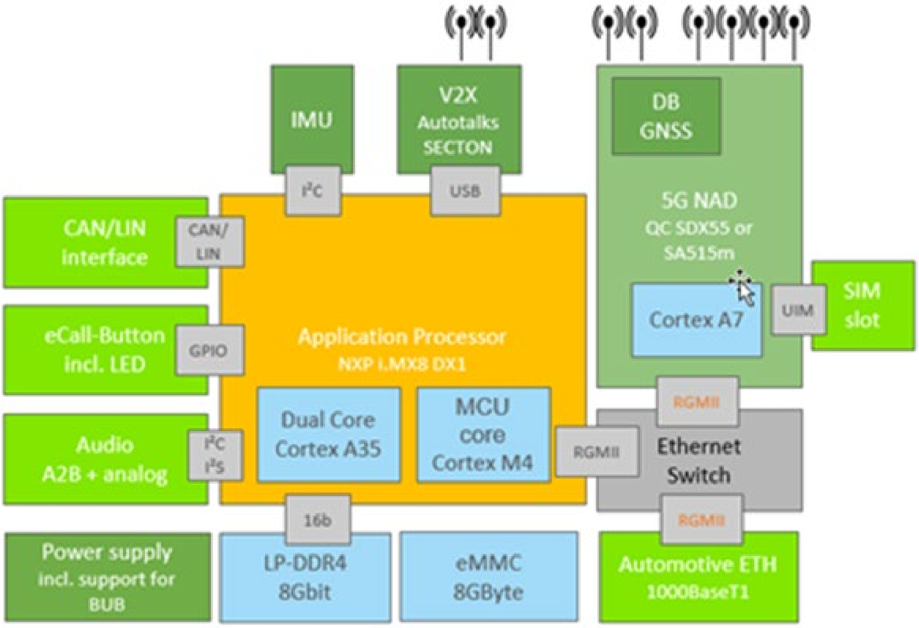


Figure 60: Vulcano 5G high-level architecture.

The data routing from Cellular to Automotive Ethernet 1000BaseT1 is available through an on-board ethernet switch. A hardware IPA (IP Accelerator) inside the 5G NAD ensures high-speed data traffic in such a configuration. A media converter is needed to perform the physical layer conversion between Automotive Gigabit Ethernet and a PC System with Standard Gigabit Ethernet (1 Gbit/s, 1000BASE-T). Besides ethernet connectivity, USB3.0 tethering is also offered. It is also possible to connect and control an external modem through the USB2.0 port of the IMX8 (successfully tested: Quectel RM500Q and RG500Q). Enabling such a dual-modem configuration, i.e. the Vulcano-5G Rel-15 modem and an external Rel-16 modem, should improve the service continuity thanks to the dual-SIM connectivity.

Valeo conducted some 5G field testing of its industrial-grade Vulcano-5G TCU on the Vodafone live network in Freiburg, Germany. The goal of this testing was two-fold: firstly, to verify if the signalling procedure for LTE - 5G NR dual connectivity establishment was successful and secondly, to perform some Layer 3 DL throughput measurements, as shown in Figure 61. The mobile network was configured in non-standalone (NSA) mode, with the E-UTRA anchor cell operating in FDD Band 3 and the NR cell operating in TDD band n78.

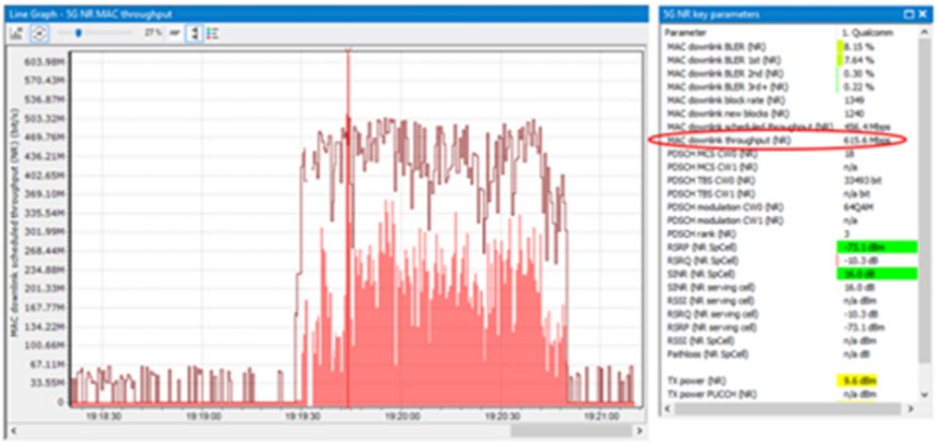


Figure 61: Throughput obtained during a file download operation.

Aside from field testing, Valeo also performed some lab testing on an Anritsu MT8000A test platform, measuring L2/RLC throughput in both NSA and SA modes, as shown in Figure 62 and Figure 63.

Figure 62: RF and Layer 2 Throughput Measurements in 5G NSA mode.

Figure 63: RF and Layer 2 Throughput Measurements in 5G SA mode.

Valeo uses Nemo Outdoor (10), a laptop-based drive test tool from Keysight, to measure and monitor the air interface wireless networks. Figure 64 reports the list of 5G parameters that Valeo monitored on Vulcano-5G v1.2.

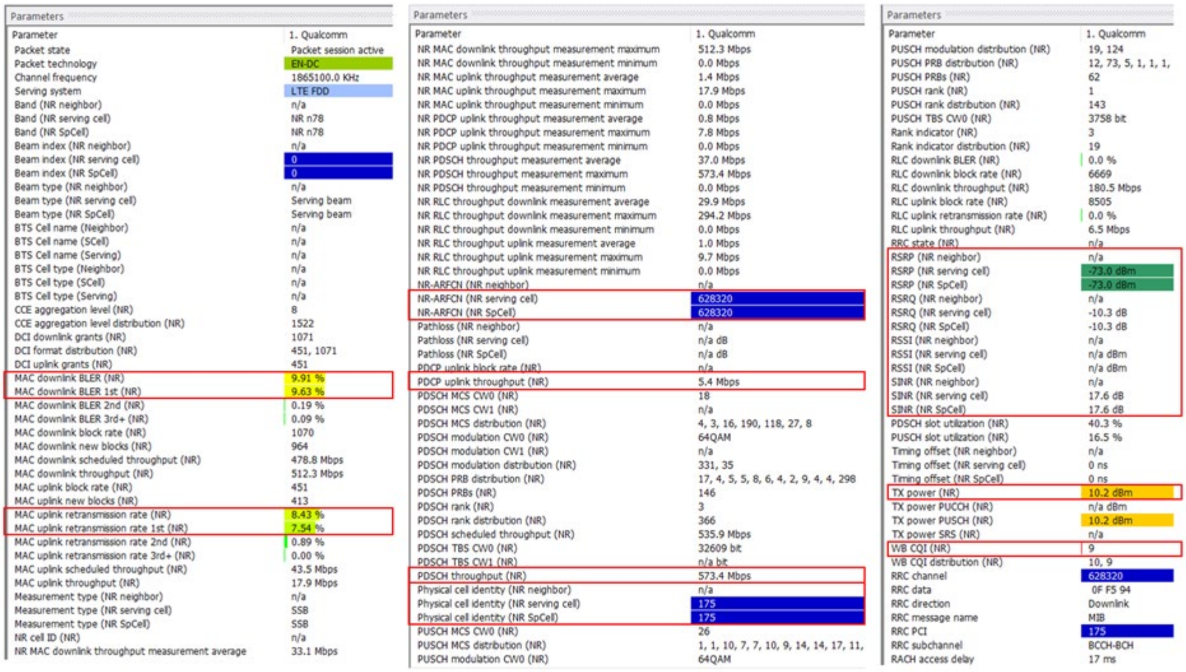


Figure 64: List of 5G parameters can be monitored on Vulcano-5G v1.2.

Some of those 5G Layer1/Layer2 parameters have been marked in red colour. Those metrics have been identified as potential input KPIS for the QoS Prediction Manager. The role of the QoS Prediction Function is to inform as quicky as possible the Valeo Teleoperation Cloud/ Cockpit of potential QoS degradations, so that countermeasures can be taken (such as reducing the speed of the vehicle, reducing the quality of the video streams in UL or stopping the remote vehicle by enabling Minimum Risk Manoeuvre takeover).

The V2X Valeo Platform (V2XVP) is a software platform based on C and C++ language that allows Telematics Control Unit to :

- Receive/send V2X messages (CAM, DENM, MAP, SPaT, IVI and CPM)
- Forward the received V2X Abstract Syntax Notation One (ASN1) messages to other ECUs (RTMaps) /client (linux) over Scalable service-Oriented MiddlewarE over IP (SOME/IP) bus
- Trigger DENM from SOME/IP client (RTMaps, linux)
- Trigger DENM from an Android HMI application
- send DENM notifications (accident, traffic jam, etc) to Android HMI application

To provide these functionalities, the V2XVP is composed of two main software components, as shown in Figure 65:

- Stack Interface Facilities Forwarding (SIFF) whose role is to connect to V2X stack API, subscribe to facilities, receive V2X notifications, pass V2X ASN1 messages to ComManager, receive from ComManager road event informations to pass them to V2X stack for DENM triggering.

- ComManager whose role is to publish on SOME/IP bus events containing V2X messages in ASN1 format, send DENM notifications over TCP to the Android HMI, receive road event informations from SOME/IP client (RTMaps, Linux) or Android hmi to pass them to SIFF for DENM triggering.

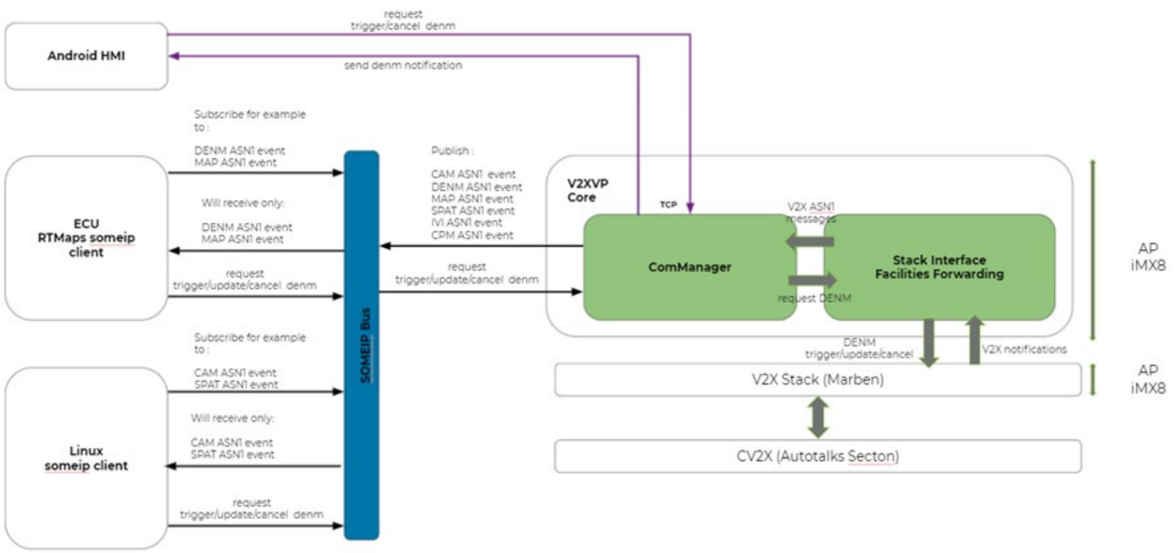


Figure 65: Vulcano V2X functionalities.

6.2. CTTC TCU

The multi-connectivity TCU provided by CTTC will be used for the automotive UC2 and will be integrated in connected vehicles to test the three services specified in UC2 in the local and cross-border scenarios. Figure 66 shows the high-level architecture of the CTTC TCU. As it can be observed at the bottom of the figure, the TCU has two V2X communication interfaces: one 5G interface provided by a stand-alone modem, and another radio interface for direct communication with RSUs and other TCUs using either ETSI ITS-G5 or C-V2X (3GPP Rel-14), but not both simultaneously.

The TCU integrates an embedded computer hosting a V2X Protocol Stack, a UDP Manager and an application client specific for UC2. The V2X protocol stack implements the facilities, transport, networking, and security layers of the V2X communication interfaces. It supports the transmission and reception of several types of ETSI-compliant facility messages, such as, among others, CAM, DENM, MAP and CPM. The UDP Manager supports the exchange of facility messages with the V2X Gateway using UDP over the 5G interface. The UC2 application client receives information of hazards detected by the Smart Sensor, sends the hazards' data to the HMI, and triggers the transmission of DENM and CAM messages through the V2X Protocol Stack. The UC2 Application Client extracts data from the CAM, DENM, MCM and MAP messages received by the V2X Protocol Stack and forwards these data to the HMI.

Funded by the Horizon 2020 Framework Programme of the European Union

The TCU includes a CAN bus interface, a Wi-Fi interface, and an Ethernet interface for on-board communications with a Smart Sensor, an HMI or dashboard. In addition, the TCU contains a GPS receiver for clock synchronization and vehicle positioning.

In order to facilitate the acquisition of measurements for the computation of KPIs, the TCU will send log messages with information associated to each V2X message that has been transmitted or received by the TCU. In particular, each log message will include, among others, the timestamp in which the V2X message was transmitted or received, the V2X message type, the identification of the transmitting entity (e.g., a TCU or V2X Gateway), and the identification of the receiving entity.

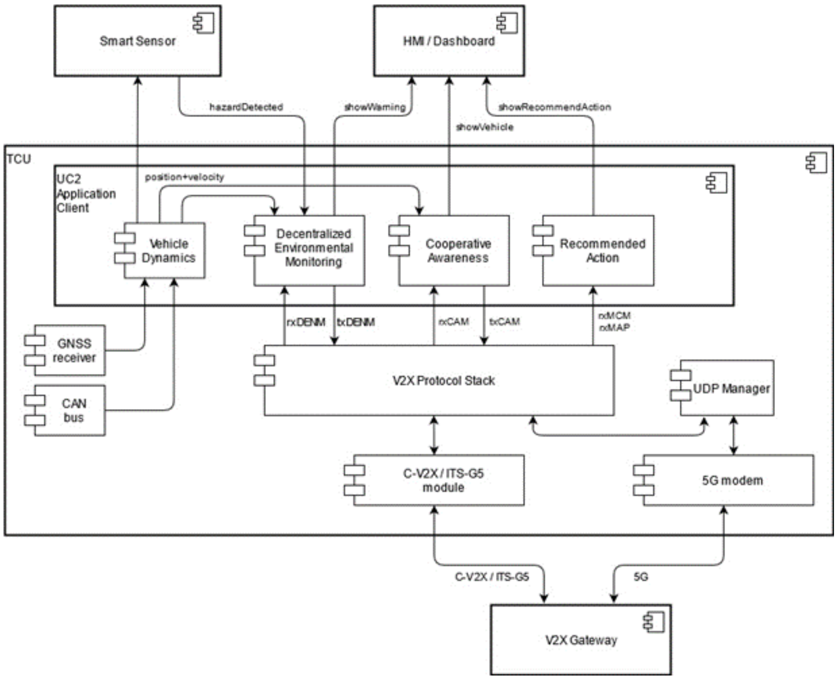


Figure 66: CTTC TCU architecture.

6.3. VEDECOM TCU

VEDECOM multi-connectivity TCU (shown in Figure 67) will be used for automotive UCs and will be integrated in a connected vehicle. Figure 68 shows the TCU architecture. The TCU consists of a compute resource hosting communication layers and applications, particularly TCP/IP and BTP/GN protocol stacks and V2X applications/facilities and other applications such as multimedia. The V2X applications/facilities include Cooperative Awareness Service (CAS), Decentralised Event Notification Service (DENS), Collective Perception Service (CPS), MAPEM (MAP Extended Message), and Manoeuvre Coordination Service (MCS). The TCU has multiple communication interfaces, particularly two 5G NR interfaces (3.5GHz and 26GHz or 3.5GHz and 3.5GHz), Wi-Fi interfaces (IEEE 802.11ac and IEEE 802.11a/b/g/n), ITS-G5/C-V2X, and GNSS receiver. The TCU interfaces with car CAN gateway and HMI device.

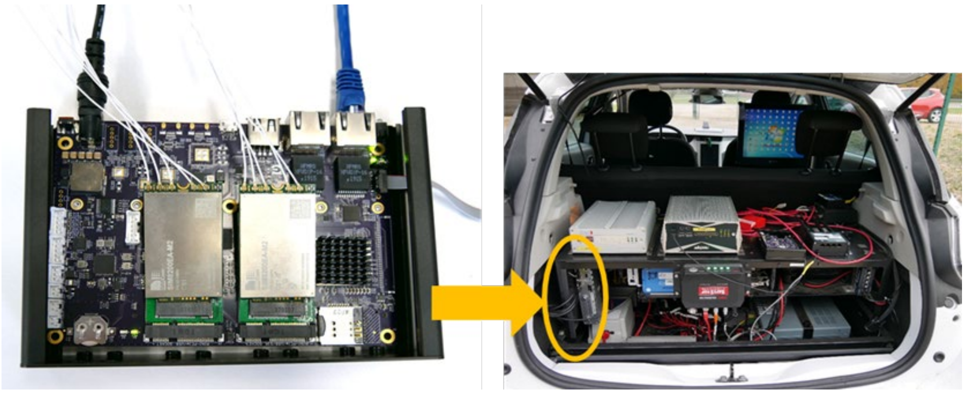


Figure 67: pictures of the VEDECOM TCU.

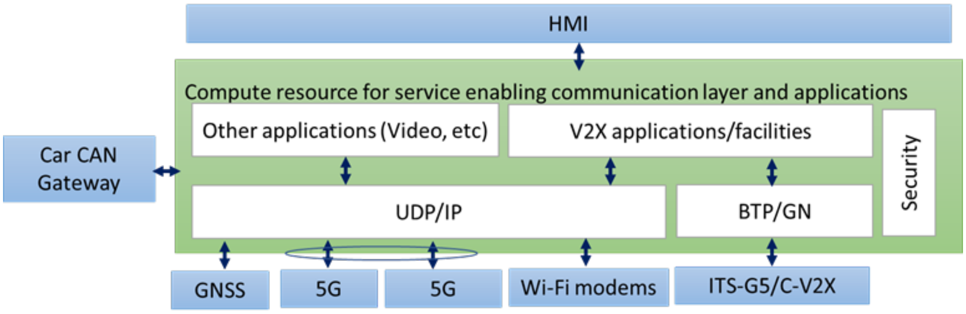


Figure 68: VEDECOM TCU architecture.

The TCU will be able to operate on the 5G frequency bands of n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n40, n41, n66, n71, n77, n78, n79, n257/n261 and n258. Two modems can be used at the same time providing ***dual-SIM connectivity***. Moreover, a ***bandwidth aggregation*** technique can be provided for applications requiring high bandwidth.

The V2X application/facilities transmit and receive V2X packets on both the UDP/IP and BTP/GN stacks, so that the packets can be transmitted/received on 5G and/or ITS-G5/C-V2X interfaces (***hybrid communications and message duplication***). The applications/facilities have duplicate packet detection function to process potentially duplicated oncoming packets.

For co-existing multiple applications, a ***differentiated QoS control*** can be applied to prioritise data flows with high importance w.r.t that with lower importance (e.g., road hazard alert w.r.t cooperative awareness message).

Finally, communication performance can be measured at the different levels: level 0 (radio, see Figure 69, level 1 (networking), and level 2 (applications). The performance logs – signal strength, throughput, delay, packet loss, etc. with timestamp and position data – can be provided to the 5GMED predictive QoS module. Moreover, upon recommendation of the ***Predictive QoS*** module, the data rate, message generation frequency of some applications, particularly Video, CAM, CPM etc can be adapted.

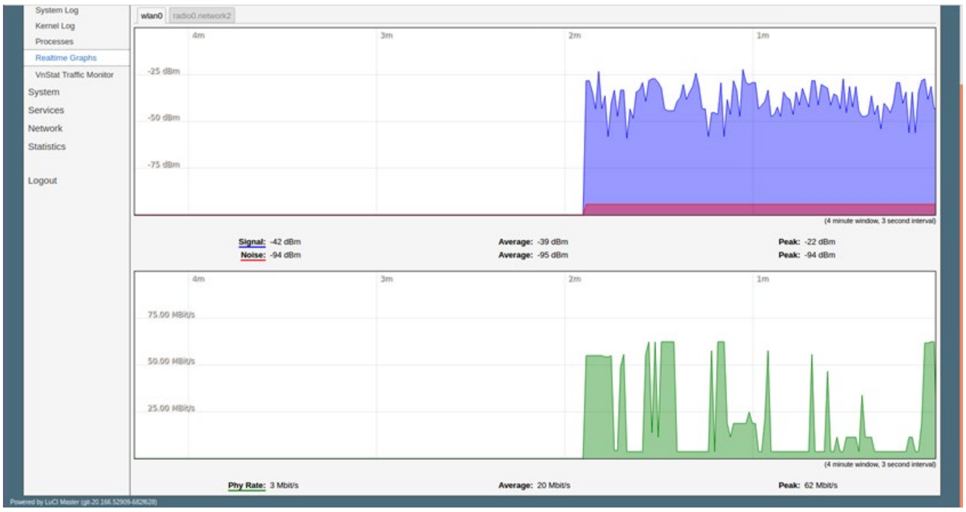


Figure 69: VEDECOM TCU performance measurements.

Funded by the Horizon 2020 Framework Programme of the European Union

7. Initial plan for deployment in small and large-scale testbeds

As described in D2.2 [30], 5GMED will validate and evaluate the performance of the use cases by employing small-scale testbeds, i.e., Castelloli (Spain), Teqmo and Satory (France), as well as in the cross-border corridor. The following subsections give an overview of the deployment activities that will be carried out, together with an estimation of the timeline and a list of dependencies.

For the sake of clarity, each task is identified through a "Task ID", which is a project internal identifier. Furthermore, we provide tables that specify the partners responsible for the task, the start date, the task duration, and also any potential dependency that may impact its execution.

Note that in D2.2 a list of UC-related tests that will be conducted in the 5GMED testbeds is provided. Moreover, D6.1 will present the detailed set of tests proposed to validate the infrastructure elements.

7.1. Castelloli

Table 33 lists the deployment tasks that have been planned for the Castelloli small-scale testbed.

Table 33: Timeline for infrastructure deployment in Castelloli.

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
SSTB-Cast-1	RETE	Lacroix V2X RSU installation, validation and commissioning	Q3 2022	1 month	
SSTB-Cast-2	RETE	Sunwave 5G small-cell installation and validation with Druid 5GC	Q3 2022	2 months	Sunwave supply chain
SSTB-Cast-3	RETE/HSP	VSAT installation	Q3 2022	1 month	Interconnection between HSP and RETE network
SSTB-Cast-4	RETE/HSP	Integration between VSAT backhauling and 5G small cell and validation	Q3 2022	2 weeks	SSTB-Cast-3
SSTB-Cast-5	RETE/CLNXFR	Installation of second 5GC instances for roaming tests	Q2 2022	1 week	
SSTB-Cast-6	RETE	Lab integration and validation	Q3 2022	2-3 weeks	

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
		of Ericsson gNB with Druid 5GC			
SSTB-Cast-7	RETE/VEDE/I2CAT	Integration and validation of V2X gateway	Q3 2022	1 month	SSTB-Cast-1

Moreover, Figure 70 presents the Gantt chart of the deployment activities listed in the previous table.

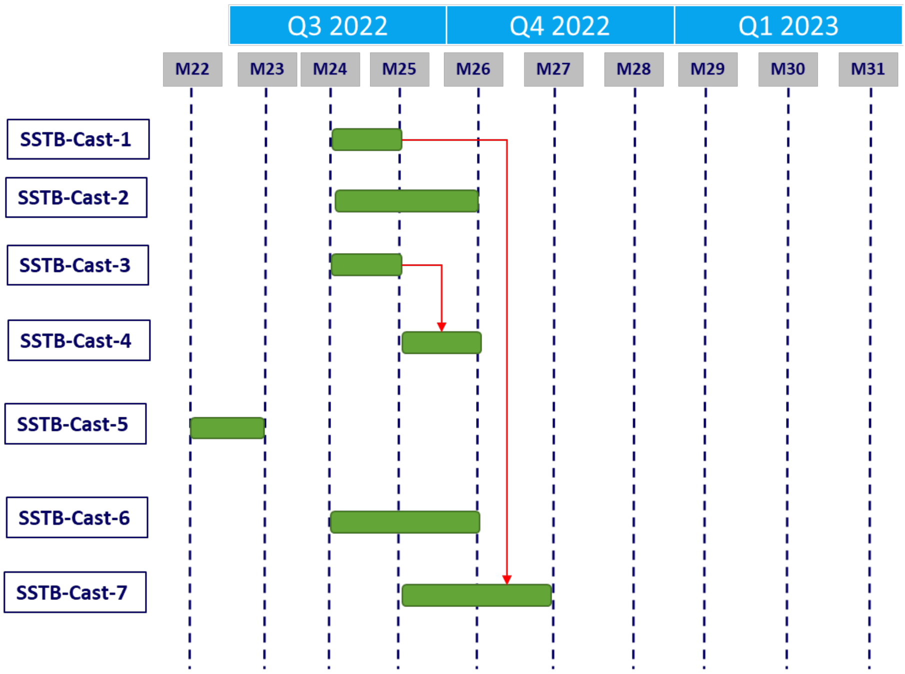


Figure 70: Gantt chart of the T3.6 activities (Castelloli).

7.2. Paris

As it is already detailed in D2.2, the Paris test site consist of two small scale trial sites, Satory and Teqmo.

Currently, Satory site has already deployed with a 5G NSA mmWave network, 1 MEC, 5 ITS-G5 RSUs, 3 roadside cameras, and 2 lidars. The network will be upgraded to SA by Q2-Q3 of 2022. Functionalities such as emulating of cross border network roaming will then be added. One or two C-V2X RSUs and one MEC will be deployed during Q2 of 2022.

Teqmo site has already deployed with two NSA cmWave networks provided by Bouygues and Orange. The site already has 20 C-V2X/ITS-G5 RSUs and cameras. The Bouygues network is expected to be upgraded to the SA mode during 2022 and the Orange network will be upgraded in 2023.

Table 34 and Table 35 presents the list of T3.6 activities planned in Satory and Teqmo, respectively. Furthermore, Figure 71 shows the Gantt chart of the tasks to be carried out in Satory, and Figure 72 reports the activities in Teqmo site.

Table 34: Timeline for infrastructure deployment in Satory (Paris).

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
SSTB-Sat-1	VEDE	-Experimental 5G network being deployed by VEDECOM and TDF using 2.6GHz. -TDF MEC installed. -DSRC installed -C-V2X need to install. -Simulate roaming with TDF to simulate two PLMNs (under discussion). -Flexible, extendible.	Q2 2022	3 months	
SSTB-Sat-2	VEDE	Experimental 5G network being deployed by VEDECOM and TDF using 26GHz. Flexible, extendible.	Q2 2022	3-6 months	

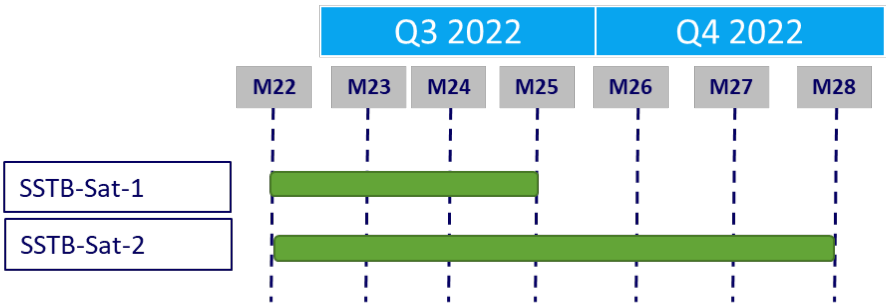


Figure 71: Gantt chart of T3.6 activities (Paris - Satory).

Table 35: Timeline for infrastructure deployment in Teqmo (Paris).

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
SSTB-Teq-1	VEDE	Bouygues network is expected to be upgraded to the SA (3.5 GHz)	To be started	6 months	
SSTB-Teq-2	VEDE	Orange network will be upgraded (3.5 GHz)	To be started	9 months	

SSTB-Teq-3						

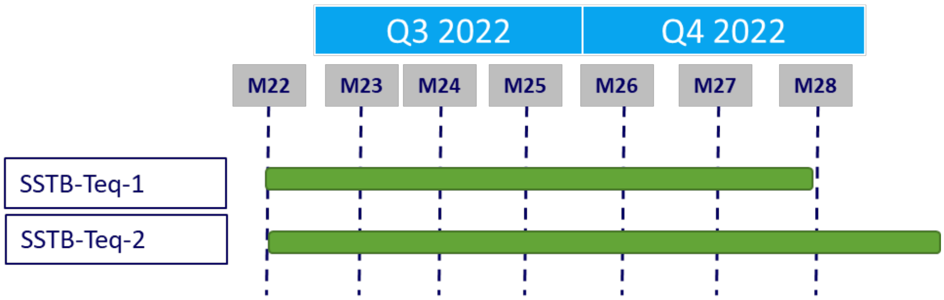


Figure 72: Gantt chart of the T3.6 activities (Paris - Teqmo).

7.3. Cross-border corridor

The 5GMED large-scale testbed corresponds to cross-border corridor and involves both the highway and the railway connecting Spain with France. Table 36 lists the ongoing tasks and the activities yet to be started. Finally, the Gantt chart of such deployment tasks is shown in Figure 73.

Table 36: Timeline for infrastructure deployment in the cross-border corridor.

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
LSTB-1	VDF	Deployment and commissioning of 4 5G gNBs	Q4 2021	7 months	
LSTB-2	VDF/RETE	Interconnection between VDF 5G RAN and Druid 5GC	Q3 2022	4 months	
LSTB-3	VDF	5G driving tests in the Spanish side and RAN optimization	Q3 2022	1 month	LSTB-1, LSTB-2
LSTB-4	RETE/HSP	Interconnection between HSP network and LFP premises	Q3 2022	2 months	
LSTB-5	COMSA	Deployment, testing and commissioning of the 70 GHz IEEE 802.11ad radio system	Q4 2022	8 months	
LSTB-6	RETE	Deployment of the MEC servers	Q3 2022	1 month	
LSTB-7	RETE	Deployment and commissioning of 2 5G gNBs to complement the VDF RAN	Q3 2022	3 months	
LSTB-8	RETE/VDF	Testing and validation of the whole Spanish 5G RAN against Druid 5GC	Q4 2022	1 month	LSTB-2, LSTB-7
LSTB-9	AXB, RETE	Installation and initial testing of ACS-GW	Q4 2022	1 month	
LSTB-10	AXB, RETE, COMSA, HSP	Integration between 5G, VSAT and 70 GHz with ACS-GW	Q4 2022	1 month	LSTB-8, LSTB-9
LSTB-11	CLNXFR	Deployment, testing and commissioning of the French 5G RAN	Q3 2022	5 months	Vendor supply chain, site permission, etc.

Task ID	Responsible partners	Description	Start date	Duration	Dependencies
LSTB-12	CLNXFR	5G driving tests in the French side and RAN optimization	Q4 2022	2 weeks	LSTB-11
LSTB-13	CLNXFR/RETE	Installation of Druid 5GC	Q3 2022	1 week	
LSTB-14	CLNXFR/RETE	Integration of French 5G RAN against Druid 5GC	Q3 2022	1 month	LSTB-13, LSTB-11
LSTB-15	RETE	Deployment, testing and commissioning of the in-tunnel 5G RAN	Q3 2022	4 months	Vendor supply chain
LSTB-16	RETE	5G driving test inside the tunnel and RAN optimization	Q4 2022	2 weeks	LSTB-15
LSTB-17	RETE	Integration of in-tunnel 5G RAN against Druid 5GC	Q4 2022	2 weeks	LSTB-13, LSTB-16
LSTB-18	RETE/AAE	Installation, testing and commissioning of C-V2X RSUs	Q3 2022	3 months	Site permissions
LSTB-19	AAE/RETE/VDF/I2CAT	Initial cross-border driving tests in highway and railway	Q1 2023	2 months	LSTB-14, LSTB-11, LSTB-2, LSTB-17

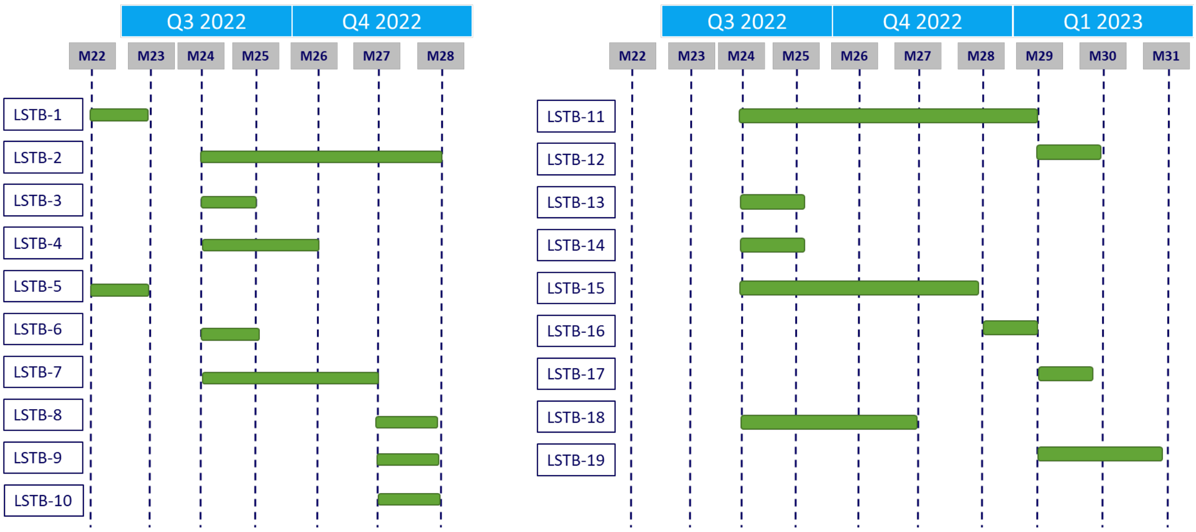


Figure 73: Gantt chart of the T3.6 activities (Corridor).

Funded by the Horizon 2020 Framework Programme of the European Union

8. Conclusions

This deliverable is the first official document reporting the design of the 5GMED architecture and has introduced the fundamental strata of the entire architecture. The infrastructure has been discussed by highlighting the main differences between the Spanish side and the French side in terms of 5G connectivity, MEC availability, and the interconnections among different network segments. This diversity represents one of the primary challenges of 5GMED that will need to be addressed throughout this project.

Moreover, D3.2 has reported innovative solutions that will be adopted to handle multi-connectivity on the train and vehicles while providing services without disruptions. The need for an end-to-end orchestrator capable of managing services running on different edge nodes across the border has also been analysed. D3.2 also addressed network slicing and introduced the 5GMED approach to it, and new mechanisms to ensure low-latecy roaming have been discussed. Finally, the roadmap reported in the last section describes the different phases of the integration, deployment, testing and validation of each component that will first be conducted in the small-scale testbed and then in the corridor. D3.2 represents the first step of these activities whose progresses will be tracked and reported in the next deliverables planned within WP3, i.e., D3.3 and D3.4.

9. References

[1] 5GMED, "D3.1 - Analysis of 5GMed infrastructure requirements and 5G HO between networks & cross-border.".

[2] HUAWEI, "HUAWEI RTN950A datasheet," [Online]. Available: https://support.huawei.com/enterprise/en/transmission-network/optix-rtn-950a-pid-8691595.

[3] ITU-T, "Recommendation G.652 - Characteristics of a single-mode optical fibre and cable," 2013.

[4] IEC, "60793-2-50:2018 - Optical fibres - Part 2-50: Product specifications - Sectional specification for class B single-mode fibres".

[5] Draka, "Single-Mode Optical Fiber datasheet," [Online]. Available: https://www.prysmiangroup.com/sites/default/files/business_markets/markets/downloads/datasheets/SMF---Single-Mode-Optical-Fiber-SSMF.pdf.

[6] D. Chakraborty, "VSAT communications networks-an overview," *IEEE Communication Magazine,* 1988.

[7] H. H. datasheet. [Online]. Available: https://www.hughes.com/sites/hughes.com/files/2022-03/HT2524-Router.pdf.

[8] IEEE, "802.11ad-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)," IEEE, 2012.

[9] 5GMED, "D5.1: Railways application requirements analysis report".

[10] ETSI, "EN 302 663 - V1.2.0 - Intelligent Transport Systems (ITS)".

[11] A. Papathanassiou, "Cellular V2X as the Essential Enabler of Superior Global Connected Transportation Services".," *IEEE 5G Tech Focus. IEEE.,* 2017.

[12] ETSI, "GS MEC 003 V2.1.1 (2019-01): "Multi-access Edge Computing (MEC); Framework and Reference Architecture"".

[13] ETSI, "GR MEC 031 V2.1.1 (2020-10), "Multi-access Edge Computing (MEC); MEC 5G Integration"".

[14] T. Tovinger, "Management, Orchestration and Charging for 5G networks," 2018.

[15] ETSI, “TS 128 533, 5G; Management and orchestration; Architecture framework,” 2021.

[16] N. a. I. s. brief. [Online]. Available: https://www.nearbycomputing.com/wp-content/uploads/2021/09/NearbyOne-and-Lenovo-Edge-Servers-the-Winning-Combination-to-Enable-5G-RAN-and-MEC-Applications.pdf.

[17] GSMA, “OPG.02, Operator Platform Telco Edge Requirements,” 2021.

[18] ICS. [Online]. Available: https://www.isc.org/.

[19] BPF. [Online]. Available: https://docs.cilium.io/en/stable/bpf/.

[20] A. M. I. S. M. a. M. C. D. Saha, “Mobility support in IP: a survey of related protocols,” *IEEE Network,* vol. 18, no. 6, 2004.

[21] S. S. a. A. P. M. Bonola, “UPMT: Universal Per-Application Mobility Management Using Tunnels,” *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, 2009,* no. M. Bonola, S. Salsano and A. Polidoro, "UPMT: Universal Per-Application Mobility Management Using Tunnels," GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, 2009, pp. 1-8, doi: 10.1109/GLOCOM.2009.5425883..

[22] 5GMED, “D4.1: Requirements and initial design for Automotive Test Cases”.

[23] 5. A. Association, “Cross-Working Group Work Item Network Reselection Improvements (NRI) v1.0. Technical Report.”.

[24] 3GPP, “TS 23.502, Procedures for the 5G System (5GS); Stage 2, v17.4.0,,” 2022.

[25] 3GPP, “ Services and System Aspects; Security architecture and procedures for 5G system (Rel 15), 3GPP TS 33.501 V15.3.1, Dec. 2018.”.

[26] 3GPP, “Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3(Rel 15), 3GPP TS 24.501 V15.2.0, Dec. 2018.”.

[27] 3GPP, “Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2(Rel 15), 3GPP TS 23.502 V15.4.0, Dec. 2018”.

[28] 3GPP, “Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2(Rel 15), 3GPP TS 38.300 V15.3.1, Oct. 2018.”.

[29] V. security. [Online]. Available: https://viacamsecurity.wordpress.com/tag/remote-site-monitoring/.

[30] 5GMED, "D2.2.: Initial definition of 5GMED test cases, deployment options and tool".

[31] 3GPP, "Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2(Rel 15), 3GPP TS 23.501 V15.4.0, Dec. 2018.".

[32] 3GPP, " Technical Specification Group Core Network and Terminals; Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3(Rel 15), 3GPP TS 24.502 V15.2.0, Dec. 2018".

[33] 3GPP, "Technical Specification Group Core Network and Terminals; Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3(Rel 15), 3GPP TS 24.502 V15.2.0, Dec. 2018.".

Funded by the Horizon 2020 Framework Programme of the European Union