5GMOBIX

5G for cooperative & connected automated MOBIlity on X-border corridors

D2.2

5G architecture and technologies for CCAM specifications

Dissemination level	Public (PU)
Work package	WP2: Specifications
Deliverable number	D2.2
Version	V1.0
Submission date	31/10/2019
Due date	31/10/2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825496.

Editors

Editors in alphabetical order		
Name	Organisation	Email
Trichias, Konstantinos	WINGS ICT	ktrichias@wings-ict-solutions.eu

Authors

Authors in alphabetical order		
Name	Organisation	Email
Akkuzu, Beste	ERICSSON - TR	beste.akkuzu@ericsson.com
Alonso, Jaime Ruiz	NOKIA-SP	jaime_jesus.ruiz_alonso@nokia-bell-labs.com
Beeharee, Ashweeni	CATAPULT	ashweeni.beeharee@sa.catapult.org.uk
Berber, Erdal	TURKCELL	erdal.berber@turkcell.com.tr
Bernárdez, Diego	CTAG	diego.bernardez@ctag.com
Blanco, Diana	CTAG	diana.blanco@ctag.com
Boujelben, Maissa	VEDECOM	Maissa.boujelben@vedecom.fr
Chassaigne, Alexander	TELEFONICA	alexander.chassaigne@telefonica.com
Choi, You-Jun	KATECH	ychoi@katech.re.kr
Correia, Fernando	NOKIA-PT	fernando.correia@nokia.com
Dang, Xuan-Thuy	TU Berlin	xuan-thuy.dang@dai-labor.de
Dimitriadis, Ioannis	WINGS ICT	idimitriadis@wings-ict-solutions.eu
Dinis, Ricardo	NOS	ricardo.dinis@nos.pt
Dörsch, Tobias	TU Berlin	tobias.doersch@dai-labor.de
Frontelo, Ignacio Benito	NOKIA-SP	ignacio.benito_frontelo@nokia-bell-labs.com
Fernandez, Pedro	UMU	pedroj@um.es
Foteinos, Vasilis	WINGS ICT	vfotein@wings-ict-solutions.eu
Giannopoulos, Emmanuel	WINGS ICT	mgiannopoulos@wings-ict-solutions.eu
Guney, Nazli	TURKCELL	nazli.guney@turkcell.com.tr
Han, Qiaomei	DUT	hqmdut@163.com
Heesang, Chung	ETRI	hschung@etri.re.kr
IJntema, Wieger	TNO	Wieger.ijntema@tno.nl
Jáuregui, Daniel	CTAG	daniel.jauregui@ctag.com
Kakes, Geerd	KPN	geerd.kakes1@kpn.com
Kalca, Artiol	VEDECOM	artiol.kalca@vedecom.fr
Khan, Manzoor	TU Berlin	manzoor-ahmed.khan@dai-labor.de
Kostopoulos, Nikos	ERICSSON-GR	nikos.kostopoulos@ericsson.com
Kountche, Djibrilla	AKKA	djibrilla.amadou-kountche@akka.eu

Laskaridis, Vasilis	WINGS ICT	vlaskaridis@wings-ict-solutions.eu
Lingling, Lv	DUT	lvlingling@mail.dlut.edu.cn
Logothetis Dimitris	ERICSSON-GR	dimitris.logothetis@ericsson.com
Maistros, Ioannis	WINGS ICT	imaistros@wings-ict-solutions.eu
Mazzeo, Mateus	NOKIA-PT	mateus.mazzeo@nokia.com
Moutinho, João	CCG	joao.moutinho@ccg.pt
Mutafungwa, Edward	AALTO	edward.mutafungwa@aalto.fi
Nikolitsa, Eutuxia	COSMOTE	enikolitsa@cosmote.gr
Okonkwo, Chigo	TU/e	cokonkwo@tue.nl
Peixoto, João	CCG	joao.peixoto@ccg.pt
Requena, Jose Costa	AALTO	jose.costa@aalto.fi
Rivas, Juan	TELEFONICA	juanfrancisco.estebanrivas@telefonica.com
Rommel, Simon	TU/e	s.rommel@tue.nl
Roth-Mandutz, Elke	Fraunhofer IIS	elke.roth-mandutz@iis.fraunhofer.de
Salido, Carlos Rosales	CTAG	carlos.rosales@ctag.com
Santa, Jose	UMU	jose.santa@um.es
Setaki, Fotini	COSMOTE	fsetaki@cosmote.gr
Shagdar, Oyunchimeg	VEDECOM	oyunchimeg.shagdar@vedecom.fr
Shi, Yanjun	DUT	syj@ieee.org
Sivrikaya, Fikret	GT-ARC	fikret.sivrikaya@gt-arc.com
Soua, Ahmed	VEDECOM	ahmed.soua@vedecom.fr
Soutelo, German	NOKIA-SP	german.soutelo@nokia.com
Stavroulaki, Vera	WINGS ICT	veras@wings-ict-solutions.eu
Stenos, Ioannis	WINGS ICT	istenos@wings-ict-solutions.eu
Trichias, Konstantinos	WINGS ICT	ktrichias@wings-ict-solutions.eu
Turhan, Gokhan	ERICSSON-TR	gokhan.g.turhan@ericsson.com
Ünlüsan, Murat	TURKCELL	murat.unlusan@turkcell.com.tr
Vlacheas, Panagiotis	WINGS ICT	panvlah@wings-ict-solutions.eu
Zekai, Orestis	WINGS ICT	ozekai@wings-ict-solutions.eu

Control sheet

Version history			
Version	**Date**	**Modified by**	**Summary of changes**
0.01	25/01/2019	K. Trichias	Table of contents proposal
0.1	28/03/2019	Multiple contributors per site	Updated ToC by section leaders
0.2	23/04/2019	Multiple contributors per site	Paragraph 4.2 (Radio network architecture GR & TR & Core network architecture GR)

0.3	30/04/2019	Multiple contributors per site	First content per trial provided by trial site contributors
0.4	03/05/2019	K. Trichias	Early feedback and improvement suggestions by editor
0.5	10/05/2019	Multiple contributors per site	Update of trial specific content, first version of standardisation, security and sustainability sections
0.6	24/05/2019	Multiple contributors per site	Final additions and corrections by CBC and TS leaders, finalized versions of Sections 2, 5 and 6
0.7	31/05/2019	K. Trichias	Executive summary and conclusion sections writing, formatting and editing review
0.8	14/06/2019	Multiple contributors	Last corrections, alignment of sections and editing finalization (delivered to reviewers)
0.9	04/10/2019	Multiple contributors	Restructuring of the entire document to reflect the restructured way of working after the 1st interim project review. New structure to reflect the CBC/TS collaboration and x-border focus.
0.95	29/10/2019	Multiple contributors	Addressing review comments
1.0	31/10/2019	K. Trichias, S. Faye	Quality check, final editing

Peer review			
Reviewer #	**Reviewer name**	**Organisation**	**Date**
Reviewer 1	**Rodrigues, Miguel**	SIEMENS	28/06/2019
Reviewer 2	**Datia, Nuno; Serrador, António; Cruz, Nuno; Teixeira, Grazielle**	ISEL	18/10/2019
Reviewer 3	**Castañeda Aguadero, Oscar**	DEKRA	17/10/2019

Legal disclaimer

The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The 5G-MOBIX Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright © 5G-MOBIX Consortium, 2019.

Table of contents

List of figures

List of tables

ABBREVIATIONS

Abbreviation	Definition
5GAA	5G Automotive Association
5GC	5G Core
5GTNF	5G Test Network Finland
AAA	Authentication, Authorisation and Accounting
AF	Application Function
ALCM	Application Life Cycle Manager
AMF	Access and Mobility Management Function
AN	Access Network
APM	Authorities/Policy Makers
ASGH	Advanced Subscriber Group Handling
AV	Autonomous Vehicle
CBAM	Cloud Band Application Manager
CBC	Cross Border Corridor
CCAM	Cooperative, Connected and Automated Mobility
CIP	Communications Infrastructure Providers
C-ITS	Cooperative - Intelligent Transport Systems
CLI	Command Line Interface
CM	Configuration Management
CMG	Could Mobile Gateway
CMM	Cloud Mobility Manager
CN	Core Network
CoCa	Collision Avoidance
COTS	Commercial Off The Shelf
CP	Control Plane
CPE	Collective Perception of Environment
CUDB	Centralized User Data Base
CUPS	Control User Plane Separation
C-V2X	Cellular Vehicle-to-Everything
D2D	Device to Device
DÉCOR	Dedicated Core Network (DCN)
DL	Downlink
DoA	Description of Action
DPO	Data Protection Officer
E2E	End to end
EC	European Commission
eMBB	Enhanced Mobile BroadBand
eMBMS	Evolved Multimedia Broadcast Multicast Services
EN	External Network
eNB	E-UTRAN Node B
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
eRSU	Extended Road Side Unit
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved Universal Terrestrial Radio Access
FDD	Frequency Division Duplex
FM	Fault Management
GA	General Assembly
GDPR	General Data Protection Regulation
GGSN	Gateway GPRS Support Node
GRX	GPS Roaming Exchange
GSMA	Global System for Mobile Communications Association

GST	Generic Slice Template
GTP	GPRS Tunnelling Protocol
gNB	gNodeB
GST	Generic Slice Template
HARQ	Hybrid Automatic Repeat Request
HEVC	High Efficiency Video Coding
HMD	Head Mount Display
HR	Home Routing
HSS	Home Subscriber Server
HW	Hardware
I2V	Infrastructure to Vehicle
IM	Identity Management
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Infrastructure Provider
IPS	Internet Protocol Service
ITS	Intelligent Transportation Systems
ITU-T	International Telecommunication Union Telecommunication Standardisation Sector
IUA	Instant Uplink Access
KCI	Key Control Indicator
KPI	Key Performance Indicator
LADN	Local Area Data Networks
LB	Load Balancer
LBO	Local Breakout
LTE	Long Term Evolution
MAA	Massive MIMO Adaptive Antenna
MANO	Management and Orchestration
MBMS-GW	Multimedia Broadcast Multicast Services Gateway

MCG	Master Cell Group
MCN	Micro Core Network
MEA	Mobile Edge Application
MEC	Multi-access Edge Computing
MEH	Mobile Edge Host
MEHW	Mobile Equipment Hardware
MEP	Mobile Edge Platform
MG	Mobile Gateway
MIMO	Multiple-Input/Multiple-Output
MME	Mobility Management Entity
mMTC	Massive Machine Type Communication
MN	Mobile Network
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
NEST	Network Slice Type
NF	Network Function
NFV	Network Function Virtualization
NGC	Next Generation Core
NR	New Radio
NRF	Network Repository Function
NSA	Non-Standalone
NSSF	Network Slice Selection Function
OAM	Operations, Administration, and Management
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OIH	Open Innovation House
OSS	Operations Support System
P2P	Point to Point
P2mP	Point to multi Point
PCF	Policy Control Function

PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PGW	Packet Gateway
PLMN	Public land mobile network
PM	Performance Management
ProSe	Proximity Services
PS	Public Safety
PTT	Push To Talk
PulSAR	Proactive Security Assessment and Remediation
QAM	Quadrature Amplitude Modulation
QCI	Quality of service Class Identifier
QoS	Quality of Service
QoE	Quality of Experience
RAN	Radio Access Network
RIO	Road Infrastructure Operators
RSI	Road Side Infrastructure
RSSI	Received Signal Strength Indicator
RSU	Roadside Unit
RTT	Round Trip Time
SA	Standalone
SAE	Society of Automotive Engineers
SAE-GW	System Architecture Evolution Gateway
SC	Small Cell
SCC	Security Control Classes
SCLI	Structured Command Line interface
S-CSCF	Serving Call Session Control Function
SDN	Software-Defined Networking
SDO	Standards Developing Organization

SeGW	Secure Gateway
SGW	Serving Gateway
SIM	Subscriber Identity Module
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SPID	Service Profile Identifier
SR	Security Realm
SSC	Session and Service Continuity
SSH	Secure Shell
SW	Software
SWD	Software Developer
TA	Trusted Anchor
TDD	Time Division Duplex
TELNET	Teletype Network
TN	Transit Network
TS	Trial Site
TSL	Trial Site Leader
TWAG	Trusted Wi-Fi Access Gateway
UC	Use Case
UCC	Use Case Category
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UPF	User Plane Function
uRLLC	Ultra Reliable Low Latency Communication
US	User Story
USIM	Universal Subscriber Identity Module
(v)UDM	(virtual) Unified Data Management
VIM	Virtual Infrastructure Management
VM	Virtual Machine

VNF	Virtual Network Function
VNFC	VNF Component
VNFM	Virtual Network Function Manager
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle-to-Everything
VRU	Vulnerable Road User
WAN	Wide Area Network
WP	Work Package
WPL	Work Package Leader
X2AP	X2 Application Protocol
XML	Extensible Markup Language

EXECUTIVE SUMMARY

The challenge for 5G-MOBIX is to qualify 5G as a core connectivity infrastructure that can address a broad set of CCAM V2X use cases in cross-border conditions, having a business appeal for a sufficiently large number of stakeholders to justify the investments required to deliver 5G mobility services in the near future, especially at currently underserved cross-border areas. To achieve that goal, the 5G-MOBIX partners have defined several challenging and beyond state-of-the-art use cases [1] to be realized across European borders, enabled by real 5G network implementations and with the support of functionality development, testing and configuration from local European sites. Additionally, the most critical cross-border issues that Mobile Network Operators (MNOs), vendors and other stakeholders must address in order to achieve uninterrupted service while crossing the borders have been identified by the 5G-MOBIX experts, while suitable solutions for each of these issues are being proposed. This deliverable, provides a detailed account of the most prominent telecommunication cross-border (x-border) issues to be evaluated as well as the requirements analysis performed per cross border corridor leading to the 5G network architecture and utilized components/functionalities, in order to support the identified CCAM Use case categories with the required QoS/QoE, while aligning the deployments with the 3GPP roadmap and addressing sustainability, security and data privacy concerns.

The proposed architecture is based on a thorough analysis of the 3GPP roadmap and expected availability of certain 5G HW and SW by the involved vendors and MNOs. Section 2 provides an overview of the relevant 3GPP Rel.14 [46] and Rel.15 [13] architectural components and functionality, which will be the starting point for all the trials, as well as the different deployment options. Specific relevant architectural components such as MEC and slicing, as well as the relevant functions, are also presented, while implementation details and timelines will differ among the various sites. Both 5G-MOBIX Cross-Border Corridors (CBC) will initially deploy a Non-Standalone 5G architecture (NSA option 3X) based on Rel.15 network equipment and Rel.14 C-V2X functionality due to the availability timelines for HW and SW by the vendors. As 5G chipsets become commercially available during the project's lifespan, the CBCs as well as the Trial Sites (TS) will move towards a full implementation with Rel.15-based UEs and/or C-V2X modems/OBUs. Most of the sites will also attempt to implement the Stand Alone 5G architecture (Option 2) towards the end of the project by replacing the NSA EPC with a 5G core (depending on the availability of the respective HW and SW by the vendors).

The selected architecture and component configuration of each CBC has been based on a thorough requirement analysis per use case category, regarding the expected KPIs that need to be met and the expected QoS while taking into consideration the frequency availability, geo-spatial and propagation characteristics for a particular regulatory environment and geography (presented in Sections 4.1 and 5.1 respectively). An analysis of the telecommunication x-border issues to be addressed, the necessary roaming support as well as the main *Functional* and *Non-Functional* requirements for cross-border deployments, have been taken into consideration, leading to targeted component and functionality selections per corridor.

Based on this thorough analysis, the selected 5G architecture, frequencies, components, interfaces and interconnections per CBC are presented in Sections **Error! Reference source not found.** and 5 respectively. The concrete contributions of the TSs with HW, SW and other components that will enable the CBC trials are also highlighted in the same sections. The considered reference architecture by both CBCs for an initial deployment of NSA option 3X with MEC components is indicative of the current limitations due to the availability of 5G HW/SW and the need for ultra-low latency communications to accommodate CCAM use cases requirements. However, the move towards SA Option 2 for the TSs and potentially for the CBCs, once the technology becomes available (within the project's lifespan), guarantees advanced testing and significant insights regarding the future deployment of 5G networks across European highways. Furthermore, the existence of the TSs guarantees the full coverage and evaluation of multiple User Stories (US) per Use Case Category (UCC), the availability of pre-testing and configuration data as well as the evaluation of additional x-border issues solutions, as described by the TS extended evaluations in Section 6.

To guarantee the successful commercial exploitation of the 5G-MOBIX solutions and the application of the learned lessons in the real world, security and data-privacy aspects have been considered while designing the 5G architecture of each of the CBCs, as presented in Section 7. These aspects also play a major role in the acceptance and penetration of the 5G technology to support CCAM and in general Intelligent Transport Systems (ITS), therefore, specific security requisites are discussed for each UCC. Finally, a detailed stakeholders analysis performed for the two cross-border corridors as part of an initial sustainability analysis, clarifies the relationships and responsibilities among them, while it paves the way for the sustainability enablers to be developed within the project (WP6) and provides an early "proof of concept" for the viability of cross-border 5G deployments to offer CCAM functionality in remote areas.

Overall, the selected 5G architecture and deployments allow the execution of advanced CCAM trials over 5G networks at European border conditions, in a safe, secure and complementary manner, addressing heterogeneous requirements. The complementarity of the 5G architecture among the Cross-Border Corridors and the Trial Sites, allows for extensive testing and tuning of certain features in a controlled environment prior to their deployment to the actual borders, where testing and evaluation time is limited, and the trialling conditions can be unpredictable.

1. INTRODUCTION

1.1. 5G-MOBIX concept and approach

5G-MOBIX aims to showcase the added value of 5G technology for advanced Cooperative, Connected and Automated Mobility (CCAM) use cases and validate the viability of the technology to bring automated driving to the next level of vehicle automation (Society of Automotive Engineers - SAE L4 and above). To do this, 5G-MOBIX will demonstrate the potential of different 5G features on real European roads and highways while creating and using sustainable business models to develop 5G corridors. 5G-MOBIX will also use and upgrade existing key assets (infrastructure, vehicles, components, etc.), also investigating the smooth operation and coexistence of 5G within a heterogeneous environment comprised of multiple incumbent technologies such as ITS-G5 and C-V2X.

5G-MOBIX will execute CCAM trials along cross-border (x-border) corridors and local trial sites assisting, contributing and complementing the corridors, using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context. The Project will also define deployment scenarios identifying and responding to standardisation and spectrum gaps. 5G-MOBIX defines critical scenarios needing advanced connectivity provided by 5G, and the required features to enable some advanced CCAM use case categories. The matching of these advanced CCAM use case categories and the expected benefits of 5G will be tested during the trials on the 5G corridors in different EU countries as well as in Turkey, China and Korea. The trials will also allow 5G-MOBIX to conduct evaluations and impact assessments as well as to define business impacts and cost/benefit analysis. As a result of these evaluations and international cooperation with the public and industry stakeholders, 5G-MOBIX will identify new business opportunities for the 5G enabled CCAM and propose recommendations for its deployment. Finally, through its findings on technical requirements, deployment enablers and operational conditions, 5G-MOBIX is expected to actively contribute to standardisation and spectrum allocation activities.

1.2. Purpose of the deliverable

This deliverable will provide a detailed account of the specifications of the 5G technologies and components that will be used in each of the 5G-MOBIX cross-border corridors (CBC) as well as the specific technological contributions of each of the Trial Sites (TS) to the CBCs. The overall 5G network architecture that the two CBC will use to support the successful operation of the defined 5G-MOBIX CCAM use case categories is also presented, along with the 5G network architecture deployed at the TS for extended evaluations.

To accomplish this goal, D2.2 builds on the work of deliverable D2.1 [1] where the 5G-MOBIX CCAM use case categories (UCC) and user stories (US) are detailed. Using this input, the use case requirement analysis is focused at cross-border operation per CBC (Section **Error! Reference source not found.**), which in turn leads to the necessary 5G network specifications needed to support the ambitious 5G-MOBIX use case categories. Based on the requirements analysis, as well as on the analysis of relevant standardisation developments (Section 2), the ES-PT and the GR-TR CBCs design and implementation of a suitable 5G network architecture is presented in Section **Error! Reference source not found.** and Section **Error! Reference source not found.** respectively, along with the detailed specifications of the used 5G components and technologies, comprising the network. This deliverable also provides, in Section 7, an overview of the extended evaluations that will take place at the TSs (due to the pragmatic difficulty of performing certain types of tests at actual borders) to enhance and complement the results of the trials performed at the CBC, along with the infrastructure needed for these evaluations.

This deliverable will be used by WP3 as a "blueprint" and a baseline for the development and roll-out of the 5G-MOBIX's 5G networks (to be built in the various CBCs and TSs), while it will also serve as detailed documentation of the deployed 5G networks for any interested stakeholder. Only 5G network and 5G technology relevant information is included in this deliverable, while the architectural information regarding the rest of the infrastructure, the vehicles and the used Key Performance Indicator (KPI performance Indicators (KPIs) mechanisms that together comprise the entire infrastructure necessary for the trials, are presented in the other WP2 deliverables as follows:

- D2.3: Specification and architecture of the Road Side (RSI) and Cloud Infrastructure [2].
- D2.4: Specification & architecture of the connected vehicles, On-Board Units (OBUs) and other on-board sensors [3].
- D2.5: Specification of the initial evaluation KPIs to be used for trial results evaluation [4].

1.3. Intended audience

The dissemination level of D2.2 is public (PU) and hence will be used publicly to inform all interested parties about the 5G infrastructure to be used for the 5G-MOBIX trials. However, this document is of special interest to the following groups:

a. *5G-MOBIX project consortium members*: This document may act as an internal technical report for all consortium members regarding the available infrastructure and its capabilities, and for the different corridor/trial partners to exchange knowledge regarding the selected 5G network implementation and configurations.

b. *The European Commission (EC):* This document can be used as a reporting method towards the EC for monitoring project progress and for keeping up to date with the latest 5G infrastructures installed around Europe. Parts of this document may also be used as a reference for future European policies or calls for research.

c. *European telecom operators & vendors:* This document is of particular interest to European telecom industry stakeholders not participating in the project, as it will provide a first insight into the proposed network deployments and 5G technologies in order to support advanced CCAM operation across Europe.

d. *All CCAM/V2X stakeholders:* Besides the aforementioned targeted groups, this document is of extreme interest to any party actively engaged (or planning to engage) with the CCAM ecosystem, as it provides details on the infrastructure and architecture used for some of the most advanced 5G-enabled CCAM trials to date, and consequently provides valuable insights into the deployment and integration necessary for 5G networks to support CCAM operation.

2. STANDARDISATION ASPECTS

The challenge for 5G-MOBIX is to qualify 5G as a core connectivity infrastructure that can address a broad set of CCAM V2X use case categories with a business appeal for a sufficiently large number of stakeholders to justify the investments required to deliver 5G mobility services in the near future, especially at currently underserved cross-border areas. This necessarily involves a closer look at the developments and activities within the relevant standardisation bodies, which have evolved significantly over the last few years to encompass scenarios that are much more advanced than the safety/efficiency applications in the domain of cooperative-intelligent transport systems (C-ITS), where the basic aim is to allow individual vehicles to communicate with each other and with the road infrastructure for safety purposes.

Within the scope of ITS, European Telecommunications Standards Institute (ETSI) published several standards that specify a cooperative awareness service [5] and a decentralized environmental notification basic service [6], whose intention is to define the message sets needed for safety critical applications. While the cooperative awareness messages are sent periodically by road users (vehicles) and road infrastructure in vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and infrastructure-to-vehicle (I2V) modes, which lie within the general category of vehicle-to-everything (V2X) communications, to inform their surrounding about their position, dynamics and attributes, the decentralized environmental notification messages are shared by road users or infrastructure (collectively called ITS stations) to provide information about a road hazard or an abnormal traffic condition, such as its type and location only when the situation is detected. Cooperative perception and multimedia content dissemination are some of the other information services offered to ITS applications using ITS communication technologies.

Derived from the IEEE 802.11 standards, the physical layer technology of ITS stations which is called ITS-G5, and defined in [7], does not require the establishment of a network, operating in an ad hoc mode to support the exchange of the described messages between ITS stations without prior network set up. A similar ad hoc communication method for short ranges also appears in the 3GPP specifications that has been made available for vehicles and their interaction with fixed stations and other road users as introduced later in **Error! Reference source not found.** of this document. First, we look at the 5G cellular communication standardization activities in the 3GPP, since 5G is the major focus of the 5G-MOBIX project, where we also try to explain how the progress in the 5G standards influences the burgeoning applications in vehicular communications.

2.1. 5G Cellular Communications in 3GPP

For the 3GPP community, the first full set of standards for 5G cellular communications is part of 3GPP Rel.15, which aims to introduce a 5G new radio (5G NR) system complemented by a next-generation core network that are both designed to address the IMT-2020 requirements of ITU [8]. To better cope with the demand from some of the network operators and vendors for an expedited delivery of 5G services, the initial set of 3GPP Rel.15 specifications were built on existing LTE networks in the form of a “Non-Stand Alone (NSA)” architecture for the early drop in December 2017 before the “Stand Alone (SA)” system was finalized in June

2018. While 3GPP Rel.15, whose timeline is shown in Figure 1, focuses on enhanced Mobile BroadBand (eMBB), the first stage of 3GPP Rel.16 which is called "5G Phase 2" tackles the problems associated with decreasing latency and increasing the number of machines/things in a confined region, namely the Ultra Reliable Low Latency Communications (URLLC) and massive Machine-Type Communications (mMTC) pillars of the IMT-2020 standards.

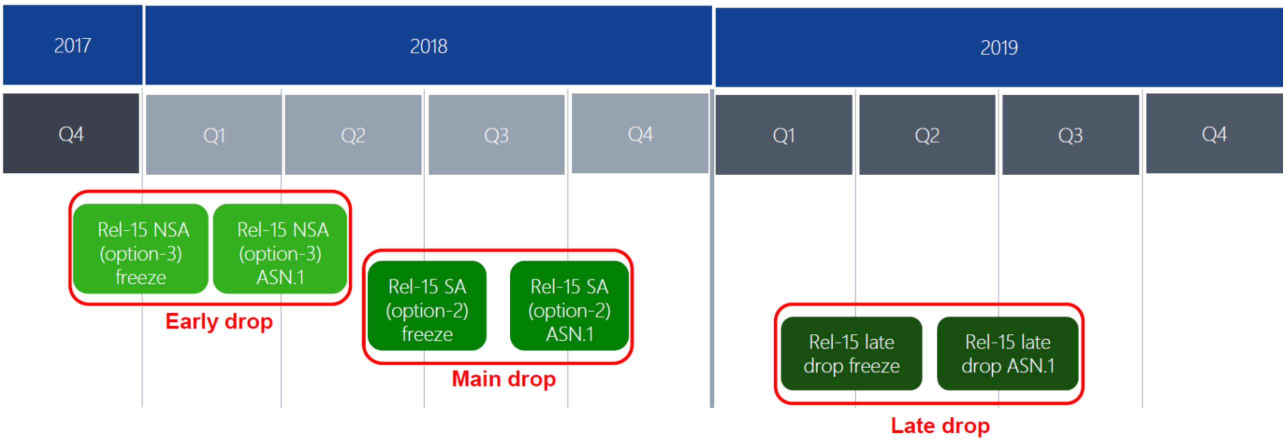

2017
2018
2019
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Rel-15 NSA (option-3) freeze
Rel-15 NSA (option-3) ASN.1
Early drop
Rel-15 SA (option-2) freeze
Rel-15 SA (option-2) ASN.1
Main drop
Rel-15 late drop freeze
Rel-15 late drop ASN.1
Late drop

Figure 1: 3GPP roadmap for 3GPP Rel.15 specifications

2.1.1. 3GPP Release 15

The 3GPP technical report TR 38.801 [9] on radio access architecture and interfaces indicates that the new RAN architecture may consist of gNBs and/or eNBs that provide 5G NR and Evolved-Universal Terrestrial Radio Access (E-UTRA, i.e., 4G) terminations towards UEs, respectively. The new core network defined in 3GPP Rel.15 is the 5G Core Network (5GC), but the standards include several options to allow connectivity to the legacy evolved packet core (EPC), as well. In total, eight options are discussed to cover all possible scenarios, where this number increases more with variants of these options [10]. Non-standalone options are those deployment configurations, for which the gNB/eLTE eNB (i.e., 3GPP Rel.15 and beyond eNB) requires an eLTE eNB/gNB as an anchor for control plane connectivity to the EPC/5GC. For one of the options, eLTE eNBs may also be the anchor for gNBs when connecting to the 5GC. Standalone options are characterised by having only a single type of base station connecting to a core network.

The options that are embraced the most by the vendors and the operators in the telecommunications industry are depicted in Figure 2. The standardisation of these options will be completed in several phases:

- PHASE 1: Non-standalone Option 3x: Completion March 2018/Final CR in December 2018.
- PHASE 2: Standalone Option 2: Completion September 2018/CR in December 2018.
- PHASE 3: Non-Standalone Option 7 and 4: Expected Q3/19, and thus 3GPP Rel.16 – Focus on backward compatibility.

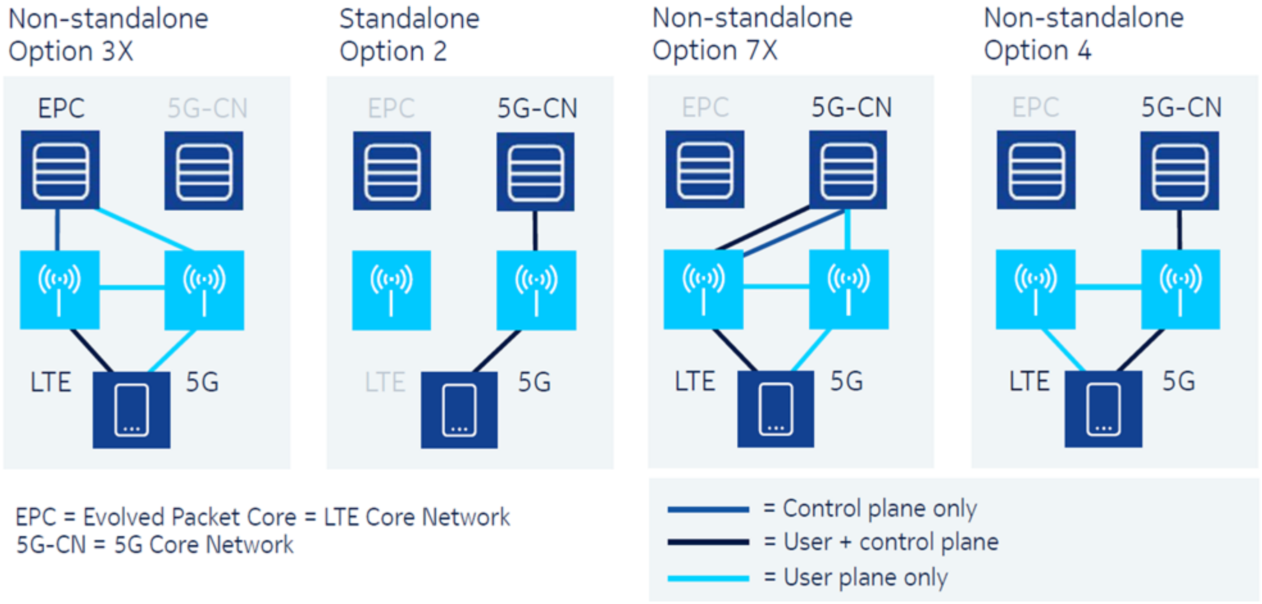


Figure 2: 5G deployment scenarios, stand-alone and non-standalone

Non-standalone options: As shown in Figure 2, in non-standalone options 3x and 7x, the data bearer is forwarded from both eNB and gNB while all signalling is anchored from the eNB to the EPC with option 3x, or to the 5GC with option 7x. Still using two types of radio access technologies, option 4 will have the signalling towards the 5GC, with the anchoring moved from the eNB to the gNB.

The most widely targeted initial deployment option for operators, which is also the focus of the 5G-MOBIX project, the option 3x, allows deployment of the 5G radio access network without waiting for the delivery of a 5GC. Due to the dual connectivity with the existing LTE network, this option has the advantage of providing robust connections especially in the regions where the number of 5G base stations has not reached a certain limit yet to guarantee a full 5G coverage. On the other hand, option 3x requires some additional interfaces for the EPC towards the element, which is newly-added to the network (i.e., the gNB), and hence, for sake of differentiating it from the legacy EPC serving only the LTE air interface, it is called the "5G EPC" in this and other 5G-MOBIX documents.

Standalone options: Not shown in Figure 2, options 1 and 3 include eNB/EPC and eNB/5GC pairs, respectively, whereas option 2 constitutes a pure 5G network, having the gNBs connected directly to the 5GC. The advantage of option 2 is that it has significantly less impact and interdependency on the legacy networks, namely the LTE radio access network and the EPC, and it is deemed a final version of the 5G architecture, but where a new core network and 5G UE support is necessary from the start.

Table 1 depicts a comparison between the NSA option 3x and the SA option 2 architectures, which suggests that to unleash the full potential of 5G systems and enable new services including URLLC and dynamic slicing, the 5GC is required along with the gNBs, and this is the main motivation for deploying the option 2.

Table 1: 3GPP Option 3x (NSA) versus Option 2 (SA)

NSA Option 3x	Vs	SA Option 2
3GPP Rel.15 + CR 12/2018	Standardisation availability	**3GPP Rel.15 + CR 12/2018**
Chipset: 2H 2018 **UE: late Q2 2019**	First mobile UEs	**Chipset: 2H 2019** **UE: Q1 2020 (expected)**
Aggregate LTE + 5G (Split Bearer)	UE max throughput DL	**5G band Carrier Aggregation**
In the case of split bearer, additional latency is introduced	Latency	**5G low latency**
Increased if dual radio transmitter is used. Complexity resulting from the LTE/5G transmission coordination	UE power consumption and complexity	**New RRC inactive state is introduced to reduce the power needed by the UE**
UE is always attached to the LTE network. With DC and split bearer, the 5G drop causes less impact on connectivity	Service continuity to LTE	**HO/redirection is needed when the 5G connection drops**
Supported	Service continuity to 2G/3G	**Not supported. Service continuity from 5G to UTRAN will be studied for 3GPP Rel.16**
Dual Connectivity **LTE-5G interworking**	New functionalities required in the LTE eNB	**Not applicable**
Handles the control plane **Split bearer traffic from the gNB**	Capacity impact to the LTE eNB	**Not applicable**
Possible but requires X2 IOT	eNB – gNB multivendor connection	**Not applicable**
Uses the Existing Core Network upgraded to accommodate the gNBs (i.e., the core network is termed 5G EPC rather than EPC)	Impact to the Core Network	**New 5G Core network is required**
Missing the new 3GPP Rel.15 features and will miss the new 3GPP Rel.16 features	New features	**Supported**
No Changes. **Voice over LTE (VoLTE) and Circuit-Switched Fall Back (CSFB) are the possible options**	Voice Support	**Need to introduce Voice over NR (VoNR - 5G) and/or Fallback to LTE (VoLTE). Voice continuity with the UTRAN will be studied in 3GPP Rel.16**
No changes	SMS Support	**New SMS delivery required**
Evolution step before options 2, 7 or 4	Evolution	**Can be a final evolution step**

2.1.2. 3GPP Release 16

This release of the 3GPP, the "5G Phase 2", will be completed in June 2020 as shown in Figure 3, and currently work is in progress within the relevant working groups. In particular, the non-standalone network infrastructure options 7 and 4 in Figure 2 will be finalized. The aim of 3GPP Rel.16 is to bring overall system advancements to the "5G Phase 1" as well as functions relevant for addressing the specific communication needs of vertical sectors.

One of the verticals directly targeted by the 3GPP is the automotive sector, and 5G-supported vehicle-to-everything (V2X) communications considers advanced scenarios that are beyond what is possible with LTE-based V2X, primarily in the area of low latency use cases. On the radio side, the 3GPP RAN1 group listed the findings of the study on NR V2X in [11] to be included in the 3GPP technical document, which shall be the basis for the next 5G NR specifications in 3GPP Rel. 16. The general 5G System architecture for 3GPP Rel.16 is specified by the 3GPP SA2 Group in TS 23.501 [13] while the 3GPP document TS 23.287 [14] targets the 5G system architecture enhancements required to support V2X services in 3GPP Rel.16. The latter specification will largely be based on the 3GPP technical report, TR 23.786 "Study on architecture enhancements for Evolved Packet System (EPS) and 5G System to support advanced V2X services" [12]. Note that the relevant V2X specifications pertaining to V2V, V2I, V2N and V2P communications using LTE/EPC networks as defined within the previous releases of the 3GPP are discussed in Annex 2 to keep the focus of the present document on 5G.

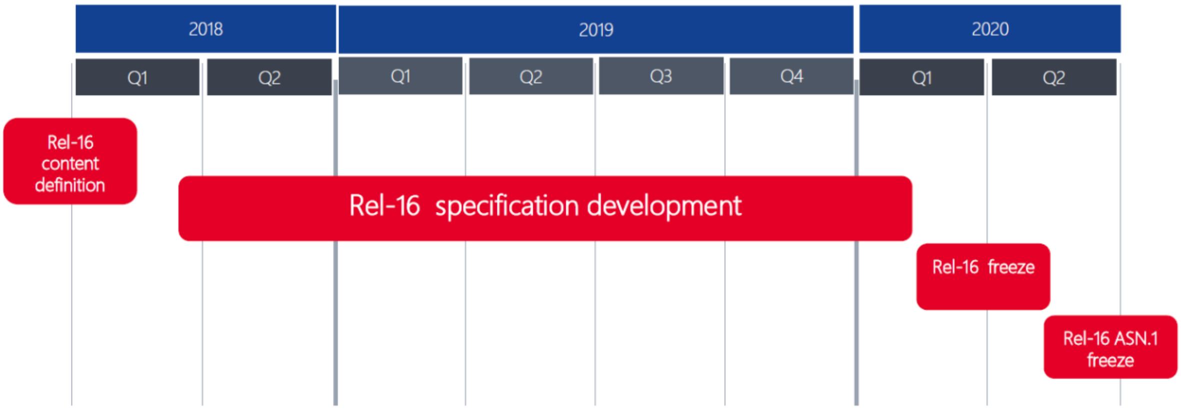


Figure 3: 3GPP roadmap for Rel.16 specifications

Another important new feature of 3GPP Rel.16 will be 5G NR-based positioning services. In the 3GPP Rel.15 specifications, despite the introduction of the new radio access technology, positioning is still handled by the LTE network. Advanced positioning capabilities of 5G NR will be crucial for applications such as emergency services and automated driving, which require advanced positioning.

For a wide range of verticals, the main achievements of the 3GPP Rel.16 standards will be the improvements and developments related with the industrial Internet of Things (IoT) and URLLC, which are basically the other two pillars of the ITU specifications on 5G systems that complement enhanced mobile broadband communications. Offering 5G technology in unlicensed bands and reaching a more accurate level of positioning will pave the way for novel services for existing subscribers of mobile operators as well as various new sectors that will benefit from 5G capabilities. The performance of MIMO systems and power consumption are also on the agenda of the 3GPP Rel.16 standards. The 3GPP document TR 21.916 [15] lists and summarizes all the 3GPP Rel.16 work items, which is a working document and will be frozen once 3GPP Rel.16 is ready.

2.2. ETSI Multi-access edge computing standard

Multi-access edge computing (MEC) is positioned as an Industry Specification Group (ISG) within ETSI, whose aim is to unite the telco and IT worlds in an effort to offer IT and cloud-computing capabilities within the RAN of mobile networks [17]. Ultra-low latency and high-bandwidth along with real-time access to radio network information that can be utilized by applications are some of the characteristics of the edge environment created by the ETSI MEC standard. On the 3GPP domain, a set of enablers to support edge computing are given in the 3GPP TS 23.501 system architecture specification [13]. In addition, it is mentioned that the 5GC may expose network information and capabilities to an Edge Computing Application Function. The idea is to handle MEC as a 5G-application function via these enablers.

The white paper [20] summarises the scenarios and challenges in deploying MEC in 4G networks and discusses the evolution towards 5G. For the 5G NSA architecture using the 5G EPC, the resulting MEC deployment options are summarised below:

- **Bump in the Wire**: In this scenario, to support low latency communications, the MEC host, which consists of the MEC platform, the MEC applications, the MEC service and the virtualization platform (data plane), sits on the S1 interface of the system architecture in between the eNB/gNB and the core network components (SGW, PGW, MME etc), and the MEC host's data plane must process user traffic encapsulated in GPRS Tunnelling Protocol – User plane (GTP-U) packets. Apart from the requirement on the MEC server to handle the GTP tunnels, this scenario poses challenges to operations such as lawful interception and charging, possibly mandating a dedicated solution such as a MEC GW to be implemented.
- **Distributed EPC**: In this scenario, through its data plane the MEC host sits on the SGi interface, connected to the distributed EPC components, where the Home Subscriber Server (HSS) is co-located with the EPC, and the MEC applications can also be positioned next to the EPC functions in the same MEC host. Since there is no need for a working backhaul to keep the local service running, this type of deployment is typically used by first responders, public safety, and mission critical industrial sites. The advantage of the distributed EPC scenario is that it requires less changes to the operator's network and leverages standard 3GPP entities for session management and charging operations.
- **Distributed S/PGW**: This scenario is similar to the Distributed EPC except that only SGW and PGW entities are deployed at the edge site, whereas the control plane functions such as the Mobility Management Entity (MME) and HSS are located at the operator's core site.
- **Distributed SGW with Local Breakout (SGW-LBO)**: Local breakout of the MEC data at the SGWs that are located at the edge sites is a new MEC architecture to achieve a greater control on the granularity of the traffic that needs to be steered such as to allow the users to reach both the MEC applications and the operator's core site application in a selective manner over the same access point name (APN).
- **CUPS MEC:** The deployment options above which distribute the EPC gateways at the edge, either co-located with or within the MEC host, can also be built using the Control and User Plane Separation (CUPS) paradigm standardized in 3GPP Rel.14 and have the new User Plane built in the MEC host allowing the traffic to be locally steered.

Among the challenges identified to support the various MEC deployment options, such as session management, lawful interception, charging, security and MEC platform subscribers' identification, mobility management is specifically critical as it affects the service continuity. Two scenarios are perceived:

- **Intra-MEC mobility**: The UE moves from one eNodeB to another but is still in the coverage of the same serving MEC host. The MEC system should be able to route the traffic to the UE via the correct eNodeB and tunnel.
- **Inter-MEC mobility/MEC hand-over**: The UE moves out of the coverage area of the source MEC host to enter the coverage area of a target MEC. In order to provide service continuity to the UE, the MEC system needs to relocate the service delivered to the UE from the source to the target MEC. In the distributed EPC, distributed S/PGW, SGW-LBO and CUPS MEC deployment options, the MEC handover is supported using 3GPP standard "S1 Handover with SGW relocation" by maintaining the original PGW as anchor. Nevertheless, it is the MEC application's responsibility to synchronize at application level and maintain the session in the case of a stateful application.

In the evolution towards 3GPP Option 2 and Service-Based Architecture (SBA), there is a clear migration pattern for the MEC deployments above, as documented in [20], [21]. In the long term, 5G deployments will increasingly integrate fixed mobile networks infrastructures with cloud computing and MEC. Orchestration capabilities, which are already a key element for exploiting cloud computing capabilities, shall become an essential part of the operation of future 5G infrastructure. Virtualisation, Network Management and Orchestration, Network Function Virtualisation (NFV), 3rd Party Support and MEC Application Management are critical capabilities for successful deployments.

2.3. Network Slicing

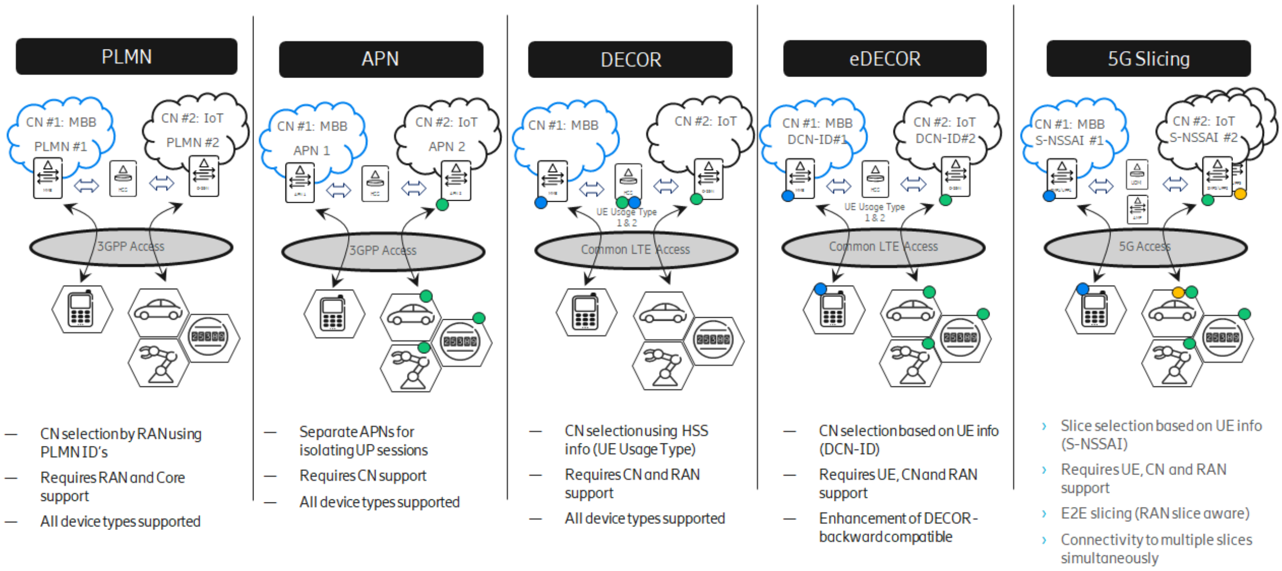
Network slicing is a concept for running multiple logical customised networks on a shared common physical infrastructure complying with agreed Service Level Agreements (SLAs) for different vertical industry customers (or tenants) and requested functionalities [16]. Consequently, a network slice could span across multiple parts of the network (e.g. access network, core network and transport network), while also could be deployed across multiple operators.

Various Standards Developing Organisations (SDO) focused on different technical domains are contributing to the network slicing progress. For instance, 3GPP focused on Radio Access Network (RAN) and Core Network (CN) while BBF and IETF focused on Transport Network (TN), etc.

Along with the SDOs, and especially the 3GPP that can be considered as the forefront ambassador for network slicing, GSMA is focused on describing the business drivers, concepts and high-level requirements of E2E network slicing from the operator's point of view. In fact, GSMA aims at generating a Permanent Reference Document (PRD) to guide future network slicing standards through its network slicing taskforce project, and it has already created some reference documents about network slicing. Specifically, GSMA has published a general document about network slicing that describes common use cases related to slices [16]. Next to this general overview document, GSMA created the document "From Vertical Industry

Requirements to Network Slice Characteristics" [19]. This document introduces some concepts such as Generic Slice Template (GST) and Network Slice Type (NEST). The GST allows for a standardised way of describing slices in a template that could be exchanged between network operators. This can be useful to create similar network slices in a roaming network. A NEST can be created based on a GST, as it is a GST with defined values. GSMA envisions to create a set of standardised NESTs (S-NESTs) but it expects also operator specific (private) NESTs (P-NESTs). The first version of a GST that standardises a characterization of network slice is already available [20].

Finally, it is worth underlining here that the concept of network slicing is a key mechanism for 5G networks, and all 5G-related specifications have been developed by 3GPP from the beginning with the aim to support end-to-end slicing mechanisms, allowing a UE to connect to multiple network slices at the same time. Until the full 3GPP capability to support end-to-end slicing is available, there are different mechanisms to support network slicing, ranging from simple and widely deployed methods such as PLMN ID and APN, i.e., mechanisms that have been available in several 3GPP releases (even from the start of GPRS) and can still be used for some type of "Network Slicing". DECOR that was added in 3GPP Rel.13 and eDECOR in 3GPP Rel.14 provides additional mechanisms for separating between "Dedicated Core networks", but with these (as with PLMN ID) a UE can only connect to one "Network Slice" at a time. 5G slicing and the corresponding selection mechanism support end-to-end network slicing. It also allows the UE to connect to multiple network slices at the same time. The various options as described are shown in Figure 4.



PLMN:

- CN selection by RAN using PLMN ID's
- Requires RAN and Core support
- All device types supported

APN:

- Separate APNs for isolating UP sessions
- Requires CN support
- All device types supported

DECOR:

- CN selection using HSS info (UE Usage Type)
- Requires CN and RAN support
- All device types supported

eDECOR:

- CN selection based on UE info (DCN-ID)
- Requires UE, CN and RAN support
- Enhancement of DECOR - backward compatible

5G Slicing:

- Slice selection based on UE info (S-NSSAI)
- Requires UE, CN and RAN support
- E2E slicing (RAN slice aware)
- Connectivity to multiple slices simultaneously

Figure 4: Considered evolution of slicing

Not shown in Figure 4, there is also the possibility to have geographically separated slices which are only available in a certain geographical area. For example, APN differentiation typically provides a partitioning of PGW resources, DECOR and eDECOR provide the possibility of selecting dedicated Core Network resources (i.e. MME and GW), while PLMN ID allows a complete separation of the resources used for dedicated networks.

Slicing can also be considered at the plane of the transport networks and WAN through resources' reservation using SDN capabilities. Also, at the level of infrastructure management slicing can be applied using automation and cloud infrastructure Virtualised Infrastructure Manager (VIM) capabilities to deploy VNFs with specific QoS characteristics through dedicated computational resources.

2.4. Roaming support for cross-border operation

International roaming is important to ensure that CCAM use cases can be seamlessly executed while the vehicles traverse from one country to the other and get serviced from different mobile network operators (MNOs). The fundamental prerequisite to guarantee service continuity is to have established and signed roaming agreements between the operators to rule network access and ensure interoperability among the network technologies deployed.

Roaming services in principle are classified as:

- *Inbound Roaming*: Subscribers from other operators access the local network and services.
- *Outbound Roaming*: Subscribers from the local network access another operator's network and services.

Furthermore, based on the physical locations accessed by the subscribers, there is a distinction between:

- *National roaming*: Mobile subscribers access other operator networks and services in the home country.
- *International roaming*: Mobile subscribers access operator networks and services while away from home country.

2.4.1. Operator Connections

To ensure service continuity while roaming, roaming agreements must be signed between operator networks to define the policies necessary to control network access for roaming subscribers and manage roaming services. Operator network connections must be established, and this can be achieved either directly or through a GPRS Roaming Exchange (GRX) or IP exchange (IPX) network as depicted in Figure 5.

- ***Direct Interconnection*** is simple and if established through private lines or VPNs (ex. MPLS) can solve QoS and security Issues. Nevertheless, it greatly increases cost especially if many international point-to-point private lines are necessary. It is noteworthy that using the Public Internet and establishing secure tunnels with IPSec can be regarded as a viable option for fulfilling pilot and prototype deployments' requirements, but not for carrier-class communications. Direct Interconnection is relevant to friendly operators with shared responsibilities.
- ***GRX based Interconnections*** are operated and managed by third parties. An MNO, through a GRX connection endpoint can be connected to multiple operator networks establishing corresponding roaming agreements and enjoys the service scalability offered through this point-to-multi point interconnection. Private lines do not need to be individually established, greatly reducing roaming costs. Nevertheless, GRX networks provide no QoS guarantee and typically leverage SS7 signalling focusing on the transmission of GPRS, EDGE, 3G, and HSPA roaming data and MMS service data.

- ***IPX based Interconnections*** is an evolution of the GRX framework towards an open and flexible environment and assumes an all-IP transformation better suited for LTE service requirements. MNOs need to find GRX services that can offer E2E SLA for future service growth and only GRX services provided by IPX networks can offer E2E SLA. Note that IPX is the appropriate network to provide Diameter connections between MNOs. In order to support scalability, resilience and maintainability, and to reduce the export of network topologies, the use of AAA (Authentication, Authorisation and Accounting) services through a PLMN-edge Diameter agent is recommended [22]. The Diameter agent, named Diameter Edge Agent (DEA), is considered as the only point of contact into and out of an operator's network at the Diameter application level. Diameter has been widely used in the S6a, S6d, S9, S13, Gx, Gxc, and Rx interfaces of the 3GPP EPC architecture.

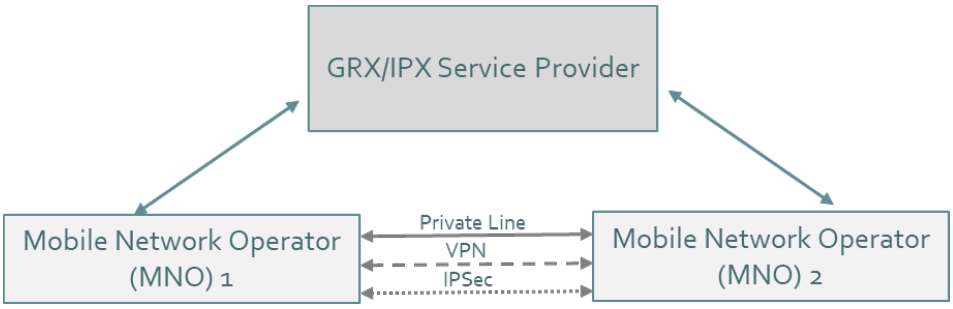

GRX/IPX Service Provider
Mobile Network Operator (MNO) 1
Private Line
VPN
IPSec
Mobile Network Operator (MNO) 2

Figure 5: Roaming Interconnection Options

2.4.2. Roaming Types

Based on the roaming service access policies used by mobile terminals, two roaming types exist:

- **Home-routed (HR)**, where subscribers always obtain service from the home PDN gateway (H-PGW) and through their home network. As the service is always managed through the same PGW (the H-PGW), service continuity while roaming is ensured, but with increased latency and resources utilisation due to the user plane traffic being routed through the GRX (GPRS Roaming Exchange) / IPX (IP exchange) networks to the Home PLMN. This roaming type is especially relevant for subscribers who have special services such as enterprise VPNs.
- **Local Break-Out (LBO)**, where subscribers obtain service from the visited PGW (V-PGW). In effect, this provides better user experience and significantly reduced roaming service delay (payload traffic does not traverse through GRX but rather stays in V-PLMN network), at the expense of service control, policy control, charging and service continuity that will be disrupted as the sessions must be released and re-established during the handover. LBO, which is a spec compliant functionality, requires re-establishment of PDN session. For LBO to operate the involvement of HSS and MME modules is required. V-PLMN is a subscription parameter stored in HSS and delivered to MME within subscription information during signalling procedures.

Subscribers are expected to connect to different 5G networks, each with its own edge location. Information needs to be shared such that all subscribers are receiving up-to-date information needed for the automated driving use case categories tested at the trial site. With cross-border handovers between separate operators it is currently observed that the subscribers are disconnected for up to a minute or even more. For automated driving vehicles, a disconnection of more than one second means that it cannot rely on the mobile network. The options to be considered for deployment are as follows:

- For 5G NSA (3GPP Option 3): Two interfaces are used as roaming interfaces that interconnect the related entities of MNOs. The first one is S6a and the second one is S8. A third interface, S10 shall be introduced in this case as an additional roaming interface, so that context information of active session is exchanged between two MMEs during handover. Handover procedure will fail, and UE will be detached from network, if S10 interface is not configured.
  - S6a is used for interconnecting MME of V-PLMN with the HSS located in H-PLMN
  - S8 is used for signalling and data transfer between SGW/PGW entities.
- For 5G SA deployments (3GPP Option 2): In 5G Core Specification, the session service continuity mode for an application is determined by SSC mode selection policy. With SSC mode 3, network ensures that UE does not lose connectivity by making a new connection before breaking the existing one to allow service continuity and this is the most appropriate mode for the seamless roaming. The service provider may provision the policy rules for UE to determine the type of mode associated with an application or a group of applications.

2.5. 5G-MOBIX feedback to and from standardisation bodies

Identifying and responding to standardisation and spectrum gaps is one of the major aims of the 5G-MOBIX project, which will leverage the current research and standardisation activities by partners in relation to specifications. 5G-MOBIX standardisation related tasks in WP6 will share the experiences and findings from the project trials in the form of recommendations to 3GPP meetings, as well as, other SDOs working in the automotive sector (CEN/ISO, UNECE, etc.). Additionally, 5G-MOBIX will use the trials to provide insights on spectrum allocation and utilisation that will be of value to national spectrum regulatory authorities, and to contribute to EU-wide 5G-V2X spectrum harmonisation discussions, particularly the ones pertaining to cross-border scenarios.

3. TELECOMMUNICATION REQUIREMENTS & CROSS-BORDER ISSUES

In this section, the functional and non-functional requirements of cross-border operation are analysed and translated into 5G network requirements and specifications needed in order to support the envisioned functionality with the promised QoS/QoE. Additionally, the specific impact that the identified telecommunication cross-border issues (see [1]) have on 5G network components / features and the deployed 5G network architecture are analysed and the insights are used to drive the selection of suitable architectural designs for the 5G MOBIX CBCs/TSs.

3.1. Telecommunication Cross-Border issues impact on 5G architecture and components

In this section, the most promising and relevant telecommunication cross-border issues (as presented in Section 2 of [1]) are further discussed and explained, while the potential solutions to resolve or mitigate each issue are also presented. Out of the potential solutions discussed among the 5G-MOBIX experts, a sub-set of them were deemed to be more promising and are hence progressed for more detailed evaluation during the 5GMOBIX trials. The complete overview of the 5G-MOBIX identified x-border issues can be found in [1] where the cross-reference can take place based on the *Issue ID*, while the analysis application x-border issues can be found in D2.3 [2] and the analysis of the vehicular and regulatory issues can be found in D2.4 [3].

3.1.1. Roaming

Issue Title	Roaming (R)	Issue ID	TR1, TR2, TR3
Description	International roaming support for V2X communication cases is required when vehicles travel to other countries. Specifically, when a UE (e.g., automated vehicle) crosses the border of a country, switching to another mobile network operator (MNO) needs to be performed in an optimum way aiming to fulfil the strict requirements of the CBC use case categories in terms of latency and service continuity. Roaming agreements between the MNOs is prerequisite.		
Conditions	*Roaming between MNOs with 5G EPC (NSA) network solutions support (TR1)*: Taking into account vendors' roadmap, this scenario seems to be the most likely to happen at the first phase of 5G deployments, exploiting the existing LTE roaming agreements. *Roaming between MNOs with 5G SA core network solutions support (TR2):* Taking into account vendors' roadmap & the standardisation status, this scenario will occur at a later phase. *Roaming between MNO with 5G EPC (NSA) network and another MNO with 5G SA core network (TR3):* Interworking functionalities need to be supported at this scenario; roaming extensions or new roaming interfaces (i.e. N26 interface) will be required.		

Consequences & impact	Long roaming latency is expected since the current LTE roaming traffic is Home Routed, meaning that subscribers always obtain service from the home PDN gateway (H-PGW) and through their home network. As the service is always managed through the same PGW (the H-PGW), service continuity while roaming can be ensured, but nevertheless with increased latency due to the user plane traffic being routed through the GRX (GPRS Roaming Exchange) / IPX (IP exchange) networks to the Home PLMN. In addition, the Visited PLMN (V-PLMN) does not normally honour QoS for roaming UEs using home routing.
Proposed Solutions	• **R1**: URLLC resource discovery and allocation before roaming • **R2**: Proper selection of roaming network mode (MNOs interconnected via GRX or direct connection) to fulfil the latency requirements. • **R3**: LBO & HR are both options to be considered per user story. • **R5**: Flexible network configuration to improve the QoS of services/users, probably considering a proper slice management with 5G SA Core solution.
Progressed Solutions	Given that international traffic of MNOs at cross-border corridors configured through GRX/IPX networks does not meet the latency and security requirements of URLLC services, direct interconnection solution is being evaluated by both CBCs. In addition, both HR (for the first phase) and then LBO solutions will be evaluated.

3.1.2. Handover

Issue Title	**(inter-PLMN) HO in hybrid cellular networks**	Issue ID	**TH1**
Description	This issue involves the handover between cellular network communication technologies with different performance capabilities. This will be particularly common when combining 5G NR with currently available 5G LTE networks.		
Conditions	5G SA to 4G LTE 5G NSA to 4G LTE		
Consequences & impact	Performance degradation in terms of throughput (impact on eMBB services), delay (impact on URLLC services) and potential period of disconnection in the handover. When the network changes imply an inter-domain handover (roaming), the consequences identified in TR1-3 issues are applicable also here.		
Proposed Solutions	• H1: Redundant connection using dual SIM. This requires a proper management of data flows in the same end node, using an intelligent router or SDN capabilities, for instance. • H2: Allocate maximum resources in the target 4G network to reduce the impact. • H3: Agreement between MNOs when a roaming situation is faced, including the solutions proposed in TR1-3. • H4: Multiple Care-of Address and network mobility solutions to make applications mobility-agnostic. In other case, applications should be developed considering network disconnections. This especially applies to IP-based applications in which re-addressing can be present in the handover. • H5: Use of intelligent algorithms that can help to anticipate the network change and trigger the handover once the resources are prepared.		
Progressed Solutions	Dual SIM is being considered in the project, given the experience provided by TSs in the form of lesson learned to the cross-border corridors. If finally chosen, the consortium has		

	expertise in the management of data flows and the application of network mobility solutions. Moreover, MNOs in the project are already exchanging user profiles to make handover possible and speed-up the process.

Issue Title	(inter-PLMN) HO with overlapping coverage	Issue ID	TH1, TH2, TH3
Description	A bad cellular planning can induce overlapping coverage problem, where the gNodeBs radio coverage are highly overlapping. In cross border cases (inter-PLMN HO → roaming) this scenario is very likely as the MNOs from both countries want to guarantee coverage in their country's territory and as a result a 'spill-over' of coverage from both sides creates unpredictable radio conditions, where the actual HO can happen well before or after the actual border.		
Conditions	gNBs radio coverage range is above the necessary limits / thresholds.		
Consequences & impact	High level of overlapping coverage leads to: · • Interference among gNodeBs and consequently low SINR (Signal to interference and Noise Ratio) leading to QoS degradation; • Signal levels are too close to each other leading to disturbance of the UE connection stability, specially, during handover (ping-pong effect); • The connection drop rate will increase depending on handover rate; • Unjustified signalling traffic load increases; • At cross border conditions, excessive radio coverage can generate unwanted roaming; • Cells unbalanced traffic load; • Uplink/Downlink unbalanced cell radio coverage; Consequently, CCAM applications will suffer negative impacts from the resulting QoS degradation.		
Proposed Solutions	• H5: Use of intelligent algorithms that can help to anticipate the handover and trigger the handover. Handover parameters shall be optimised; • H6: In the dual SIM scenario an intelligent switch will decide for the handover and manage this process to be as stable as possible; • H7: Network mobility solutions should be properly adopted for mobility-agnostic applications; • H8: Radio access network parameters configuration, for example: transmission power, antenna tilt and height, site location.		
Progressed Solutions	The most promising and sustainable solution is H8 and in a second stage H5 solution can be used as a network fine tuning procedure, increasing QoS		

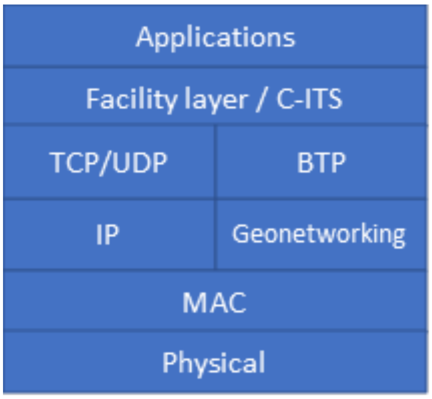
Issue Title	(inter-PLMN) HO with coverage gaps	Issue ID	TH1, TH2, TH3
Description	The distance among the neighbouring countries eNBs / gNBs or the radio planning of the two neighbouring MNOs, results in areas close to the border where no MNO can provide services or UE connection to a network is not even possible. These areas of no coverage are		

	identified as coverage gaps and result in complete service interruption, until connectivity can be re-established with one of the networks.
Conditions	There is no 5G network coverage and the user has no connectivity.
Consequences & impact	User experiences a period with no connection-> all types of applications will be negatively impacted by a service interruption.
Proposed Solutions	• H9: Satellite communications may be used to provide service in the areas that 5G connectivity experiences gaps. The moment the network parameters for the other MNO are met, the connection will change from satellite communication back to 5G. During the handover process all data flow will be considered. • H10: Handover to 4G or even 3G if required. Initiate resource allocation to meet the requirements • H11: Proper network planning & optimization should be performed
Progressed Solutions	Actual CBC implementation is unlikely to face this issue, however as part of the trialling solution H10 may be evaluated at the CBC. Solutions H9, H10 and H11 will be evaluated as part of the TS extended evaluations (See Section 6)

Issue Title	**(inter-PLMN) HO in higher layers**	Issue ID	**TH2, TH3**
Description	A handover can imply the change of network address with impact on running UDP/TCP communications and the disconnection of the data path for the services running on-board. Moreover, a change of MNO in a roaming situation can imply a different set of protocols used in each domain.		
Conditions	IP re-addressing IPv4 to IPv6 IPv6 to IPv4 ITS-specific protocol to TCP/IP TCP/IP to ITS-specific protocol Different application-level protocol		
Consequences & impact	This kind of incompatibility would result in a disruption of the communication flow if a proper transition solution or agreement between MNOs is not given.		
Proposed Solutions	• H12: An algorithm (with or without using machine learning) to enable optimal UPF relocation. Follow the Session and Service Continuity (SSC) modes for different UE and application mobility scenarios (clause 5.6.9 of 23.501). • H13: Applications should be properly developed to mitigate possible network disconnections due to mobility. • H14: A common deployment of ITS and or TCP/IP protocols involving the domains of different operators should be considered under roaming circumstances. • H15: Usage of non-connection-oriented protocols such as UDP, or disruption tolerant protocol like DTN, ICN can be implemented on applications when possible. • H16: Deployment of application-level protocols among MNOs with proper agreements to support the continuity of service operation.		
Progressed Solutions	Services to be deployed in CBC will be a proper support by the target MNOs regarding network and above layers. In any case, software developers have seriously considered the		

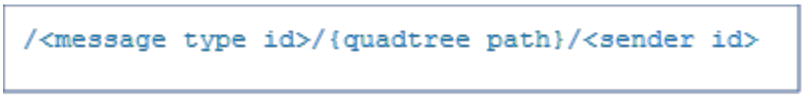
	possibility of losing connection, so applications are prepared to re-connect when needed. Underlying network and transport protocols to be used will remain the same for MNOs piloting the same services within particular user stories.

3.1.3. Networking

Issue Title	GeoNetworking	Issue ID	TN1, TN3
Description	The GeoNetworking header is part of the GeoNetworking Protocol [23], to be used by the GeoAdhoc router. In parallel with the GeoNetworking protocol, the Basic Transport protocol is used for multiplexing of messages. While GeoNetworking/BTP is used for ad-hoc networks, IP/TCP/UDP is used for non ad-hoc networks. All protocols are used for routing messages to the intended stations. Only the IP/TCP/UDP protocol has no mechanism to route only to a certain geographical area. In addition, the GeoNetworking protocol has means to sign the messages whereas IP/TCP/UDP has no mechanism to sign messages. The stack layout comparing IP and GeoNetworking is shown below.  Applications Facility layer / C-ITS TCP/UDP BTP IP Geonetworking MAC Physical		
Conditions	This is valid for ITS messages sent over cellular and fixed networks.		
Consequences & impact	The resulting consequences can be categorized as follows: • *<u>Current standards to send ITS messages over cellular and fixed networks are inadequate</u>*: The current standard for C-ITS messages has got the signature integrated in the networking layer. For this reason, there is no clear solution to use the ITS messages with cellular and fixed networks. When the GeoNetworking/BTP header is discarded and replaced with the IP/TCP/UDP header also the signature is discarded. When keeping the GeoNetworking/BTP header a redundant networking layer is kept. • *<u>Extra overhead because of the GeoNetworking/BTP header</u>*: The header size for GeoNetworking and BTP is around 140 bytes. When including the certificate (without intermediate certificates) this can grow up to 270 bytes. This is a significant addition in size for several types of ITS messages (see for example table 1). Looking at cellular communication 270 bytes will probably cost around 2 to 4 extra resource blocks (depending on the coding scheme) and can negatively impact the latency of the delivery of the message. The total message size including the geonet and btp headers is shown below.		

<table>
<tr><td></td><td>
<table>
<tr><th>CAM Message</th><th>160 bytes</th></tr>
<tr><td>Geonet/btp header</td><td>44 bytes</td></tr>
<tr><td>Security header</td><td>96 bytes</td></tr>
<tr><td>Certificate</td><td>133 bytes</td></tr>
<tr><td>Total</td><td>433 bytes</td></tr>
</table>
</td></tr>
<tr><td>Proposed Solutions</td><td>
When using the cellular network, communication will in most cases take place via unicast. No real solutions have been seen yet with eMBMS 1(Downlink) and for the uplink only Unicast is possible. Because of this, adding a message exchange service when using the cellular network is inevitable. For exchanging messages between vehicles and the network, different solutions have already been tried out (e.g. MQTT, AMQP or sending the raw GeoNetworking packet over UDP). The most promising of these solutions seems to be the one using MQTT. The MQTT protocol is already standardized and focusses on the delivery of messages in an efficient manner. Using MQTT the vehicles can select themselves to which areas they need to subscribe. This way no intelligence is needed at the server side to detect where vehicles are driving (or are heading for). The vehicle simply subscribes to the areas of interest and publishes its own messages to the area it is driving.

The GeoNetworking header and BTP header can be left out since routing will be done using TCP/IP. To make sure messages will only be sent to the relevant vehicles a specific topic structure is proposed consisting of a quadtree path, specifying a certain area (also called tile). Vehicles subscribe to a certain topic where the topic covers a certain area. By using quadtree coding the tiles can be translated to topics as shown below.


/<message type id>/{quadtree path}/<sender id>

Security can be added using TLS for transport layer security, together with a trusted message service. Optionally, it is still possible to add extra security by signing the messages. Relevant work is ongoing in order to add the signature to the facility layer (see [24]).
</td></tr>
<tr><td>Progressed Solutions</td><td>The above MQTT solution will be evaluated, while other alternatives may also be examined.</td></tr>
</table>

Issue Title	Hybrid Networking	Issue ID	TN2
Description	As vehicles and RSUs perform multi-tasking beyond CCAM functionality, in most cases the vehicles and RSUs will be able to communicate over multiple different communication technologies. Besides the challenges created by this co-existence (dealt with in the other x-border issues), it also creates the opportunity to improve overall performance through the intelligent utilization of heterogeneous communication resources.		

Conditions	CCAM enabled vehicles and/or roadside units are equipped with multiple different communication means (5G, 4G, PC5, satellite communication etc.)
Consequences & impact	Optimal connectivity over selective communication resources as well as increased flexibility in cases of overloading.
Proposed Solutions	An SDN controller could be implemented in the MEC and redirect the traffic flow based on the available technology. The decision to forward the traffic to specific technology (5G, 4G, Satellite communication, PC5) will be made by the SDN controller knowing beforehand which technology is available in the vehicle or in a geographic area where sometimes coverage gaps may exist.
Progressed Solutions	The solution is envisioned to be evaluated in the FR trial site.

Issue Title	**Inter-MEC connectivity**	Issue ID	**TN4**
Description	How to interconnect MECs deployed at different MNOs network across a border. The main problem is the high latency between MECs in the cross-border with MNOs that are usually interconnected through 3rd party GRX/IPX networks.		
Conditions	MECs interconnected through GRX/IPX networks or directly interconnected but with international traffic routed to the centre of the IP network, resulting in significant latencies, not suitable to serve stringent CCAM applications / functions.		
Consequences & impact	High latency introduced by GRX/IPX networks impacts the QoS of applications requiring URLLC. The traditional routing via the MNOs core which may be located hundreds or thousands of km away becomes problematic as well. Lack of security may also be a problem.		
Proposed Solutions	• **R1**: Direct interconnection • **R2**: Direct interconnection with IP network configured with border link (international traffic not routed to centre of MNOs IP network) • **R3**: Direct Interconnection with Segment Routing (SR) between the two MNO Edge DCs (Delay minimized and assured by SR)		
Progressed Solutions	Both cross border corridors of 5G MOBIX have progressed the solution of a direct interconnection among the two MNOs (and consequently the respective MECs), as can also be seen by the reference architecture. However, the exact implementation will vary as the ES-PT corridor will interconnect the MECs over the S-GW (R2) while the GR-TR corridor will interconnect them over the P-GW (NSA architecture) (R1). More alternatives will potentially be evaluated as the infrastructure at the CBCs evolves during the project lifetime.		

3.1.4. Data Protection & Privacy

Issue Title	**Different personal data protection regulations in non-EU countries**	Issue ID	**SDP0**
Description	Different data protection regulations apply when processing personal data subject in Europe, Turkey, China and Korea. Therefore, many legal, organisational and technical challenges need to be overcome for lawful processing of these data.		

Conditions	No concrete condition
Consequences & impact	Different level of data protection may cause services to be unavailable, which could require personal data protection.
Proposed Solutions	Harmonization of data protection regulation, or establishing agreements between countries
Progressed Solutions	All the above solutions will be evaluated to a certain extend at the extended evaluations taking place at the TSs (See Section 6).

Issue Title	**CCAM messages considered as personal data**	Issue ID	**SDP1**
Description	Without proper legal basis, lawful processing of personal data could not be achieved. Indeed, legal issues arise at the enforcement of the GDPR to CCAM. For example, CAM and DENM messages (and other CCAM messages) are considered personal data but are required for the normal functioning of the CCAM systems.		
Conditions	No concrete condition		
Consequences & impact	CAM and DENM messages should be provided with some kind of protection to ensure the confidentiality of the personal data (location, car identification, etc.)		
Proposed Solutions	It is suggested the usage of a method of identities pseudonymisation to avoid traceability		
Progressed Solutions	Some proposals are being discussed at the moment, but there is no final standardised solution to be applied.		

Issue Title	**Organisational procedures between different countries**	Issue ID	**SDP2**
Description	Partners in 5G-MOBIX processing data from citizens of different countries need to put proper organisational procedures to handle data protection. These include (but are not limited to): • Data processing cartography, • Training, • Privacy risk assessment, • Data breach procedures, • Documentation		
Conditions	X-border scenarios when a 3rd party is involved (foreign country)		
Consequences & impact	Manage personal data leaking incident increase its complexity.		
Proposed Solutions	Harmonization of data protection regulation, or establishing agreements between countries		
Progressed Solutions	All the above solutions will be evaluated to a certain extend at the extended evaluations taking place at the TSs (See Section 6).		

Issue Title	**Technical difficulties in cross-border scenarios**	Issue ID	**SDP3**

Description	The technical mechanisms that are applied in order to support the legal requirements on lawful data processing could find difficulties in a cross-border scenario. These mechanisms include (but are not limited to): • Data encryption • Data minimization • Anonymization/ pseudonymization • Differential privacy mechanism • Informed consent • Privacy by design and by default • Assessment of these deployed technical
Conditions	X-border scenarios when a 3rd party is involved (foreign country)
Consequences & impact	These protection mechanisms could be incompatible between EU and non-EU countries, which could result on more difficult handovers.
Proposed Solutions	Identify the technical problems and propose a solution.
Progressed Solutions	All the above solutions will be evaluated to a certain extend at the extended evaluations taking place at the TSs (See Section 6).

3.1.5. Miscellaneous

Issue Title	**Service & device isolation**	Issue ID	**TS1**
Description	Both the C-V2X and ITS G5 technologies can operate over the 5.9GHz band dedicated to ITS, particularly if the applications are those for road safety and efficiency. However, the two technologies are not inter-operable and hence they will interfere the other's operation when a same frequency channel is used.		
Conditions	C-ITS stations (vehicles and RSU) equipped with the C-V2X technology coexist with C-ITS stations equipped with ITS G5 technology trying to use the same frequency resource.		
Consequences & impact	High packet error rate and long delay for both C-v2X and ITS-G5 communications. Channel saturation. The worst case refers to the complete failure of C-V2X and ITS-G5 communications, leading to a situation where the road safety is at risk.		
Proposed Solutions	• M1: Dedicated and independent channel(s) to C-V2X and ITS G5 communications. • M2: use of a detection mechanism of the other technology (detection energy, beacon, preamble, collision, etc.) in order to free the resource. • M3: Reservation of a transmission period by the C-V2X by sending a signal of energy detectable by the ITS-G5.		
Progressed Solutions	All the above solutions will be evaluated to a certain extend at the extended evaluations taking place at the TSs (See Section 6).		

3.2. Functional and non-functional requirements for cross-border operation

In terms of functional and non-functional requirements, the needs of all the corridors/trial sites have been collected by the respective network experts, based on their respective supported user stories and focusing on cross border operation (all TSs employing multiple PLMN solutions). The responses of the experts are not necessarily limited by the current availability of 5G technology within the lifetime of the 5G-MOBIX project, but rather reflect their expert opinion on the required features to fully support (continuously and with the required QoS) the cross-border user stories addressed in the specific CBC/TS.

The estimation of the importance of each of the functional and non-functional requirements per site is based on the MoSCoW method of requirements prioritization [26], which is a well-established management method, prioritising the requirements of any system into (M)ust-haves (highest priority), (S)hould-haves, (C)ould-haves and (W)ould-haves (lowest priority). The detailed responses of each CBC and TS of 5G-MOBIX for all the below mentioned functional and non-functional requirements can be seen in Annex 1. The resulting prioritisation of requirements is then aggregated to produce a project-wide view on the necessary requirements that need to be met in order to fully and adequately serve the selected use case categories, and to simultaneously provide insights on the proposed prioritization of 5G technologies and features adoption and deployment, according to leading European experts. The provided MoSCoW grading by the sites' experts has been translated to a criticality/prioritization scale per requirement, with an additional gravity assigned to the prioritization of the cross-border corridors (as more relevant), following the translation scheme presented in Table 2. By aggregating the collected points for each requirement, each one is then assigned a 5G-MOBIX criticality/prioritization grade between 1 (low criticality/priority) and 10 (high criticality/priority) – (see *Annex 1* for more details).

Table 2: Translation table from MoSCoW grading to a 5G-MOBIX criticality/priority scale

MoSCoW Grade	M	S	C/W
CBC scale points	2	1	0
TS scale points	1	0.5	0

The exact definitions of the main identified Functional and Non-Functional requirements by the 5G-MOBIX experts are given below, while the insights regarding their criticality for the successful support of the evaluated use case categories and consequently the prioritization that should be followed in technology/feature adoption and deployment in upcoming 5G networks roll-outs are depicted in Figure 6 and **Error! Reference source not found.**, respectively. The main *functional* requirements identified by the 5G-MOBIX corridors/trial experts are:

- *GRX/IPX/VPN MNO Interconnections with SLAs*: Roaming Interconnections (GRX/IPX) between MNOs must offer QoS SLAs, especially when utilised for user plane traffic;
- *Virtualisation support*: Computing virtualisation infrastructure should provide support of function virtualisation via virtual machines or containers;
- *Multi-tenancy*: The provided architecture must cater for the delivery of services with the requested QoS to multiple tenants over a single network deployment;

- *Network Slicing*: Towards supporting multi-tenancy over the 5G-MOBIX framework, slicing is required in order to preserve security and isolation between tenants, and to maintain the QoS guarantees (latency/bandwidth);
- *Mobility support*: High-speed Mobility needs to be supported without compromise on the perceived QoS (Latency/Throughput);
- *eMBB services support (Transport)*: High capacity fronthaul/backhaul transport network needed;
- *eMBB services support (Radio)*: 5G-NR links of 100 MHz BW must be supported by the RAN and the UE;
- *eMBB services support (Core)*: Core network (5G EPC and/or 5GC) should support 5G NR functionalities;
- *URLLC services support (Transport)*: Strict requirements of URLLC services in terms of transmission delays and synchronisation must be supported by the fronthaul/backhaul;
- *URLLC services support (Radio)*: The 5G NR should support all required URLLC functionalities (i.e. mini-slot scheduling, grant free UL, pre-emption scheduling, etc.);
- *URLLC services support (Core)*: Distributed core with functionality at the edge is necessary (i.e. CUPS);
- *Interaction among MEC/Edges of different MNOs*: Tight interaction between edges of multiple operators must be implemented;
- *4K video streaming:* The application must handle the multicast of 4K video among the platoon trucks for "see-what-I-see" functionality;
- *ITS Centre Coordination among Countries*: Cooperation at the higher level should exist to assure that ITS policies and eventual control persists after border crossing.

Based on the above analysis and the CBC/TS experts' input, the main functional requirements identified within 5G-MOBIX are prioritized as depicted in Figure 6. The 5G-MOBIX experts consider the support for core eMBB functionality as well as the support for virtualization as the most critical components for delivering high quality CCAM services. Both these features should become available with the deployment of 5G core solutions (i.e. SA implementations). Closely behind, mobility support and URLLC functionality will allow for further CCAM applications to be supported, while issues such as GRX, ITS centre and MEC interconnection come lower on the priorities list.

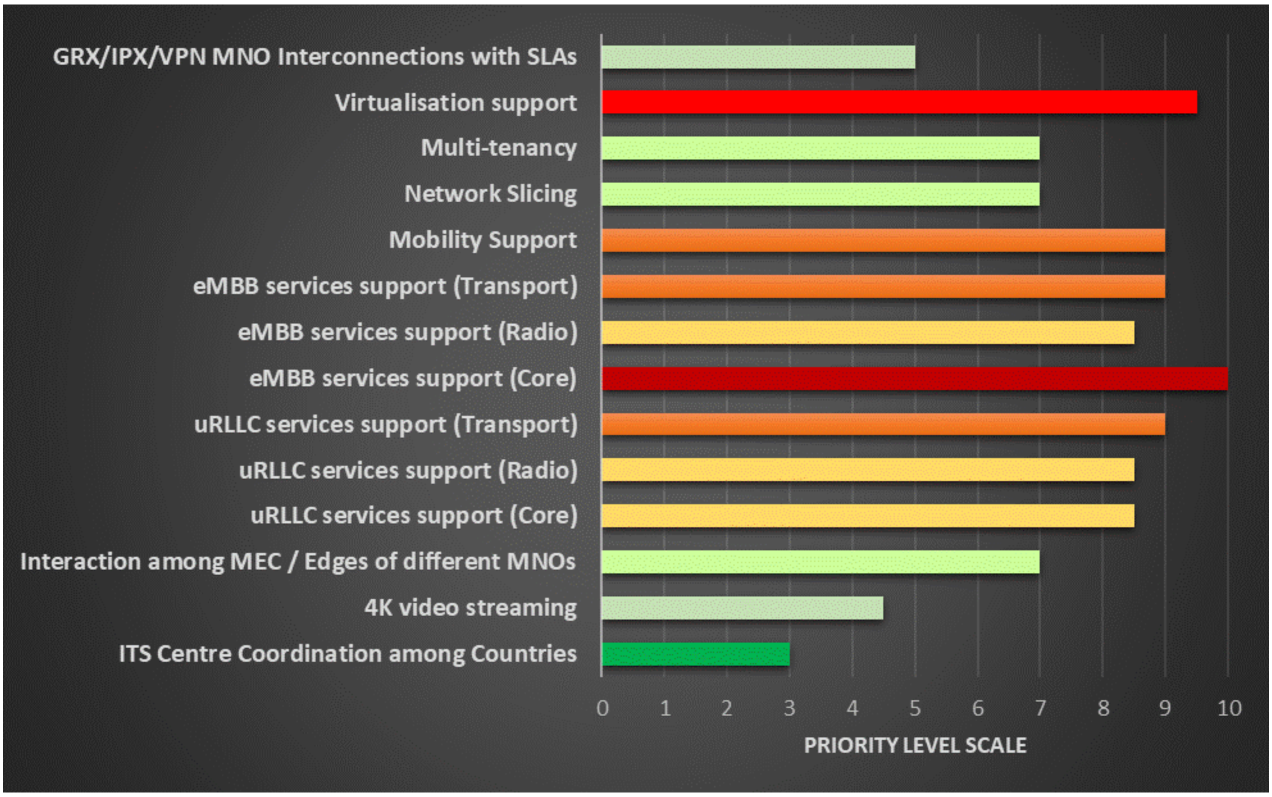


Figure 6: 5G-MOBIX identified functional requirements criticality / prioritization

The main identified *non-functional* requirements by the 5G-MOBIX corridors/trial experts are:

- *Roaming Agreements*: Roaming Agreements must be in place and contain all necessary network service characteristics;
- *Interoperability with Legacy Technologies*: The proposed deployment must be interoperable with the existing network technologies as deployed by the MNOs;
- *Feasibility for commercial deployment*: The provided architecture must be feasible for commercial deployment by the MNOs and should not assume big bang implementations, but progressive and risk-contained evolution;
- *Extensibility/Upgradability*: The designed solution must be future-proof by continually keeping pace with state-of-the-art developments and innovations;
- *Scalability*: The 5G-MOBIX use case categories design must be scalable and allow for large scale deployments;
- *Reliability*: The designed solution must ensure the reliability required by each user story;
- *Provided Architecture must be realized by Q1/2020*: The architecture should use technology available for real-life demonstration;
- *Physical security of equipment and infrastructure*: Ensure that the topology designed will contain sites where sensitive and expensive network and application equipment are physically protected and secured;

- *Digital/cybersecurity concerns*: All network equipment and application servers must be sufficiently protected from denial of service and intrusion attempts;
- *Coexistence with other technologies*: The proposed deployment must coexist/interwork with other technologies, already deployed by the MNOs (e.g. NB-IoT);
- *Authorities participation in trials*: To ensure safety, access, authorization and political support: Municipalities, Road Authorities, Highway Concessionaires, etc.

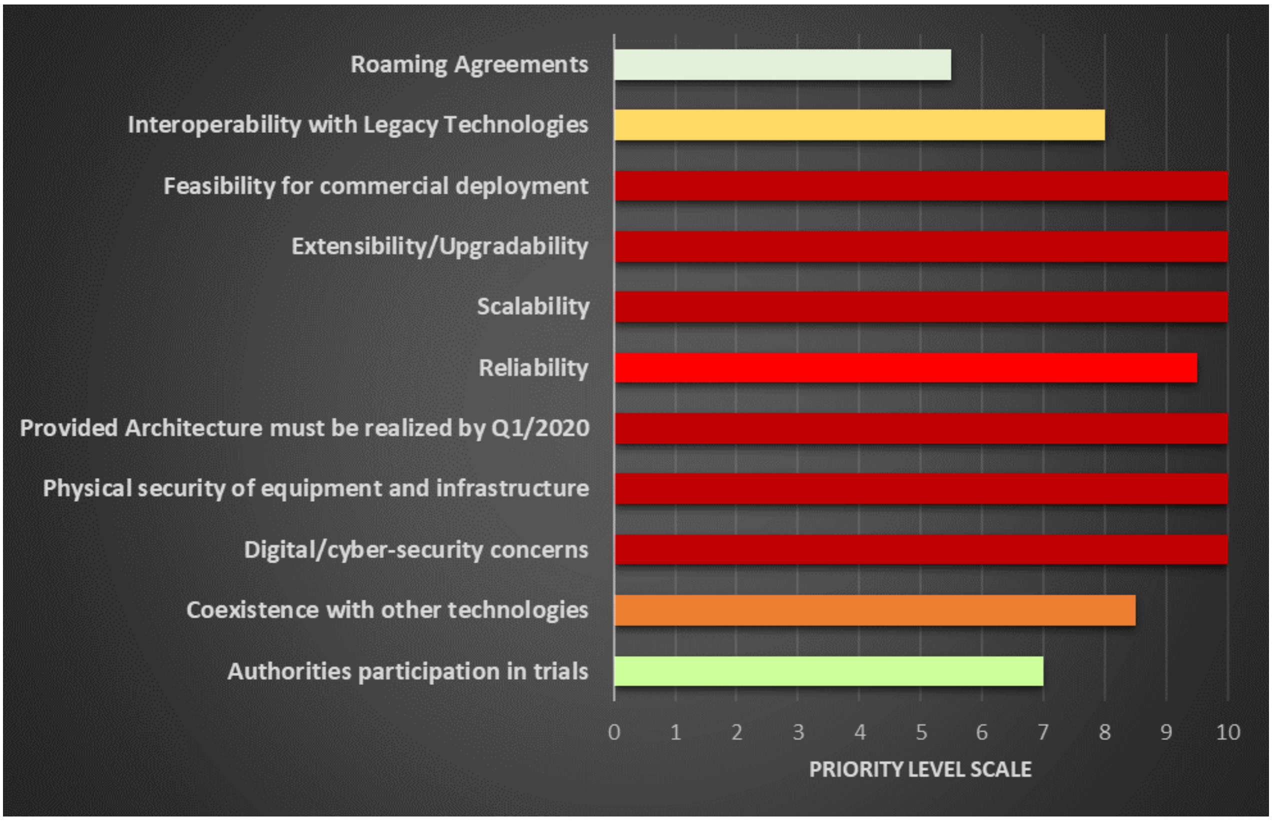


Figure 7: 5G-MOBIX identified non-functional requirements criticality / prioritization

Based on the above analysis and the CBC/TS experts' input, the main non-functional requirements identified within 5G-MOBIX are prioritized as depicted in **Error! Reference source not found.**. This time a smaller deviation is observed, as multiple non-functional requirements are considered highly-critical for the successful support of CCAM use cases. Scalability, upgradability, physical and cybersecurity, commercial feasibility and reliability are considered key factors that *must* be present for 5G networks to be able to realistically extend their functionality and reach to a state where they would successfully support the stringent CCAM applications.

3.3. Cross-border sustainability

The sustainability of the 5G network infrastructure and technologies deployed in 5G-MOBIX requires continued commitment of an ecosystem of various stakeholders at each site. In this context, we identify six major types of stakeholders (besides End Users), in partial alignment with those specified in [37], while also defining their relationships in the context of a cross-border sustainable operation, presented in Table 3.

- Mobile Network Operators (**MNO**).
- Communication Infrastructure Providers (**CIP**).
- Authorities/Policy Makers (**APM**).
- Road Infrastructure Operators (**RIO**).
- Original Equipment Manufacturers/Automobile Makers (**OEM**).
- Software Developers (**SWD**).

Table 3: Inter-stakeholder relationships and sustainability impact at x-border corridors

Relationship	Description	Sustainability Impact
MNO < -- > OEM 1	• MNO deploys 5G infrastructure • OEM is the tenant of MNO	• 5G-MOBIX solutions that are tailored to the needs of OEMs for autonomous driving will be integrated in the commercialized MNO networks. The relationship will capture the requirements of large vehicles. • The study under this relationship will guide for sustainable business models between MNO and OEMs.
MNO < -- > CIP 2	• CIP provides the communication infrastructure • MNOs operate	• This relationship will feed in the recommendations for equipment/solutions updates to CIP
MNO < -- > RIO 3	• RIO is the tenant of MNO	• This relationship will allow the study of new business models, CCAM infrastructure deployment, and recommendations for cross-country regulations.
SWD < -- > OEM 4	• OEM generates requirements • SWD develops the software	• This relationship will open new channels of collaborations between the start-ups/SMEs and OEMs
SWD < -- > MNO 5	• SWD make use of the MNO's exposed APIs	• This relationship will study the flexibility/programmability of 5G mobile networks specific to Autonomous Driving

MNO < -- > MNO 6	- Different MNOs may have different business and deployment plans	- This relationship is very important to study, as this will result in valuable recommendations for 5G deployment, business cases, and standardisation.

Based on the defined actors and relationships the following initial sustainability analysis has taken place for each of the two 5G MOBIX CBCs.

3.3.1. Spain Portugal Cross-border Corridor

This cross-border corridor hosts most of the roles on its both sides, as depicted in Figure 8.

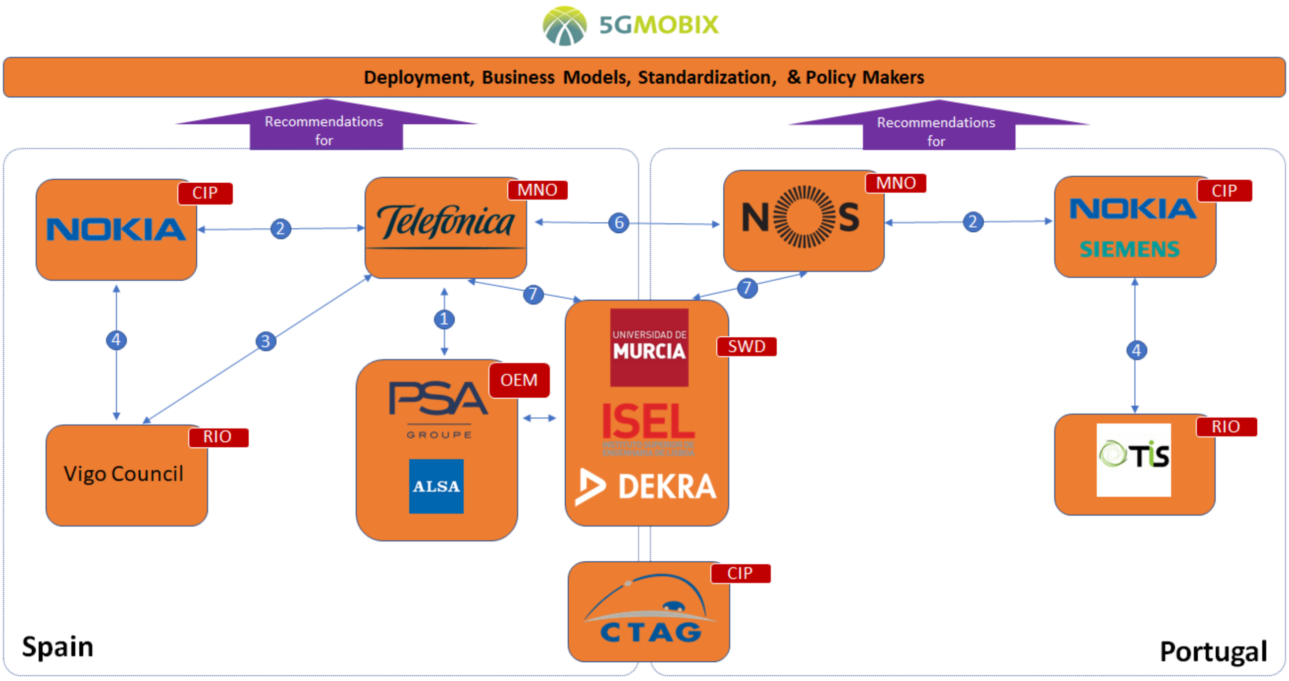


Figure 8: Stakeholders and their relationships involved in Spain - Portugal corridor

NOS believes that 5G will be a catalyst in industry transformation. So, it is strongly committed to prepare the network for the new services where 5G technology is an enabler. The eMBB services will be the firsts to be commercially available as soon as NOS is entitled to operate in 5G Bands, followed by URRLC and mMTC vertical use cases, which are expected to be released in 2021 by the time the 3GPP Rel-16 standard is closed and chipsets, are made available.

The 5G-MOBIX radio access network will be supported by NOS at the 3.5 GHz primary frequency band and at LTE 2.6 GHz NOS licensed frequency band. The 3.5 GHz spectrum will be granted temporarily by

Portuguese Authority ANACOM for carrying out technical trials, which later could be moved inside NOS 5G licensed frequency bands. NOS will also assure the interconnection of 5G-MOBIX Cellular sites to 5G EPC and Multi-access Edge Computing (MEC) node that will be deployed by Nokia on NOS Regional Data Centre located at Riba de Ave.

The participation in this project is an opportunity to study the signal propagation at 3.5 GHz band, test RF equipment (i.e. active antennas), and validate service thresholds and spectrum clearance that will be important to launch the 5G commercial network. In addition, the technical experience acquired in this project, specifically with the C-V2X use cases, will be crucial to prepare the URLLC services that NOS aims to deliver on domestic roads and cross-border corridors.

In the Spain - Portugal corridor two local authorities are involved in terms of network sustainability in the cross-border territories. On one hand, Dirección Generalde Tráfico (DGT)[1], Government of Spain, is the national Administration responsible for setting the different legal instruments and main rules concerning road traffic, mobility and road safety and, as well, is the leader organisation responsible of designing the road safety and mobility policy and strategy in Spain. DGT has an active role in the coordination of Spanish activities in terms of quality, integration of 5G-MOBIX infrastructure with the current systems, provide recommendations and develop dissemination activities. DGT will set the right mobility and road safety policies, strategies and regulations in Spain.

On the other hand, Instituto da Mobilidade e dos Transportes, (IMT)[2] is the Portuguese National Traffic Authority in charge of regulation and deployment options in Portugal. IMT is a central body with jurisdiction over the entire Portuguese National territory. It is headquartered in Lisbon and has decentralized services in the most important cities of the country. IMT has an active role inside 5G-MOBIX regarding institutional supervision, oversight and support, at Member State level, which is essential to ensure the quality of the project as a whole. As a National Traffic Authority, they will contribute the coordination of the different test of the user stories in terms of Portuguese National Traffic Authority.

3.3.2. Greek Turkish Cross-border Corridor

The partners directly involved in the Greek-Turkish corridor are a good mix of fitting roles represented by the consortium partners. The partners, their roles, and their relationships are depicted in Figure 9.

Considering COSMOTE's roadmap in terms of 5G, upon the completion of 5G-MOBIX project, COSMOTE would have already launched commercially 5G, mainly for eMBB use cases, in the main cities of Greece (i.e. Athens, Thessaloniki, etc.), at the most important touristic hot spots and other key interest points (i.e. ports, airports, motorways, etc.). Beyond 2021, the maturity of 5G technology combined with the completion of 3GPP Rel-16 specifications will allow COSMOTE to focus on new vertical use cases (i.e. URLLC & IoT) and launch services with applications' requirements like the ones to be tested at 5G-MOBIX GR-TR cross-border

[1] http://www.dgt.es/es/

[2] http://www.imt-ip.pt/sites/IMTT/Portugues/Paginas/IMTHome.aspx

corridor.

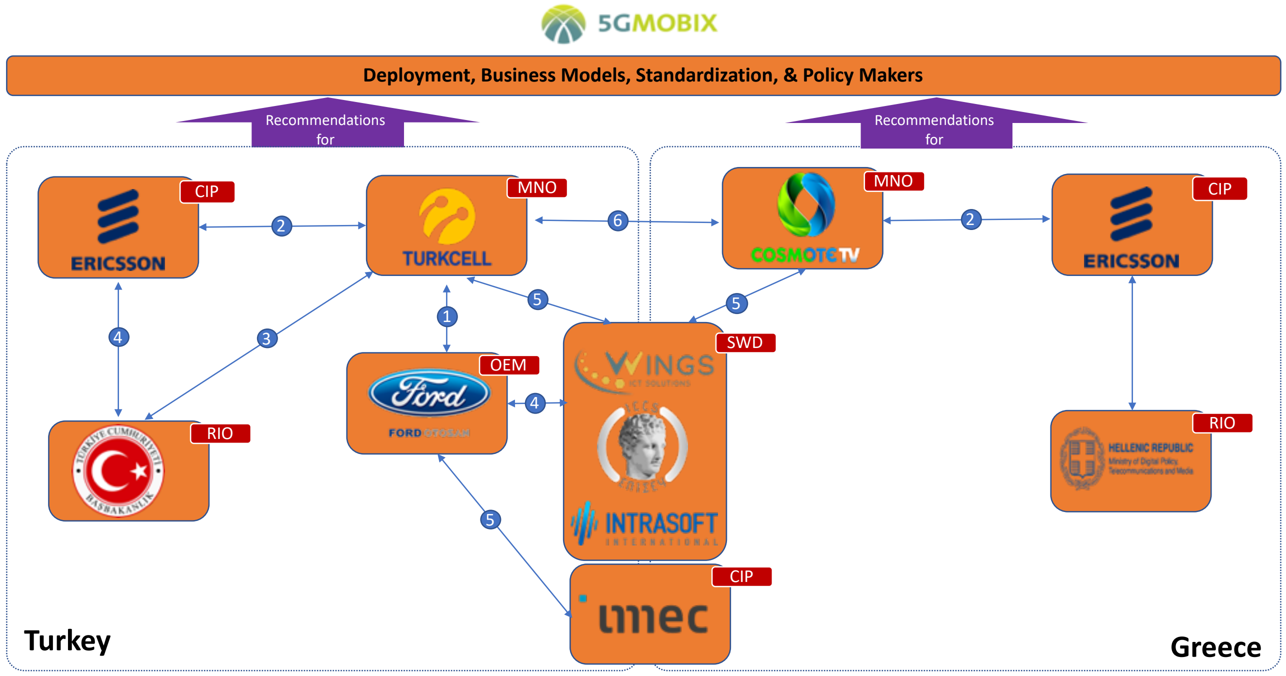


Figure 9: Stakeholders and their relationships involved in Greek-Turkey corridor

COSMOTE, through the active participation of the responsible departments in the 5G-MOBIX GR-TR cross-border corridor trial, will have gained technical expertise in launching services with strict requirements in terms of low latency & reliability from the design/planning phase up to the operational one. For instance, given that the 5G-MOBIX GR-TR cross-corridor trial is expected to use 5G NR spectrum at the 3.5GHz frequency band, a key strategic frequency band for 5G deployments, in collaboration with COSMOTE's licensed LTE spectrum at 2.6GHz band, acting as LTE anchor layer in 5G NSA case, will allow COSMOTE RF planning & optimization teams to gain significant know-how on radio resources' utilization and possible interference issues that might arise. Furthermore, apart from gaining technical experience, COSMOTE will have the chance to evaluate the suitability of existing roaming model for those use case categories in scope of the 5G-MOBIX GR-TR cross-border corridor trial.

In addition, the selected architecture of the 5G-MOBIX GR-TR cross-border corridor, described in this deliverable, could be the basis of the distributed core architecture solution of COSMOTE network, and consequently the Deliverable D2.2 could be a useful Architecture Blueprint. Specifically, for the 5G-MOBIX GR-TR cross-border corridor trial, COSMOTE's production site at Alexandroupoli (CO-like), where the overlay 5G EPC is planned to be deployed, must be upgraded to a core edge Data Centre (DC) site, resulting in the first core edge DC at COSMOTE network with strict requirements in terms of low latency & availability. Finally, it is envisaged that the designed solution, which is aimed to be future-proof and scalable, can serve as a stepping stone for COSMOTE to conduct business feasibility studies within Deutsche Telekom Group aiming at expanding the GR-TR cross-border corridor solution throughout the Greek motorways and towards the cross-border corridors of Greece with its other neighbouring countries (EU & non-EU ones).

For the GR-TR corridor, the Turkish Directorate General of Customs Enforcement will arrange a site visit, in which the site officers will demonstrate the actual process of a truck crossing the Turkish BCP (İpsala). Necessary brief will also be given by the customs experts at the site. The brief will include site entry, site exit, x-ray scanning and other inspection processes. İpsala BCP is planned to be reconstructed totally by mid-2020 by the Turkish Administration. Therefore, the customs officers will also present the necessary plans/drawings for use of the project consortium in the preparations for demonstration.

Moreover, from the Greek side, both the Ministry of Transportation and the Ministry of Communications and Digital Policy have already given their support to the project through Letters of Support from the proposal stage. The consortium representatives have proceeded in informing the ministerial authorities (Ministry General Secretaries for the Ministries of Transportation, Communication and Digital Policy and Foreign Affairs). The endeavours of 5G-MOBIX are very relevant and of interest to the jurisdictions of the Greek authorities and specifically of the aforementioned ministries. It is expected that 5G-MOBIX will receive formal permissions to install infrastructure and perform the pilots in the coming months. Moreover, these ministries are a very compelling dissemination and exploitation channel for 5G-MOBIX, as officers from the Greek authorities have expressly mentioned that they consider the project results as a roadmap for future developments in the national infrastructure.

3.4. 5G-MOBIX common architecture

3.4.1. Architectural considerations

Several considerations regarding the used 5G architecture is required to enable vehicle-to-everything (V2X) communication for improved traffic management, increasing road safety and autonomous driving. Currently, All CBC operators (Telefonica, NOS, Turkcell and Cosmote) are connected through the GRX network. This is also the most commonly used and preferred option in commercial networks to provide simplicity and reduce costs. However, if there is a strict Round Trip Time (RTT) requirement that cannot be met by GRX network (as is the case with 5G-MOBIX UCCs), direct interconnection could be also considered as an option. Even though this approach can be challenging for commercial networks (scalability issues), it may provide a viable alternative for demanding automotive scenarios.

From Core Network topology point of view, there are two key requirements that need to be considered carefully to be able to realize the 5G-MOBIX UCCs. The first point is service continuity, and the second one is latency. Therefore, the proposed design shall provide service continuity while crossing the border, live up to latency requirements and meet the realities of current standards and deployments in commercial networks.

Three deployment options have been studied considering the current capabilities of network components. In order to meet the stringent UCC requirements and realize the foreseen trials, a number of configurations/integrations have to take place depending on the chosen topology. In the first phase of the project, 5G-NR will be introduced in NSA mode and NSA Option-3x will be used. In respect to this, 5G supported EPC called as 5G EPC or EPC+ will be used at Core Network level. When 5GC components become available, in a later phase of the project and if the timelines allow for migration to SA, the proposed architectures can be easily migrated to 5GC where 5G-NR and 5GC(AMF, UPF) are directly connected and all signalling and data traffic are carried via 5G components (some Trials Sites such as the Netherlands will have SA from the beginning of the trials). The three considered deployment options are presented and discussed below, while for each one of them the commercial components, the necessary overlay components as well as optional components are indicated in order to provide a better understanding of the deployment integration effort required.

Deployment Option-1

- Option-1 (Figure 10) is compliant to home routed roaming architecture defined in 3GPP standards with several improvements that provide service continuity while crossing the border, as discussed in Section 2.4.
- All signalling and user plane traffic traverse through existing GRX networks.
- Local breakout functionality may be used in this case. So that, when roaming starts and re-establishment of PDN session occurs, PGW of v-PLMN is selected instead of PGW of H-PLMN. This will help reducing latency, as the impact of GRX is mitigated.

Deployment Option-2

- Option 2 (Figure 11) is partially spec compliant to home routed roaming standards due to the fact that in this option all user-plane traffic is carried out via a kind of direct interconnection that will be established between two MNOs, although signalling traffic keeps passing through GRX.
- The advantage of this option is that it has the ability to reduce latency. Therefore, LBO function as presented in Section 2.4.2 may not be required to further reduce latency.

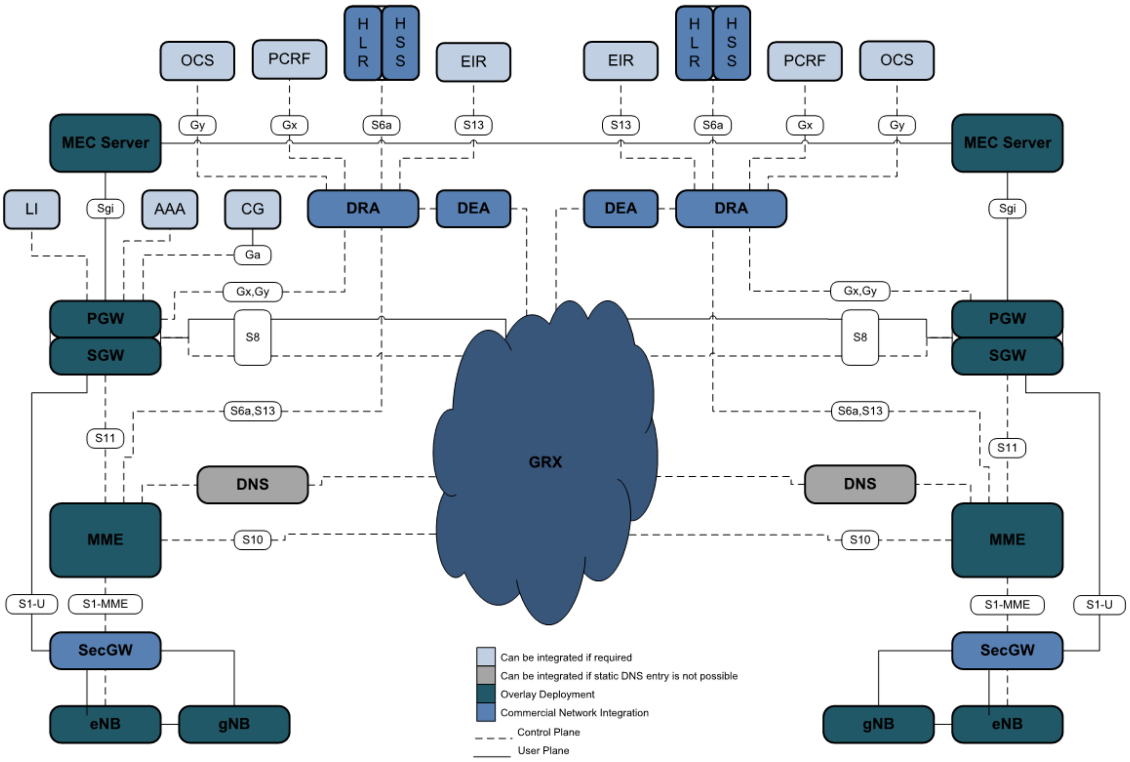


Figure 10: Deployment Option 1 – Full GRX interconnection

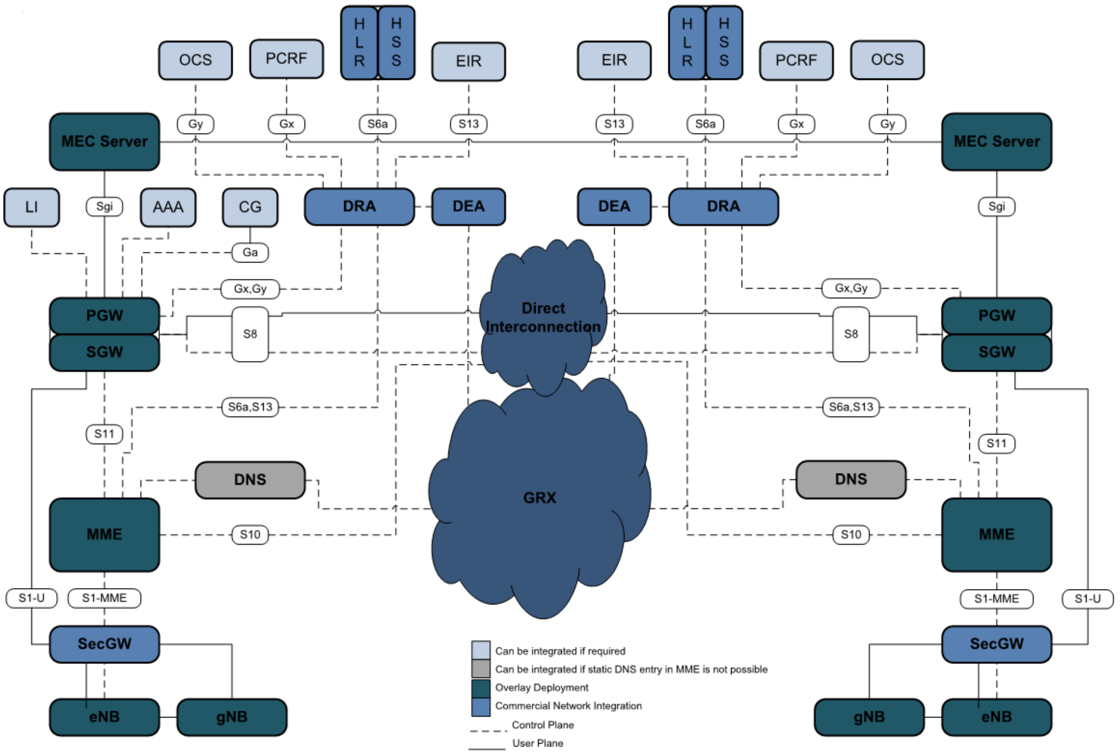


Figure 11: Deployment Option 2 – GRX interconnection for CP traffic & Direct interconnection for UP traffic

Deployment Option-3

- Option 3 (Figure 12) is based on overlay dedicated networks where all signalling and user plane traffic are carried out via a direct interconnection link. This results in significantly reduced latency for both UP and CP traffic.
- This option is easier to deploy from an operator point of view, as interfacing to commercial network may be optional or conditional.
- This option raises scalability concerns for wide deployments, which may be overcome based on 5GC technologies and upcoming releases of 5G.

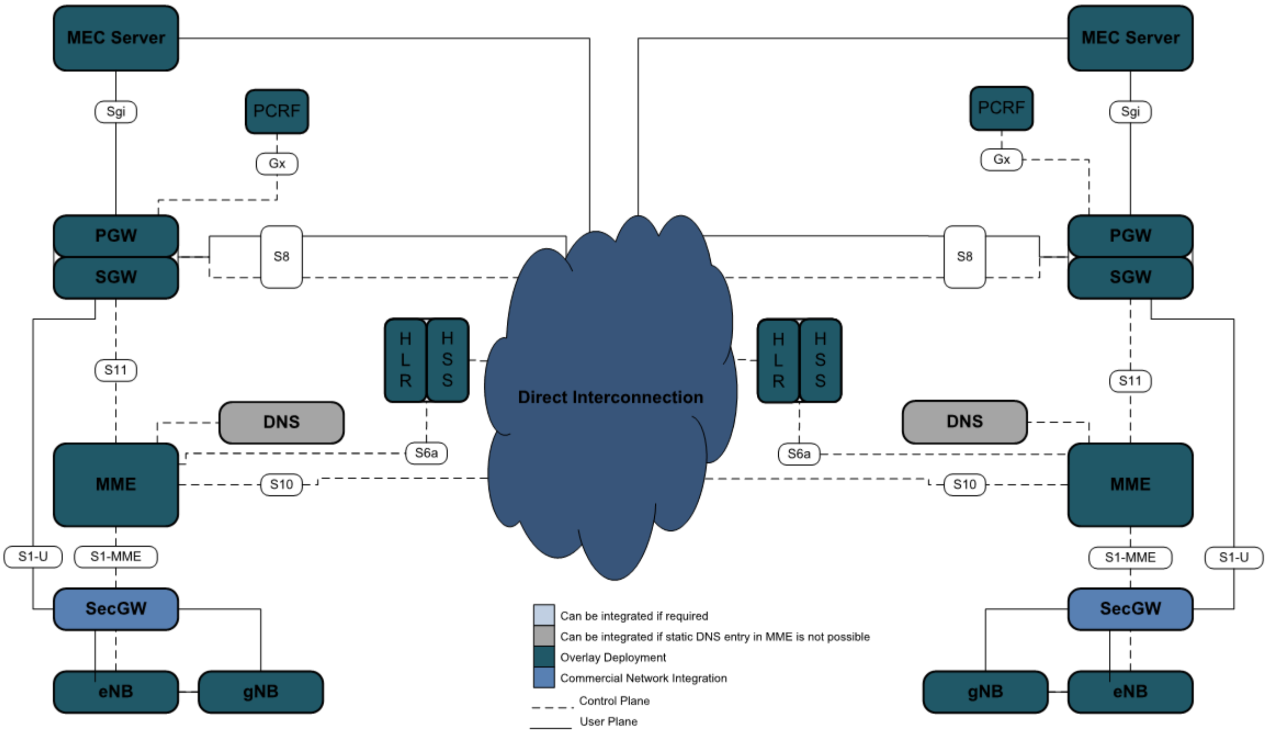


Figure 12: Deployment Option 3 – Direct interconnection

The networks experts (MNOs and vendors) of both the ES-PT and GR-TR cross-border corridors have agreed that the only viable option for 5G network interconnection which could support the advanced 5G-MOBIX UCCs is deployment option 3, as the involvement of the GRX at any stage of the architecture would introduce unacceptable latency when crossing the border and would hence not be able to support the necessary CCAM functionality. Therefore, ***Deployment Option 3 is the 5G-MOBIX common architecture***, which will act as the basis for the 5G network deployments in the ES-PT and GR-TR corridors. The implementations at the two CBCs will of course vary, as the network components will originate from different European vendors (Nokia and Ericsson respectively), also allowing for the testing and evaluation of multiple network configurations and settings.

3.4.2. Overview of 5G components & configurations utilized in 5G-MOBIX

Each of the 5G-MOBIX participating CBCs/TSs has selected appropriate networking technologies and infrastructure to accommodate the selected use case categories presented in D2.1 [1], based on the requirements analysis presented in Sections 4 and 5. The basis of this selection is of course guided by the architectural considerations analysed in Section 3.4.1, as well as 3GPP work on support of V2X functionality over 5G networks, as presented in ***Annex 2***. In order for 5G-MOBIX trials to commence on time (on M18), the architecture used initially will be based on partial implementation of Rel.15 [28], while migration to full Rel.15 solutions or even SA deployment will be examined by the involved stakeholders of each CBC/TS basis, as they become available.

As 5G-MOBIX focuses on cross-border deployments both Home Routing and Local Break Out (see [29][30]) solutions will be investigated, to support efficient roaming between different PLMNs, mostly in the two CBCs of the project, assisted by findings and testing at the TSs. As, some of the features of LBO will only be available in SA options with the deployment of a 5G core, these alternatives will be investigated upon the instantiation of such a 5G architecture on one of the CBCs (pending on the availability of the technology and the stakeholder's roadmap). Additionally, differentiated MEC and Edge computing deployments will be available in all the 5G-MOBIX sites, allowing for a plurality of configurations and testing scenarios, leading to optimal deployments for cross-border functionality. Table 4 provides a "bird's eye view" of the 5G-MOBIX sites by aggregating the main architectural choices and 5G components selected by each CBC/TS.

Table 4: Overview of the main architectural attributes of the 5G-MOBIX sites

CBC/TS	3GPP Deployment Option	Number of gNBs	Experimentation Frequency	MEC	Roaming	Additional info
ES-PT	3x / (2)	8	2100 MHz (B1), 2600 MHz (B7), 3.5 GHz (n78)	Distributed (Far edge & central)	HR/LBO	
GR-TR	3x / (2)	4	2600 MHz (B7), 3.5 GHz (n78)	Edge computing (SGi to PGW)	HR/LBO	Coexistence with NB-IoT
DE	3x / (2)	2	2100 MHz (B1), 3.5 GHz (n78) 700 MHz (n12)	eRSU with MEC	N/A	
FI	3x / (2)	2	2600 MHz (B7) 3.5 GHz (n78)	Commercial + SDN based	Multi-PLMN	Multi-PLMN testing
FR	3x / (2)	2	700 MHz (4G), 800 MHz (4G), 1800 MHz (4G), 2100 MHz (3G/4G), 2600 MHz (4G), 3700-3800 MHz (n77)	Commercial Ericsson + MANO/SDN based distributed MEC (Edge)	TBD	Seamless Handover

NL	3x / 2	8	800 MHz (LTE B20), 1800 MHz (LTE B3), 700 MHz (5G NR n28), 3.5 – 3.7 GHz (5G NR n78) 26.65 GHz (5G NR n258)	Multiple (Kubernetes based)	HR/LBO	Multi-PLMN testing with peering

CN	3x / (2)	2	3.5GHz(n78)
			4.9 GHz(n79)
			2.6GHz(n41)
				Yes	TBD	

KR	2	3	22-23.6 GHz	N/A	N/A	Network S

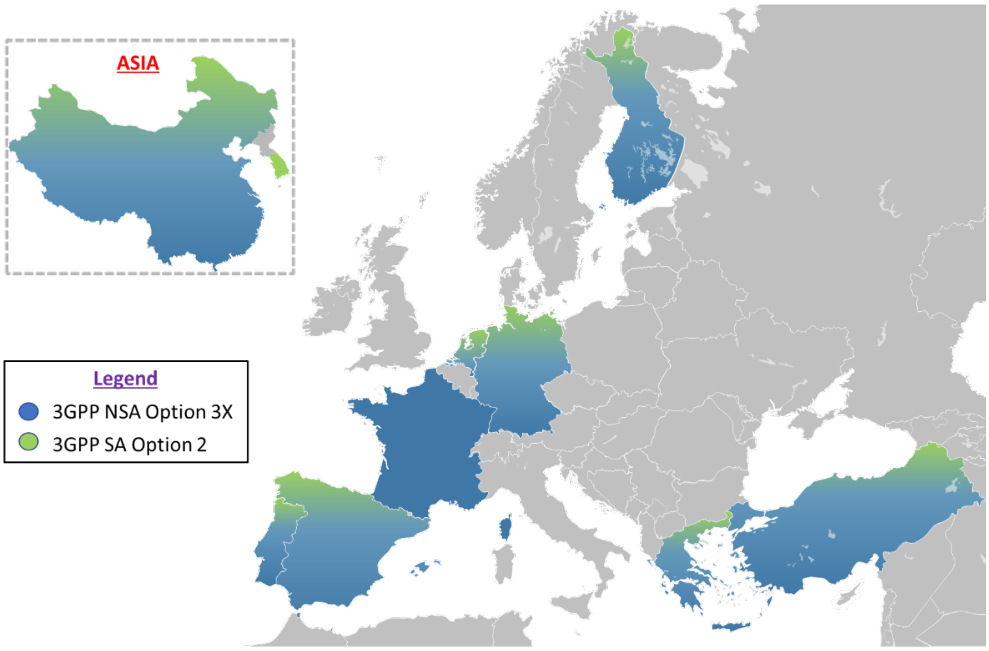


Figure 13: 3GPP Deployment options to be realized per 5G-MOBIX CBC/TS

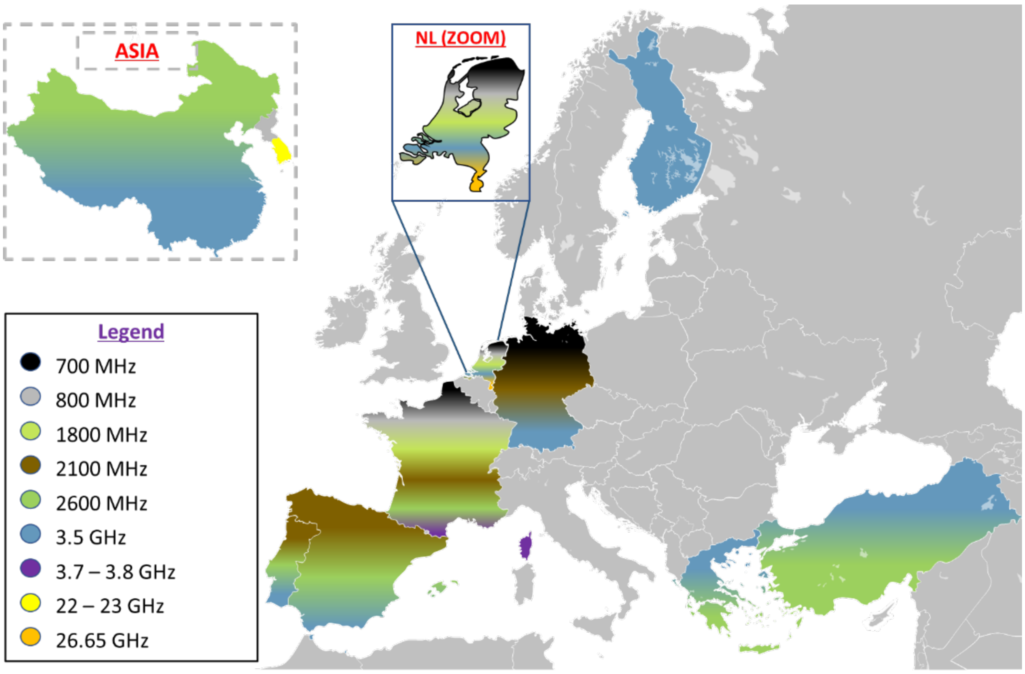


Figure 14: Utilized frequency per CBC/TS for the 5G-MOBIX trials

The variety and complementarity offered by the different deployments of the 5G-MOBIX corridors and sites is even better understood by graphically depicting some of the main characteristics of each deployment. Figure 13 depicts the selected 3GPP deployment option (NSA vs SA) for each CBC/TS, while Figure 14 graphically depicts the available and utilized frequencies for the 5G-MOBIX trials. It must be noted that except for the Dutch TS which is going to implement SA Option 2 with already existing experimental 5G core, the rest of the CBCs/TSs will attempt to deploy a SA network based on commercial 5G core availability and are hence dependent on the availability of such equipment and the roadmap of the collaborating vendors.

In the following two sections, the architectural requirements and the selected 5G network architecture for the two cross-border corridors of 5G-MOBIX is described in detail (Sections 4 and 5 respectively). The contributions of the collaborating TSs in each case are also described in these sections. The 5G network architectural details of the TSs, which will be used for the extended evaluations of the 5G-MOBIX use case categories, as described in Section 6, are presented in the Annexes of this deliverable.

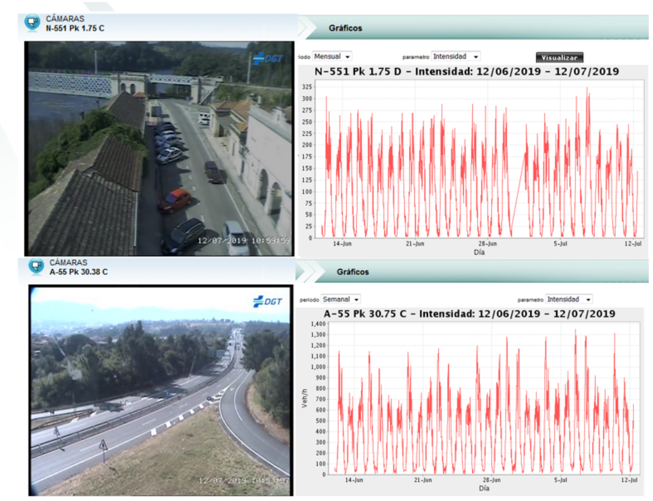
4. SPAIN – PORTUGAL (ES-PT) 5G ARCHITECTURE & TECHNOLOGIES

This section deals with the definition of the architectural requirements and selected 5G architecture to be deployed in the ES-PT corridor of 5G-MOBIX. The section initially provides a "bird's eye view" of the main requirements and structural elements of ES-PT CBC, before detailing the planned 5G architecture with respect to the radio access network architecture, the core architecture and the 5G and V2X technologies that are to be deployed (based also on the standardisation analysis provided in Section 2). Finally, the contributions of the collaborating TSs to the ES-PT CBC are also presented in this section.

4.1. Considered 5G network requirements

4.1.1. Radio network requirements

In order to establish some realistic requirements on the capacity and scalability of the 5G deployment required in this project real car data traffic needs to be captured and correctly mapped to the network infrastructure in terms of throughput, availability, latency and other factors. Traffic numbers in the Spain-Portugal border have been obtained via the official DGT (Dirección General de Tráfico) for the roads which are the object of experimentation in the ES-PT corridor.



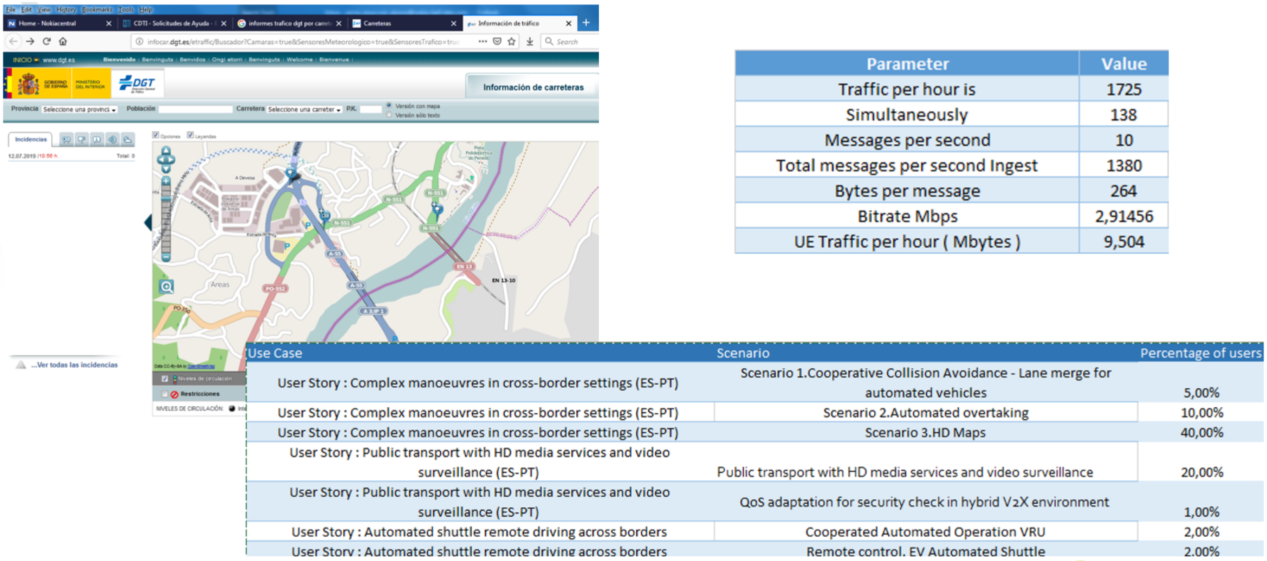
Roads	KM	Intensity (vehicles/hour)
A-55	30	1400
N-551	27	325

- Real Traffic and Peak Traffic

Source: http://infocar.dgt.es/etraffic/Buscador?Camaras=true&SensoresMeteorologico=true&SensoresTrafico=true&Paneles=true&IncidenciasOTROS=true&IncidenciasEVENTOS=true&IncidenciasRETENCION=true&IncidenciasOBRAS=true&IncidenciasMETEOROLOGICA=true&IncidenciasPUERTOS=true&IncidenciasRESTRICCIONES=true&provincia=36&poblacion=&carretera=55084&PK=30&version=texto&pagina=null&caracter=acontecimiento&accion_buscar=Buscar

Figure 15 - Vehicle Traffic Intensity

The query being used is repeatable and provides the traffic intensity in vehicles per hour in both A-55 and N-551 roads. Based on this data, it is possible to estimate the number of control messages required per second and compute the network traffic in MBytes per hour. Then we need to establish some weights for the specific use cases that the project will address regarding the percentage of users which are allocated to every use case.

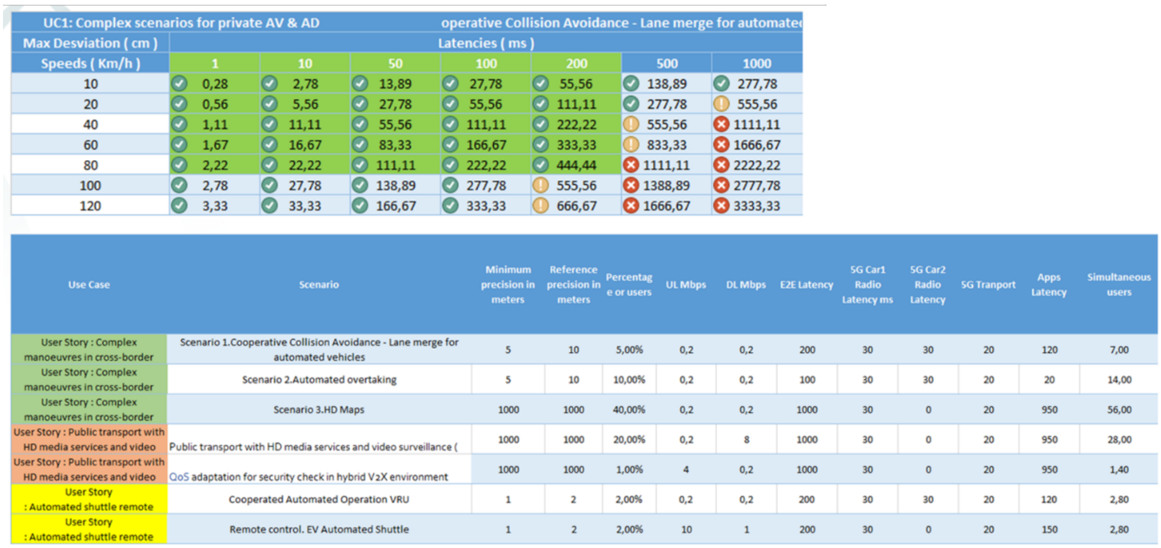


Parameter	Value
Traffic per hour is	1725
Simultaneously	138
Messages per second	10
Total messages per second Ingest	1380
Bytes per message	264
Bitrate Mbps	2,91456
UE Traffic per hour (Mbytes)	9,504

Use Case	Scenario	Percentage of users
User Story : Complex manoeuvres in cross-border settings (ES-PT)	Scenario 1.Cooperative Collision Avoidance - Lane merge for automated vehicles	5,00%
User Story : Complex manoeuvres in cross-border settings (ES-PT)	Scenario 2.Automated overtaking	10,00%
User Story : Complex manoeuvres in cross-border settings (ES-PT)	Scenario 3.HD Maps	40,00%
User Story : Public transport with HD media services and video surveillance (ES-PT)	Public transport with HD media services and video surveillance	20,00%
User Story : Public transport with HD media services and video surveillance (ES-PT)	QoS adaptation for security check in hybrid V2X environment	1,00%
User Story : Automated shuttle remote driving across borders	Cooperated Automated Operation VRU	2,00%
User Story : Automated shuttle remote driving across borders	Remote control. EV Automated Shuttle	2,00%

Figure 16 - Messages Network Traffic and UCs

For the latency case it is very important to know which is the maximum latency which is allowed to remotely drive a car. This KPI applies for the UC1 (Complex scenarios for private AV & AD as well as for the operative Collision Avoidance - Lane Merge use case). Taking into consideration the applications latency in the E2E chain will allow us to create a trustable table in which the final latency is depicted.



UC1: Complex scenarios for private AV & AD	operative Collision Avoidance - Lane merge for automate						
Max Desviation (cm)	Latencies (ms)						
Speeds (Km/h)	1	10	50	100	200	500	1000
10	✓ 0,28	✓ 2,78	✓ 13,89	✓ 27,78	✓ 55,56	✓ 138,89	✓ 277,78
20	✓ 0,56	✓ 5,56	✓ 27,78	✓ 55,56	✓ 111,11	✓ 277,78	! 555,56
40	✓ 1,11	✓ 11,11	✓ 55,56	✓ 111,11	✓ 222,22	! 555,56	✗ 1111,11
60	✓ 1,67	✓ 16,67	✓ 83,33	✓ 166,67	✓ 333,33	! 833,33	✗ 1666,67
80	✓ 2,22	✓ 22,22	✓ 111,11	✓ 222,22	✓ 444,44	✗ 1111,11	✗ 2222,22
100	✓ 2,78	✓ 27,78	✓ 138,89	✓ 277,78	! 555,56	✗ 1388,89	✗ 2777,78
120	✓ 3,33	✓ 33,33	✓ 166,67	✓ 333,33	! 666,67	✗ 1666,67	✗ 3333,33

Use Case	Scenario	Minimum precision in meters	Reference precision in meters	Percentage or users	UL Mbps	DL Mbps	E2E Latency	5G Car1 Radio Latency ms	5G Car2 Radio Latency	5G Tranport	Apps Latency	Simultaneous users
User Story : Complex manoeuvres in cross-border	Scenario 1.Cooperative Collision Avoidance - Lane merge for automated vehicles	5	10	5,00%	0,2	0,2	200	30	30	20	120	7,00
User Story : Complex manoeuvres in cross-border	Scenario 2.Automated overtaking	5	10	10,00%	0,2	0,2	100	30	30	20	20	14,00
User Story : Complex manoeuvres in cross-border	Scenario 3.HD Maps	1000	1000	40,00%	0,2	0,2	1000	30	0	20	950	56,00
User Story : Public transport with HD media services and video	Public transport with HD media services and video surveillance (	1000	1000	20,00%	0,2	8	1000	30	0	20	950	28,00
User Story : Public transport with HD media services and video	QoS adaptation for security check in hybrid V2X environment	1000	1000	1,00%	4	0,2	1000	30	0	20	950	1,40
User Story : Automated shuttle remote	Cooperated Automated Operation VRU	1	2	2,00%	0,2	0,2	200	30	30	20	120	2,80
User Story : Automated shuttle remote	Remote control. EV Automated Shuttle	1	2	2,00%	10	1	200	30	0	20	150	2,80

Figure 17 - E2E Latency and Remote Driving

Reliability of the system needs to be understood as important as throughput and latency. So, calculations including these figures are relevant including which are the guaranteed throughputs and latency with associated reliability for a given service deployment time period, as shown for some of the associated user stories in Figure 18.

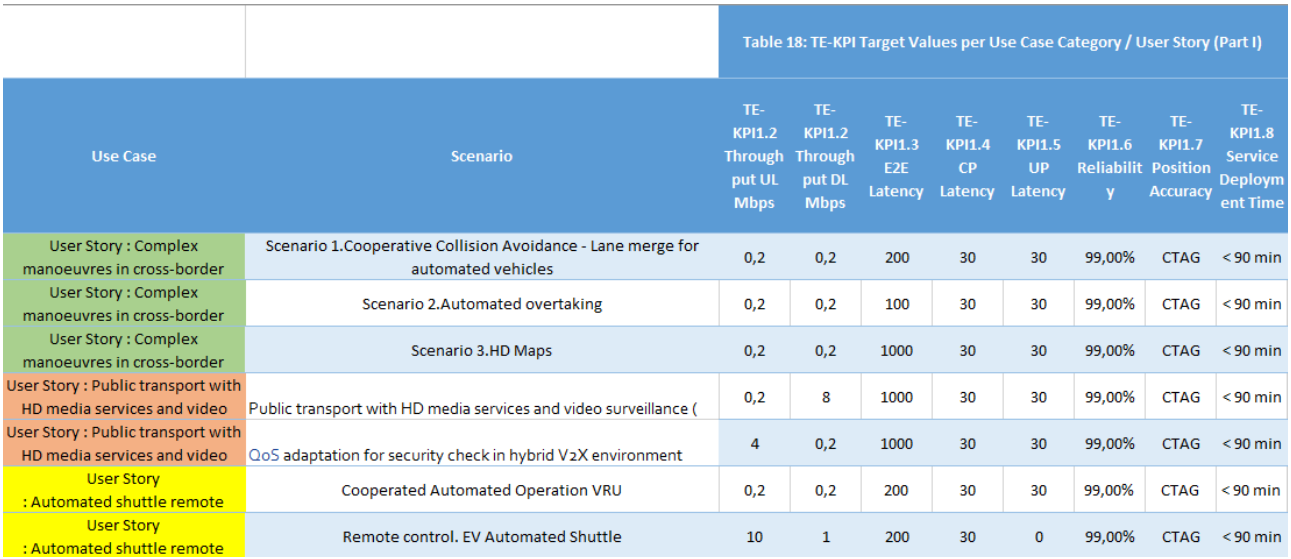


Table 18: TE-KPI Target Values per Use Case Category / User Story (Part I)

Use Case	Scenario	TE-KPI1.2 Throughput UL Mbps	TE-KPI1.2 Throughput DL Mbps	TE-KPI1.3 E2E Latency	TE-KPI1.4 CP Latency	TE-KPI1.5 UP Latency	TE-KPI1.6 Reliability	TE-KPI1.7 Position Accuracy	TE-KPI1.8 Service Deployment Time
User Story : Complex manoeuvres in cross-border	Scenario 1.Cooperative Collision Avoidance - Lane merge for automated vehicles	0,2	0,2	200	30	30	99,00%	CTAG	< 90 min
User Story : Complex manoeuvres in cross-border	Scenario 2.Automated overtaking	0,2	0,2	100	30	30	99,00%	CTAG	< 90 min
User Story : Complex manoeuvres in cross-border	Scenario 3.HD Maps	0,2	0,2	1000	30	30	99,00%	CTAG	< 90 min
User Story : Public transport with HD media services and video	Public transport with HD media services and video surveillance (	0,2	8	1000	30	30	99,00%	CTAG	< 90 min
User Story : Public transport with HD media services and video	QoS adaptation for security check in hybrid V2X environment	4	0,2	1000	30	30	99,00%	CTAG	< 90 min
User Story : Automated shuttle remote	Cooperated Automated Operation VRU	0,2	0,2	200	30	30	99,00%	CTAG	< 90 min
User Story : Automated shuttle remote	Remote control. EV Automated Shuttle	10	1	200	30	0	99,00%	CTAG	< 90 min

Figure 18 - Throughput, Latency and Reliability

The network deployed in Spain for supporting the 5G-MOBIX use case categories will be based on the 5G-NR NSA architecture. The radio access network will consist of two base station sites. Evaluating the current 4G LTE coverage is a key factor for ensuring the correct anchoring in the midterm phase in which the control plane needs to be driven by LTE Infrastructure.

To explore the current LTE coverage, we have taken RSSI measurements in the border area as well as the associated sector identifiers and frequencies. Every sector ID in a cell ID has a single frequency so once we have obtained the data with real field measurements, we can render Google Earth View outputs to get a visual snapshot of the setup, as shown in Figure 19. Additional detailed data was also rendered in the maps and a specific application has been developed for gathering this kind of high-level measures as shown in Figure 20.

The initial anchoring LTE frequency selected is 1800 MHz, which offers more than 120 dBm of power. Video throughput measures have also been taken interspersed as the same application allows measuring video bit rate from HLS adaptive streaming sources.

Data has been captured both in the border plus the Spanish and Portuguese areas not so close to the border, which should be covered too. Special attention has been paid to obtain data from the cells in NOS base stations deployed for the current LTE commercial deployment, their frequencies and locations where roaming transitions typically take place. This is critical to deploy new small cells that will be close to the commercial network, avoiding frequency interference. At least two of frequencies will be used, the LTE anchoring one (which might be 1800 MHz or 2100 MHz) and the 5G frequency (which will be at 3500 MHz).

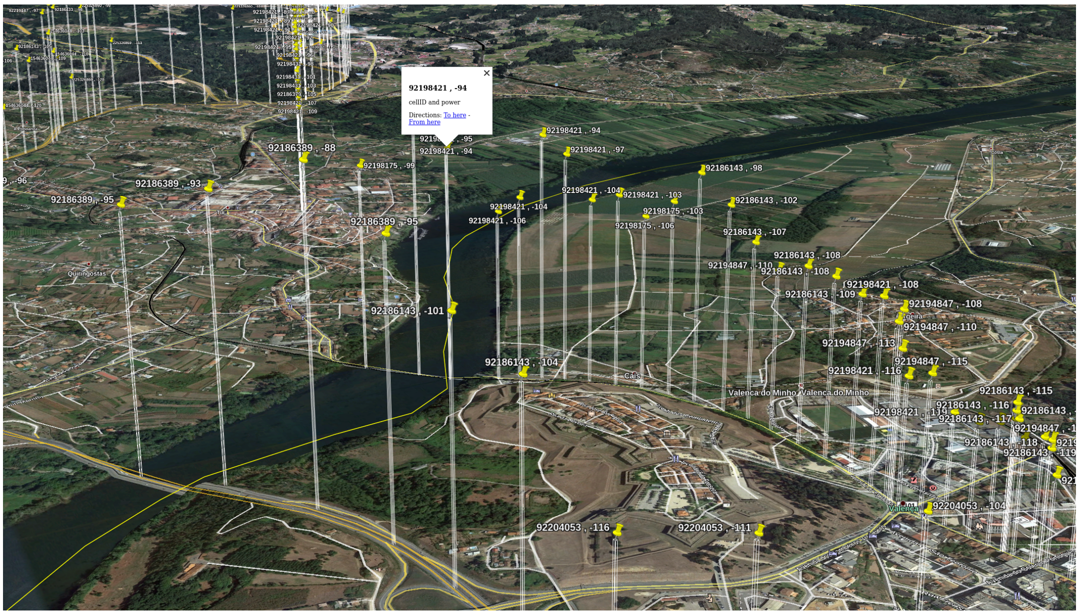
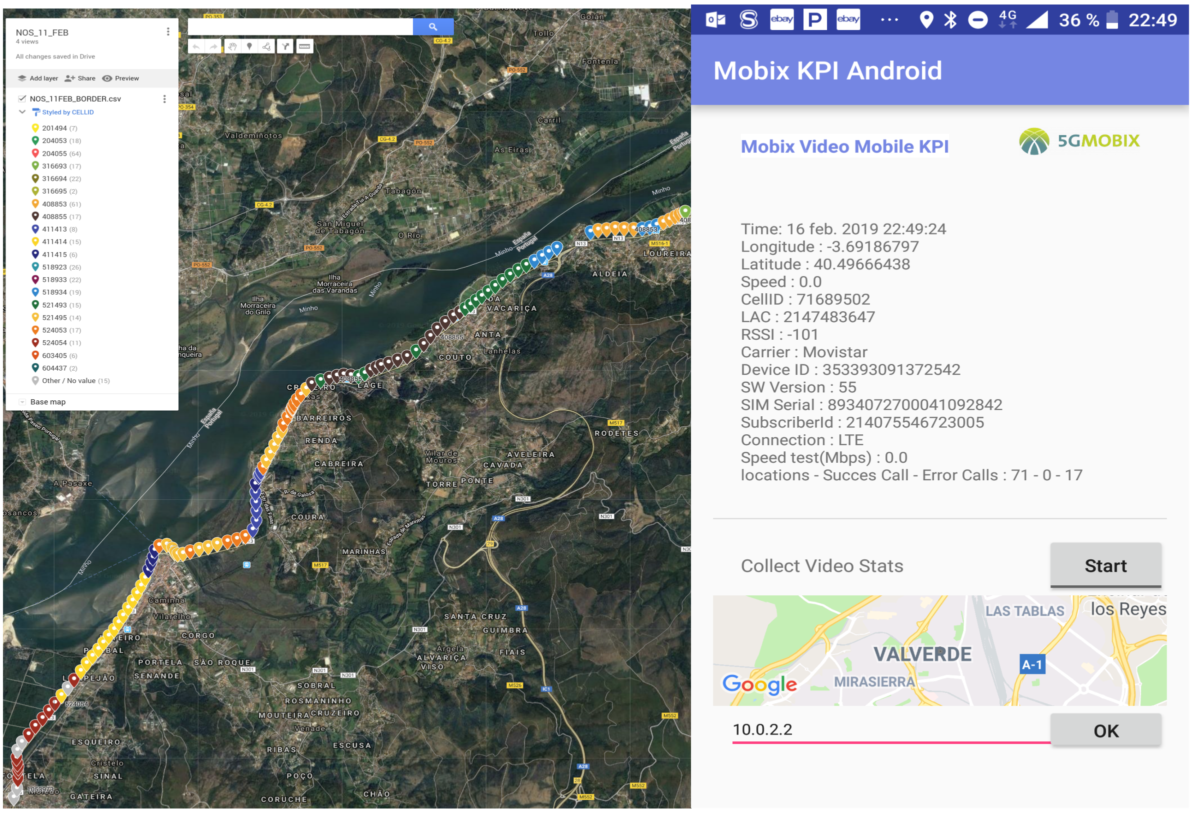


Figure 19: Visual snapshot of the ES-PT setup


NOS_11_FEB
4 views
All changes saved in Drive

NOS_11FEB_BORDER.csv
Styled by CELLID

- 201494 (7)
- 204053 (18)
- 204055 (64)
- 316693 (17)
- 316694 (22)
- 316695 (2)
- 408853 (61)
- 408855 (17)
- 411413 (8)
- 411414 (15)
- 411415 (6)
- 518923 (26)
- 518933 (22)
- 518934 (19)
- 521493 (15)
- 521495 (14)
- 524053 (17)
- 524054 (11)
- 603405 (6)
- 604437 (2)
- Other / No value (15)

Mobix KPI Android

Mobix Video Mobile KPI

Time: 16 feb. 2019 22:49:24
Longitude : -3.69186797
Latitude : 40.49666438
Speed : 0.0
CellID : 71689502
LAC : 2147483647
RSSI : -101
Carrier : Movistar
Device ID : 353393091372542
SW Version : 55
SIM Serial : 8934072700041092842
SubscriberId : 214075546723005
Connection : LTE
Speed test(Mbps) : 0.0
locations - Succes Call - Error Calls : 71 - 0 - 17

Collect Video Stats

10.0.2.2

Figure 20: Data captured from the ES-PT corridor

A hybrid overlay approach will be probably used in the corridor combining limited and controlled part of the commercial network with parallel deployment of some trial radio installations altogether with a small set of Small Cells.

4.1.2. Core network requirements

During the first phase of the project the two networks will be connected by roaming, registering in Spain the users of Portugal Network as roamers and vice-versa. The roaming users will be using the local network for the 5G-MOBIX experimentation, allowing direct access to the MEC supported functionality. In the first phase of the project most of the available modems will be only NSA capable, so the Spanish-Portuguese corridor will be focused in solutions for 5G Rel.15 NSA (option 3x).

In the second phase of the project, alternative approaches will be studied by NOS and Telefonica to support user's mobility between the two networks across the border. Access to both home and visiting networks MEC servers will be critical, or in alternative, the use of Local MECs as routers to the Visiting MECs should be in place, in case only home roaming is supported. The performance and latency must be assessed with KPI measures in order to evaluate the cost of different roaming approaches.

4.1.2.1. Core options

The 5G network deployment scenario options can be seen in Figure 2, from where the most relevant for the current project are the NSA (option 3x) and SA (option 2). These allow for an incremental network deployment in accordance to the vendor timeline for the technology availability in the market and respecting the involved MNOs network deployment and migration strategy per region.

At the first phase of the project, the NSA (option 3x) will be supported and at the second phase it is aimed to support SA (option 2)).

4.1.2.2. MEC deployment

Depending on each deployment scenario, different user stories may be deployed using several combinations of sites for the installation of the application servers, providing different competitive advantages. To support V2X in all the 4G covered areas, one vMEC can be deployed very near the radio (Far Edge) and another vMEC in the Core Network (Central Data Centre). Figure 21 classifies depict both types of deployments:

- *Far edge*: providing the smallest latency but requiring deploying the MEC services in many locations. Ideal for localized deployments like factories;
- *Aggregated edge*: providing low latency, covering several radio nodes, ideal for city size deployments;
- *Regional*: this deployment is ideal for services that must be provided at region level, the solution is optimal for the deployment of capacity in a regional area, covered with a few MECs;
- *Central*: massive deployment, the new applications will be available in the whole network just by deploying a few MEC servers.

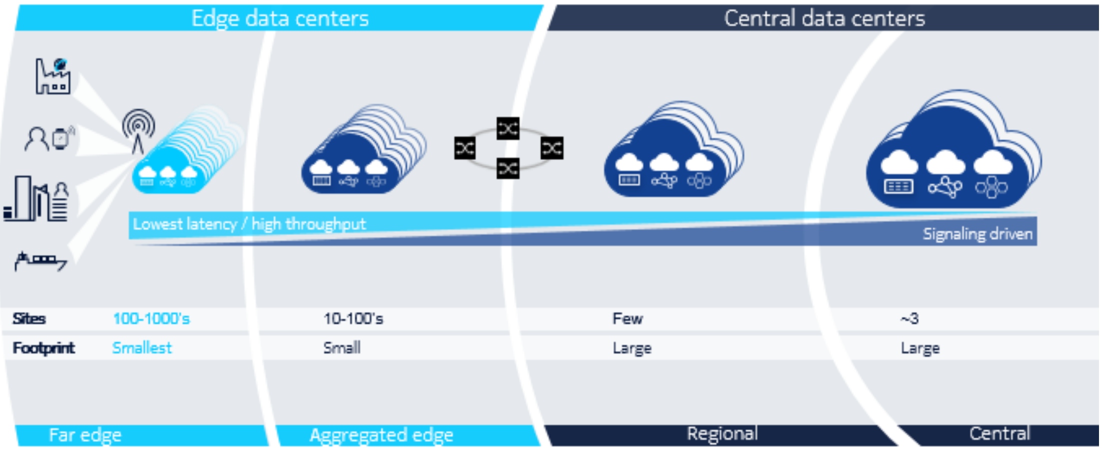


Figure 21: Coverage areas and MEC deployment location

4.1.2.3. Roaming

International traffic of both MNOs is configured through GRX/IPX networks that do not meet the latency and security requirements of URLLC services. MNOs direct interconnection is being deployed in order to reduce the delay of traffic between MECs of both countries. The signalling plane does not have same strict requirements so can stay on the GRX/IPX network.

NOS IP/MPLS network will interconnect with Telefónica in Vigo. It is the aggregation point of the Telefonica's transport network, therefore the scalability is improved. The latency is reduced because it is the shortest way of connecting the MECs (there is a NOS point of presence in Vigo) and the ITS platform (in Porriño). This is the most practical solution considering the topology of Telefonica's commercial network.

In the first phase of the project, the core could support roaming 3GPP Rel.15 only, as defined in [29]. In Rel.16, the 3GPP specification [30] will introduce new roaming approaches. In the case of roaming, the AMF determines if a PDU Session is to be established in Local Breakout (LBO) or in Home Routing architectures. In the case of LBO, the procedure is like in the case of non-roaming with the difference that AMF, SMF, UPF and PCF functions are in the visited network. PDU Sessions for Emergency services are never established in the Home Routed mode.

In the case of the V2X, the most efficient architecture for roaming is the LBO because the source of information and entry point will be the MEC Server located in the Visiting Network, so this will be the preferred implementation. The implementation of these procedures will be evaluated by NOS and Telefonica to support this scenario. Until the LBO is supported, the Home Routing procedure could be supported, but this will require the authorization by NOS and Telefonica operators. Finally, for initial testing, two SIM cards can be used also in automotive modems to support connectivity using several simultaneous network connections. Unfortunately, by mid-2019, there are no commercial 5G automotive modems available with dual SIM support.

4.2. E2E Architecture

The End-to-End ES-PT cross-border trial architecture is based on the commonly agreed 5G-MOBIX architecture (see Section 3.4) and is depicted in Figure 22. Both mobile network operators (MNOs), Telefonica and NOS, plan to deploy overlay 5G EPC architecture, NSA (option. 3x) at their Data Centres, located close to their respective border sides, in order to fulfil the strict latency requirements imposed by the use case categories to be demonstrated at this CBC.

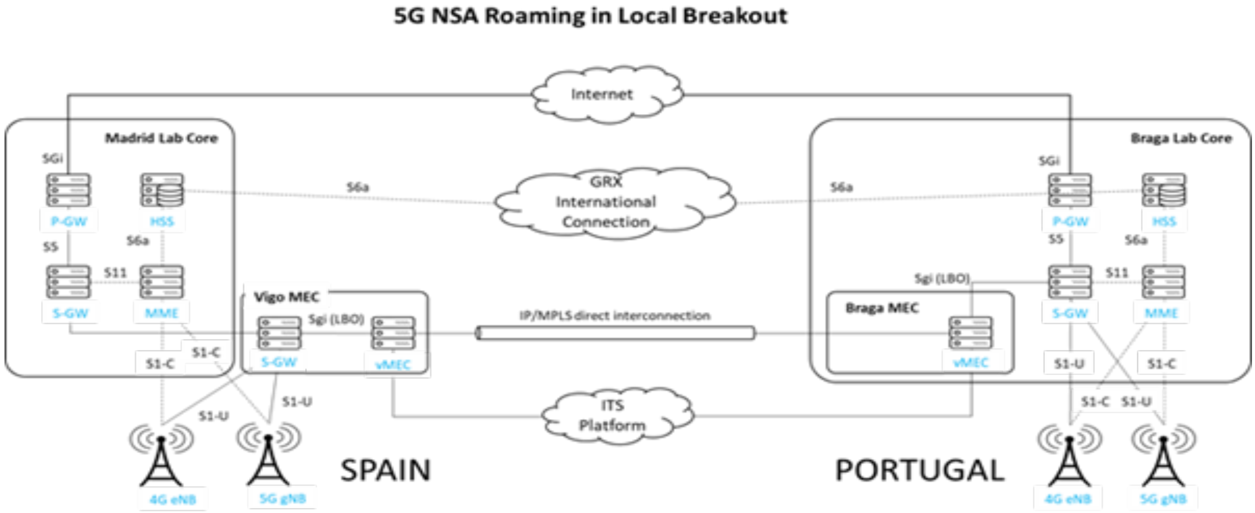


Figure 22: ES-PT corridor End-to-End Architecture

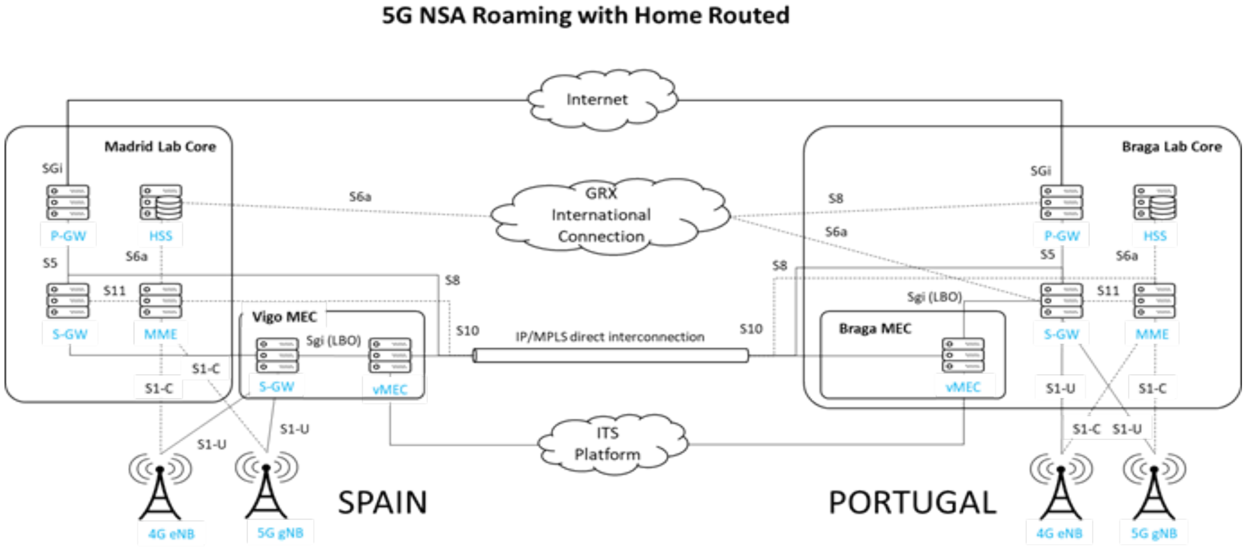


Figure 23: ES-PT E2E with Home Routed

Home Routed option of deployment is also depicted in Figure 23 with 5G NSA Option 3x and ETSI MEC deployed with distributed SGW with Local Breakout (SGW-LBO) event though it will imply high latency and will not be suitable for real-time applications.

For the trial purposes, the radio and core network equipment to be deployed by both MNOs is provided by NOKIA. At the first phase of the project, the NSA (option 3x) will be supported, and later upgraded to support SA (option 2) in the second phase. Existing EPC core will be upgraded to 5G Core to support SA (option 2).

The Portuguese MEC (NOS) will be deployed in Riba de Ave edge data centre, in the same point where the core network is going to be installed (90 km from the cross-border). The Spanish edge MEC (Telefonica) will be deployed in Vigo (30 km from the cross-border). However, the core of the network is in Madrid (560 km from the cross-border). The Local Breakout (LBO) is essential to reduce the E2E latency of local traffic in order to accomplish with use case categories latency requirements, that otherwise would have to go to the Core Network installed in Madrid, MECs in both countries are going to be deployed using the Distributed SGW with Local Breakout (SGW-LBO) option defined by ETSI. A multi-PLMN solution will be used in order to separate commercial traffic from trial traffic.

As listed in Table 5 a total of 8 gNB sites will be installed to cover the trial areas, and roaming will be tested with Home Routing and Local Breakout procedures.

Table 5: ES-PT corridor 5G deployment

3GPP Deployment Option	Number of gNBs	Experimentation Frequency	MEC	Roaming
1st Phase - NSA Option 3x 2nd Phase - SA Option 2	8	4G - 1800 MHz (B3) 5G - 3.5 GHz (n78)	Distributed (Far edge & central)	HR / LBO

4.3. Radio Network Architecture

4.3.1. NOS Portugal RAN

In Section **Error! Reference source not found.**, the different 3GPP architecture options were presented. For the ES-PT Corridor, Nokia will provide a complete test network on the Portuguese side of the border, comprised with several Base Stations, vMEC and a Micro Core network, to be operated by NOS, using its own spectrum and infrastructure. This network will be deployed in overlay with the existing NOS commercial network.

Given the project timeline and terminals availability, the initial deployment will be done in Non-Standalone option 3x (EN-DC NSA3x) with an LTE anchor layer on band 1800 MHz (Band 3) and 5G NR mMIMO on band 3700 MHz (n78). SA Option 2 support will come in a later stage, when 5GCN becomes available for deployment.

The NSA option 3x uses the concept of split bearer (Figure 24), which is a data bearer that is set up between two nodes (here: between the LTE S-GW and the 5G Secondary gNB), but at the PDCP level the actual data can be split and sent over two different channels (5G radio and LTE radio via X2 relay). The PDCP layer at the UE will take care of reordering the received packets. The features on 5G-LTE support flow control over the X2 and data split in both UL and DL for the SN-terminated split bearer between the 5G gNB and LTE eNB. The feature SgNB Addition and Release for NSA mode 3X allows switching from MCG bearer to split data radio bearer and vice versa at a SgNB connected via X2 for the NSA option 3x operation (Figure 25).

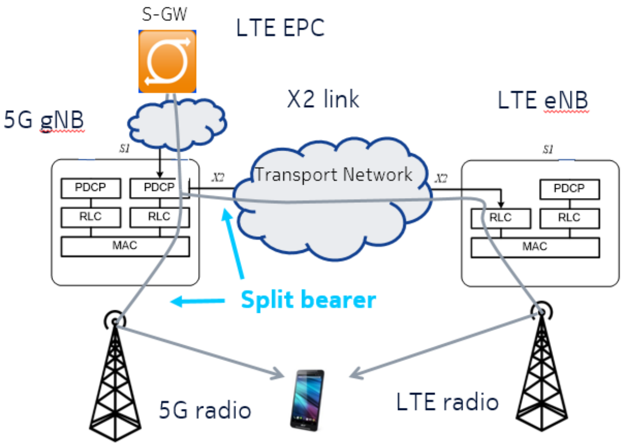
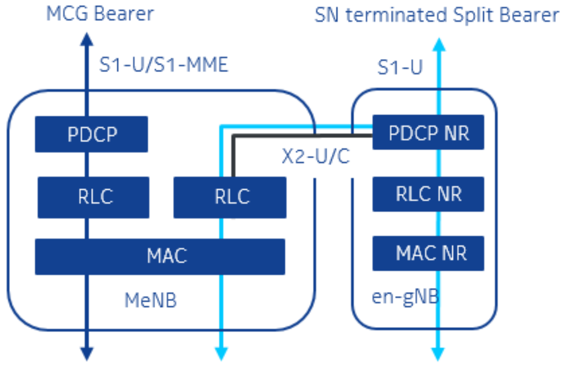


Figure 24: 5G NSA 3x split bearer

Initially, UE attaches to the Master eNB. Later, the MeNB can perform SgNB addition, for one non-GBR bearer (SN-terminated split bearer) either without 5G carrier measurement or based on the 5G carrier measurements. The supported X2AP messages to add or release NR for a UE are:

- SgNB Addition Preparation.
- MeNB initiated SeNB Release.
- SgNB initiated SeNB Release.
- SgNB Reconfiguration Completion.
- SN Status Transfer.
- Data forwarding from MeNB to SgNB.
- Data forwarding from SgNB to MeNB.



MCG	Master Cell Group
MeNB	Master eNB
SCG	Secondary Cell Group
SgNB	Secondary gNB
en-gNB	Node providing NR UP and CP protocol terminations towards the UE, and acting as Secondary Node in EN-DC.

Figure 25: 5G NSA 3x split bearer

In a later stage, from Q2 2020 onwards, it will be possible to upgrade this test network to SA option 2, according to 3GPP TS23.501 [13]. This upgrade would require minimal to no HW reconfiguration, depending on the new user stories to be implemented. It will be possible to keep an LTE layer or to reconfigure the equipment to 5G NR.

The 5G radio access network will be mainly supported on NOS sites where there is already physical infrastructure available to house the radio equipment, power, fibre and masts to fix the antennas. However, until the spectrum allocation process is completed by Portuguese regulator ANACOM, which is expected to happen in early 2020, the 5G-MOBIX project will be installed on a test network that will be completely segregated from the commercial network. In the first phase of the project, the 5G radio access network is going to be deployed at 3700 MHz, with an LTE anchor layer at 1800 MHz, which will be granted temporarily for carrying out the technical trial. In a second phase, it will be possible to migrate the network to 5G commercial spectrum that will be held by NOS.

The use cases categories UCC1 and UCC2, will be tested on A3 and A28 interurban motorways, which will be covered by 3 Macro nodes deployed on existing NOS sites. The UCC3 will be assured by 2 Small Cells that will be installed on the old cross-border bridge managed by Infraestruturas de Portugal (IP). The predicted theoretical coverage and the site locations are shown in the Figure 26 and Figure 27.

A more complete and general description of the UCs location is available in the deliverable D2.1, section 3.3. The components of the AirScale system which is Nokia's proposal to instantiate the NOS 5G network for the 5G-MOBIX trials, are described in detail in ***Annex 3***.

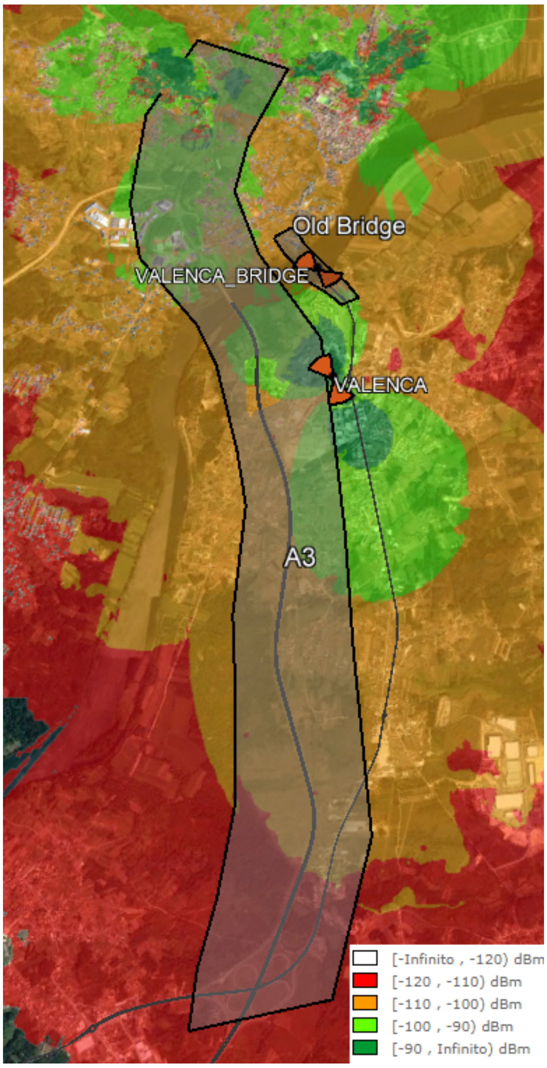


Figure 26: Cross-border area theoretical 5G coverage

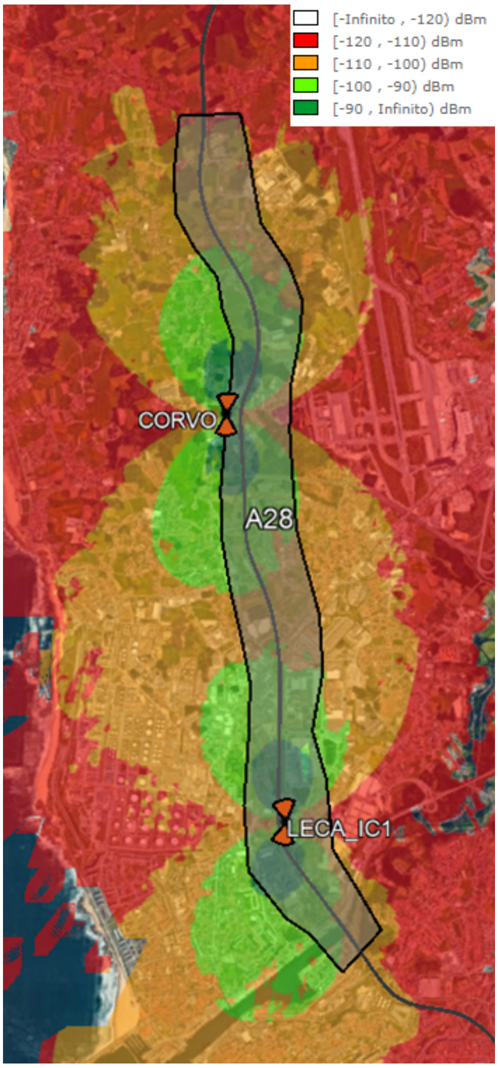


Figure 27: Porto area 5G theoretical 5G Coverage

4.3.2. Telefonica Spain RAN

Telefonica is currently covering the Spanish corridor with 4G radio, mainly at frequencies 1800 MHz and 800MHz and a few L2600 MHz nodes. In the ES-PT border, Telefonica has deployed4Galready radioaccess supported by 7 nodes at 1800 MHz and 800 MHz frequencies. This 4G radio will be used for the anchoring of the 5G NSA radio. The corridor Vigo-Tui (Spanish border) is fully covered by 4G radio by Telefonica, but only a few nodes will be broadcasting using 5G radio, mainly in two points: the border with Portugal and the Porriño area where there is a car simulation circuit at CTAG premises. So, Telefonica efforts are firstly focused in covering these two areas. In Figure 28 we can see the two 4G dominant nodes that Telefonica will be using for 4G anchoring at 1800 MHz and 800 MHz in the border area: one is covering the motorway border bridge, while the other is covering the road and train border bridge.

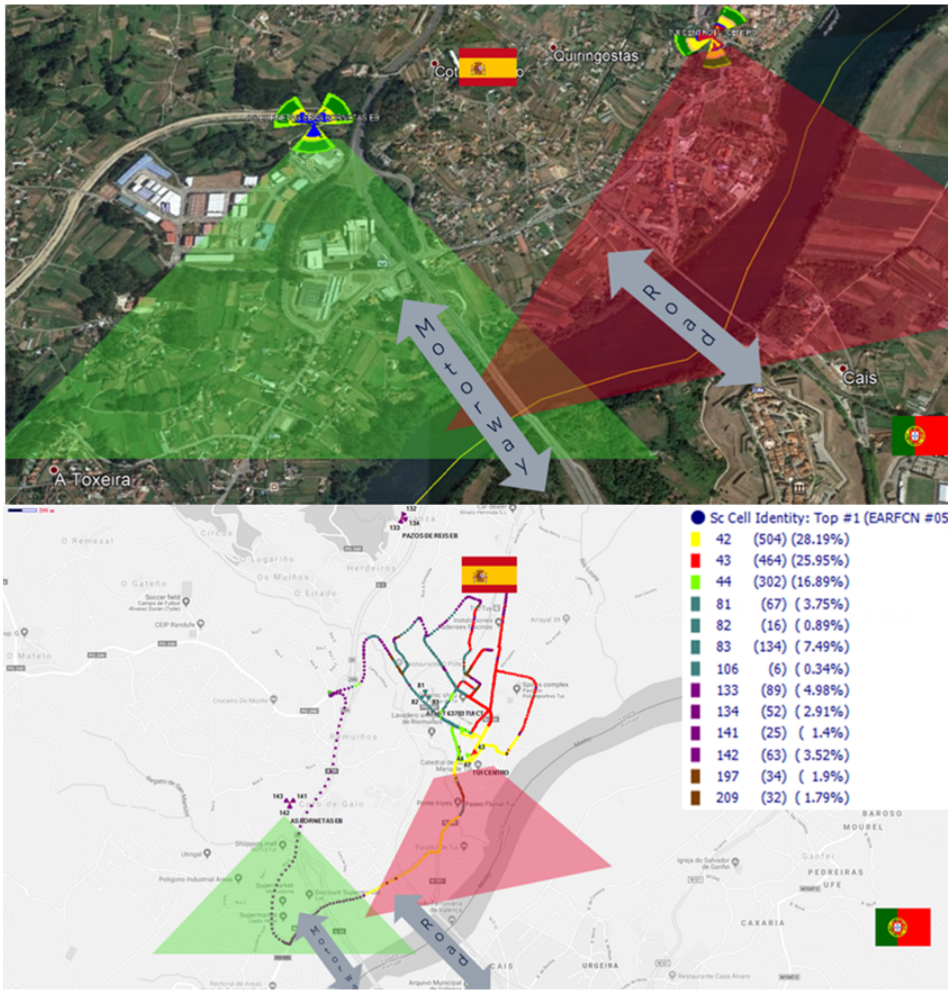


Figure 28: Border 4G anchoring coverage for road transport: border bridges (at the top) and Border 4G anchoring Measurements: 800MHz LTE (at the bottom).

In the scope of the 5G-MOBIX project timeline, the 5G new nodes will be placed at the same location of the current 4G sites. This solution is the most efficient for the following reasons:

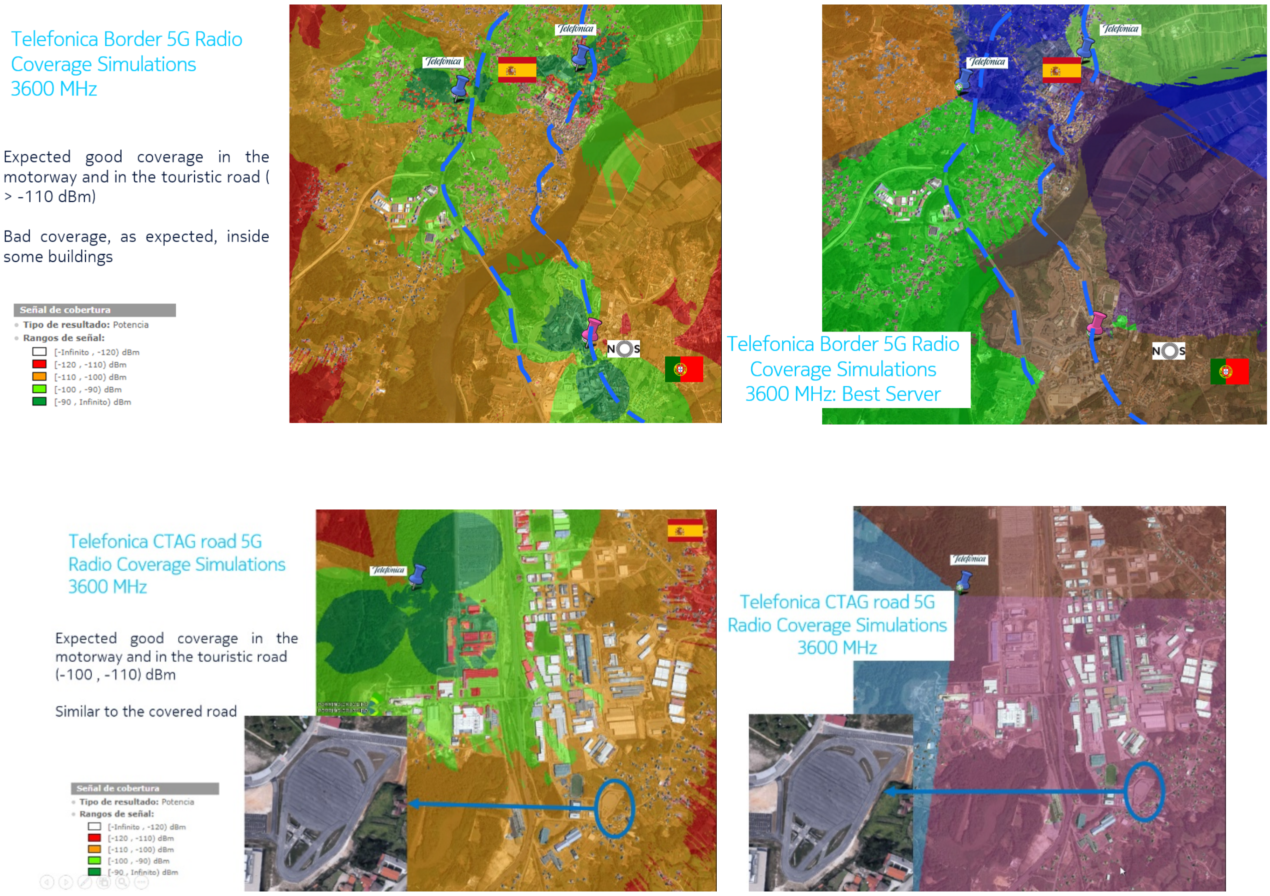
1. The sites are currently available.
2. These sites are both well covering the border area, and even several kilometres inside the Portugal border.

Currently Telefonica is using 40 MHz baseband bandwidth for 1800 MHz frequency and 20 MHz baseband bandwidth for 800 MHz frequency. These baseband bandwidths are more than enough for the required 5G NSA 3.x anchoring.

In Spain, a spectrum auction was held in July 2018 for the 3600-3800 MHz range. The spectrum was divided into forty 5 MHz blocks (total of 200 MHz) and finally the auction raised 438 M€. The Telefonica n78 5G NR 90 MHz baseband capacity is not continuous spectrum after the auction, there are three continuous blocks.

The Spanish regulator "Ministerio de Economía y Empresa" is currently trying to defragment the 3400-3800 MHz band to help operators have large contiguous spectrum blocks and facilitate high throughput multi-Gb/s 5G Services. The 5G frequency selected by Telefonica for the initial deployment for 5G NR is the 3600 MHz frequency band, where Telefonica owns 90 MHz total baseband: One block of 20 MHz (3440-3460), another block of 20 MHz (3540-3560) and one block of 50 MHz (3750-3800). The initial plan for Telefonica is to start testing in the corridor border in the block of 50 MHz (3750-3800), but this can be moved to another frequency in case the Spanish regulator decides to defragment the 3400-3800 MHz band as initially declared. Currently we do not have a fixed date for this reallocation of blocks, neither the firm commitment to do so.

The main features of the antenna that is planned to be deployed in the selected Spanish nodes of the 5G-MOBIX corridor, can be found in in ***Annex 3***. Building coverage simulations are being carried out to understand the expected 5G NR covered area in the corridor. These simulations are generated with Xirio software from Aptica.


Telefonica Border 5G Radio Coverage Simulations 3600 MHz

Expected good coverage in the motorway and in the touristic road (> -110 dBm)

Bad coverage, as expected, inside some buildings

Telefonica Border 5G Radio Coverage Simulations 3600 MHz: Best Server

Telefonica CTAG road 5G Radio Coverage Simulations 3600 MHz

Expected good coverage in the motorway and in the touristic road (-100 , -110) dBm

Similar to the covered road

Telefonica CTAG road 5G Radio Coverage Simulations 3600 MHz

Figure 29: 5G Radio Coverage Simulations (*)

Figure 29, shows coverage simulations in the corridor Valenca-Tui and CTAG car circuit in the 3600 MHz band, where we can see the level is good enough for the covered areas both in the touristic road and in the crossing border motorway as well as CTAG. In the same picture, we can also see the Best Server node covering the different areas in consideration. The CTAG car circuit is in the same coverage area as the motorway of the corridor. The level is in the range (-110, -100) dBm, depicted in colour orange, which is similar to the open motorway area level.

4.4. Core network architecture

4.4.1. Telefonica Spain Core Network

Figure 30 shows the 5G Rel.15 NSA 3.x with distributed core that will be supported by Telefonica for the initial deployment phase of 5G-MOBIX. The 5G Core solution is built on top of the NOKIA Cloud Mobile Gateway (CMG), which supports mobile gateway functionality and can be deployed on a generic computing infrastructure in a cloud environment.

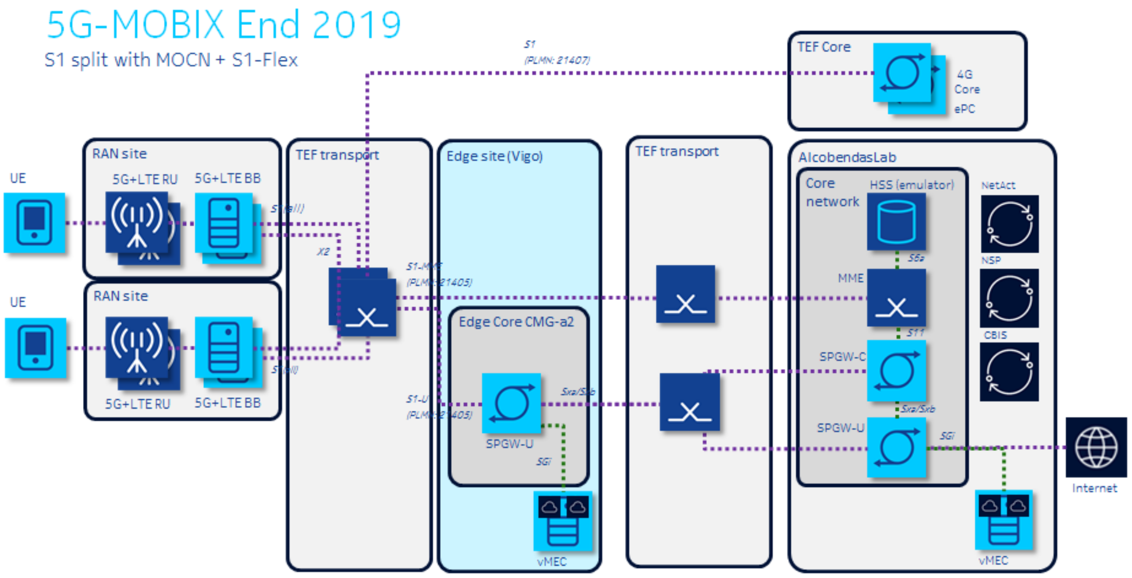


Figure 30: 5G Distributed Core with two MEC deployment sites

The CMG can support multiple gateway functions including PGW, GGSN, SGW, SAE-GW (combined SGW/PGW/GGSN), TWAG, and ePDG. A CMG instance consists of multiple virtual machines (VMs) running on a generic computing infrastructure such as x86 servers. Each VM is dedicated to a specific set of functions that can be replicated across many similar VMs. A group of VMs is represented as a single instance of an application as they operate in sync with other similar VMs in the group to support a network function. The ability to add multiple VMs for each function allows the CMG to scale horizontally and support a scaling range of a few thousand to several million devices. The VM, within a CMG instance, is agnostic of other virtual machines present in the shared server environment. The CMG system architecture has three system components, as shown in Figure 31:

- x86 host.
- Virtual machine (VM).
- CMG guest operating system (OS).

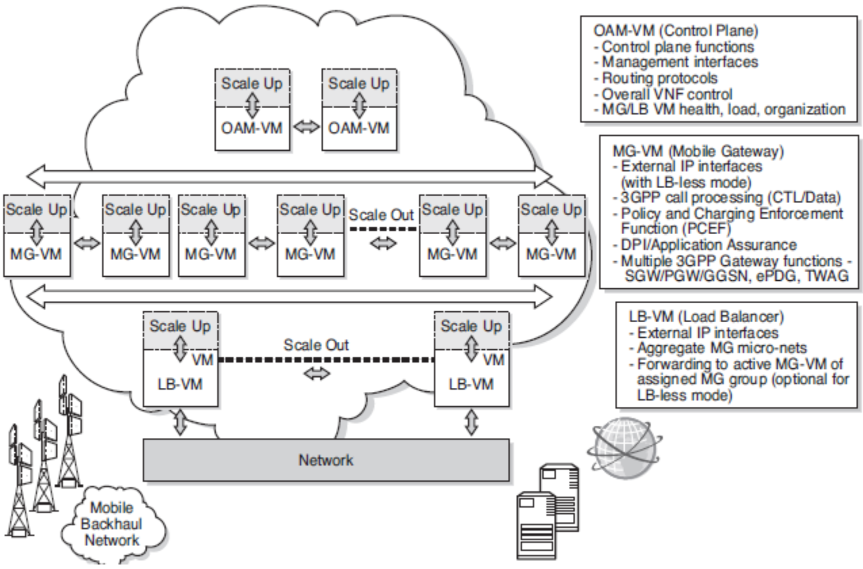

Scale Up
OAM-VM
Scale Up
OAM-VM
Scale Up
MG-VM
Scale Out
LB-VM
Network
Mobile Backhaul Network
OAM-VM (Control Plane)
- Control plane functions
- Management interfaces
- Routing protocols
- Overall VNF control
- MG/LB VM health, load, organization
MG-VM (Mobile Gateway)
- External IP interfaces (with LB-less mode)
- 3GPP call processing (CTL/Data)
- Policy and Charging Enforcement Function (PCEF)
- DPI/Application Assurance
- Multiple 3GPP Gateway functions - SGW/PGW/GGSN, ePDG, TWAG
LB-VM (Load Balancer)
- External IP interfaces
- Aggregate MG micro-nets
- Forwarding to active MG-VM of assigned MG group (optional for LB-less mode)

Figure 31: CMG VNFC Architecture

OAM-VM — The OAM-VM component performs Control Plane (CP) functions that include VNF and VNFC management, routing protocols, management interface (SNMP, TELNET, SSH, and CLI) for the configuration, KPI-KCI periodic XML report generation, and so on.

LB-VM — The LB-VM component provides network connectivity to the mobile gateway function and load distribution across the MG-VMs. It also forwards the GTP-C/GTP-U and UE addressed packets to the MG-VM. The LB-VM can provide a single common IP address for network interfacing elements (MME, eNB, SGW, PGW, TWAG, and ePDG). LB-VM is optional for GTP-U traffic. CMG supports SGW and PGW/GGSN functions when deployed without LB-VM.

Alternatively, each signalling and DP interface can be configured on separate IP addresses. The ability to separate individual functions or merge multiple functions on individual interfaces allows maximum flexibility for various deployment cases of a CMG instance.

The Cloud Mobility Manager (CMM) is designed to operate in a cloud environment running on top of standard, multipurpose IT hardware to deliver the scalability, flexibility, high availability, and performance to meet growing network signalling loads for consumer mobile and Internet of Things / Machine Type Communications (IoT/MTC) services. Built with a cloud-native architecture, the CMM provides web-scale and state-efficient design needed to meet the growing control plane demands — scale and flexibility — for 4G, IoT/MTC and the transition to 5G. Deployed as either a Standalone MME or combined MME/SGSN, the CMM uses field proven application software, which ensures feature and service consistency with both physical and appliance-based products. CMM runs on standard, IT computing hardware and OpenStack-KVM and VMware-ESXi virtualised operating environments. As an MME, the CMM performs the following high-level functions in the EPC network:

- Manages User Equipment (UE) registration, authentication, and mobility;

- Manages UE bearer setup and management for data and voice over LTE services;
- Supports Inter-Radio Access Technology (I-RAT) handovers with 2G/3G 3GPP networks and non-3GPP networks to provide and maintain UE services as users move about the network;
- Supports dual connectivity for 5G Non-Standalone deployment options 3A/3X. As an SGSN (Gn/S4-SGSN), the CMM performs the following high-level mobility and session-management functions in the GERAN/UMTS network;
- Manages UE registration, authentication, mobility and charging;
- Manages UE Packet Data Protocol (PDP) context/bearer setup and management for data services;
- Tunnels user plane IP packets from the radio access towards the GGSN/S-GW and vice versa.

4.4.2. NOS Portugal Core Network

At the Portuguese side of the border, Nokia will also provide the 5G Core comprised with a Micro Core Network solution, to be operated by NOS (Figure 32).

Given the project timeline and terminals availability, the initial deployment will be done using 5G Rel.15 NSA 3x. At a later stage when terminals and 5G CN becomes available for deployment the initial Micro Core will be upgraded to SA Option 2.

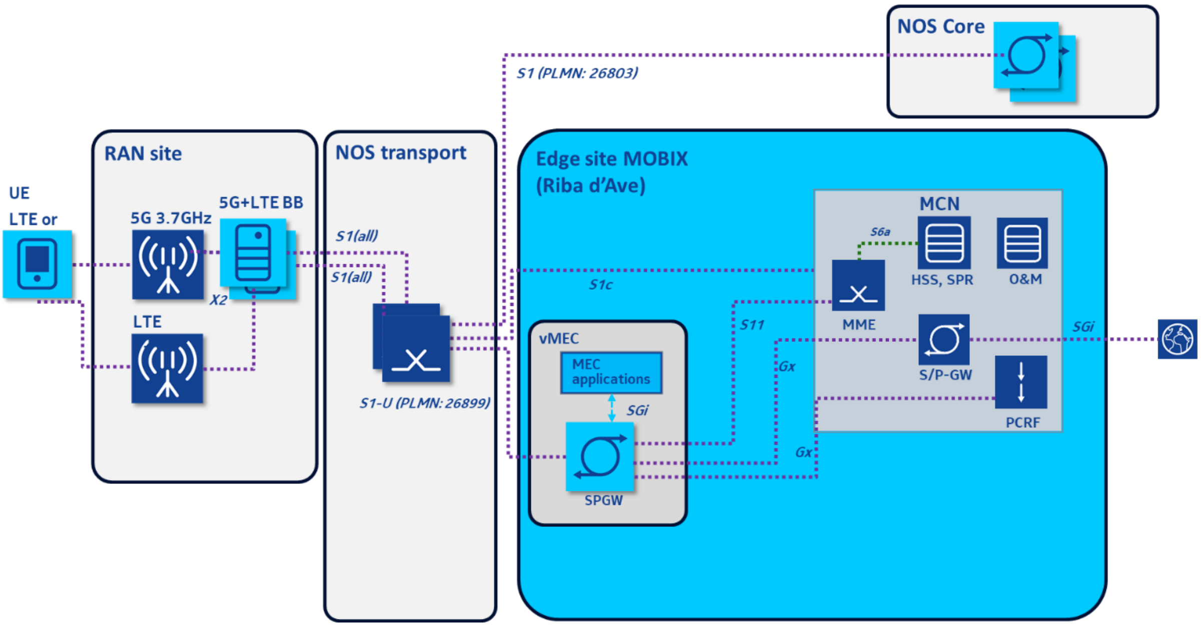


Figure 32: NOS Network S1 split with MOCN + S1-Flex

4.5. Technologies to be deployed

The tables in this section describe the most relevant 5G technologies and attributes for 5G networks (Mobile Core and RAN) to be deployed in the ES-PT CBC by the respective MNOs.

Table 6: 5G technologies and attributes for 5G network deployed by NOS Portugal

Mobile core	EPC, with later upgrade to 5G CN
Virtualised	Yes
Virtualised infrastructure	Described in 4.5.4 Micro Core Network
Network Slicing	Yes, for SA option 2
Orchestrator	TBD
Multiple access Edge Computing	Yes, described in 4.5.2 Multi-access edge computing
Radio Access Network	LTE + 5G NR
# of sites	4
Vendor	Nokia
# of cells per site	2
# of antennas per cell	1 4T4R for 2600MHz, 1 mMIMO 64T64R with 128AE for n78
Frequencies used	1800MHz, 3500MHz (B3 and n78)
Frequency Bandwidth	20MHz on B3, 100MHz on n78
Carrier aggregation	Yes, as part of EN-DC solution

Table 7: 5G technologies and attributes for 5G network deployed by TELEFONICA in Spain

Mobile core	3GPP Rel.15 HSS + MME+ EPC management system (NSP) plus Edge Core CMG-a2
Virtualised	Yes
Virtualised infrastructure	Nokia Cloud Mobile Gateway (CMG)
Network Slicing	Not in the first phase (first half of the project)
Orchestrator	Nokia CloudBand Application Manager (CBAM)
Multiple access Edge Computing	Yes
Radio Access Network	NSA 3.x 4G/5G
# of sites	3
Vendor	NOKIA
# of cells per site	3
# of antennas per cell	1
Frequencies used	licensed 4G (1800 MHz, 800 MHz), licensed 5G (3600 MHz)
Frequency Bandwidth	20 MHz 4G Anchoring + 40 MHz 5G NR
Carrier aggregation	Not in the first phase

4.5.1. Cellular V2X

4G and 5G C-V2X technologies will be used in the domain of the project, and according to the following approach:

- When 4G networks are available, LTE and PC5 will be used for the exchange of V2X messages and according to 3GPP Rel.14;
- When 5G technology is available and deployed, V2X messages will be exchanged according to 3GPP Rel.16.

4.5.2. Multi-access edge computing

Available MEC options have been thoroughly outlined in Section 2.2. MEC provides a new ecosystem and value chain. The Nokia virtualised Multi-access Edge Computing platform is deployed at the campus/venue and/or the operator's nationwide network for various purposes:

- Hosting edge content;
- Providing the essential networking functions to ingest live video streams into the 4G and 5G user plane or for Local Breakout to content and applications on vMEC;
- Hosting edge applications for processes automation and venue management, such as VR360 Live, Edge Video Orchestration, Augmented Reality and Video Analytics, locally on site.

Figure 33 below depicts the various micro services supported by the vMEC solution to be deployed at the ES-PT CBC, while Figure 34 shows the ES-PT high level E2E architecture.

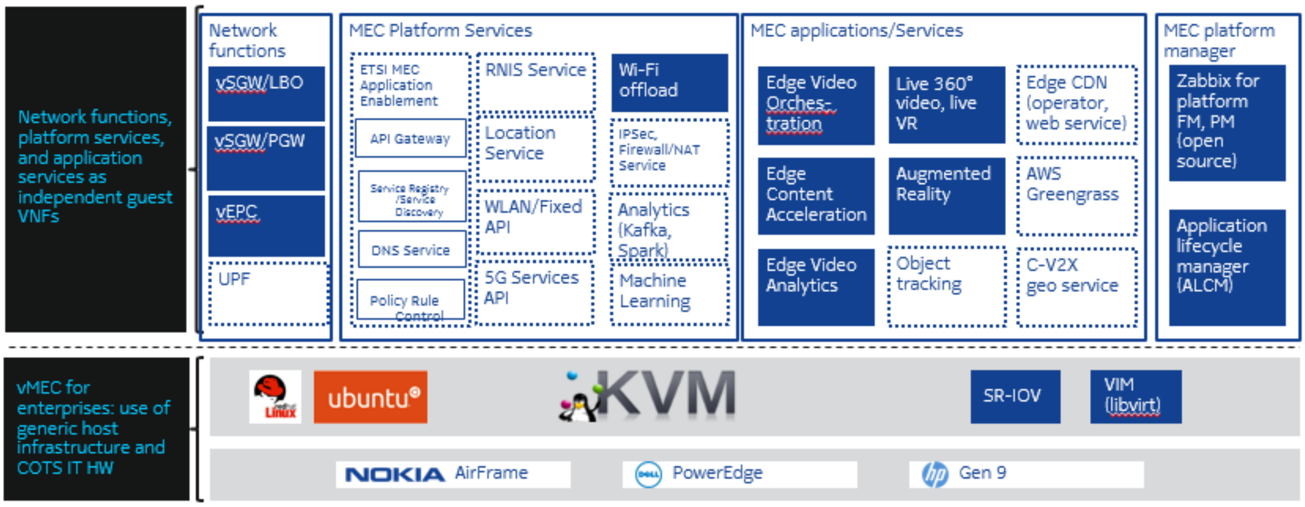

Network functions, platform services, and application services as independent guest VNFs
Network functions
vSGW/LBO
vSGW/PGW
vEPC
UPF
MEC Platform Services
ETSI MEC Application Enablement
API Gateway
Service Registry /Service Discovery
DNS Service
Policy Rule Control
RNIS Service
Location Service
WLAN/Fixed API
5G Services API
Wi-Fi offload
IPSec, Firewall/NAT Service
Analytics (Kafka, Spark)
Machine Learning
MEC applications/Services
Edge Video Orches-tration
Live 360° video, live VR
Edge CDN (operator, web service)
Edge Content Acceleration
Augmented Reality
AWS Greengrass
Edge Video Analytics
Object tracking
C-V2X geo service
MEC platform manager
Zabbix for platform FM, PM (open source)
Application lifecycle manager (ALCM)
vMEC for enterprises: use of generic host infrastructure and COTS IT HW
redhat Linux
ubuntu®
KVM
SR-IOV
VIM (libvirt)
NOKIA AirFrame
DELL PowerEdge
hp Gen 9

Figure 33: vMEC microservices and infrastructure for the solution (highlighted in dark blue)

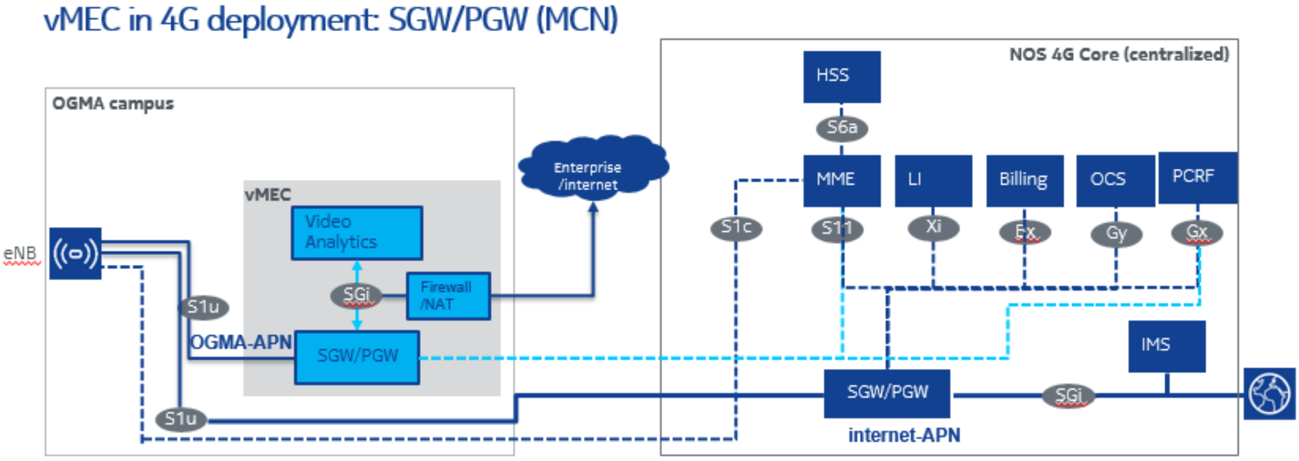


Figure 34: ES-PT high level E2E solution architecture

The vMEC platform provides northbound interfaces for FM and PM, as well as a command line interface for CM. Integration to Zabbix OSS is documented and integration to NetAct can be delivered as a project-based implementation, based on customer request and is not included in the offer presented.

The Application Life Cycle Manager (ALCM) is a software only solution provided as a MEC service to manage the life cycle of other virtualised MEC services and applications deployed on x86 based COTS IT hardware. In the context of this document when referred as "MEC application" it must be understood as also including MEC services, as from ALCM point of view, they are not distinct. ALCM provides Structured Command Line Interface (SCLI) to manage the life cycle operations of applications. ALCM provides similar functionality as Virtual Network Function Manager (VNFM) defined by ETSI MEC. ALCM provides capability to do package management of applications and lifecycle operations on application instances. Therefore, ALCM is most times the first service to be deployed in a virtual MEC environment. It also provides the ability to upgrade MEC services and applications to newer software versions. ALCM is meant to be the frontend for all operations on Nokia virtualised MEC system to be performed by the MEC administrator. ALCM, when installed, runs as a standalone virtual machine that interacts with the host virtualisation layer (libvirt) to manage the MEC services and applications. ALCM is deployed on the same COTS IT hardware host on which the MEC services and other MEC applications are meant to be deployed and administered. ALCM can deploy securely both applications signed by Nokia as well as those signed by trusted MEC administrator non-Nokia entities.

4.5.3. Network Slicing

During the first phase of the project (NSA (option 3x)), slicing will not be utilized on the ES-PT CBC. Depending on the technology availability and stakeholder's deployment roadmap, slicing will be available when 3GPP SA (option 2) is deployed at the ES-PT CBC, at a later phase of the project.

4.5.4. Micro Core Network

The Nokia Long term Evolution (LTE) Micro Core is an integrated LTE core network solution targeted at small private networks deployments and using the latest innovations in LTE technology. The Micro Core is aiming at being integrated into small factor servers and rapidly deployable equipment. The Nokia Micro Core Network (MCN) has been designed to address efficiently the needs of vertical markets players such as Public Safety (PS) agencies, or Energy and Transport Companies and Utilities. Especially, thanks to its high availability feature the MCN is designed to support critical missions where human life is at stake and which require a mix of data (email, video, web, messaging, sensors, security, etc.), voice and Push to Talk (PTT)) functionality with the right quality of services including PS Quality of service Class Identifier (QCI).

The Nokia MCN integrates in a modular approach all, or part (depending on the use case) of the 3GPP standards-compliant packet core comprising of the Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), Home Subscriber Server (HSS), Policy and Charging Rules Function (PCRF) functionalities in a very compact and modular software solution. Thanks to its compactness and modular approach, the Nokia MCN is covering the whole range of network deployment ranging from autonomous LTE deployable bubbles to fixed LTE wireless networks.

The Nokia MCN solution provides a complete 3GPP compliant EPC based on Nokia hardware products. It supports User Equipment (UE) authorization and authentication, admission control, intra-LTE UE mobility, user traffic forwarding with QoS differentiation and policing, it is flexible and cost efficient. It is designed to drive maximum performance on given Nokia hardware platforms. The solution is easily portable, runs on regular Linux OS and it supports different deployment options (especially thanks to its modularity and deployment flexibility), to fulfil customer specific needs for performance and capacity.

The Nokia MCN operation and maintenance system provides easy provisioning and control of the distributed application system. The operation and maintenance can be done through a web-based interface adapted to non-telecom operators. This interface gives access to PM, FM and diagnostics. The design of the Nokia MCN is considering the specification of the 3GPP R11, the Nokia serviceability guidelines, the Nokia product security guidelines and the National Security Agreement (NSA) recommendations and its main components are:

- GUI Server (Graphical User Interface)
- Controller Agent
- Application Container.

These components can be seen as separate processes that can run on different computing nodes (either physical nodes or virtual machines in the future). From the functional point of view, the distributed NFs compose an EPC with standard 3GPP interfaces as shown on Figure 35. Although listed in the diagram, P-CSCF and S-CSCF are part of IMS Lite optional functionality, which is not included in the offer.

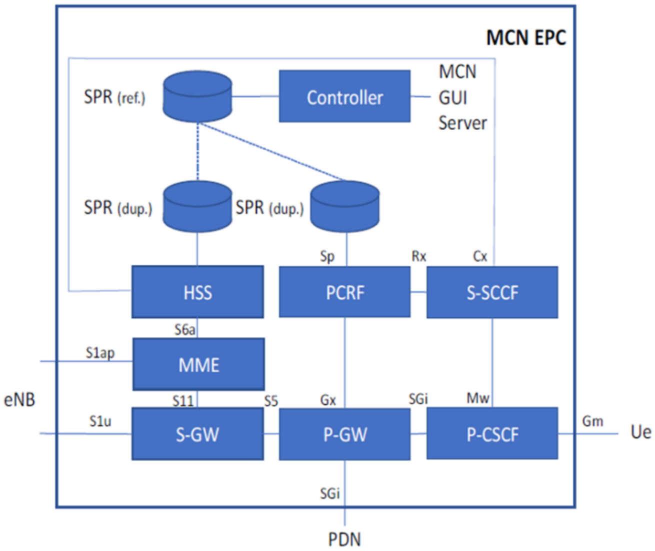


Figure 35: MCN functional entities

MCN can be deployed with or without a GUI server which is subpart of the whole project. GUI server is intended for:

- Monitor the state of single or multiple MCN deployments.
- Modify and provision configuration of MCN NFs, SPR database.
- Licence management.
- Centralized alarm management for all MCN deployments monitored by the GUI.

RAN monitor: collect FM messages from eNBs connected to the MCN instance.

4.6. Contributions from Trial Sites

The 5G network components, features and technologies for the ES-PT cross-border corridor will be provided by Nokia Spain and Nokia Portugal (as described in this section), based on early releases of their commercially available projects, giving 5G-MOBIX the opportunity to be among the first to experience in its trials the advanced performance delivered by these products. It can be understood that the Nokia 5G products are highly advanced proprietary equipment and features which are the result of years of research and development, and as such cannot really be combined or integrated (at least not within the context of 5G-MOBIX) with 5G products of other (competitive) vendors or even open source 5G equipment / features developed and utilized in the local trial sites of 5G-MOBIX.

For this reason, the concrete contributions of the TSs to the ES-PT CBC have been focused on autonomous vehicles components (including OBU extensions), road-side infrastructure HW and SW as well as Cloud / Edge platform functionality and CCAM application development. As D2.2 is focusing on 5G network infrastructure and technologies, these contributions are not relevant for this deliverable and are hence described in the other WP2 deliverables. More specifically:

DE contribution to ES-PT

Although no concrete 5G network components of DT TS can be integrated at the ES-PT CBC, DE TS CCAM infrastructure and AVs components are designed to take advantages of 5G features and common architectures to be realized in this project. Therefore, these components can be deployed in ES-PT CBC CCAM infrastructure to trial additional scenarios and requirements and to evaluate the performance of 5G infrastructure at ES-PT CBC. The general contribution to ES-PT CBC are: 1) evaluation of 5G support for V2I communication between DE eRSU and AVs to address cross-border issues; 2) benchmarking extended sensor solution with DE LDM/EDM HD-maps; 3) identification of constraints and extensions recommendation for CBC infrastructure to support the dynamic and multi-tenant integration of TS software and hardware components. Further details of the contributions to CCAM infrastructure and AV components from DT TS are provided in D2.3 [2] and D2.4 [3] respectively.

FI contribution to ES-PT

The FI TS will not contribute directly in terms of deployment of 5G radio access or core network equipment or software towards the ES-PT CBC. However, the FI TS will contribute device-side (OBU) and CCAM applications that enhance the CBC user story functionality in inter-PLMN and multi-PLMN environments. These contributions are outlined separately in deliverables D2.3 [2] and D2.4 [3] (respective sections on specific TS contributions to CBCs).

FR contribution to ES-PT

FR TS is not contributing to the 5G technology architecture in the ES-PT corridor. The French site will rather contribute on the Infrastructure side by providing specific MEC applications such as Geo-cast capability (more details in the respective section of deliverable D2.3 [2]) as well as on the vehicle side by proposing a seamless Handover function (more details in the respective section of deliverable D2.4 [3]).

NL contribution to ES-PT

Although no concrete 5G radio access or core network components of NL TS can be integrated at the ES-PT, ES-PT can use the results of the research in deploying SA solution in NL, since the rollout of SA in ES-PT site in phase 2 which is later than the NL trial site's SA solution roll-out. More details of the contribution of NL site to 5G architecture and technologies are described in Section 6.1.1.2. Contribution on infrastructure side and vehicle side are described separately in deliverables D2.3 [2] and D2.4 [3].

5. GREECE -TURKEY (GR-TR) 5G ARCHITECTURE & TECHNOLOGIES

This section deals with the definition of the architectural requirements and selected 5G architecture to be deployed in the GR-TR corridor of 5G-MOBIX. The section initially provides a "bird's eye view" of the main requirements and structural elements of GR-TR CBC, before detailing the planned 5G architecture with respect to the radio access network architecture, the core architecture and the 5G and V2X technologies that are to be deployed (based also on the standardisation analysis provided in Section 2). Finally. The contributions of the collaborating TSs to the GR-TR CBC are also presented in this section.

5.1. Considered 5G network requirements

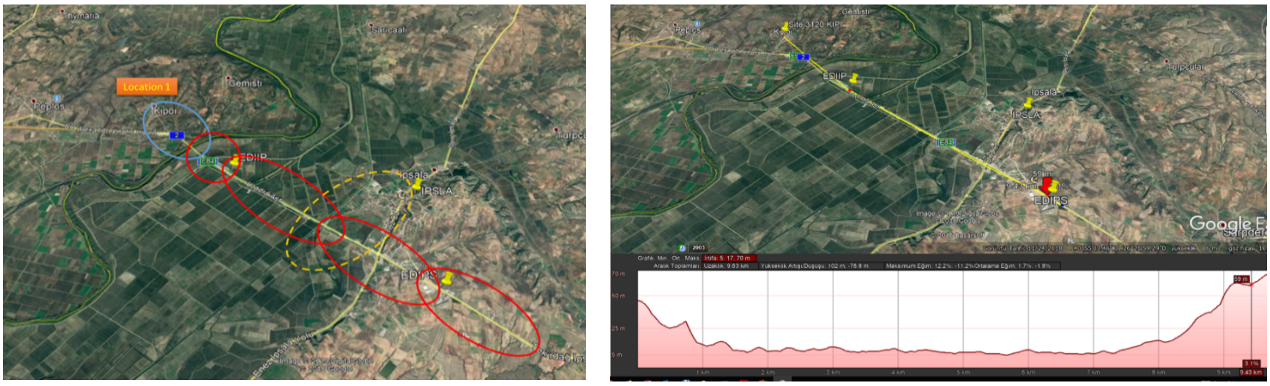
5.1.1. Radio network requirements

The network to be deployed in the GR-TR corridor for supporting the 5G-MOBIX use case categories will be based on the 5G-NR NSA architecture. The radio access network will consist of one base station site in the Kipoi area (Greek side) and three base stations in the area of Ipsala (Turkish side). The specific sites have been selected among several candidate site locations, based on the following site selection criteria:

- Line of sight (LOS) between base stations locations to ensure continuous 5G coverage on the selected GR-TR cross-border route to be used by the L2/L4 vehicles;
- Re-use existing base station towers of both MNOs where it is feasible to deploy new 5G NR equipment with minimum impact on site construction works and to acquire site licence considering EMF constraints;
- Availability of necessary site facilities, such as access to power from the grid and fibre backhaul cables or high-throughput MW links.

The evaluation of the selected locations in terms of continuous 5G coverage has already been carried out by Ericsson Greece & Turkey with the use of their commercial radio planning tool (Planet). Some of the results are depicted in the figures below (Figure 36 – Figure 38).

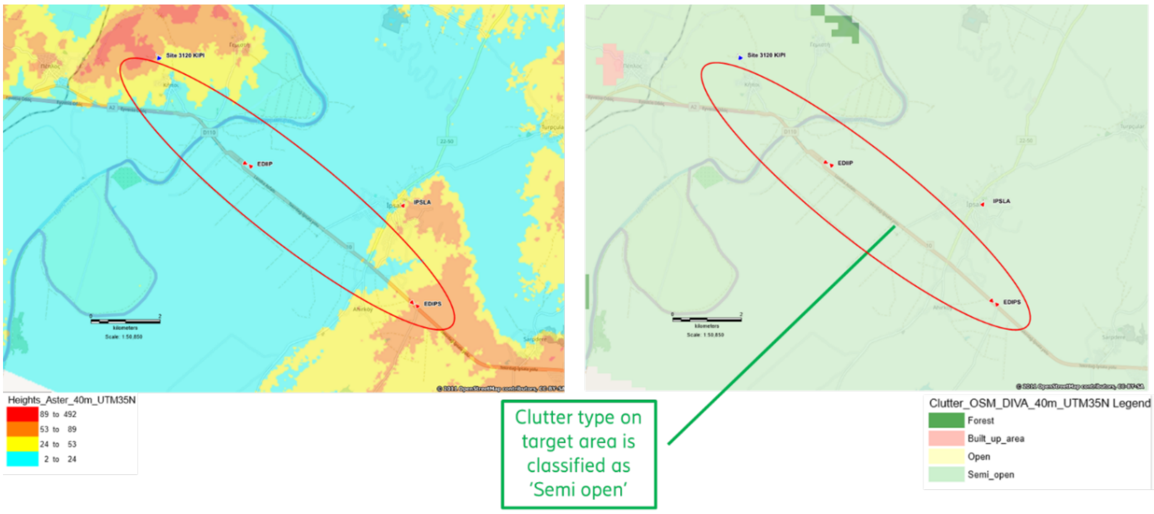
It should be noted that for these initial coverage predictions the Planet General propagation model (not tuned) has been used, while specific assumptions have been made in terms of UEs (4m height, 23dBm output power and 0 dBi antenna gain).



a)

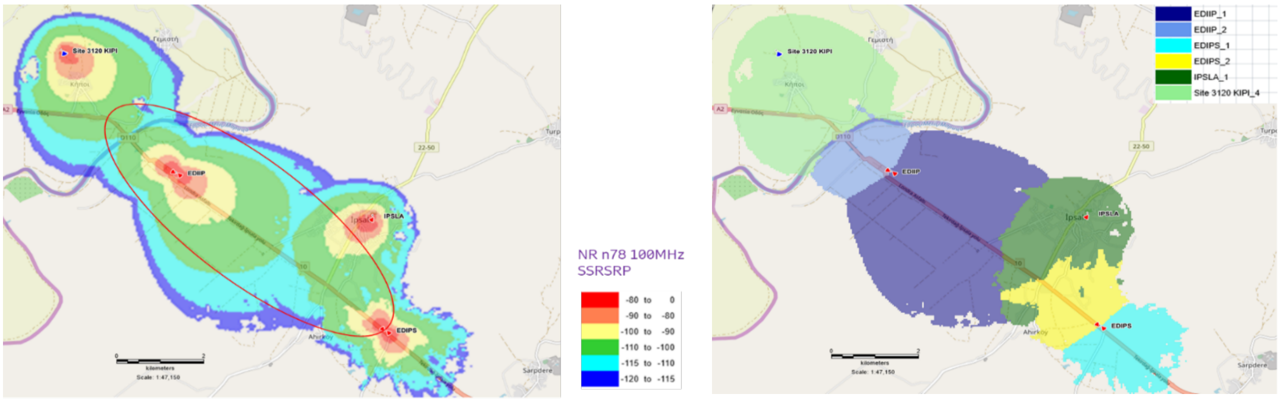
b)

Figure 36: Terrain analysis for the Ipsala – Kipoi border location at the GR-TR borders showing a) the GR-TR inter-site distance and b) terrain height information.



Clutter type on target area is classified as 'Semi open'

Figure 37: Clutter type analysis of the Ipsala – Kipoi border location at the GR-TR border



(a)

(b)

Figure 38: Prediction of (a) coverage and (b) Best server area of the Ipsala – Kipoi border location

5.1.2. Core network requirements

5.1.2.1. *Core options*

Both Cosmote & Turkcell plan to initially deploy 5G EPC (Option 3x), in a virtualised environment, which could be extended to a dual core solution (5G EPC + 5GC) at a later phase, depending on the availability of a 5GC solution provided by Ericsson, common provider for both MNOs.

An important core network requirement in this trial is the support of inter PLMN-handover, as analysed below at section 5.1.2.3. Currently, the 5G EPC cannot support cross-border handover with session continuity; an issue that is solved with the use of 5G Core (SSC [Session and Service Continuity] mode3). As discussed in Section 3.4 and based on the 5G-MOBIX proposed common architecture, the two networks will be interconnected using a direct connection.

In order to support the QoS requirements of each user story, the implementation of network slicing, which allows the creation of multiple virtual networks atop a shared physical infrastructure, is considered. Depending on the phase of the core solution deployment (5G EPC or 5GC), there are various network slicing mechanisms analysed at section 5.5.3.

5.1.2.2. *MEC deployment*

Considering the high mobility nature of both use case categories to be supported at GR-TR cross-corridor trial, edge computing as a distributed cloud architecture is planned to be supported. Specifically, Cosmote & Turkcell will both deploy at their edge core sites, located in close proximity to the gNBs of the cross-border trial, all functionalities of the 5G EPC, including HSS, MME, SGW & PGW. In fact, the MEC data plane will sit on the SGi interface. It is worth mentioning that the Control/User Plane Separation (CUPS) option is also considered, aiming to address more efficiently the local user plane distribution.

5.1.2.3. *Roaming*

On the ground that the 5G NSA technology currently available uses LTE as the basis, the established roaming agreements between Cosmote (MCCMNC 20201) and Turkcell (MCCMNC 28601) sufficiently cover the prerequisite. Important technical considerations to be addressed during inter-PLMN handover include the service continuity and latency requirements of the GR-TR corridor use case categories, which significantly affect the roaming type to be selected among the available options, either Home Routing or LBO (as discussed in Sections 2.4 and 3.4).

Latency requirements also impact the roaming network mode to be used. Currently, both operators are connected through third party roaming-hubs using GRX or IPX networks. This is the preferred option to reduce roaming costs and the default method currently, as GRX/IPX-based interconnections allow for service scalability through point-to multi-point connections provided by the third parties. When strict quality of service and security requirements are in place and cannot be guaranteed by the established

GRX/IPX networks, direct interconnection between MNOs is also an option, nevertheless with a significantly increased operational cost that must be considered per business case.

5.2. E2E Architecture

The end-to-end GR-TR cross-border trial architecture is depicted in Figure 39. Both mobile network operators, Cosmote & Turkcell, plan to deploy overlay 5G EPC (NSA, opt. 3x) architecture at their edge Data Centres (DCs), located close to the border' sides to fulfil the strict latency requirements imposed by the use case categories to be demonstrated at this cross-border trial site. For the trial purposes, the radio and core network equipment to be deployed by both mobile network operators (MNOs) is provided by Ericsson. The application servers will connect to the edge DCs, where the overlay vEPC functionalities will be deployed, while the 5G UE – application servers' connectivity will be provided over the PGW SGi interface.

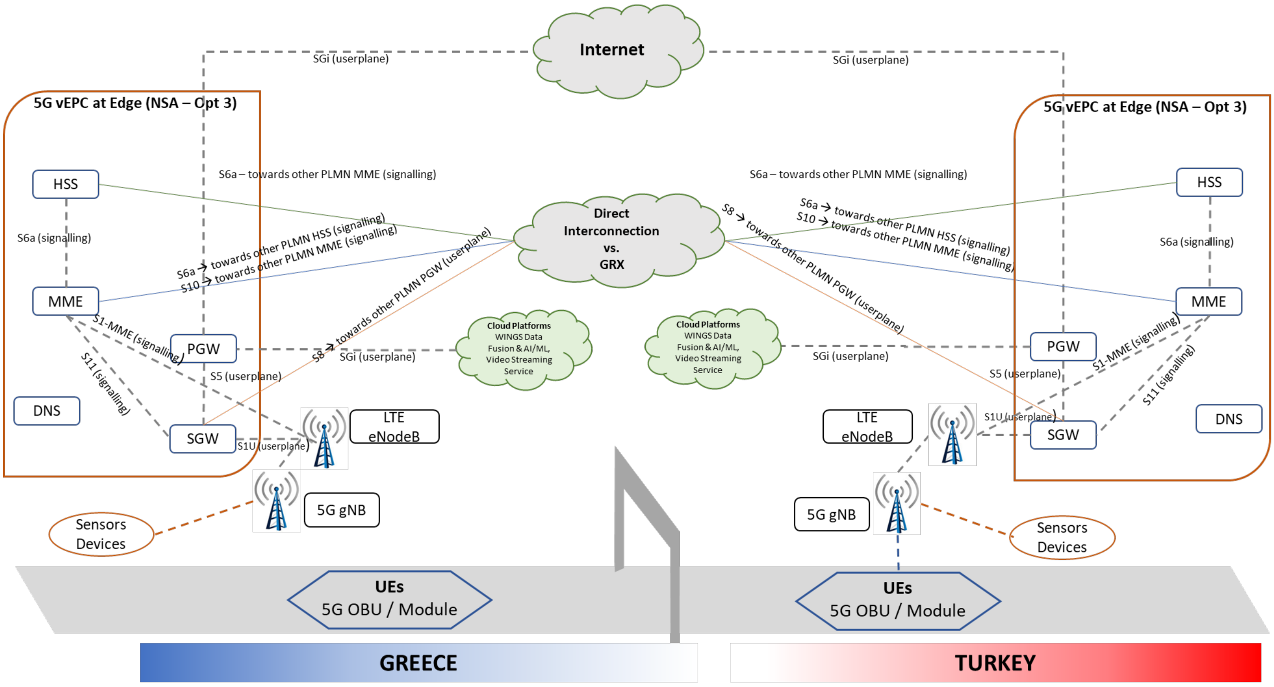

Internet
SGi (userplane)
SGi (userplane)
5G vEPC at Edge (NSA – Opt 3)
5G vEPC at Edge (NSA – Opt 3)
HSS
S6a (signalling)
MME
S6a – towards other PLMN MME (signalling)
S6a → towards other PLMN HSS (signalling)
S10 → towards other PLMN MME (signalling)
Direct Interconnection vs. GRX
S6a – towards other PLMN MME (signalling)
S8 → towards other PLMN PGW (userplane)
S6a → towards other PLMN HSS (signalling)
S10 → towards other PLMN MME (signalling)
S8 → towards other PLMN PGW (userplane)
HSS
S6a (signalling)
MME
S1-MME (signalling)
S11 (signalling)
PGW
S5 (userplane)
SGi (userplane)
Cloud Platforms
WINGS Data Fusion & AI/ML, Video Streaming Service
Cloud Platforms
WINGS Data Fusion & AI/ML, Video Streaming Service
SGi (userplane)
PGW
S5 (userplane)
S1-MME (signalling)
S11 (signalling)
DNS
SGW
S1U (userplane)
LTE eNodeB
LTE eNodeB
S1U (userplane)
SGW
DNS
5G gNB
5G gNB
Sensors Devices
Sensors Devices
UEs
5G OBU / Module
UEs
5G OBU / Module
GREECE
TURKEY

Figure 39: **GR-TR corridor End-to-end Architecture**

The Ericcson Enterprise Core solution (see Section 5.4) has network functions like MME/SGW/PGW/HSS/PCRF running on top of it. In all the proposed network deployment options, RAN components and MME/SGW/PGW will work as overlay network functions. However, HSS and PCRF components can be provided by commercial network which requires MME and PGW communicates through DRA for S6a and Gx interfaces. Latency is taken into consideration and location selection for the deployment of core components has been made considering the shortest route of traffic as per the existing topology of operators. Distributed core architecture addresses the low latency requirement and therefore v-EPC will be deployed at edge data centres where possible, based on the current topology. CUPS usage is also considered; however, it is not supported in the current releases of the Ericsson products.

5.3. Radio network architecture

This section provides a summary of the network nodes and Radio Access Network (RAN) architecture. The RAN provides the access links between the User Equipment (UEs)/On-Board Units (OBUs) and the Virtual Evolved Packet Core (vEPC) network. The access links are divided in user plane and control plane parts. The user plane carries the V2X payload traffic while the control plane carries control signalling for user plane traffic. The radio access network consists of the following network components:

- Distributed radio units (active and passive) offering 4G/5G cell coverage.
- Compute processing units (eNB, gNB) controlling the radio connections with connected vehicles as well as managing the radio cell resources including connection mobility control. The compute processors will run 4G and 5G RAN SW functionality tailored to enhance V2X applications.
- Ericsson Network Management System for fault, configuration and performance management.

The proposed RAN network architecture will be implemented according to the 3GPP R15 Non-Standalone (NSA) architecture, as depicted schematically in Figure 40.

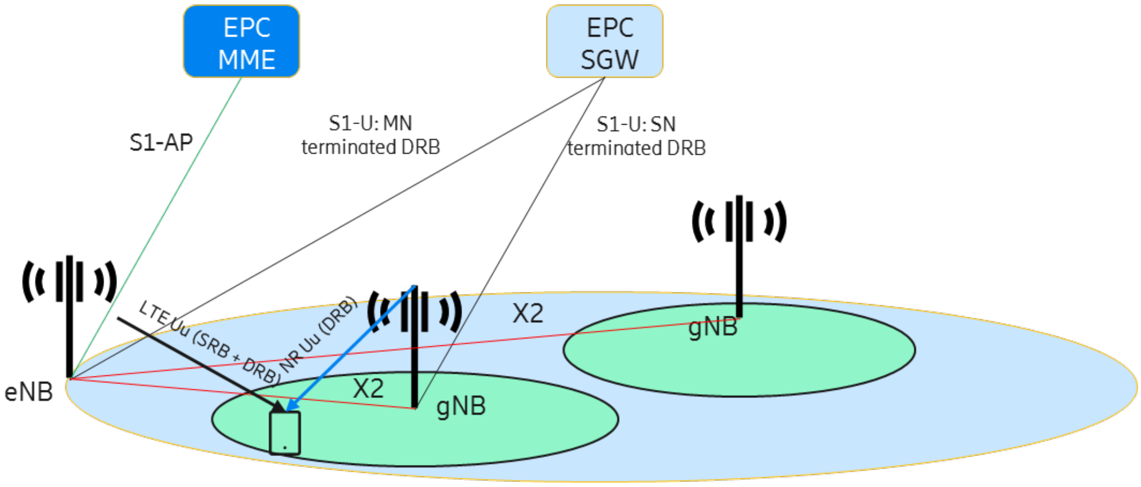


Figure 40: New Radio NSA Option 3x Architecture connectivity diagram for GR-TR CBC

The 3GPP specifications for option NR NSA option 3x are presented in Section 2.1.1 OBUs capable of DC functionality will always be connected to LTE-A RAN and will connect to NR RAN when available. The eNB will act as the Master eNodeB (MeNB) and the gNB as the Secondary Node (SgNB). A Data Radio Bearer (DRB) can be either a SN terminated split DRB assuming NR RAN is available or if it is not a MN terminated DRB. In case of a split DRB, DL traffic is split at the Packet Data Convergence Protocol (PDCP) layer on the gNB. User traffic can be sent directly over the NR air interface or can be forwarded over the X2-U to the eNB and from there further to the UE over the LTE air interface. In the uplink direction, user traffic can be sent over the LTE air interface or the NR air interface. If the LTE leg is used, uplink user traffic is gathered at the PDCP layer on the gNodeB.

The following sections will provide an overview of the overlay RAN network of both Cosmote & Turkcell, and a short description of Ericsson's RAN solution (HW & SW features) that will be deployed at both networks aiming at a reliable, high quality and low latency V2X connectivity.

5.3.1. 4G/5G overlay RAN network overview

A new RAN overlay network will be deployed by both Cosmote & Turkcell in order to minimize the impact on the existing RAN commercial services as well as provide the freedom for frequent SW release upgrades of the network domains. This RAN overlay network can be achieved by deploying an eNB operating at 2.6 GHz with a carrier bandwidth of 20 MHz. This LTE layer will be used as an anchor layer to the NR carrier. In addition, a new gNB will be deployed at 3.5 GHz with a carrier bandwidth of 100 MHz using an Active Antenna System (AAS). A conceptual E2E 4G/5G RAN connectivity to 5G-vEPC is shown in Figure 41.

Ericsson's E-UTRA-NR Dual Connectivity (EN-DC) solution, based on Option 3x, will be deployed by both network operators. A brief description of Ericsson's RAN equipment & SW features to be implemented in the GR-TR CC is given in **Ericsson RAN components for the GR-TR CBC**.

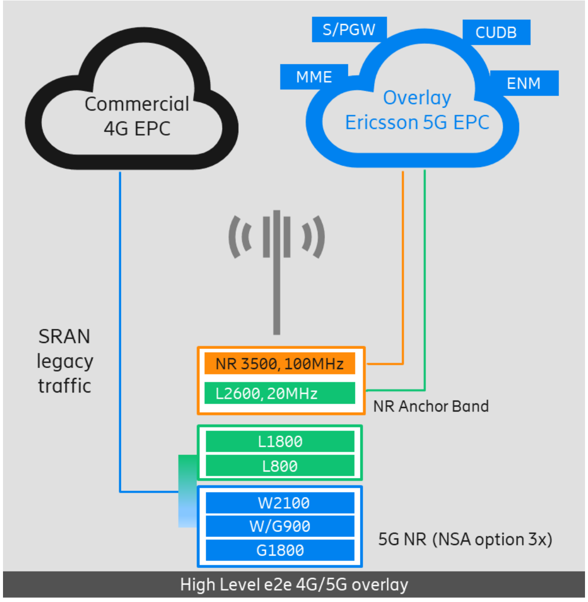


Figure 41: E2E 4G/5G RAN connectivity to 5G-vEPC

5.3.2. RAN SW

The proposed Ericsson RAN SW will include 4G LTE-A and 5G NR RAN. The LTE-A SW includes software-driven innovations that bring essential 5G technology concepts to today's 4G+ cellular networks, which enables a flexible 5G evolution as well as improving network performance allowing introducing an array of new services and applications. The LTE-A SW is part of the Ericsson's 5G plug-ins portfolio and it builds on

3GPP R13/15 specifications. In addition to the LTE-A software, a 5G NR, compatible to 3GPP R15, will be deployed to offer NR NSA services. This includes:

- Operating system for the NR gNB, including the SW platform;
- Functionality needed for basic configuration, fault, software, and performance management;
- Functionality needed for user plane traffic management between the gNB and the core network;
- Functionality needed for traffic management between the gNB and the connected eNB through X2 interface;
- Functionality needed for traffic management between the gNB and the UE through the air interface UE.

It is noted that PC5 link is not supported in the current NR/LTE-A SW releases. Therefore, Ericsson will provide unicast connectivity for the V2X messages between the OBUs and the V2X application servers.

5.3.3. 5G SW plug-ins

5G plug-ins is an advanced LTE SW portfolio which enables 5G type of technologies in LTE networks. The 5G SW plug-ins portfolio includes RAN functions to support the 5G NSA deployment and to efficiently handle V2X services. These functions are discussed in the following paragraphs.

5.3.4. Intelligent connectivity

LTE-NR Dual Connectivity (EN-DC) operates by overlaying NR to LTE networks connecting to the 5G-enabled Evolved Packet Core Network (EPC) through the S1 interface. It enables the devices to setup a split bearer, which uses two separate connections, one to a Master Node (MeNB) and one to a Secondary Node (SgNB). In NSA, the MN is the eNB and the SN is always the NR. Control signalling towards the UE and the core network is handled by the eNB. Downlink user data is transferred on either LTE or NR connection. The X2 interface is used between the eNB and the NR Node. When a split bearer is established, the user-plane towards the device and the core network is terminated in the Secondary NR Node. The user data sent to the device using LTE is transferred through the X2 interface. This referred to as 3GPP Option 3x. A flow control scheme is used for the user data over the X2 interface (X2-U) to keep buffers in the eNB filled at the right level.

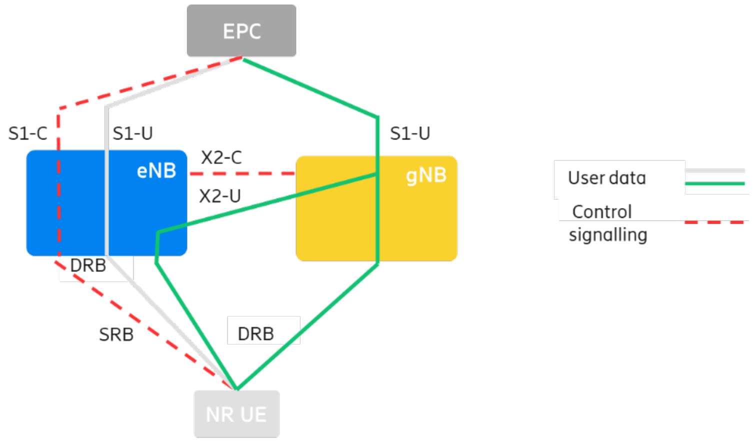


Figure 42: NR NSA (EN-DC) overview

A split bearer is typically established as soon as the UE is in NR coverage. It is removed when the UE/device leaves NR coverage. It is noted that mobility is handled in LTE by removing the split bearer if the device finds a better LTE cell than the serving cell. If all prerequisites are met, the split bearer can be set up again in the target LTE cell.

NSA Interfaces

- S1-C: Connects RAN to EPC. Used for S1-C signalling connection, terminated by the eNB;
- S1-U: Connects RAN to EPC. Carries S1-U user plane bearer. It is terminated by the eNB for legacy UE's, and certain bearers of the NR UE such as VoLTE. While it is terminated by the gNB for the NR UE bearer;
- X2-C: Connects the eNB and the gNB and carries X2 control signalling;
- X2-U: Connects the eNB and the gNB and carries user data of Split bearer;
- E6: Control plane interface between the Packet Processing block in the gNB and the Radio processing block in the eNB.

5.3.4.1. Latency reduction

In current 3GPP standardisation efforts there are design targets related to latency and reliability of V2X services. For example, according to [32] the end to end latency requirements for a cooperative driving for vehicle platooning Information exchange between a group of UEs supporting V2X application range between 10ms to 25 ms depending on degree of automation.

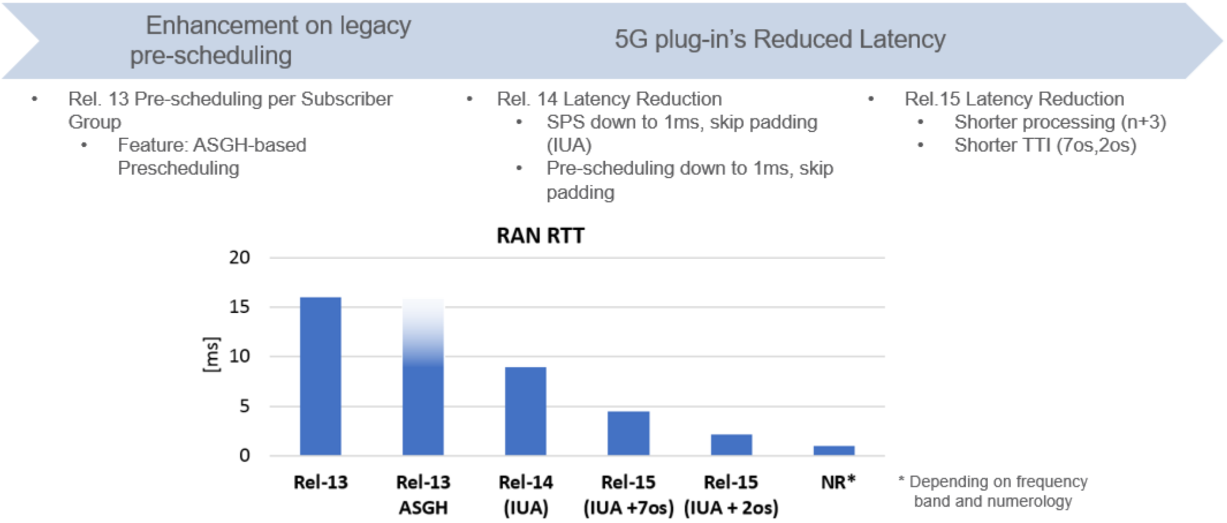


Figure 43: RAN latency towards 5G NR though Ericsson's 5G Plug-ins

To reduce the RAN round-trip time (RTT) latency and create a mobile platform addressing a variety of use cases, Ericsson has developed an advanced portfolio of RAN functionalities meeting critical latency requirements. As an example, Figure 43 shows the Ericsson RAN SW functionality development plans for reducing RAN RTT latency to values below a 1 ms.

The proposed mechanism builds on two steps developed in 3GPP Rel.14 and 15 specifications. Specifically, R14 Instant Uplink Access (IUA), which will be part of the offered solution, eliminates the need for explicit scheduling request and individual scheduling grants. Through pre-allocation of radio resources IUA can reduce the average radio RTT latency (i.e., UL and DL) to 9 ms, which is a significant improvement compared to traditional LTE R13 RTT latency of 16 ms. The second method, which is specified in 3GPP Rel.15, enables shorter transmission durations. The concept is to compress the whole transmission chain of waiting for a transmit opportunity in order to transmitting the data. Consequently, the associated control and feedback is performed faster.

The compression is done by introducing transmissions with duration shorter than a subframe. In downlink, this is done by splitting the data part of the subframe into several parts. Each of these short transmission durations can be scheduled separately with a new in-band control channel. In addition to downlink, the uplink subframe is split into multiple shorter transmit durations and are scheduled from the same in-band control channel. The subframes are either split into two parts, four parts or into roughly six parts for the lowest latency mode. At the highest splitting level, a one-way transmission can be done in a total of about 0.5ms including processing of data. Support for reduced latency as specified in Rel.15, including faster HARQ and shorter TTI is planned for deployment at a later stage.

5.3.5. RAN Software and 5G NR

Ericsson's 5G NR SW is part of Ericsson Radio System (ERS) 5G Platform enabling smooth coexistence with existing LTE technology and ease migration from LTE to NR. The first NR release to turn on 5G in commercial networks is already available in Q2.2019. The base NR SW package enables the following key functionality:

- Connected Mode DRX.
- Coverage Extension High-Band.
- Coverage Extension Mid-Band.
- IPsec.
- LTE-NR Dual Connectivity.
- NR Micro Sleep Tx.
- NR Mobility.
- Physical Layer Mid-Band.
- Scheduler Mid-Band.
- Streaming of PM Events.
- Uplink-Downlink Decoupling.
- Transport, synchronisation and security for NR.
- O&M function for NR.

Additional functionality will be added in subsequent releases. The 5G NR SW is upgraded and released 4 times per year, one release per quarter. Details regarding the implementation of some of these key features such as UL-DL decoupling, Massive MIMO, massive IoT and more are given in ***Annex 4***.

5.4. Core network architecture

Both mobile network operators, Cosmote & Turkcell, will deploy an overlay 5G EPC core network that will be connected to each operator's equivalent overlay 5G NR radio, creating thus a private 5G NR network. In fact, Ericsson's Enterprise Core solution, which consists of Evolved Packet Core (EPC) and User Data Consolidation (UDC) functionalities, will be deployed.

In the following sections, a brief description of Ericsson's Enterprise Core solution will be provided, while also the core network architecture of Cosmote & Turkcell will be presented.

5.4.1. Ericsson Enterprise Core Solution

Ericsson Enterprise Core solution is a dedicated pre-assembled system consisting of Evolved Packet Core (EPC) and User Data Consolidation (UDC) components. The network is either operated by the Industry customer via Enterprise Operations Support System (OSS), or it is operated by Ericsson Managed Services. Data connection and related services are provided by the EPC, voice and video communication together with multimedia telephony services are provided by IMS and the user data is stored and handled by the UDC component. User provisioning is handled via Enterprise OSS.

Ericsson Core Standalone solution is ready to be connected to a dedicated or existing Radio Access Network (RAN). This way it creates a stand-alone private LTE network, which may optionally be connected to other networks. Ericsson Core is a robust solution where stability of the system is guaranteed by the highly available integrated elements. The solution comes with a pre-configured and verified feature set and capacity in terms of the supported maximum number of users (subscribers/users and devices). Enterprise Core Standalone is providing local EPC and UDC services, whereas in Enterprise Core Distributed case, centralized UDC services are used. Figure 44 illustrates different functions in the different components and the main interfaces between them. The different components used in the solution are Evolved Packet Core (EPC) and User Data Consolidation (UDC).

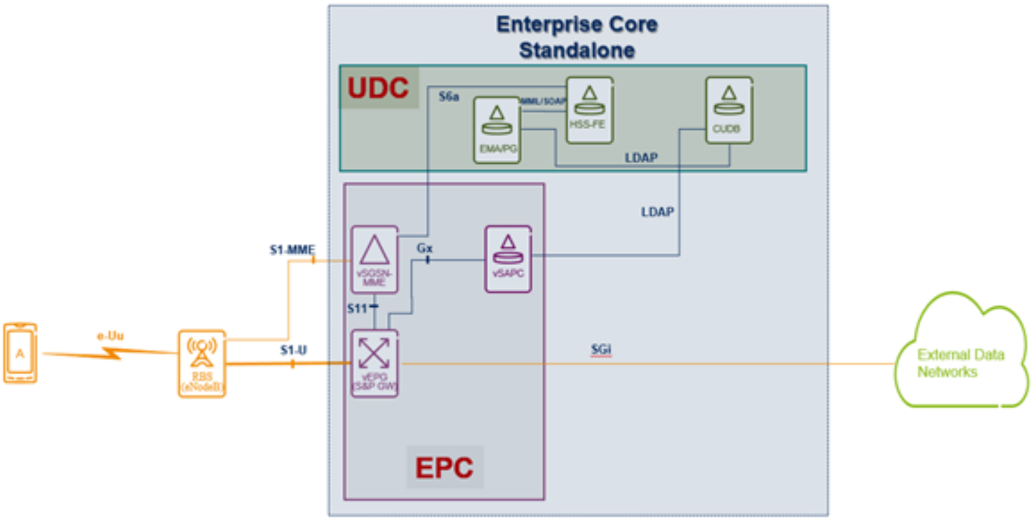


Figure 44: Enterprise Core 5G network architecture.

5.4.2. Cosmote Hellas 4G/5G Core network overview

From the Cosmote side, Ericsson Enterprise Core solution will be deployed at Cosmote's edge DC in a virtualised environment, dedicated only for providing 5G vEPC (vS-PGW, vMME) and vUDC (vHSS & CUDB) functionalities. Since Cosmote has already network-wide enabled NB-IoT functionality, it is proposed to connect the IoT devices by using the commercial IoT vEPC packet core network. Therefore, the overlay core network will only handle critical type V2X traffic with low latency and high throughout requirements. Non-critical and high-latency IoT traffic will be carried over the commercial LTE-A network. Connectivity between the IoT cloud application servers and existing packet core/IoT application servers (IoT Accelerator) should be designed for device and data management.

Finally, it should be noted that the MEC/application servers will be connected at the same edge DC where Cosmote's overlay 5G vEPC is deployed, while 5G UE – MEC/application servers' connectivity will be provided over PGW SGi interface.

5.4.3. Turkcell Turkey 4G/5G Core network overview

From the Turkcell side, the Ericsson Enterprise Core solution, will be used as well for providing 5G vEPC and vUDM functions; same as at Cosmote Hellas side. With this solution vS-PGW, & vSGSN-MME network functions will be provided for vEPC part whereas vHSS and vCUDB network functions for vUDM part.

This vEPC core will also be used for providing NB-IoT access will be interacting NB-IoT UE, sensors etc. as well as Ericsson IoT Accelerator platform which will be provided on Cosmote Hellas side. MEC servers will be connected at the same site where the vEPC is deployed and 5G UE – MEC connectivity will be provided over PGW SGi interface.

5.5. Technologies to be deployed

Table 8 and Table 9 provide a summary of the 5G technologies to be deployed by each operator in the trial site.

Table 8: 5G technologies and attributes for 5G network deployed by Cosmote Hellas

Mobile Core	5G EPC (NSA, opt.3x)
Virtualised infrastructure	Yes (but dedicated for vEPC/vUDM, no space for additional VNFs/virtual servers)
Network Slicing	DECOR functionality is supported over 5G EPC
Orchestrator	N/A
Multiple access Edge Computing	MEC/Application servers will be connected next to PGW SGi interface
Radio Access Network	5G NR (NSA) & LTE
# of sites	1 NR & 1LTE (anchor)
Vendor	Ericsson
# of cells per site	1
# of antennas per cell	1 massive MIMO (64T/64R (128 antenna elements))

Frequencies used	licensed 4G (2600 MHz), licensed 5G (3500 MHz)
Frequency Bandwidth	20 MHz 4G Anchoring + 100 MHz 5G NR
Carrier aggregation	Not in the first phase

Table 9: 5G technologies and attributes for 5G network deployed by Turkcell Turkey

Mobile Core	5G EPC (NSA, opt.3x)
Virtualised infrastructure	Yes (but dedicated for vEPC/vUDM, no space for additional VNFs/virtual servers)
Network Slicing	DECOR functionality is supported over 5G EPC
Orchestrator	N/A
Multiple access Edge Computing	MEC servers will be connected next to PGW SGi interface
Radio Access Network	5G NR (NSA) & LTE
# of sites	3 NR & 3LTE (anchor)
Vendor	Ericsson
# of cells per site	2/2/1
# of antennas per cell	1 Massive MIMO (64T/64R (128 antenna elements))
Frequencies used	licensed 4G (2600 MHz), licensed 5G (3500 MHz)
Frequency Bandwidth	20 MHz 4G Anchoring + 100 MHz 5G NR
Carrier aggregation	Not in the first phase

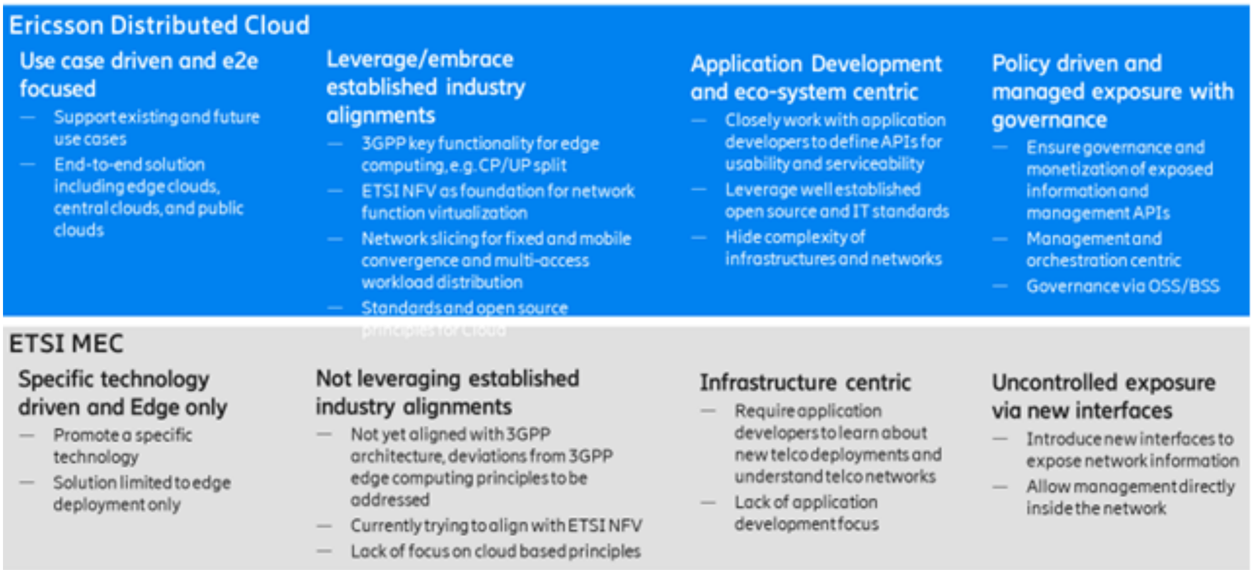
5.5.1. Cellular V2X

During the initial phase of the GR-TR CBC implementation V2X messages may be exchanged among vehicles through LTE based PC5. This functionality will be supported by the IMEC provided C-V2X module build according to 3GPP Rel.14 specifications and described in detail in D2.4 [3]. Once 5G chipsets become available the OBU will be updated accordingly and the C-V2X communication will follow Rel.15 specification. Should the 3GPP Option 2 deployment be instantiated at a secondary phase in the GR-TR CBC, the C-V2X Control functionality should also become available, enhancing the V2X communication.

5.5.2. Multi-access edge computing

Ericsson is not part of ETSI MEC organisation, as ETSI MEC is not aligned with 3GPP architecture. Instead, Ericsson supports and promotes Distributed Cloud architecture. Specifically, distributed cloud is a cloud execution environment that is geographically distributed across multiple sites, including required connectivity in between, managed as one entity and perceived as such by applications. The key characteristic of distributed cloud is the abstraction of cloud infrastructure resources, where the complexity of resource allocation is hidden to an application. Distributed cloud is based on SDN, NFV and 3GPP edge computing technologies to enable multi-access and multi-cloud capabilities and unlock networks to provide an open platform for application innovations.

Ericsson vEPC is supporting Distributed Cloud functionality, enabling optimization of networks to handle for instance low latency applications or local, high, network loads. Distributed Cloud & ETSI MEC comparison is given in Figure 45.



Ericsson Distributed Cloud

Use case driven and e2e focused
- Support existing and future use cases
- End-to-end solution including edge clouds, central clouds, and public clouds

Leverage/embrace established industry alignments
- 3GPP key functionality for edge computing, e.g. CP/UP split
- ETSI NFV as foundation for network function virtualization
- Network slicing for fixed and mobile convergence and multi-access workload distribution
- Standards and open source principles for cloud

Application Development and eco-system centric
- Closely work with application developers to define APIs for usability and serviceability
- Leverage well established open source and IT standards
- Hide complexity of infrastructures and networks

Policy driven and managed exposure with governance
- Ensure governance and monetization of exposed information and management APIs
- Management and orchestration centric
- Governance via OSS/BSS

ETSI MEC

Specific technology driven and Edge only
- Promote a specific technology
- Solution limited to edge deployment only

Not leveraging established industry alignments
- Not yet aligned with 3GPP architecture, deviations from 3GPP edge computing principles to be addressed
- Currently trying to align with ETSI NFV
- Lack of focus on cloud based principles

Infrastructure centric
- Require application developers to learn about new telco deployments and understand telco networks
- Lack of application development focus

Uncontrolled exposure via new interfaces
- Introduce new interfaces to expose network information
- Allow management directly inside the network

Figure 45: Distributed Cloud & ETSI MEC comparison

In 5G-MOBIX project, MEC servers' connectivity with the access network and UEs will be provided over PGW SGi interface. Ericsson vEPC will be deployed closer to RAN network together with MEC servers to provide low latency connectivity.

5.5.3. Network Slicing

At the initial stage of the MOBIX project, Ericsson will create a private 4G/5G network that will be used to process V2X traffic. This can be achieved by enabling DÉCORE functionality (see Section 2.3). However, since in the framework of the MOBIX project an overlay end-to-end network is designed, the required RAN traffic isolation can be achieved by planning a separate IMSI series for the V2X use cases. The roaming restrictions feature is used to restrict the access to a Location Area (LA) or a Geographical Area (GA) for the V2X specified subscribers. When subscribers are denied access to an LA or TA, an operator-configured cause code may be sent to the subscribers. Therefore, in this case:

- A list of IMSI number series for which the roaming restrictions based on IMSI number series functionality needs to be configured;
- A list of TAs or LAs where roaming restrictions will apply.

This can be considered as a basic network slicing mechanism by creating 2 separate networks to handle different applications, i.e., a commercial network for mobile broadband use cases and the private 4G/5G network for V2X applications.

Following the above strategy, the overlay 4G cell, which is used as NR anchor band, will be operated at B7 (2600 MHz) band and using 20 MHz of spectrum bandwidth. B7 band will be exclusively used for V2X applications restricting access to mobile broadband users. Similarly, 5G will be operated at n78 (3420-3600 MHz) band using 100 MHz of spectrum bandwidth, n78F will be exclusively used for V2X applications restricting access to commercial mobile broadband users.

5.6. Contributions from Trial Sites

The 5G network components, features and technologies for the GR-TR cross-border corridor will be provided by Ericsson Hellas and Ericsson Turkey (as described in this section), based on early releases of their commercially available projects, giving 5G-MOBIX the opportunity to be among the first to experience in its trials the advanced performance delivered by these products. It can be understood that the Ericsson 5G products are highly advanced proprietary equipment and features which are the result of years of research and development, and as such cannot really be combined or integrated (at least not within the context of 5G-MOBIX) with 5G products of other (competitive) vendors or even open source 5G equipment / features developed and utilized in the local trial sites of 5G-MOBIX.

For this reason, the concrete contributions of the TSs to the GR-TR CBC have been focused on autonomous vehicles components (including OBU extensions), road-side infrastructure HW and SW as well as Cloud / Edge platform functionality and CCAM application development. As D2.2 is focusing on 5G network infrastructure and technologies, these contributions are not relevant for this deliverable and are hence described in the other WP2 deliverables. More specifically:

DE contribution to GR-TR

Although no concrete 5G network components of DT TS can be integrated at the GR-TR CBC, DE TS CCAM infrastructure and AVs components are designed to take advantages of 5G features and common architectures to be realized in this project. Therefore, some of these components can be integrated with GR-TR CBC CCAM infrastructure and AVs, e.g., LDM and EDM maps software are installed on RSU and OBU, which rely on V2I communication. This allows alternative solutions to cross-border issues developed at DE TS to be trialled as additional scenarios and requirement to evaluate the performance of 5G infrastructure at GR-TR CBC. Details of the contributions to CCAM infrastructure and AV components from DT TS are provided in D2.3 [2] and D2.4 [3] respectively.

FI contribution to GR-TR

The FI TS will not contribute directly in terms of deployment of 5G radio access or core network equipment or software towards the GR-TR CBC. However, the FI TS will contribute device-side (OBU) and CCAM applications that enhance the CBC user story functionality in inter-PLMN and multi-PLMN environments. These contributions are outlined separately in deliverables D2.3 [2] and D2.4 [3] (respective sections on specific TS contributions to CBCs).

FR contribution to GR-TR

FR TS is not contributing to the 5G architecture in the GR-TR cross-border corridor. However, it will contribute on the vehicle side by providing an Encoding and Decoding Functionality for Video Streaming Applications when the link quality changes in the presence of multi-connectivity technologies. More details on this contribution can be found in the respective section of deliverable D2.4 [3].

6. EXTENDED EVALUATIONS

Besides the concrete contributions of the Trial sites to the Cross Border Corridors in terms of HW, SW, platforms, etc., which will be integrated into the CBC infrastructure as described in Sections 4.6 and 5.6 and in deliverables D2.3 [2] and D2.4 [3], the TSs will also engage in additional trials utilizing their own infrastructure (see Annexes). These additional trials or extended evaluations are targeted at complementing the CBC trials by i) evaluating different User Stories and scenarios than the CBCs under a specified UCC, in order to provide deeper insights into the performance of the selected UCCs, ii) addressing and evaluating additional x-border issues than the ones that the CBCs are capable of evaluating, hence providing a more complete analysis of the issues and the most suitable solutions (see [1] for a complete list of which x-border issue is evaluated in which CBC/TS), iii) pretesting network and infrastructure settings, configurations and interconnections in order to facilitate the CBC trial execution by providing optimized information prior to the trials and iv) performing a much larger number of trial tests under controlled conditions, which is not possible at the real-world cross-border settings, in order to verify and enhance the findings of the CBC trials.

This section provides an overview of the complementary work to be carried out at the various TSs per UCC, as well as relevant information for the infrastructure of the TSs that will be used for these extended evaluations.

6.1. UCC#1 Advanced Driving - extended evaluation

The Advanced Driving UCC (UCC#1) is spearheaded by the ES-PT CBC, while complementary trials will take place in the FR, NL and CN Trial Sites. These TSs will contribute to the final evaluation of this UCC in the following manner.

6.1.1. Complementarity & added value to CBC trials

6.1.1.1. FR trial site

For Automated Driving use case category, FR TS is proposing to implement a Collective Perception Service from roadside infrastructure by sending CPM messages to the vehicles (more details are provided in D2.3). Some CPMs as well as other messages (such as CAM, DENM in work zones) need to be sent only to the vehicles which are directly concerned by the event. Current usage of multicast/broadcast communication modes to transmit these packets totally ignore the geo-position of the vehicles resulting on inefficient networking. Besides, the end to end dissemination of these messages is quite difficult due to the different addressing approaches.

To address this problem, FR trial site is suggesting implementing geo-networking on MEC, which is promising for the solution's scalability, while taking into consideration the related challenges. Specifically, when unicasting over Uu interface with TCP/IP networking, the Geo Header will contain a lot of overhead not required for the TCP/IP connection. As direct consequence, URLLC performance will be degraded and will result in a higher latency.

When 5G networks are used for Advanced Driving UCC, security issues are to be taken into consideration. Public Key Infrastructure (PKI) is a promising solution to ensure security aspects of 5G networks. However, the usage of a PKI in automated driving use cases to assure the integrity and authenticity of the messages exchanged between vehicles presents a certain number of challenges. In fact, the continuity of authenticity and integrity of automated vehicles crossing the border are the most primordial security requirements that must be satisfied in order to enable such manoeuvre. Therefore, an authentication-based handover scheme that ensures seamless and secure mobility management of automated vehicles crossing the border is needed.

6.1.1.2. NL trial site

The NL trial site will develop a solution for making an inter-PLMN handover in de NSA and SA case. The trial site will start with a non-optimized handover and go with incremental steps to a more optimized handover. Session continuity and no session continuity will be researched in the context of NSA to SA or SA to SA handovers. The timeline for deploying a SA core network in planned in 2020 and the main focus of the NL trial site will be on SA deployment. With this deployment pre trials are executed. In addition, LADN and service discovery is implemented to have the vehicle connect to the closest edge. Both technologies should be aligned to make sure the application is aware of the "changing" edge locations and set of applications that run on them.

A knowledge sharing workshop will be organized to share the lessons learned from the SA deployment in NL. As the CBC is planning to rollout SA later in time then the NL trial site, the CBC can use the results of the research in deploying a SA solution in the CBC.

Complete end-to-end 5G network slicing will also be implemented. The trial site will deploy at least two network slices in the KPN and TNO network. Two slices will be deployed for, V2X messages and generic data. The slices will be deployed end-to-end, which means in the radio and the core. It is unlikely that the CBC will implement slicing, therefor this research is complementing to CBC with an extra research angle.

6.1.1.3. CN trial site

CN trial plans to contribute to CBC trials/evaluations as follows: (1) Focus on edge computing for X-border scenarios with Multi-MEC handover. This situation is applicable to a handover between MEC platforms. It resolves a problem that provision of application data by an MEC platform to UE is interrupted when the UE is being handed over between access network devices, thereby providing continuous services to the UE. (2) Coordinated overtaking with collision avoidance and lane changing maneuvers. When a vehicle is in a procedure of overtaking with collision avoidance, its sub-procedure is lane changing maneuvers. This vehicle would go out of track if these two procedures do not coordinate well. The procedure would jump into the sub-procedure and without no reason jump out at collision avoidance procedure. (3) Provide seamless CCAM service for constantly changing areas. CCAM service can help when the signal areas with full coverage, seamless CCAM service is similar to Multi-MEC handover technology, CCAM service focus more on signal processing, including antenna and radio technology, it handles the difficulty of differentiating the signal from one agent at an area and the other area.

6.1.2. Additional facilities for UCC#1 evaluation

6.1.2.1. FR trial site

CAM messages are generated by ITS vehicles and broadcasted over PC5 interface. Thus, all ITS stations (including other vehicles, RSU, MEC) within the coverage area of the sender will receive CAM and decode it to obtain information about its geo-position. Since MEC will receive all CAM messages from ITS vehicles within its coverage area, it is able to maintain information about their geolocation. For advanced driving operations, some messages like CAM or DENM need to be relayed to the concerned distant vehicles which are out of the coverage of the sender or which are already in the coverage but don't have PC5 interface. FR TS proposes to relay these messages by the MEC node using its 5G coverage. However, if MEC will use broadcast transmission mode, all vehicles in the 5G network coverage will receive these messages, including those which are not relevant.

For all these reasons, FR TS is proposing to use Geo-casting by the MEC in order to filter destination vehicles based on their location compared to the geo-cast area (identified by its geo-address), which will clearly enhance the network efficiency. Besides, MEC will be able to identify non PC5 vehicles (in the coverage area of the sender) in order to forward the message to them. Furthermore, FR TS is proposing a relevant solution to the overhead problem by sending geo-cast messages without geo header. In fact, the message will be sent with its initial format over IP without adding the geo-header since the destination vehicles (and their addresses) were already selected by the MEC.

From security perspective, the 5G communication architectures deployed in different countries could implement different authentication procedures with different security levels. This heterogeneity could lead to incompatibility problems especially when dealing with handover procedure at cross border and could even be the source of some security threats. To cope with this problem, the French trial site suggests using common trust domain EU CCMS (European Union C-ITS Security Credential Management System). Moreover, the FR site suggests deploying Virtual Access Node (VAN) on the MEC which will be used as intermediate Certification authority that will issue certificate to the vehicles. Having two MECs connected in the border via high speed connectivity (fiber) allows the VANs to collaborate in order to verify the certificate signature and the certificate chain to authenticate the automated vehicles crossing the border. Indeed, we suppose that each VAN can monitor automated vehicles under its control, which can be ensured by the SDN functions.

A more detailed description of the FR TS 5G infrastructure can be seen in ***Annex 7***.

6.1.2.2. NL trial site

Currently there is no CBC where a SA is implemented on both sides. Bringing a SA core to a CBC is to complex. At the local trial site more focus can be given to testing different core setups, including SA to SA and NSA to SA.

A more detailed description of the NL TS 5G infrastructure can be seen in ***Annex 8***.

6.1.2.3. CN trial site

This site brings the method of coordinating overtaking with collision avoidance and lane changing manoeuvres. The experiment of this scenario would cause collisions of vehicles if it does not go properly, so the site is unmanned when experiments are in progress. The expected results of this evaluation would be that vehicle can overtake when its lane is changing with collision avoidance.

A more detailed description of the CN TS 5G infrastructure can be seen in ***Annex 9***.

6.2. UCC#2 Platooning - extended evaluation

The Platooning UCC (UCC#2) is spearheaded by the GR-TR CBC, while complementary trials will take place in the DE and CN Trial Sites. These TSs will contribute to the final evaluation of this UCC in the following manner.

6.2.1. Complementarity & added value to CBC trials

6.2.1.1. DE trial site

The implementation of the platooning user story "eRSU-assisted platooning" at the German TS detailed in [1] cover more complex scenarios compared to the implementation at GR-TR CBC. Most significant requirements for the communication infrastructure at DE TS are the heavy reliance on eRSU infrastructure for the dynamic deployment of CCAM services and the deep integration of 5G networks and distributed MEC infrastructure to guarantee QoS requirements, service continuity, and efficient resource management. As a result, while also adopting the high-level 5G NSA option 3x, the deployment of 2 LTE/5G networks at DE TS has varied features and focuses allowing the trials of alternative and complementary E2E architecture supporting "Vehicle platooning" UC. We next provide an overview of the differences of DE TS 5G overall architecture, supported scenarios, and evaluation of the UC trials at DT TS. Specific details of the DE TS 5G architecture are provided in Annex 5.

5G architecture overview

Core networks: Two LTE/5G network cores are deployed at DE TS, a MNO's 5GC and an in-house developed vLTE core. This allows the trials of platooning operations with similar settings and requirements of CBCs, e.g., Multi-PLMN handover. Additionally, the vLTE core allows experimentation with alternative novel approaches, which are not available with MNO deployment, i.e., E2E network and service orchestration, network slicing, multi-domain network, simulated security scenarios, among others.

RAN: The autonomous driving trials at DE TS are carried out on the same road with real traffic. A great focus is put on the digitalization of the road to support AV's operations. Therefore, the RAN network serves as the main communication infrastructure for sensor data and messages exchange among different entities, e.g., AV, distributed sensors, CCAM services, among others. The deployment of MEC component to the road side eRSU (near edge) enhances the road infrastructure to a computing platform with heterogeneous radio technologies, which extends the central cloud platform by using 5G network as the backbone. The interaction between the road infrastructure provider and communication service providers must rely on flexible infrastructures and an autonomous and efficient management platform.

Roaming: To fully test cross-border settings, 5G System roaming architectures specified in 3GPP TS 23.501 will be implemented/configured, i.e., with local breakout with service-based interfaces within the Control Plane or with home routed and service-based interfaces within the Control Plane. The interactions between EPC and eRSU infrastructure (in non-3GPP access mode) will also be investigated. Novel mobility management approaches that employ the distributed, software defined, and virtualized infrastructure are also designed to extend the 5G capabilities.

C-V2X: With a great focus on roadside infrastructure for AD, 5G C-V2X architecture is implemented at DE TS. In combination with the flexible MEC and cloud computing platform, various V2X communication approaches are designed to provide context and location based CCAM services with the required QoS and service continuity.

MEC: Edge computing plays an important role in the DE TS network solutions to support AD, especially near edge at roadside infrastructure as opposed to solutions based on cloud and MEC in transport network segments. In combination with the low latency MEC infrastructure directly attached to the 5G core, self-organizing AD infrastructure can be realized with increased QoE and efficiency. Such infrastructure is envisioned to enable new business models and interaction platform for MNO, road infrastructure provider, ITS service providers.

Network slicing: The AD test road at DE TS also serves as a platform for investigating interactions among stakeholders who build, design, and operate the road and communication infrastructure under certain policy framework. To enable such complex stakeholder relationship and diverse business objectives, a flexible and adaptive E2E infrastructure is required to achieve dynamic service composition and resource efficiency. As the result, on-demand service provisioning for changing network and computing requirements of the AD scenarios can be possible with an autonomous composition of suitable edge, cloud and network resources in a way that maximizes resource efficiency and stakeholders' objectives. All infrastructure components are made slice-able and governed by an autonomous management and orchestration platform.

Trial scenarios overview

The DE TS infrastructure is designed to investigate vehicle platooning operation in mixed traffic. 5G communication network plays an important role of connecting various software, sensors, and a computing platform to create a digital road for AVs. The trials cover various scenarios for testing AD in cross-border settings, stakeholder interactions, multi-domain network management, etc. Some example scenarios are:

- MNO network handover during platooning operation with overtaking manoeuvre.
- Autonomous CCAM services composition and deployment in distributed edge with traffic situation awareness.
- Data flows management for the discovery of sensor data source and their compositions distributed and mobile data fusion and AD decision making components.

Trial evaluation and complementary

The DE AD infrastructure is designed as an open system allowing mixed use cases and technologies to be incorporated to enable AD operations. As a testbed, novel approaches and interaction models can be implemented to investigate the constraints and to benchmark the realization of AD implementations. At DE TS, novel approaches for E2E management and service-oriented realization of various infrastructure components to achieve higher level of autonomy and resource efficiency are developed and tested. The evaluation of these approaches can provide reference performance limitations and possible extension to improve the standardized and constrained deployment at another CBC and TS.

6.2.1.2. CN trial site

CN site will test in areas such as bridge, long steep slope, ramp, toll station and some others. These scenes tend to be no overtaking for some safety regulations. It is difficult to place enough infrastructures because of the harsh environment with limited room. When a platoon runs on the bridge or long steep slope, it is more important for each vehicle to receive the information in case any risky situation. Also, platooning with remote driving is different from single vehicle with remote driving. Not only the head of the platoon will be controlled, the rest of vehicles will be monitored as well. Especially, the tail of the platoon would show the detail of the whole scale of situation of the platoon.

6.2.2. Additional facilities for UCC#2 evaluation

6.2.2.1. DE trial site

With the main focus on eRSU assisted platooning scenarios and E2E service and network orchestration. The DE TS deployment features an extensive deployment of 10 eRSUs along the test road. Beside the primary 5G infrastructure for E2E connectivity, the eRSUs are also directly connected with P2P WLAN and mmWave backbone. As the result, the eRSUs network can be a digital layer on itself to support AD operations. It also serves as a fallback and reference benchmark infrastructure to test demanding AD modes without interrupting the trials. The eRSUs infrastructure is closely integrated with extensive roadside sensor deployment and the central cloud-based management and orchestration platform. Although each component is designed to be modular with well-defined interfaces for each functional block, a fully integrated infrastructure is required for the intended trials. Such extensive deployment of DE TS is rather difficult to be replicated at other CBCs and TSs. However, certain infrastructure components could be integrated with CBCs deployment for added capability. The functional design and interfaces of the DE TS components are therefore closely aligned with those of other 5G MOBIX CBCs and TSs.

A more detailed description of the DE TS 5G infrastructure can be seen in ***Annex 5***.

6.2.2.2. CN trial site

Platoons in CN site will be implemented in such scenes like bridge, long steep slope, ramp, toll station. The experiment of this scenario must simulate some tough environments because current infrastructures have no appropriate conditions to build such RSUs or communication base stations. The evaluation results would show that platoons can past safely in flat areas and relatively high rate of safety when go past through rough condition areas.

A more detailed description of the CN TS 5G infrastructure can be seen in ***Annex 9***.

6.3. UCC#3 Extended Sensors - extended evaluation

The Extended Sensors UCC (UCC#3) will be implemented in both the ES-PT and GR-TR CBCs (with different USs), while complementary trials will take place in the DE, FI and NL Trial Sites. These TSs will contribute to the final evaluation of this UCC in the following manner.

6.3.1. Complementarity & added value to CBC trials

6.3.1.1. DE trial site

The implementation of the extended sensor user story “dynamic map with surround view” at the German TS detailed in [1] covers more complex scenarios compared to the implementation at GR-TR CBC. Like the implementation of platooning UCC, the most significant requirements for the communication infrastructure at DE TS are the heavy reliance on eRSU infrastructure for the dynamic deployment of CCAM services and the deep integration of 5G networks and distributed MEC infrastructure to guarantee QoS requirements, service continuity, and efficient resource management. We next extend the complementary discussion of DE TS infrastructure for platooning in Section 6.2.1.1 w.r.t extended sensor trials. Specific details of the DE TS 5G architecture are provided in Annex 5.

Trial scenarios overview

5G communication network plays an important role of connecting various software, sensors, and a computing platform to create a digital road for AVs. The trials of "dynamic map with surround view" user story cover various scenarios for testing AD in cross-border settings, stakeholder interactions, multi-domain network management, etc. Some example scenarios are:

- MNO network handover during AD operation with share environment perceptions.
- Autonomous CCAM services composition and deployment in distributed edge with traffic situation awareness. The focus is on surround view and perception services with high QoS and QoE experiment demands.
- Data flows management for the discovery of sensor data source and their compositions distributed and mobile data fusion and AD decision making components.

Trial evaluation and complementary

The DE AD infrastructure is designed as an open system allowing mixed use cases and technologies to be incorporated to enable AD operations. As a testbed, novel approaches and interaction models can be implemented to investigate the constraints and to benchmark the realization of AD implementations. At DE TS, novel approaches for E2E management and service-oriented realization of various infrastructure components support the demanding 360° surround view and massive sensor data exchanges among AVs and AD road components. The evaluation of these approaches can provide reference performance limitations and possible extension to improve the standardized and constrained deployment at another CBC and TS.

6.3.1.2. *FI trial site*

The CBCs utilize MEC platforms for processing of sensor data (typically video) received from the vehicles. In all cases the MEC platforms are associated with a specific PLMN and the vehicle discovery and registration to a particular MEC is static. To that end, migration from one MEC to another only occurs when vehicle roams between the PLMNs. This may present some challenges, for instance, when visited MEC has limited capacity. The FI TS user story "US3 Extended sensors with redundant Edge processing" will address this challenge by developing and evaluating dynamic approaches for MEC discovery, registration and migration. When considered in terms of the cross-border issues identified in the project, FI TS places specific focus on the following telecommunications related issues (outlined previously in D2.1 [1]):

- TC2 Performance Continuity
- TS2 Edge Service lifecycle

6.3.1.3. NL trial site

The NL trial site will develop a solution for making an inter-PLMN handover in the NSA and SA cases. Complete end-to-end 5G network slicing will also implemented. These contributions are also described in section 6.1.1.2. The solutions will be tested and developed for both UCCs.

6.3.2. Additional facilities for UCC#3 evaluation

6.3.2.1. DE trial site

Refer to section 6.2.2.1 for the summary of specific infrastructure components and ***Annex 5*** for detailed description of DE TS 5G infrastructure.

6.3.2.2. FI trial site

The FI TS user story US3 Extended sensors with redundant Edge processing provides the context for evaluating scenarios that involve dynamic discovery, registration and migration between MEC platforms belonging to different PLMNs. As noted previously this is distinct from the static approaches is originally considered in the CBCs.

The evaluation scenarios leverage the multi-MEC multi-PLMN environment provided at the FI TS. Specific test cases include one case, whereby, a vehicle sending video upstream to video processing/aggregation service located in a MEC. The set of services provided via the MEC include distributed map generation based on crowdsourced video/images, cooperative situation detection (e.g. real-time obstacles detection and information sharing) and information sharing through edge caching. In the first test case, the vehicle is connected to PLMN1 and may be dynamically assigned a new video processing/aggregation service with a different MEC server (associated with PLMN2) due to capacity constraints in MEC of PLMN1. In another test case, the vehicle located in the coverage area of PLMN1 receives the aggregated information from video processing service in the associated PLMN (that is, PLMN1). When the vehicle roams to a different PLMN2 it will be dynamically associated to a different broadcast service from MEC of PLMN2 (contingent on the availability of availability of resources on this visited MEC).

The FI TS environment provides a useful testing ground due to the higher-level experimentation feasible on the site (unlike the more controlled CBC sites). This includes possibilities to test dynamic MEC functionalities under different 4G/5G network configurations and handover scenarios. A more detailed description of the FI TS 5G infrastructure can be seen in ***Annex 6***.

6.3.2.3. NL trial site

Currently there is no CBC where a SA is implemented on both sides. Bringing a SA core to a CBC is too complex. At the local trial site more focus can be given to testing different core setups, including SA to SA and NSA to SA.

A more detailed description of the NL TS 5G infrastructure can be seen in ***Annex 8***.

6.4. UCC#4 Remote Driving - extended evaluation

The Remote Driving UCC (UCC#4) is spearheaded by the ES-PT CBC, while complementary trials will take place in the FI, NL, CN and KR Trial Sites. These TSs will contribute to the final evaluation of this UCC in the following manner.

6.4.1. Complementarity & added value to CBC trials

6.4.1.1. FI trial site

The user stories under the remote driving UCC in the ES-PT CBC (see [1]) is implemented in corridor areas that consider a single PLMN on either side of the border. This includes portions of the corridor under coverage of one PLMN further away from the border, plus an area in the vicinities of the border (on either side) whereby there is overlapping coverage form the two different PLMNs. The latter area presents the region for testing the performance impacts on remote driving service as the vehicle drives across the border and roams from PLMN to another (in conventional roaming process).

However, there exist other multi-PLMN scenarios, which cannot be easily recreated in the aforementioned CBC setting. One of these cases is when a remote driving scenario occurs for a vehicle under the coverage area of two or more PLMNs (even from the same country). This presents an opportunity to allow the vehicle maintain redundant attachment to multiple PLMNs and ensure zero connection downtime even as one PLMN connection degrades or is lost.

The FI TS user story "*US2 Remote driving in a redundant network environment*" addresses this challenge remote driving service continuity that leverages the presence of multi-PLMN coverage in various road segments. Moreover, the user story considers the case when roaming between PLMNs also triggers transfer of control of the vehicle from one remote operations center (ROC) to another (current CBC only considers a single ROC). When considered in terms of the cross-border issues identified in the project, FI TS places specific focus to the following telecommunications related issues (outlined previously in D2.1 [1]):

- TR1 NSA Roaming Latency
- TH1 Hybrid Handover Latency

6.4.1.2. NL trial site

The NL trial site will bring added value beyond the CBC trial by implementing positioning based on 5G mm-wave technology. The trial site will first develop the mm-wave positioning around the 26 GHz frequency. Then this technology will be evaluated by the trial site and the results will be shared with the CBC. Also, it is the intention to make a comparison with sub-6GHz technology for which an algorithm will be developed that can handle mm-wave and sub-6GHz. Next to this, different modalities of positioning will be evaluated depending on degradation of sensors. Also, the capacity boost, reduced interference and a more viable connection introduced by mm-wave will be evaluated.

The CBC will not implement mm-wave and therefore the NL trial site will have the possibility to extend the CBC research scope with mm-wave positioning & application of mm-wave to other aspects of the UCC (such as video streaming). A potential evaluation of the developed algorithm at sub-6GHz may be considered, depending on the outcome of the tests at NL Trial Site, allowing to forecast improvement that could be achieved at the CBC if mm-wave were deployed.

6.4.1.3. CN trial site

CN trial site will have real-time 5G-based HD video. An HD video backhaul test has been performed, which employed a manned vehicle to transmit HD video back to the control center via 5G. Meanwhile, the control screen showed road condition in real time. The next step is to make a remote driving test in multiple trial scenes, especially places like a tunnel, which would influence the transmission of 5G signal. Also, the topography and landform condition is essential for evaluation of 5G-MOBIX CCAM. Remote driving in CN trial site will pay more attention to the topography and landform condition such as steep slope or tough terrain situation. Thus, vehicles must take actions according to their situation.

6.4.1.4. KR trial site

The KR trial site considers remote driving vehicle (RDV) based on mmWave-band V2I/N communications (22~23.6 GHz), to ensure the safety of the RDV. The real-time high definition multi-video live streams (front, left and right side, and rear) and surrounding environmental data sharing with a remote site will be considered. Besides, the KR trial site also focuses on forward-object tracking to compensate for network delay due to uncertain network congestion. To achieve key performance indices, the KR trial site brings mmWave-band V2I/N communication as a 5G NR infrastructure with a standalone system while ES-PT CBC trial sites using 5G NR (3.5GHz). The test results of the KR trial site will be compared with the European trail site for improving overall remote driving performance in terms of massive data rate and latency.

6.4.2. Additional facilities for UCC#4 evaluation

6.4.2.1. FI trial site

The FI TS user story user story *US2 Remote driving in a redundant network environment* provides the context for evaluating multi-PLMN scenarios in the remote driving context. The current ES-PT CBC is currently considering remote driving where the vehicle has only one PLMN attachment at any given time. However, as noted previously in Section 4.6, there are tentative plans for transferring and testing multi-PLMN solutions in the ES-PT CBC.

In the FI-TS, two scenarios are considered for evaluation. In the first scenario, a vehicle in remote driving mode while simultaneously attached to two PLMNs. In this multi-PLMN case the remote driving service restoration or continuity is tested when attachment to the active (home) PLMN is lost. Additionally, Impact on remote driving service quality analyses when this redundancy is provided in a multi-RAT (LTE, 5G-NR) multi-PLMN environment. In the second inter-PLMN (roaming) scenario a vehicle in remote driving mode traverses from one network to another whilst the vehicle leverages the inherent redundancy in PLMN coverage overlapping areas. Performance impacts on remote driving are analyzed as in previous case. Additionally, impact is also analyzed for remote driving service quality when roaming between PLMNs with two different RATs (LTE, 5G-NR). The latter evaluation scenario may also include the handover from ROC to another (emulating the cross-border case). A further complex test case that could be considered is when roaming from one country to another also requires the vehicle to maintain dual-PLMN connectivity.

As was noted previously, the evaluation scenarios leverage the multi-PLMN environment provided at the FI TS, whereby, the site has access to up to ten distinct PLMN IDs. Furthermore, the experimental nature of the FI TS network, allows compact analysis of critical network events, e.g. inducing network failure, that may trigger multi-PLMN redundancy mechanisms. Moreover, the multi-PLMN network testbed allows testing different 4G/5G network configurations and handover scenarios. A more detailed description of the FI TS 5G infrastructure can be seen in ***Annex 6***.

6.4.2.2. NL trial site

The NL trial site will deploy a 26GHz mm-wave 5G network for investigation of 5G positioning with mm-wave. The NL trial site has obtained a test license for this frequency. As the deployment will be based on experimental mm-wave hardware and as its integration puts strong requirements on the radio access network, it is not feasible to deploy a mm-wave network at the CBC.

A more detailed description of the NL TS 5G infrastructure can be seen in ***Annex 8***.

6.4.2.3. CN trial site

5G-based HD video in this site could be transmitted with no information loss in real time. When a video is transmitted, the video would be processed by using some image processing technologies, if the video is recorded from actual cross-border, the processing step would cost plenty of time. That would cause a long delay which would reduce the safety and operability of remote driving. The evaluation results would show that 5G-based HD video can play smoothly, and the delay time can be reduced to less than 20ms. The infrastructure supporting these requirements can be seen in more detail in ***Annex 9***.

6.4.2.4. KR trial site

The KR trial site will bring a remote driving vehicle based on mmWave-band V2I/N communications (22~23.6 GHz) while ES-PT CBC trial sites develop remote driving technology based on 5G NR with a frequency of 3.5GHz. The KR trial site focuses on how we provide high bandwidth capabilities in order to provide real-time multi-video streams (front, left and right side, and rear) and surrounding environmental data sharing with a remote site. Since the KR trial site and ES-PT CBC trial site use different 5G frequency bands (22~23.6GHz vs. 3.5GHz) and 5G NR system (NSA vs. SA), the test results will be compared with the results from ES-PT CBC trail sites in terms of massive data rate and latency. A more detailed description of the FR TS 5G infrastructure can be seen in ***Annex 10***

6.5. UCC#5 Vehicle QoS support - extended evaluation

The Vehicle QoS Support UCC (UCC#5) is spearheaded by the ES-PT CBC, while complementary trials will take place in the FR and KR Trial Sites. These TSs will contribute to the final evaluation of this UCC in the following manner.

6.5.1. Complementarity & added value to CBC trials

6.5.1.1. FR trial site

ES-PT CBC are envisaging to implement only 5G to 5G roaming between two MNOs on the border which implies that 5G coverage is available all the time. FR trial site is considering that 5G coverage gap may exist when compared to the already existing 4G network, especially at early deployment of the 5G networks. Thus, FR trial site is considering the coexistence of hybrid network technologies (4G, 5G, Satcom) with different link qualities.

The coexistence of these hybrid network technologies can lead to incompatibility problems especially when dealing with handover mechanism and which could be a source of many security attacks. In fact, due to the reduced size of deployed cells, the handover could occur frequently which can increase the risk of security attacks. Therefore, the deployment of security schemes that can fit the coexistence of hybrid network technologies with different link QoS and that ensure a safe handover operation are mandatory.

6.5.1.2. KR trial site

KR trial site considers a user story where passengers inside a vehicle enjoy data consuming services such as online gaming, video streaming, social networks, etc. with the help of tethering. It will attract more and more attention since the more cars get equipped with the advanced levels of the autonomous driving, the more drivers feel the necessity of staying connected to spend the free time, which can be a main driver for this use case. In this respect, both public sector (including local government) and public transportation operator may have strong interest since citizens using public transportation can be benefited from the onboard public Wi-Fi service. Also, wireless equipment vendors can have strong interest considering the attractiveness of the new market opportunity.

Moreover, KR trial site aims to validate the feasibility of mmWave-band V2I/N communications by showcasing a variety of onboard mobile services and its performance far superior to the other existing V2X communications in terms of data rate and latency.

6.5.2. Additional facilities for UCC#5 evaluation

6.5.2.1. FR trial site

Inter operator roaming proposed by ES-PT CBC will cause connection loss while the vehicle is moving from one country to another. Meanwhile, FR trial site considers that supporting service continuity is mandatory for the implementation of QoS related scenarios. In order to ensure this, FR site will implement seamless Handover between the different technologies present at the closed test site (5G<->Satcom, Satcom<->4G, 5G<->4G, 5G<->5G) with QoS adaptation performed by the vehicle to adjust its transmission parameters according to the available link quality (see D2.4 for more details). The preparation and the execution phases of Handover are based on OBUs intelligence at the vehicle (more details are provided in D2.4)

In order to enable such intelligence and to ensure its flexibility through programmable network architecture, FR trial site considers that a Software defined Networking (SDN) needs to be implemented. Based on SDN functionalities deployed on the MEC, a PKI certificate-based handover scheme will be implemented by FR trial site which can monitor automated vehicles movements and predict their future positions. Therefore, the latter will allow the identification of the target cells and anticipate on this information in order to initiate an authentication handover that ensures a seamless and secure mobility management of automated vehicles in the presence of a hybrid environment of technologies.

A more detailed description of the FR TS 5G infrastructure can be seen in ***Annex 7***.

6.5.2.2. KR trial site

KR trial site is particularly focusing on providing broadband Wi-Fi service inside a vehicle including public transportation like a bus. In order to support such in-vehicle wireless connectivity, mmWave-band mobile backhaul link between base stations installed along the road and onboard terminals deployed at a vehicle will be implemented and tested. Since KR trial site is the only TS in the project that is currently developing 5G NR-based V2I/N system operating at a mmWave band (22~23.6 GHz), KR trial site is not a part of actual cross-border, but considered as a separate trial site that could bring added values to the project.

Since the 5G NR-based V2I/N system operates in mmWave band, such broadband onboard connectivity is enabled by supporting system bandwidth of up to 1 GHz, and it is also designed to support various key enabling technologies to solve the technical challenges typically encountered in mmWave-band vehicular communications. One of most important key technologies to be showcased with the trial platform is fast open-loop beam switching technique which allows vehicle terminals to perform Tx and Rx beam switching without any feedback from base station. A more detailed description of the FR TS 5G infrastructure can be seen in ***Annex 10***

6.6. Overview of extended evaluations

An overview of the complementarity and contributions of the TSs with respect to the CBCs and the commonly addressed UCCs, can be seen in Table 10.

Table 10: 5G-MOBIX Use Case Categories & User Story classification

Trial site	Advanced Driving	Vehicles Platooning	Extended Sensors	Remote Driving	Vehicle QoS Support
ES-PT	Complex manoeuvres in cross-border settings		Complex manoeuvres in cross-border settings	Automated shuttle remote driving across borders	Public transport with HD media services and video surveillance
	Automated shuttle remote driving across borders		Public transport with HD media services and video surveillance		
GR-TR		Platooning with "see what I see" functionality in cross-border settings	Extended sensors for assisted border-crossing		
			Platooning with "see what I see" functionality in cross-border settings		
DE		eRSU-assisted platooning	EDM-enabled extended sensors with surround view generation		
FI			Extended sensors with redundant Edge processing	Remote driving in a redundant network environment	
FR	Infrastructure-assisted advanced driving				QoS adaptation for Security Check in hybrid V2X environment
NL	Cooperative Collision Avoidance		Extended sensors with CPM messages	Remote driving using 5G positioning	
CN	Cloud-assisted advanced driving	Cloud-assisted platooning		Remote driving with data ownership focus	
KR				Remote driving using mm Wave communication	Tethering via Vehicle using mm Wave communication

7. CYBER-SECURITY & DATA PRIVACY ASPECTS

5G is being developed with new architectural concepts and capabilities to enable new business models and to provide enhanced applications and services to network subscribers. To ensure that 5G fulfils its promise, all security matters accompanying the 5G architecture need to be addressed. The security architecture presented here has been developed in the 5G-ENSURE project [38] and can be seen as an evolution based on the existing security architectures for 3G [39] and 4G [40]. The basic concepts, e.g. domains and strata, remain, but have been adapted and extended to fit and cover the 5G environment.

In [41] and the 5GPPP (Phase I) Security Landscape white paper [42], the need for a new security architecture for 5G is discussed and motivated and an initial draft is presented. The work covered here, backed by the 5GPPP WG on Security, leverages on what has been described in both documents. The most important architectural aspects missing in the earlier 3G/4G security architectures are those of *softwarization*, virtualisation, trust models covering all players in the 5G ecosystem, multi-domain/multi-tenant (also slice concept) management and orchestration and new mission critical cyber threats.

In Section **Error! Reference source not found.** the main 5G security premises in CCAM are addressed. Then an overview of security concepts is shown in 7.1.1. Thus, security threats and risks are discussed in Section 7.1.2 and privacy properties driven in 5G in Section **Error! Reference source not found.**. In Section 7.2 the required architectural security modules in 5G are listed. In Section 7.3 the impact of the GDPR law in 5G operation is analysed. And finally, the security requirements are listed in Section 7.4.

7.1. 5G Security Premises in CCAM

In our current network infrastructure, we are becoming massively interconnected, which implies that we must coexist with people and systems of unknown trustworthiness. This infrastructure depends on the proper functioning of many systems, which have serious potential security vulnerabilities. Their exploitation could cause massive disruptions. These problems must be properly addressed, and, preferably, before a disaster happens, especially in CCAM environments where human lives are at stake.

Few large development projects are developed on time, on budget, and with acceptable functionality. Complex systems require intelligent, well-trained, and experienced workforce, especially when critical requirements are involved. The absence of any particular expertise can reflect adversely in the resulting systems. The vulnerabilities in the existing infrastructure are poorly understood, and the risks that may result from them tend to be seriously underestimated. This lack of awareness of developers, vendors, users, and even governments, can result in critical problems that could have been avoided.

7.1.1. Overview of security in networks

In general, the security areas that receive more importance in networked systems are: confidentiality, authorization, integrity, privacy and non-repudiation. Regarding 5G systems it was decided to categorize the identified threads based on the ITU-T x.805 “security dimensions” [43] herein reported: access control**,** authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy.

In terms of information management, it is important to notice the relevance that confidentiality has. The information sent by an individual should not be in any case revealed to any party that is not the intended original recipient, as well as the secure storage of the data plays a key role into the security ecosystem. Additionally, confidentiality also implies that inferring the parties’ identity implied in the communication should be avoided. In consequence, this issue is related to limiting the access to the authorized individuals to systems, avoiding the entrance of non-trusted foreign users that may result in unwanted behaviours.

Although an attacker could not extract any information from the exchange, it can modify the messages to spoil the communication and, therefore, integrity mechanisms must be included in the system. In this line, the only action an attacker may perform is related to the system itself, inducing a malfunctioning on it. Thus, the availability of the services must be assured as well.

Desires for privacy and anonymity are generally incompatible with the desire for accountability, attempts to create completely anonymous services tend to run counter to practical notions of authenticity, integrity, revocability, or non-reputability. There are also privacy risks relating to monitoring and surveillance activities, which include the misuse of the information obtained. Ideally, a trade-off must be found between privacy and accountability, and that balance must be carefully guarded. Therefore, it is desirable to minimize the information that is monitored and to strictly control who has access, and to ensure the correct identity of all individuals engaged in risky activities. Otherwise, deviations may result in compromise of privacy or accountability, or both.

7.1.2. Security in 5G networks

The first assumption that is made about 5G security is that it must include all security already provided in pre-5G networks, and improve them if necessary, to cope with the new services and user needs. Apart of that, standardization bodies have been adding to the new 5G technology some novel concepts such us Network Function Virtualisation (NFV), Cloud Computing, Software-Defined Networking (SDN), Multi - access Edge Computing (MEC) and Network Slicing, in order to reach a full *softwarised* mobile network. In addition, new communication scenarios have been incorporated to the standard with different and specific requirements of QoS. Apart from the usual service of providing voice and data connectivity to mobile customers (Enhanced Mobile Broadband), Ultra-reliable and low latency communications (URLLC) and massive machine-type communications (mMTC/IoT) are now considered. Keeping all these new services safe and secure is a great challenge and may introduce new threats that should be addressed. 5G-MOBIX project is more related to this URLLC that supports perfectly the requirements of vehicular networks.

Since the adoption of IP protocol in the core network in 4G, mobile networks have inherited all the security threads and risks of IP networks and the Internet world. 5G has indeed a more difficult challenge with the addition of millions of IoT devices that will be connected, that are the perfect target to attackers in order to perform DoS and botnets attacks among others. In addition to this, 5G has to focus on the huge fleet of vehicles that circulates roads and highways and analyse the new threads and risk that this new king of network may introduce, especially when there may be human lives in risk.

According to their new security requirements introduced by the new actors, the NGMN Alliance, an important organization focused on providing guidelines and recommendations about 5G, helped us to identify some of the most probable threats that could appear. We list them in Table 11.

Table 11: Threats and risks related to 5G

5G technologies	Threats
5G Access Networks	• Expected high traffic either malicious or accidental. Reduce traffic changers whenever possible and be flexible for maintaining system performance. • Risk of key leakage between operator's links. • Optional security implementation offers security threat. • Subscriber device level security in 5G due to roaming routed IP traffic in 5G. • Exhaustion of signalling plane with several devices that gain access simultaneously. • Exhaustion of signalling plane with several simultaneously and intermittently data transfer devices. • Stopping services for several devices due to traffic overload is sometimes a trick by an attacker. • Bulk configuration leading to bulk provisioning.
VNF	• Inter-operability issues. Different VNF providers. • DoS / DDoS attacks • Software flaws could appear in different VNF implementations • VM escape attack, when a malicious virtual machine can escape out of the virtualisation environment and hypervisor influence
MEC	• MEC deployment billing risk. Periodic polling from UE to core network to cross check received charging records from edge. A new or similar mechanism like that of 3GPP. • MEC applications run on the same platform of network function. A new framework for either providing access to only trusted MEC devices or making MEC and network operator independent of trust. • Influence on network by an allowed third party. Network operators must limit network distortion to a certain level. • Providing security service to a third party. Expose security services to trusted applications only

	• MEC environment user plane attacks. It is required to carefully study the scenario specially in case of a few caches and new architecture. • Sensitive security assets on Edge. Proper encryption, assurance of security, protection of decryption keys. • Exchange of data between Edge and Core. Encryption of the sensitive asset. • Trust establishment between the edge and the core functions. Authentication between communication resources. • MEC Orchestrator communication security. Guarantee of the security level as per recognized scheme. • Multiple new nodes, RD and many LI points will raise security risk. Follow strong physical security and identified method of implementation and location for LI/RD functionality.
Slicing	• Attacks on internetwork slices communication. An attacker can disrupt the communication between slices to prevent the proper life cycle management of slices. • Impersonation attack. An attacker can impersonate as a physical host platform to allocate unavailable resources. Moreover, an attacker can impersonate as network slice manager to steal network slice creation parameter • Security policy mismatch. Variance of security policies and security protocols for different slices allow attackers to access the NS system and control entities via less secure slice. • DoS attacks. An attacker performs a DoS attack either on vitalization platform or physical resources to exhaust the available network resources for other slices • Side channel attacks. An attacker gain access to one slice and attack a set of slices which share the same primary hardware. • Privacy attacks. Infrastructure providers or VNF suppliers steal the cross-slice user information. • Hypervisor attacks. Perform attacks against the hypervisor to jeopardize the virtualization of resources. These attacks include, software errors in hypervisor, backdoor entry via hosting OS, DoS attacks and attacking the hardware resources
Latency	• Security mechanism for latency targets. • Subscriber authentication within visited network. • Re-authentication request for the loss of service on a user plane.
Privacy	• Personal data leaking will suppose very high fines from the GDPR law application. • Different personal data regulations between EU members and third parties may produce problems due to the existence of non-matching security policies between them.

SDN	• Forged or faked traffic flows • Man in the middle attacks • Reply attacks • DoS attacks • Back door entrance • Clone or deviate network traffic • Fake switches- and controller-based attacks

7.1.3. Privacy in 5G networks

For the perspective of 5G networks, services and users exchanges messages that may contain private-data of individuals, like identity, location, personal information, etc. The main question is how these messages could be collected, stored and used without disclosing this private data. In 5G networks, the following key privacy properties are considered.

Table 12: 5G Networks Key privacy properties

Privacy properties	Description
Anonymity	In this property, an object is not capable of being identified among its peers (i.e., in anonymity set). An end-to-end anonymity aims the identity of an entity is being hidden from others, even in a same anonymity set.
Unlinkability	In unlinkability, the individual's information is usually unlinkable between two or more users in a system. In the evolving 5G network, unlinkability is highly important and it can be enforced at various domains in the 5G networks, such as SDN, VPN, routing, and back-end servers (i.e., data aggregators, cloud servers).
Undetectability	In 5G network, several objects (such as, machines, applications, users.) will communicate and exchange information between each other. However, an attacker may have an interest to detect the communicating entities by eavesdropping on information/data exchanged. Therefore, in 5G network the information and/or objects must be undetectable to the attacker.
Unobservability	In this property, an attacker may not be able to observe whether two or more entities are participating in the communication. In other words, if an entity had sent a message over the communication then an adversary (i.e., active or passive) should not be able to observe the targeted entity, such as sending mobile healthcare data to the physician.
Pseudonymity	A pseudonym is an instance of an object that is unlike than the objects real names. In the 5G networks, typically several stakeholders will be involved. As these stakeholders can access the personal information, a smart object must

	have several instances (i.e., pseudonymity). These instances are only be known by the involved entities those are exchanging information with the smart objects.

7.2. Architectural security modules in 5G

For the 5G security, many standardization bodies are collaborating on defining a coherent security solution for all the included aspects in 5G technologies. For example, the International Telecommunication Union (ITU) collects inputs form many local organizations and defines high quality technical recommendations that are easy to implement in 5G networks. The International Engineering Task Force (IETF) is also taking part on 5G standardization, due to the presence of the IP protocol and specific protocols like 802.11p for vehicular signalling. The European Telecommunications Standards Institute (ETSI) has issued two access control specification for 5G networks and standardized the MEC-related environment.

Particularly for the 5G security architecture, the 3GPP defined a security framework in different domains: at network, end-users and application levels. This definition introduces several security entities, defines general security requirements regarding key management, authentication and access control, data confidentiality, data integrity and privacy for the subscribers. Further works regarding 5G security architecture was performed by the 5G PPP security group, leading by 5G-ENSURE project. As a result of these project, a new security architecture for 5G was proposed, that is summarized in the following lines.

The basic concepts in this security architecture are domains, strata, security realms, and security control classes. The definitions of these concepts are:

- A **Domain** is a grouping of network entities according to physical or logical aspects that are relevant for a 5G network. This concept is leveraged from TS 23.101 [40].
- A **Stratum** is a grouping of protocols, data, and functions related to one aspect of the services provided by one or several domains. This concept is leveraged from TS 23.101 [40],
- A **Security Control Class (SCC)** is a new concept introduced that refers to a collection of security functions (including safeguards and countermeasures) to avoid, detect, deter, counteract, or minimize security risks to 5G networks, in particular, risks to a network's physical and logical infrastructure, its services, the user equipment, signalling, and data.
- A **Security Realm (SR)** captures security needs of one or more strata or domains. As such, it is like the Security Feature group concept as defined in TS 33.401 [39].

The framework of the security architecture is flexible as it can be extended with definitions of new domains, strata, etc. This makes it possible to adapt the framework to future network solutions with new functionality and services.

A deeper overview of the architecture entities and concepts are available in the **annex 11**.

7.2.1. Mapping Components in the 5G security architecture

Following, we present some considerations regarding the implementation and enforcement of key security aspects in the 5G architecture. We note that for a security architecture to be useful beyond a mere "abstract thought experiment", it must be reflected in the design of real operational networks. To this end, it must be possible to map the security components on the architectural model of 5G systems and to the high level 5G architecture presented in this document.

One of the main advances in 5G architecture is the *softwarisation* of 5G systems allowing efficient management and orchestration procedures providing a flexible sliced service platform for different types of service verticals running on a common infrastructure. We see two major features here; the first is *softwarisation* and the second is slicing and they can be straight forward mapped onto the security architecture. The softwarisation functionality is, in essence, management functionality (orchestration, slice control, etc.) and should as such be mapped onto management domains and the management stratum, i.e. the management security realm. Slicing relies to a large extent on virtualisation and use of shared infrastructure services for compute and storage. The security needs here would then be covered by the virtualisation and infrastructure security realm.

The 5G security architecture will certainly reuse components of the existing 4G architecture when appropriate. Examples of such solutions are the 4G security features developed to cope with threats to radio base stations in physically exposed locations (e.g. when the AN Domain is EUTRA) and tampering threats to user credentials in devices (the USIM Domain is protected by the UICC). Other areas as discussed above, will exhibit new aspects of security e.g. less emphasis on protection at physical and logical domain borders and more on defence-in-depth, the new need for "roots of trust" in virtualised settings to ensure legitimate use of resources as well as authenticated points of deployment.

7.2.2. 5G-Ensure Security Enablers

The 5G-ENSURE produced a useful output that could be reused in this project: Security and Privacy Enablers [41]. They are the major building blocks to achieve 5G security, privacy and trust. Grouped into five clusters, the enablers are all security features, products or services, developed within the 5G-ENSURE project with two major software releases (1.0 and 2.0). The clusters and associated enablers are:

Table 13 5G-Ensure Security enablers

Enabler	Description
AAA	Advanced secure functions to support 5G use cases. Impact: 5G support for IoT and satellite systems. Trust and liability levels. • Basic AAA • Internet of Things. • Fine-grained authorisation.

Privacy	Increased users' assurance and confidence in 5G through enhanced user data protection implemented with solutions at several layers. Impact: Creation of services and business models on top of 5G. • Enhanced identity protection. • Device Identifier Privacy. • Device-based Anonymization. • Privacy policy analysis.
Trust	Tools using new trust models, including M2M(Machine to Machine)interactions. Impact: Trustworthy dynamic 5G multi-stakeholder system. • Trust builder. • Trust metric. • VNF Certification. • Security indicator.
Security Monitoring	Security by operations, i.e., monitoring and auditing 5G security. Impact: Resilient 5G system to implement new services. • Satellite network monitoring (SatNav). • Proactive Security Assessment and Remediation (PulSAR). • Generic collector interface. • System security state repository. Malicious traffic generator for 5G protocols
Network Management & Virtualisation Isolation	Secure network control plane including virtualised networks and network services. Impact: Mitigate security threats in SDN. • Access control mechanisms. • Component-interaction audits. • Bootstrapping trust. • Micro-segmentation. • Flow control.

All the 5G-ENSURE enablers (a total of 21) are summarized online [44] with a short paragraph explaining their contributions and a contact person of the responsible partner. For a deeper view we recommend reading public D3.9 of this 5G-Ensure project titled "5G PPP Security Enablers Technical Roadmap". For each 5G-MOBIX user story of each use case category we identified the security enablers applicable, reusing their implementation and avoiding starting from scratch. After performing that matching process, it was stated that very few enablers can be profitable. The 5G-MOBIX user stories (use cases) are strongly related to

Vehicle-to-Everything (V2X) communication, and 5G-ENSURE did not provide any enabler for this kind of use cases.

7.3. Impact of European GDPR regulation on 5G Security

The European General Data Protection Regulation (GDPR) [45] is a regulation on personal data protection and privacy for all individual citizens of European Union (EU) and the European Economic Area (EEA). It is designed to harmonize all the previous existing data protection laws and replacing the directive 95/94/EC. It has been in force since May 25, 2018. Due to the coincidence in time with the development of 5G standards by the 3GPP WGs, all data protection and privacy issues has been considered from the very beginning in the development of those 5G standards. However, it is undeniable that GDPR will have a strong impact on 5G. The most important parts of this law and the most relevant for the 5G-MOBIX trials are summarized in ***Annex 12***.

7.3.1. Analysis of GDPR impact on 5G

GDPR is producing a strong impact on 5G actors. Vendors, operators and standardization bodies are facing the application of this restrictive law from the beginning. In general, data protection by design and by default should be increasingly adopted by standardization. Different working groups in 3GPP are currently working in close coordination with the security working group (SA WG3), designing identifiers and protocols, and specifying test cases for privacy assurance in 5G. The same is true for vendors, that are implementing 5G standards and developing proprietary solutions. Vendors must have, besides data protection by design and default, privacy impact assessment built into their product development lifecycle and should advise operators about the privacy impact of new technologies. Additionally, the operators must analyse how the GDPR affects their business model and take proactive steps in achieving compliance, for example, by appointing a competent Data Protection Officer (DPO).

Companies can reduce the probability of a data breach and thus reduce the risk of fines in the future, if they choose to use encryption of personal data by default. The processing of personal data is naturally associated with a certain degree of risk. Especially nowadays, where cyber-attacks are nearly unavoidable for companies above a given size. Therefore, risk management plays an ever-larger role in IT security and data encryption is suited, among other means, for these companies. The GDPR recognizes these risks when processing personal data and places the responsibility on the controller and the processor in Art. 32 to implement appropriate technical and organisational measures to secure personal data. This article deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, actors always must consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures must be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organisational measure to secure data in the list of Art. 32 of the GDPR, which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress. When choosing a method, actors must also apply the criteria catalogue above. To answer the question of what is currently considered "state of the art" DPOs usually rely on the definitions set out in information security standards like ISO/IEC 27001 or other national IT-security guidelines.

Encryption of personal data has additional benefits for controllers and/or order processors. For example, the loss of a state-of-the-art encrypted mobile storage medium which holds personal data is not necessarily considered a data breach, which must be reported to the data protection authorities. In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount a fine is imposed as per Art. 83 of the GDPR.

With penalties that can reach as high as 20 million euros or 4 percent of total worldwide annual turnover, there is a huge financial risk for operators in case of potential non-compliance. There are also real risks to reputation or brand image. Therefore, operators must take the GDPR obligations very seriously, and vendors and standardization bodies must make sure that operators are able to comply with the GDPR.

7.3.2. GDPR application in X-Border scenarios

The focus of 5G-MOBIX research is analyse, detect and design possible solutions to issues that could arise in a very specific vehicular x-border scenarios, where several countries, EU members or not, are involved. Between EU members there should not be problems because all of them depends on the same GDPR law, implemented in similar ways by each country. The problem arises when one of the countries does not belong to the EU, which could result in different personal data protection regulations. Our initial research has resulted on several issues in the application of different personal data protection regulations in x-border scenarios:

- **SDP0**: Different data protection regulations apply when processing personal data of data subject in Europe, Turkey, China and Korea. Therefore, many legal, organisational and technical challenges need to be overcome for lawful processing of these data.
- **SDP1**: Without proper legal basis, lawful processing of personal data could not be achieved. Indeed, legal issues arise at the enforcement of the GDPR to CCAM. For example, CAM and DENM messages are considered personal data but are required for the normal functioning of the CCAM systems.
- **SDP2**: Partners in 5G-MOBIX processing data from citizen of different countries needs to put proper organisational procedures to handle data protection. These includes (but not limited to): Data processing cartography, Training, Privacy risk assessment, Data breach procedures, Documentation.
- **SDP3**: The technical mechanisms that are applied in order to support the legal requirements on lawful data processing could find difficulties in a cross-border scenario. These mechanisms include (but are not limited to): Data encryption, Data minimization, Anonymization, Differential privacy mechanism,

Informed consent, Privacy by design and by default, Assessment of these mechanisms. These mechanisms should be implemented in the appropriate entities of the 5G-MOBIX reference CCAM architecture to be adapted for each 5G-MOBIX partner.

They are identified (SDPx) due to traceability purposes along the project.

7.4. Security requirements on 5G-MOBIX architecture and Technologies

7.4.1. Generic requirements

In the design of the new security architecture, special care has been taken to ensure the security architecture can embrace all new technologies and concepts used in 5G that are significant evolution steps from 4G.

5G will rely heavily on *softwarisation* and virtualisation of the network to enhance flexibility and scalability. One important development to achieve this is to refine the network slicing technologies and multi-access edge computing (MEC) to more dynamically offer various kinds of services to different tenants. Virtualisation is the underlying enabling technology for this. Another development of equal importance is the large-scale introduction of SDN allowing flexible and dynamic (re-)defining of the networking infrastructure.

The incorporation of many new target use cases in 5G brings new business models with many new actors taking part in the provisioning of services. This means that new, multi-party trust relations will be present and should be modelled and handled from a security perspective.

In an environment where many different actors independently manage resources that they own or lease, all aspects of management become critical from a security point of view. In particular, 5G has to handle multiparty management of security (e.g. provisioning of keys and credentials) and security management (e.g. ensuring that secure services are available and runs securely). Orchestration of virtualised environments, services and SDN's will also require secure management.

5G networks will be more complex and dynamic than earlier generations of mobile networks as e.g. new (virtualised) network nodes and slices can be added to and removed from the network at any time. To identify and model attack vectors in this dynamic environment and to be able to offer strong network protection, security control points must be defined based on establishing boundaries between different actors' network functions and slices and their interfaces.

With the increasing number of target use cases, the new multi-party trust relations and the new technologies employed, 5G will comprise an even increasing number of security and non-security protocols and network functions. To identify and keep track of threats and attack vectors, and required protection mechanisms and their coverage, 5G networks must be modelled in a structured way together with the security controls that need to be deployed to offer the necessary trust and confidence.

Additional to the previous analysis, in Table 14 you can see more specific requirements that 5G PPP security working group has been taken into account.

Table 14 Specific Requirements to be considered

Requirement ID	Description
Security Automation **(Sec-Auto)**	5G infrastructures' heterogeneity and complexity require security to be dealt at multiple levels and across domains. Therefore, automation of 5G security is vital to successful functioning and adaptation of 5G technologies. This is also in favour of 5G security to be composed and dynamically adapted upon context at hands, as a service (5G Security As-A-Service: SecaaS).
Security Monitoring **(Sec-Mon)**	5G systems must support security monitoring capable of detecting advanced cybersecurity threats and support coordinated monitoring between different domains and systems (e.g. mobile and satellite). New innovative approaches to predict, detect and counter these challenges may need to be considered. For example, we may think of relying on analytics for enhanced security operations (based, for instance, on Machine Learning and Artificial Intelligence approaches) to develop intelligence driven security capabilities able to gain a more accurate understanding of the risks and exposures of SDN infrastructures. One of the future solutions could be to collect and analyse in real time events and logs within each slice (from RAN to vertical services) and among slices (this approach is identified as "Fast Data" technologies, due to its reactivity time and the very short storage duration to achieve massive collect of information).
Security Management **(Sec-Mgmt)**	End-to-End security management and orchestration should be put in place considering correlation and coherence/consistency between data exchanged/shared at Security Architecture Inter-domain interfaces. For example, an appropriate use of Big Data technologies may allow consistency evaluation between RAT and Verticals in terms of customer 5G security context (i.e. notification of country localization during service delivery). Customers, slice owners and vertical services should be aware of their technical 5G contextualization, particularly to asses and address their security needs. For example, security KPIs and proofs should be available and collected at the 5G infrastructure. 5G systems and components must provide functionality to mutually assess their trustworthiness before, and during interactions. Furthermore, if required by local regulation, 5G infrastructure operator must have means to demonstrate their provided level of security.

An analysis of the security and privacy requirements of each of the 5G-MOBIX use case categories is also an important aspect of our work, and the templates for each of the UCCs have already been defined, as can be seen in ***Annex 12***, and will be filled in by the 5G-MOBIX experts as pre-trial preparation.

7.4.2. Requirements on 3GPP networks

Requirement ID	Description
Security in 3GPP networks **(Sec-3GPP)**	The security of 3GPP networks should be implemented according to the ETSI TS 33.401 and ETSI TS 33.501. The vehicle and network must be mutually authenticated and authorized to use the network and related services.

7.4.3. Requirements on C-V2X

Requirement ID	Description
Security in C-V2X networks **(Sec-CV2X)**	The security of C-V2X should be implemented according to the 3GPP TS 33.185. V2V and V2I communication must be protected applying secure cryptographic methods to provide confidentiality and integrity to the transited information.

7.4.4. Requirements on ETSI ITS

The complete set of security requirements for 5G-MOBIX high level reference architecture have been provided in the deliverable D2.3 and contain requirements related to C-ITS.

7.4.5. Requirements on ETSI MEC

Requirement ID	Description
Security in MEC systems	• The MEC system shall provide a secure environment for running services for the following actors: the user, the network operator, the third-party application provider, the application developer, the content provider, and the platform vendor.

(Sec-MEC)	• The MEC platform shall only provide a MEC application with the information for which the application is.

7.4.6. Requirements on GSMA Network slicing

Requirement ID	Description
Inter-tenant/Slice Isolation **(Slice-Isolation)**	Infrastructure sharing by multiple network operators will require strict isolation at multiple levels to ensure the expected security level. Various aspects of control-plane, data-plane and resource isolation must be guaranteed to ensure zero correlation among different slices/tenant operations. Tenant/slice isolation is important to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality. Therefore, inter-tenant/slice isolation security of sensitive data, should at least be equal that of physically separated networks. Moreover, this strong slice/tenant isolation should be demonstrable, and evidence should be collected and computed over the entire infrastructure.
5G Liability **(5G-liabiliry)**	The chain of trust and liability of multi-tenants should be managed and auditable for each service, component supplier, operator and customer. 5G Liability schemes must be defined and applied, particularly to address breach of Trust/Security (backdoor, Quality impact, regulation impacts, data leakage, etc.) between parties. 5G Liability could be reinforced by VNF certification, SDN Controller or Orchestrator evaluation, or proper orchestration of virtualised security functions. For instance, it is important to address the security of the VNF itself as an element, e.g., VNF hardening, VNF verification/certification/attestation and corresponding industrial processes, VNF code robustness, to name a few.
Security liability Schemes **(Liabiliry-Schem)**	New responsibility schemes should be proposed, in coherence with existing regulation, regarding the distribution and allocation of responsibilities and obligations in a multi-tenant *softwarised* telecom infrastructure, and, in particular, for potential delegation of regulation obligation to non-regulated third parties (today Licence obligations are *intuitae personae* and may not be sub-delegated).

7.4.7. Requirements on Data protection & Privacy

Requirement ID	Description

5G Security and Privacy level above 4G level **(Sec-privacy)**	5G must provide a security and privacy level higher, or at least equal, to the security and privacy level in 4G. That is, 5G must be able to deliver and maintain SLA to verticals in terms of: availability, security, resilience, latency, bandwidth, access control from an end-to-end perspective. Furthermore, 5G systems and components must provide strong mutual authentication and authorization and should not be negatively affected by the security of legacy systems which it interworks with.
5G regulation conformity **(Sec-regulation)**	5G technology should be developed in compliance with legislation/regulation that apply or could be anticipated (for instance Lawful Interception and Data Retention Regulations appeared as difficult to comply with and must be considered in the case of slicing implementation).
Enabling Value Added Services with end-to-end encryption **(E2E-encryption)**	Enabling value-added security services in the context of encrypted traffic. To comply with privacy regulations and protection of user data, traffic encryption is expected to be generalized across 5G networks. End-to-end encryption may hamper the use of multiple value-added security services such as attack detection, QoS monitoring and fine-grained access control among others. In this respect, high level privacy guarantees may have the adverse effect of lowering security guarantees. Therefore, the development and wide adoption of 5G should happen alongside new technologies and capabilities that enable value-added security services in the context of encrypted traffic, thus conciliating between security requirements and privacy guarantees.
Sec-Pricacy-3GPP-PC5-law	When using the PC5 sidelink, the following privacy requirements apply: • Subject to regional regulatory requirements and/or operator policy for a V2X application, the data sent in the PC5 transmission should not allow vehicle's identity to be tracked or identified by any other UE or non-V2X entity beyond a certain short time period required by the V2X application Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the data sent in the PC5 transmission should not allow a single party (operator or third party) to track vehicle's identity in that region.
Sec-Pricacy-3GPP-PC5-Pseudonimity	In addition, the following privacy requirements apply: • The identifiers in the V2X messages should minimize the risk of leaking the UE or user permanent identities. • Vehicles pseudonymity should be provided to conceal personal data from attackers.

	The application layer Vehicles identity in the V2X messages should be protected from eavesdropping.
Sec-Pricacy-3GPP-PC5-transparency	GP26- Implement transparency measures. The interactions with the user (which should not be limited to the Terms and conditions) enable to cover the legal transparency requirements.
Sec-Pricacy-3GPP-PC5-legitimacy	• Design the product/service with legitimate purpose and proportionality in mind. The actors must ensure that themselves and their subcontractors or suppliers do not process user data if not needed, and do not pursue an illegitimate purpose with regard to user data.

8. CONCLUSIONS

This document describes in detail the 5G network architecture selected (and to be implemented) in each cross-border corridor (and trial site) of the 5G-MOBIX project as well as the reasoning behind the selection of each component and the considerations considered in each case. As part of the CBC 5G deployments, the envisioned concrete contributions of the various TSs to their respective CBCs in terms of infrastructure are also presented along with the extended evaluations per UCC to take place at the TS locations. This document will serve as one of the main reference documents describing the foundation of the project's trials and providing valuable insights regarding the availability of diverse functionalities across the 5G-MOBIX sites. It will also be used by WP3 (implementation) and WP4 (trialling) as a planning document, which will guide their progress and define the boundaries of their work.

As presented herein, the architectural choices of all the 5G-MOBIX sites are based on currently available technologies (HW & SW) from 3GPP, the integration and collaboration possibilities with non-3GPP technologies (e.g. MEC) as well as the foreseen roadmap for development of 3GPP Rel.15 and beyond equipment. Based on this input both CBC deployments have been planned on a commonly agreed reference architecture, which will be expanded by each of the CBCs to serve the purposes of their distinct UCCs. The capabilities of the available technologies have been weighted against the requirements originating from the automotive sector and the expected KPIs to be met for certain state-of-the-art CCAM use cases that need to be supported in cross-border conditions. This requirements analysis has been performed under the specified conditions dictated by the geo-spatial characteristics of each of the corridors as well as regulatory and deployment issues (e.g. 5G frequencies availability in each country), resulting in the optimum selection of features and technological components to be deployed at each CBC. The initial deployment for all sites will be based on early releases of 3GPP Rel.15 equipment and will hence be restricted to an operation with a 4G anchor (NSA), except for the NL TS (and partially the Asian sites) which will set-up their sites with an SA architecture from the first phase of trialling. Technology and device availability in the near future will determine the degree of evolution of each of the CBCs, which aspire to reach a SA 5G deployment by the end of the project.

The planned network roll-out to support the CBC trials has been based on a tight CBC/TS collaboration with components and feature contributions from the TSs to the CBCs, taking part of the "weight" and allowing for a more streamlined development, while more challenging and advanced testing is also envisioned at the TS facilities where the controlled conditions allow for larger number of trials with less "real-world" restrictions. The 5G network architectures proposed in this document, have also taken into consideration the initial sustainability, security and data privacy concerns expressed by the immediately involved stakeholders, while further work to be carried out within 5G-MOBIX on these aspects will result in fine-tuning of the configuration/set-up of some of the used components.

REFERENCES

[1] 5G-MOBIX Deliverable D2.1, "5G-enabled CCAM use cases specifications", April 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.1-Use-case-specifications-v1.0.pdf

[2] 5G-MOBIX Deliverable D2.3, "Specification of roadside and cloud infrastructure and applications to support CCAM", July 2019.

[3] 5G-MOBIX Deliverable D2.4, "Specification of Connected and Automated Vehicles", July 2019.

[4] 5G-MOBIX Deliverable D2.5, "Initial evaluation KPIs and metrics", July 2019.

[5] ETSI EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.

[6] ETSI EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.

[7] ETSI EN 302 663: Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.

[8] ITU Recommendation M.2083-0: IMT Vision - "Framework and overall objectives of the future development of IMT for 2020 and beyond".

[9] 3GPP TS 38.801: Study on new radio access technology: Radio access architecture and interfaces.

[10] 3GPP Work Item RP-161249: Architecture configuration options for NR.

[11] 3GPP TS38.885, 'Study on NR Vehicle-to-Everything (V2X)', https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3497

[12] 3GPP TR23.786, 'Study on architecture enhancements for the Evolved Packet System (EPS) and the 5G System (5GS) to support advanced V2X services', https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3244

[13] 3GPP TS 23.501: System Architecture for the 5G System.

[14] 3GPP TS 23.287 "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services," v15.0.0, Mar. 2018.

[15] 3GPP TR 21.916 "Summary of Rel.16 Work Items," v0.1.0, Sep. 2019. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3493

[16] Delegated Regulation - C(2019)1789 - for C-ITS, https://ec.europa.eu/transport/sites/transport/files/legislation/ c20191789.pdf

[17] ETSI Multi-acccess edge computing main web page: https://www.etsi.org/technologies/multi-access-edge-computing

[18] GSMA Network slicing, Use case requirements, https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/NS-Final.pdf

[19] GSMA, 'From Vertical Industry Requirements to Network Slice Characteristics, August 2018, https://www.gsma.com/futurenetworks/wp-content/uploads/2018/09/5G-Network-Slicing-Report-From-Vertical-Industry-Requirements-to-Network-Slice-Characteristics.pdf

[20] MEC Deployments in 4G and Evolution Towards 5G
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf

[21] MEC in 5G Networks.
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[22] LTE Roaming Guidelines https://www.gsma.com/newsroom/wp-content/uploads/2013/04/IR.88-v9.0.pdf

[23] EN 302 636-4-1 (2013-10) Geographical addressing and forwarding for point-to-point and point-to-multipoint communications.

[24] TR 103 630 (2019-09) Pre-standardization Study on ITS Facility Layer Security for C-ITS Communication Using Cellular Uu Interface.

[25] GSMA, 'Generic Network Slice Template', v1.0, May 2019, https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v1.0-4.pdf

[26] MoScoW method explained, ToolsHero, https://www.toolshero.com/project-management/moscow-method/

[27] 3GPP TR 22.885: Study on LTE support for Vehicle to Everything (V2X) services (Release 14).

[28] 3GPP Work Item RP-190766: 5G V2X with NR sidelink.

[29] 3GPP TS 23.502, "5G; Procedures for the 5G System" , June 2018, https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/15.02.00_60/ts_123502v150200p.pdf

[30] 3GPP TS 23.122, "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode" , March 2019, https://www.3gpp.org/ftp/Specs/archive/23_series/23.122/23122-g10.zip

[31] 3GPP TS 23.503 "Policy and charging control framework for the 5G System (5GS); Stage 2", v16.0.0, 2019-03-26

[32] 3GPP TS 22.186: Enhancement of 3GPP support for V2X scenarios; stage 1.

[33] C. Campolo et al., "5G Network Slicing for Vehicle-to-Everything Services," IEEE Wireless Communications, vol. 24, no. 6, pp. 38-45, 2017.

[34] F. Hasegawa et al., "High-Speed Train Communications Standardization in 3GPP 5G NR," IEEE Communications Standards Magazine, pp. 44-52, 2018.

[35] S. Chen et al., "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G," IEEE Communications Standards Magazine, vol. 1, no. 2, pp. 70-76, 2017.

[36] J. Jonson, "Example of journal article," Title of journal, pp. 1-10, 2019.

[37] [5GPPP-2019] 5GPPP Automotive Working Group, "Business Feasibility Study for 5G V2X Deployment", Version 2, February 2019.

[38] 5G-ENSURE Project home page - http://www.5gensure.eu/

[39] 3GPP TS 33.401, "Security architecture" https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.

[40] 3GPP TS 23.101, "UMTS architecture" https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=782.

[41] 5G-ENSURE project Deliverable D2.4 "Security Architecture Draft", http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.4-SecurityArchitectureDraft.pdf.

[42] 5GPPP White Paper, "5GPPP Phase1 Security Landscape," https://5GPPP.eu/wp-content/uploads/2014/02/5GPPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf.

[43] ITU X.805 "Security architecture for systems providing end-to-end communications," 2003-10-29, https://www.itu.int/rec/T-REC-X.805-200310-I/en

[44] 5G-ENSURE Project home page - Security enablers list - http://www.5gensure.eu/security-enablers

[45] European General Data Protection Regulation (GDPR) 2016/679, https://gdpr-info.eu/

[46] 3GPP TR 21.914: Technical Specification Group Services and System Aspects; Release 14 Description; Summary of Rel-14 Work Items.

[47] 3GPP TS 22.185: Service requirements for V2X services.

[48] 3GPP TS 23.285: Architecture enhancements for V2X services.

ANNEXES

Annex 1 – Functional and Non-Functional requirements analysis

The aggregated presentation of each of these requirements along with an estimation of the importance of each one of them for the respective trials, provides insight regarding the complementarity of the corridors/trial sites, the differentiated nature of the supported use case categories, and network design directions to be taken by each of the trials. The estimation of the importance of each of the functional and non-functional requirements per site is based on the MoSCoW method of requirements prioritization [26], which is a well-established management method, prioritizing the requirements of any system into (M)ust-haves (highest priority), (S)hould-haves, (C)ould-haves and (W)ould-haves (lowest priority). For the purposes of 5G-MOBIX the MoSCoW scale has been adjusted to reflect the (**M**)andatory, the (**R**)ecommended and the (**O**)ptional requirements/features per site as is explained in Table 15.

Table 15: 5G-MOBIX requirements classifier based on the MoSCoW method

MoSCoW term	5G-MOBIX Compliance classifier
MUST have	**(M)ANDATORY**
SHOULD have	**(R)ECOMMENDED**
COULD have	**(O)PTIONAL**
WON'T have (and would haves)	**(O)PTIONAL**

The main aggregated functional requirements of all the 5G-MOBIX corridors/trial sites along with their classification of importance according to the corridor/trial site experts is presented in Table 16. The aggregated results per requirement was shown as a graph in Figure 6, while the means for calculating the total priority points per requirement are explained in Section 3.2 and more specifically in Table 2.

Table 16: 5G-MOBIX aggregated functional requirements and their importance classification per site

Requirement	Component / Section	GR-TR	ES-PT	FI	FR	DE	NL	CN	KR	Total Priority points
GRX/IPX/VPN MNO Interconnections with SLAs	Roaming	R	R	R	R	R	R	M	O	5
Virtualisation support	All/E2E	M	M	M	R	M	M	M	M	9.5

Multi-tenancy	All/E2E	M	M	M	O	R	O	M	R	7
Network Slicing	All/E2E	M	M	M	O	R	O	M	R	7
Mobility Support	All/E2E	M	M	M	M	M	N/A	M	M	9
eMBB services support	Transport Network (SDN)	M	M	M	M	R	R	M	M	9
eMBB services support	Radio Network	M	M	R	M	M	N/A	M	M	8.5
eMBB services support	Core Network	M	M	M	M	M	M	M	M	10
uRLLC services support	Transport Network (SDN)	M	M	M	M	M	R	M	R	9
uRLLC services support	Radio Network	M	M	M	M	R	R	M	R	8.5
uRLLC services support	Core Network	M	M	R	R	M	M	M	R	8.5
Interaction among MEC / Edges of different MNOs	Radio Network	M	M	R	R	M	M	O	O	7
4K video streaming	Application	M	N/A	O	R	M	N/A	O	M	4.5
ITS Centre Coordination among Countries	Application	R	R	R	O	O	R	O	O	3

Almost equally important to the functional requirements of the networks under construction, the non-functional requirements identified per corridor/trial site will guarantee the long-term uninterrupted operation, financial profitability and regulatory conformance of the networks to be deployed for the 5G-MOBIX trials. Similarly, to the functional requirements, each trial and the involved MNOs have indicated the level of criticality of each of these commonly identified requirements using the same scale, based on the MoSCoW method, as presented in Table 17. The aggregated results per requirement was shown as a graph in Figure 6, while the means for calculating the total priority points per requirement are explained in Section 3.2 and more specifically in Table 2.

Table 17: 5G-MOBIX aggregated non-functional requirements and their importance classification per site

Requirement	Component / Section	GR-TR	ES-PT	FI	FR	DE	NL	CN	KR	Total Priority points
Roaming Agreements	Roaming	M	M	O	R	R	O	R	O	5.5
Interoperability with Legacy Technologies	All/E2E	M	R	M	M	M	M	M	O	8
Feasibility for commercial deployment	All/E2E	M	M	M	M	M	M	M	M	10
Extensibility/Upgradability	All/E2E	M	M	M	M	M	M	M	M	10
Scalability	All/E2E	M	M	M	M	M	M	M	M	10
Reliability	All/E2E	M	M	M	M	M	R	M	M	9.5
Provided Architecture must be realized by Q1/2020	All/E2E	M	M	M	M	M	M	M	M	10
Physical security of equipment and infrastructure	All/E2E	M	M	M	M	M	M	M	M	10
Digital/cyber-security concerns	All/E2E	M	M	M	M	M	M	M	M	10
Coexistence with other technologies	All/E2E	M	M	M	R	R	M	R	M	8.5
Authorities participation in trials	Application	M	M	R	M	M	O	O	R	7

Annex 2 – ITS and V2X standardization aspects

In cellular communication systems, traditionally mobile user terminals are served by base stations, which in turn are connected to the core network of mobile operators, introducing transmission delays and set up time for the connection establishment phase as well as requiring end-to-end dedicated network resources for the terminals in a call or session. On the other hand, as also identified by 3GPP in TR 22.803 V12.0.0 (2013), it is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825496.

feasible to provide valuable services to user terminals of 3GPP systems even when they are not under the coverage of any base station if they are in close proximity to each other, which also embraces the public safety community, addressing their requirements for the case of emergencies.

The introduction of device-to-device (D2D) communications and Proximity Services (ProSe) in the 3GPP Rel.12 of the 3GPP standards for LTE-Advanced enabled the following functionalities:

- Direct communication: In order to ensure effective reuse of frequencies and minimize additional implementation for existing terminals, D2D communications in 3GPP use a subset of the uplink radio resources for transmission, sharing the available frequencies with cellular communications. Two modes of operation are possible for direct communication depending on the assistance of E-UTRAN Node B (eNB) being present for resource allocation and configuration, where more efficient communications are envisioned when eNB is taking an active part as opposed to the fully autonomous D2D mode. Even though the involvement of the eNB for signalling is optional, data transmission is performed directly between terminals without going through the core network in both cases.
- Device discovery: Targeting a more commercial usage of D2D communications compared to direct communication that has a more public safety-oriented role, specifications were added in 3GPP Rel.12 to enable discovering other devices near a mobile terminal to help operators monetize this particular functionality to provide value-added location-based services.

D2D communications were improved in 3GPP Rel.13 to meet the public safety requirements for in-network, partial and outside network coverage scenarios whereas only in-network coverage is addressed for non-public device discovery cases. These D2D services may be supported on the same, or on different, frequency carriers than those used for cellular network connectivity.

1) LTE V2X

Capitalizing on the D2D proximity services capability defined in previous releases that are enhanced for high-speed and high-density vehicular use cases, V2X communication was introduced to 3GPP systems in Rel.14 and further enriched in Rel.15 (Table 18) to realize the safety critical applications appearing in other standards such as the ETSI-ITS.

Table 18: 3GPP LTE-V2X attributes of Rel.14 and Rel.15

Attribute	LTE V2X Rel.14	LTE V2X Rel.15
Specification finalization date	2017/03	2018/06
Use Cases	Basic Safety	Enhanced safety
Value proposition	Foundation for V2X services in 3GPP cellular networks	Latency is reduced and reliability is increased by introduction of new parameters, e.g. ProSe Per Packet Reliability (PPPR)

Reference 3GPP document	TR 21.914	TR 21.915

3GPP specifies two interfaces for vehicle communications, where one is derived from D2D connectivity and the other is directly related with cellular communications as shown in Figure 46. On the other hand, the ProSe discovery feature introduced in Rel.12 to the 3GPP standards is not required for V2X services.

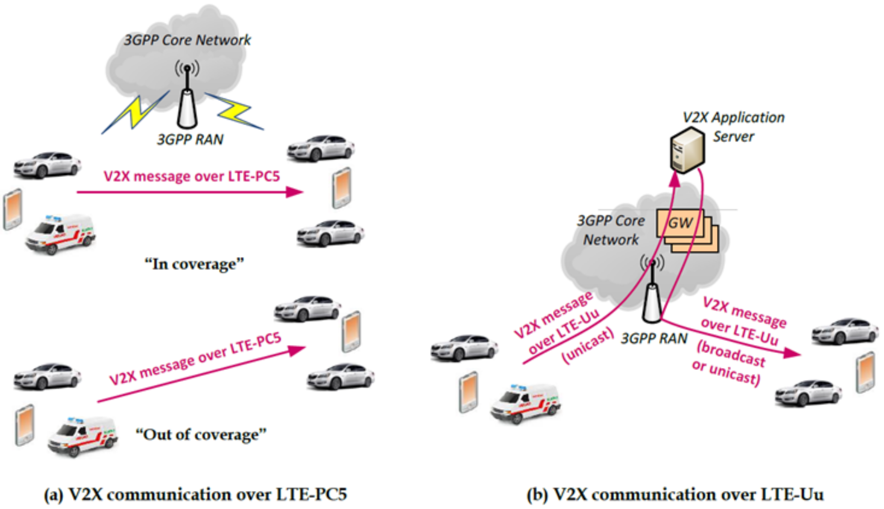


Figure 46: V2X communication over PC5 interface and LTE-Uu interface - Reference TR 21.914 [46]

- V2X communication over PC5 interface: User Equipment (UEs) are directly connected through the PC5 in the sense that a V2X message is received by all UEs that are in sufficient proximity to the transmitting UE [46]. Whenever the UEs are under the coverage of an eNB, links may also exist with the eNB for resource allocation and configuration management, and the UEs may use the network-scheduled operation mode (i.e., centralized scheduling). If no link with the eNB is formed, the autonomous resources' selection mode (i.e., distributed scheduling) should be exercised before V2X messages can be sent over the PC5 interface.
- V2X communication over LTE-Uu interface: UEs are connected to eNBs through the LTE-Uu interface, which indicates that a V2X message may be received by vehicles and other mobile users more distantly located than what the PC5 interface allows. LTE-Uu can be unicast and/or Multimedia Multicast Broadcast Services (MBMS) based.

In the 3GPP document TS 22.185 [47]: "Service requirements for V2X services", V2X applications are considered to belong to one of the four types demonstrated in Figure 47 below, highlighting the distinction between a V2X communication interface (PC5 or LTE-Uu) and a V2X application (V2V, V2I, V2N or V2P).

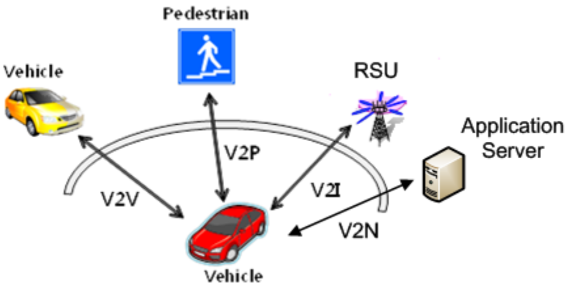


Figure 47: Types of V2X applications (V2V, V2P, V2I and V2N) - Reference TS 22.185 [47]

The entities displayed in Figure 47 can collect information from their surroundings through other entities or the sensors in their proximity, and share the knowledge generated by processing that information in order to provide "cooperative awareness" that will be used by intelligent services such as cooperative collision warning or autonomous driving. Since these intelligent transportation services and the message sets that underlie these services are already defined by standards developing organisations, 3GPP only handles the transportation of messages, like the cooperative awareness messages of ETSI-ITS, instead of trying to develop alternative new message sets to support various V2X applications.

In Figure 47, a road-side-unit (RSU) is shown as an entity for V2I applications, where 3GPP introduces this term to make the documents easier to read for the ITS industry that is accustomed to a stationary infrastructure entity supporting V2X applications that can exchange messages with other entities also supporting V2X applications. In [47], RSU is defined as "a logical entity that supports V2X application logic using the functionality provided by either a 3GPP network or a UE (referred to as UE-type RSU)". See the Annex A of [48] for RSU implementation options.

An overview of the four different types of V2X applications is shown in Table 19. Note that a valid subscription and authorization from a network operator is required for all applications even when an eNB is not used for communication, where the standard demands that the network operators provide a means to authorize UEs supporting V2X applications to perform V2X communication while the authorization for UEs that support V2X are done separately for V2N communications.

Table 19: V2X application categories according to TS 22.185 [47]

	V2V	V2I	V2N	V2P
Involved end users	Vehicles only	A vehicle and an RSU or locally relevant application server serving a particular geographic area	A vehicle and an application server	A vehicle and a vulnerable road user
Proximity/Locality	Yes	Yes	No	Yes

Communication link type	Direct communication (PC5) or LTE-Uu via infrastructure supporting V2X (i.e., an RSU or an application server)	LTE-Uu or PC5 in case of UE-type of RSU	LTE-Uu	Direct communication (PC5) or LTE-Uu via infrastructure supporting V2X (i.e., an RSU or an application server)
Objective	Safety/Broadcast: location, dynamics, attributes	Sharing information about a certain geographic area	General purpose services	Warning to pedestrians and warning to vehicles

The major service requirements defined for typical V2X applications in [47] are related to latency, message size, frequency, range and speed:

- Latency: Maximum latency of 100 ms for V2V/P with 20 ms maximum allowed latency in some specific use cases (i.e., pre-crash sensing), 100 ms for V2I and 1000 ms for V2N
- Message size: Transfer of message size up to 1200 bytes for event-triggered messages and 50-300 bytes for periodic broadcast messages
- Frequency: Maximum 10 messages per second per transmitting UE
- Range: A communication range sufficient to give the driver(s) ample response time (e.g. 4 seconds).
- Speed: Maximum relative velocity is 500 km/h for V2V, maximum absolute velocity is 250 km/h for V2V and V2P, maximum absolute velocity is again 250 km/h for V2I application supporting UEs.

ARCHITECTURE: Another relevant standard document is 3GPP TS 23.285 [48]: "Architecture enhancements for V2X services" focuses on the V2X architectures, functional entities involved in V2X communication, interfaces, provisioned parameters and procedures [48].

A logical function, "the V2X Control Function", is introduced to Evolved Packet Core (EPC) in 3GPP Rel.14 to perform the basic network related actions required for delivering V2X services to UEs. An example of these V2X services is the provisioning of the UEs with the necessary parameters to allow them to use V2X applications in a certain PLMN, also covering the "not-served by E-UTRAN" case (i.e., out of coverage scenario).

Roaming and inter-PLMN architectures for PC5 and LTE-Uu based V2X communications as well as architectures for MBMS via MB2 or xMB reference points for LTE-Uu based communications are also depicted in [48].

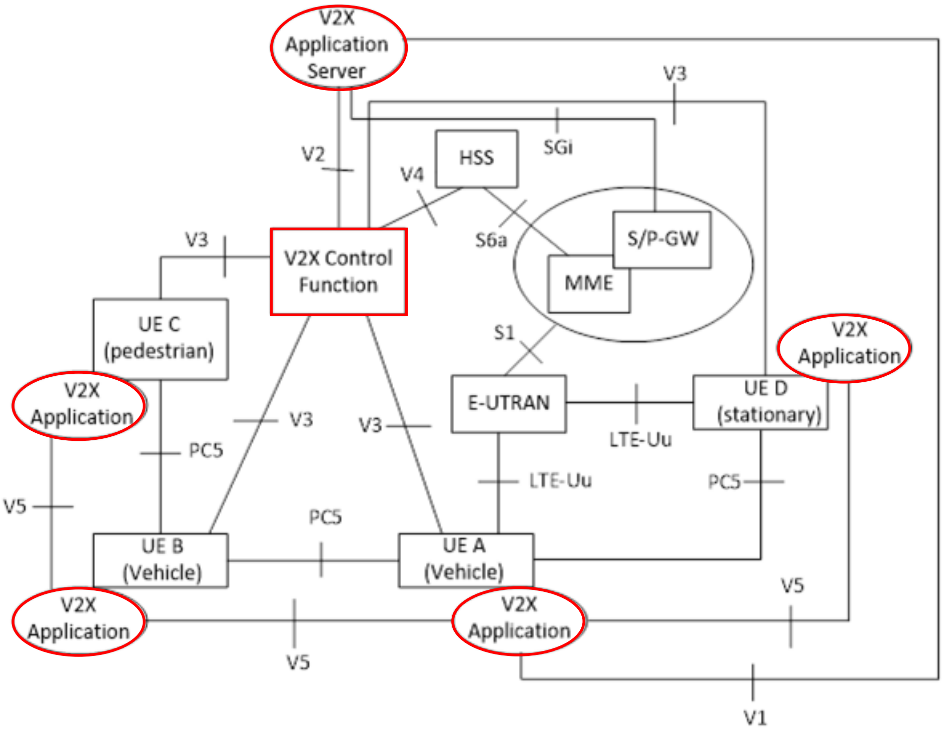


Figure 48: Non-roaming architecture for PC5 and LTE-Uu based V2X communication [48]

DEPLOYMENT: In Annex D of the 3GPP TR 22.885 Rel.14 document [27], three deployment options are listed for V2X communications:

1. Infrastructure-less V2X operation: All UEs are configured with the same parameters, and out of E-UTRAN coverage communication parameter provisioning can be used until new parameters are obtained from the network when entering back into the network coverage. Since the network is unavailable, some of the use cases described in [27] that require network services and subscription confirmation cannot be realized.
2. Multi-MNOs shared V2X services scenario: Analogous to existing mobile network deployments, each UE has a subscription with an MNO, which controls its access to V2X spectrum and services, and the UEs from different MNOs should be able to communicate with each other. It is expected that UEs fall back to the infrastructure-less operation mode if they leave coverage.
3. Single MNO managed V2X scenario: A single mobile operator manages all V2X services and owns the whole V2X spectrum, and thus a valid subscription to this MNO should exist or this MNO should allow other MNO subscriptions to be used for authorization. Two subcases are also defined based on whether the control channel for V2X services are separated from the WAN spectrum of the MNO or not: (1) split-control and (2) co-channel deployment.

2) NR V2X

The work for a sidelink communication, which uses the new radio (NR) interface designed for 5G cellular communications in 3GPP Rel.15 of the 3GPP standards (see Section 2.1.1), started for the first time in 3GPP

Rel.16 following the standardisation of the NR, with the work item RP-190766 entitled "5G V2X with NR sidelink", which was finalized in March 2019 [28]. The goal with NR V2X is not to replace the LTE sidelink for providing basic road safety services, but to rather support interworking with LTE V2X, complementing it for the 25 advanced V2X services that were categorized into four groups by the SA1 committee of 3GPP: platooning, advanced driving, extended sensors and remote driving. In 3GPP Rel.16, TS 22.186 specifies the requirements for these four advanced V2X use case categories together with two more areas covering general aspects and vehicle quality of service support [32]. Some of the use case categories (e.g. extended sensors) require high data rates, along with low latency and high reliability. Also, the inter-operability between LTE V2X and NR-V2X needs to be defined, where NR V2X will support unicast and groupcast in addition to the broadcast functionality supported by LTE sidelink.

The NR V2X work item, which started in April 2019, is planned to be finalized in March 2020, and it will be included in TR 37.985. However, many required features could not be introduced in 3GPP Rel.16 due to the stringent timeline. These features include:

- Positioning using the sidelink feature to fulfil the requirements of approximately 30 cm positioning accuracy.
- Relaying between vehicles e.g. bridging wider distances in case of out-of-coverage.
- MIMO enhancements.

In addition, organisations such as the 5GAA has defined new use cases for the future, which are likely to appear in Rel.17 and beyond of the 3GPP specifications for V2X.

3) <u>ETSI ITS Standards</u>

Within Europe, Cooperative Intelligent Transport Systems (C-ITS) has been standardised by ETSI and CEN/ISO, based on the Mandate M/453 in 2009. The ETSI ITS group has developed specifications for a short-range communication technology referred to as ITS-G5, based on the standard IEEE 802.11p. Both ETSI and CEN/ISO have also specified message sets to support the C-ITS applications. In February 2014 the so-called "Release 1 specifications" developed by CEN and ETSI were issued. This group of more than 70 specifications were the starting point for several pilots and pre-deployment projects in Europe. The specifications were also used by Car-2-Car Communication Consortium and C-Roads Platform to define "profiles" to align specifications in order to reach a minimum level of interoperability for C-ITS services. This work has been used as a technical input for the Delegated Regulation on C-ITS.

The European Commission has adopted this Delegated Regulation – C(2019)1789 – for C-ITS on March 13, 2019 [16]. The act is based on the ITS Directive 2010/40/EU, which accelerates the deployment of these innovative transport technologies across Europe. This act defines new rules for stepping up the deployment of C-ITS on Europe's roads. In this act, descriptions of the 16 V2V services and 15 I2V services are given, including the description of the service and the triggering conditions to start sending C-ITS messages. The non-3GPP standards for the messages from ETSI and CEN can be found in Annex I of [16].

The C-ITS messages may be sent between vehicles and/or roadside infrastructure via both short-range and long-range communication technologies. The current version of the act describes only the additional requirements and specifications for short-range communication via ITS-G5 in the frequency band 5.855 – 5.925 GHz in Annex II of [16]. This technology for the listed C-ITS priority services may be combined with long-range communication via 5G network infrastructure or with direct C-V2X communication (via PC5 air interface) with LTE or 5G NR radio technologies for the use case categories of 5G-MOBIX.

Within ETSI several work items were initiated and finalized to include 3GPP-technologies in updates or amendments of the ETSI ITS specifications, where the applications and facilities layer (=messages) as well as the network layer (with non-IP protocols BTP and GeoNetworking) of the ETSI ITS standards are agnostic to the underlying radio technology.

The additional new ETSI ITS specifications for Cellular-V2X via PC5 air interface are:

- ETSI TS 102 636-7-1 V1.1.1 (2019-01) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 7: Amendments for LTE-V2X; Sub-part 1: Amendments to ETSI EN 302 636-4-1 (Media-Independent Functionality): includes the GeoNetworking packet structure for LTE-V2X access layer technology.
- ETSI TS 102 636-7-2 V1.1.1 (2019-01) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 7: Amendments for LTE-V2X; Sub-part 2: Amendments to ETSI EN 302 636-5-1 (Basic Transport Protocol): includes the BTP packet structure for LTE-V2X access layer technology (with MAC, RLC, PDCP and non-IP headers). To be included in ETSI EN 302 636-5-1 V2.2.0 (2019-02) (Under approval).
- ETSI TS 103 613 V1.1.1 (2018-11) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems using LTE Vehicle to everything communication in the 5.9 GHz frequency band: includes LTE-V2X access layer specifications with references to 3GPP LTE specifications.
- ETSI TS 103 574 V1.1.1 (2018-11) Intelligent Transport Systems (ITS); Congestion Control Mechanisms for the C-V2X PC5 interface; Access layer part.

Updates of these ETSI ITS specifications for 5G C-V2X shall be expected when 3GPP specifications on C-V2X with 5G NR via the PC5 interface are finalized and approved in 3GPP Rel.16.

Annex 3 – ES-PT CBC components & features details

Nokia AirScale components to support NOS network (PT)

1) ***AirScale 5G BTS***

Nokia proposes Classical 5G BTS portfolio for simple deployment to provide the necessary network and technology for 5G-MOBIX trials.

2) Classical BTS

The Classical BTS is the 3GPP compliant Nokia AirScale, which consists of:

- one AirScale sub-rack AMIA including backplane for high bandwidth connectivity between processing plug-in units.
- one or two AirScale Common ASIK plug-in unit(s) for transport interfacing and for centralized processing.
- one-to-max-six AirScale Capacity ABIL plug-in unit(s) for baseband processing and for optical CPRI and eCPRI interfaces to the radio units.
- one-to-max-six AirScale Active Antennas Subsystems.

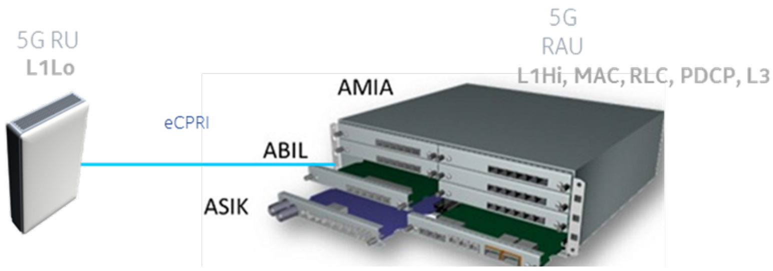


Figure 49: Nokia AirScale 5G NR base station

In the minimum configuration, the AirScale baseband consist of AMIA Subrack with one ASIK and one ABIL card. One ASIK card can host up to three ABIL cards. The common ASIK plug-in unit offers:

- Ethernet transport.
- Synchronization.
- Local O&M.
- Optional L2nrt and L3 layers (in case of Cloud BTS L2nrt and L3 layers hosted in Airframe).

Transport connections from the ASIK cards to the backhaul offer various capacities starting from 1GB up to 25GB depending on the used connectors and fiber. It supports QoS aware Ethernet switching which allows single backhaul interface to be used for all RATs without external cell site gateways. The ABIL is used for 5G operation only together with the ASIK card and handles L1 processing with or without L1 high/low split and L2rt processing. Frontend connection to radio unit is planned to support both CPRI and eCPRI. All AirScale Subracks can be shared between the deployed RATs, where 5G RAT is then limited on one half of the Subrack and the other half is used e.g. by 4G or SRAN.

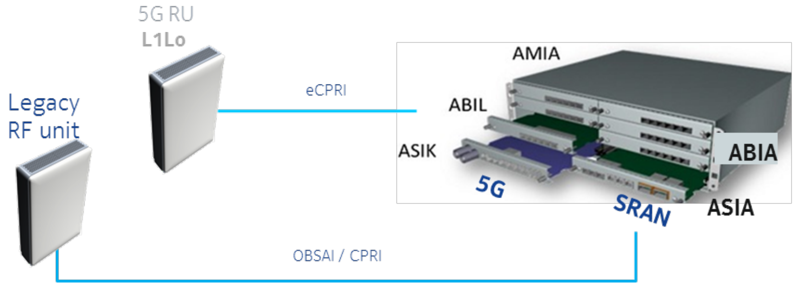


Figure 50: AirScale sub rack sharing - 5G and SRAN within the same AirScale AMIA module

3) AirScale System Module

AirScale System Module is OBSAI/CPRI compatible and has all the required control and baseband functions for the supported radio access technologies. The basic functionalities of AirScale System Module are:

- Baseband processing and de-centralized control.
- Transport control and integrated Ethernet, and IPv4/v6 and IPSec Transport.
- BTS clock and timing generation and distribution.
- BTS operation and maintenance.
- Central radio interface control.

Nokia AirScale System Module consists of a high capacity indoor AirScale subrack (AMIA) or a high capacity outdoor AirScale subrack (AMOB) with AirScale Common (ASIx) and AirScale Capacity (ABIx) plug-in units. AirScale System Module Indoor (AirScale SM Indoor) includes the following modules and plug-in units/modules:

- AMIA, Indoor subrack with backplane and fans.
- ASIx, Indoor Common plug-in unit.
- ABIx, Indoor Capacity Extension plug-in unit.

4) AirScale Indoor Subrack, AMIA

The features of AirScale Indoor Subrack, AMIA are as follows:

- 3U height.
- 8 Plug-in Units.
  - 2x Common Units.
  - 6x Capacity Units.
- Volume: 23 litres.
- Weight: ~23 Kg fully equipped.
- Operational temperature range: -5°C to + 60 °C.
- 19" rack, shelters, pole, wall, indoor cabinet (FCIA), outdoor cabinet with protection (FCOB).

5) AirScale Indoor Common Plug-in Unit, ASIK

The features of AirScale Indoor Common Plug-in Unit, ASIK are as follows:

- Indoor AirScale common unit supporting 5G.
- Supporting up to 3 capacity units.
- Control, transport, O&M processing integrated.
- Synchronisation and timing functions.
- Power supply and thermal control of system module.
- System Extension Interfaces for chaining of multiple AirScale System Modules.

- Up to 2 ASIK units in Subrack.

6) AirScale Indoor Common Plug-in Unit, ASIA

The features of AirScale Indoor Common Plug-in Unit, ASIA are as follows:

- Indoor AirScale common unit supporting 2G, 3G and 4G.
- Supporting up to 3 baseband capacity units.
- Control, transport, O&M processing integrated.
- Synchronisation and timing functions.
- Power supply and thermal control of system module.
- System Extension Interfaces for chaining of multiple AirScale System Modules.
- Up to 2 ASIA units in Subrack.

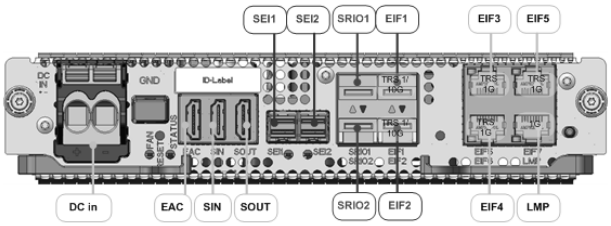


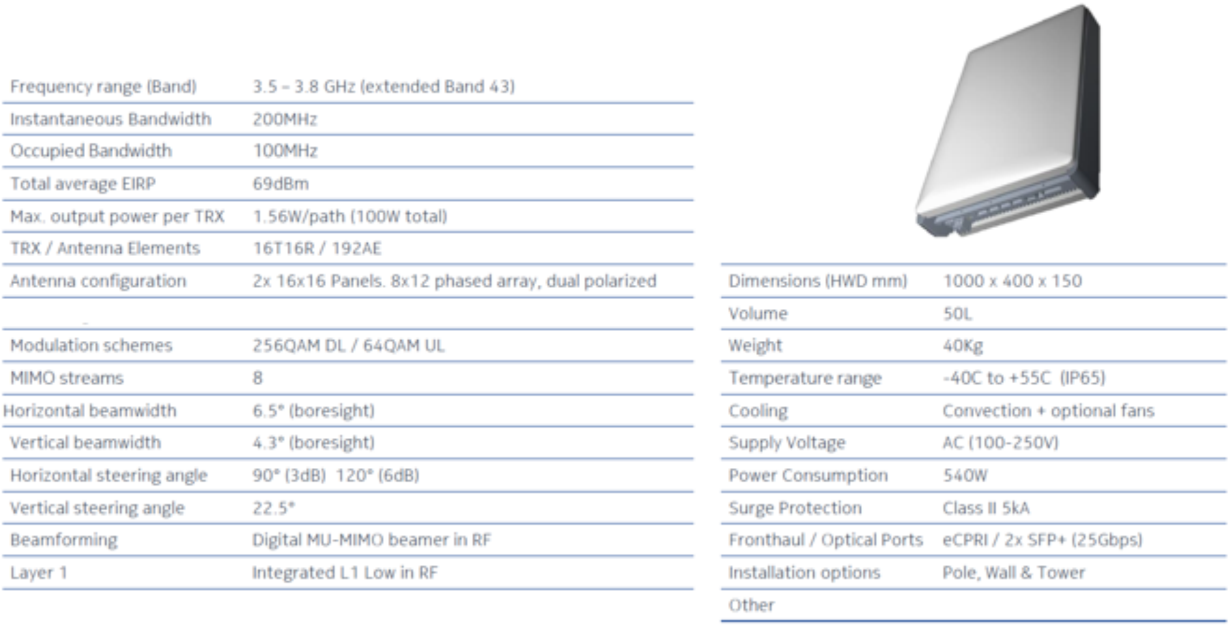
Figure 51: AirScale Indoor Common plug-in Unit, ASIA

7) AirScale Capacity Plug-in Unit, ABIA

AirScale Capacity plug-in unit, ABIA occupies half the width of a 19-inch subrack with an IP class of IP20. AirScale System Module Indoor can consist of up to six AirScale Capacity (ABIA). ABIA unit has six optical RF interfaces up to 6 Gbps OBSAI or 9.8 Gbps CPRI. ABIA can be shared for multiple technologies, e.g. WCDMA and LTE.

Nokia components in Telefonica network (ER)

8) 3500-3800 MHz 5G NR antenna



Frequency range (Band)	3.5 – 3.8 GHz (extended Band 43)
Instantaneous Bandwidth	200MHz
Occupied Bandwidth	100MHz
Total average EIRP	69dBm
Max. output power per TRX	1.56W/path (100W total)
TRX / Antenna Elements	16T16R / 192AE
Antenna configuration	2x 16x16 Panels. 8x12 phased array, dual polarized
Modulation schemes	256QAM DL / 64QAM UL
MIMO streams	8
Horizontal beamwidth	6.5° (boresight)
Vertical beamwidth	4.3° (boresight)
Horizontal steering angle	90° (3dB) 120° (6dB)
Vertical steering angle	22.5°
Beamforming	Digital MU-MIMO beamer in RF
Layer 1	Integrated L1 Low in RF

Dimensions (HWD mm)	1000 x 400 x 150
Volume	50L
Weight	40Kg
Temperature range	-40C to +55C (IP65)
Cooling	Convection + optional fans
Supply Voltage	AC (100-250V)
Power Consumption	540W
Surge Protection	Class II 5kA
Fronthaul / Optical Ports	eCPRI / 2x SFP+ (25Gbps)
Installation options	Pole, Wall & Tower
Other	

Annex 4 – GR-TR CBC components & features details

Ericsson RAN components for the GR-TR CBC

1) 4G/5G compute baseband 6630

To implement the NSA architecture two (2) baseband 6630 units will be used. The Baseband 6630 provides 4G and 5G functionality featuring an extremely high processing capacity. Baseband 6630 is based on Ericsson Multi-Core Architecture (EMCA) composed of up to 256 processor cores driven by a state-of-the art multi-threat processing SW. This offers large processing capacity needed to handle LTE-A functionality as well as 5G NR. The baseband 6630 supports both Common Public Radio Interface (CPRI) and evolved CPRI (eCPRI) interface connectivity, which means that it can be used either for connecting to passive or Active Antenna System (AAS), the latter based on the new eCPRI transport technology.

The first baseband will act as radio access processing platform for the LTE-A SW providing an NR anchor layer for the control plane according to NSA option 3x implementation. The interface towards the distributed radio unit will be based on a star configuration according to CPRI transport protocol. The second baseband will act as radio access processing platform for the 5G NR protocol providing V2X OBU connectivity to the 5G virtual Evolved Packet Core network (vEPC) via 5G NR user plane.

Figure 52: Baseband 6630 front panel

2) Active Antenna System (AAS) AIR 6488 B42F

The AIR 6488 unit will be used to deploy NR coverage in the selected macro site. The NR carrier will have an instantaneous bandwidth (IBW) of 100 MHz and will be operated in the band B42F (3420-3600) MHz. Active Integrated Radio, AIR 6488 is an AAS with 64 transmitters and 64 receivers, i.e., AAS TDD 64TR. AIR 6488 enhanced radio performance can be achieved thought interference suppression by applying beam-forming capabilities in the downlink (DL) and uplink (UL). System capacity can be increased by scheduling users on different layers supporting both Single User MIMO (SU-MIMO) and Multi User MIMO (MU-MIMO). Application coverage is improved through beam-forming in both the vertical and horizontal dimensions. The AIR 6488 unit is a massive MIMO product supporting advanced RAN functionality. The main benefits compared to conventional macro solutions are:

- Enhanced coverage - high gain adaptive beamforming.
- Enhanced capacity - high order spatial multiplexing and multi-user MIMO.
- Advanced RAN features - vertical and horizontal beamforming.
- Improved network performance - low inter-cell interference.

Figure 53: AIR 6488

3) Ericsson Radio System, Radio 2212 B7

Radio 2212 is an outdoor 2T/2R macro radio with 2x80W output power. The small size of the radio unit makes it an ideal solution for locating the distributed passive radio unit near the antenna. An optic cable connects the radio to the baseband 6630. The distributed radio can be connected in a star configuration or in a cascade configuration with optical cable links, if needed. The radio 2212 will be used to implement LTE-A coverage in the selected macro site. The LTE-A carrier will have an instantaneous bandwidth (IBW) of 20 MHz and operated in band B7 (2620-2690) MHz.

4) GPS03 for Network Synchronisation

The GNSS receiver system is used as a reference source for frequency or time synchronisation of the gNB/eNB. The primary components of the GPS receiver system are the GPS antenna or dual band antenna (GPS+GLONASS) /LNA, the GRU (GPS Receiver Unit) and interconnecting cable.

5) UL-DL decoupling

UL/DL decoupling is the cornerstone of the NSA architecture and it will be enabled in the 5G NR mobile network. For EN-DC, it provides improved 5G coverage by selecting the best service between LTE and NR for uplink and downlink separately.

When using a split bearer UL/DL decoupling allows the NR spectrum with superior peak data rate and latency to be used for configured downlink. The configured uplink leverages the superior LTE coverage.

The UL and DL data transmissions are based on NR measurements, enabling separate leg switching. When the NR UL quality becomes sub-optimal, the UL user plane transmission is switched to the LTE leg. When the bearer can take advantage of the high quality of the NR coverage again, it switches back from LTE to the NR leg.

Similarly, when the NR DL quality becomes sub-optimal, the user plane transmission is switched to the LTE leg. When the bearer can take advantage of the high quality of the NR coverage again, it switches back from LTE to the NR leg.

6) Massive MIMO (mMIMO) Mid-band Enabler

mMIMO is an important functionality that will enable a flexible cell coverage to tailor the specific site application environment. This is achieved with cell shaping for Mid-Band.

Three profiles (macro, hot spot, high-rise) are supported for cell shaping. All common channels are aligned to these cell shapes as well as the envelop of the UE specific traffic beams. Further, Ericsson proprietary implementation of common channel cell shaping provides additional coverage gain vs. industry common implementation.

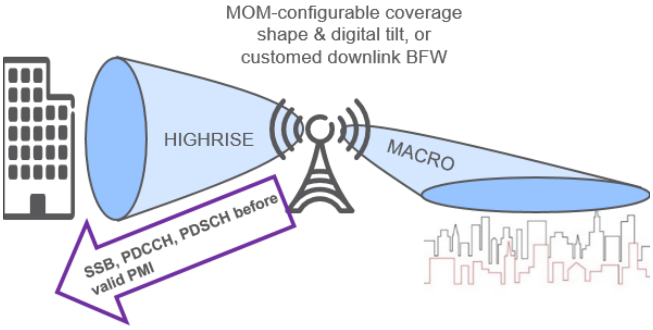

MOM-configurable coverage shape & digital tilt, or customed downlink BFW
HIGHRISE
MACRO
SSB, PDCCH, PDSCH before valid PMI

Figure 54: Common Beamforming with Configurable Coverage Shape

Initial testing indicates coverage benefits up to 3-4 dB (depending on deployment scenario and specific comparison), compared to the industry common solution.

In addition, Massive MIMO (mMIMO) Mid-band function offers enhanced capacity and data rate coverage with beamforming. In the initial release, mMIMO supports Single-User, SU- MIMO, with up to 4 layers. Both horizontal and vertical beamforming are supported. The first NR release implements codebook-based beamforming for better coverage and higher single user peak rate.

SU-MIMO reaches the following peak throughput rates in assuming a TDD (Time Division Duplexing) pattern with 3 DL and 1 UL slots and 1+1 DMRS (Demodulation reference symbols):

- 1.45 Gbps in downlink with 256 QAM.
- 108 Mbps in uplink with 64 QAM.

7) <u>Mobility</u>

Mobility for NR NSA capable devices that are outside NR coverage (for example, without an established split DRB) is handled as in legacy LTE.

If the UE has established a split DRB in NR coverage, LTE intra-frequency mobility is supported. The NR leg for a split DRB is released if an adjacent LTE cell, based on the A3 measurement report, has better characteristics than the serving LTE cell. The secondary node terminated split bearer is reconfigured as master node terminated DRB. In this case, LTE intra-frequency handover is performed the same as in legacy LTE with the next A3 measurement report. A blind (that is, configuration-based) or a measurement-based NR leg setup is initiated once the handover procedure is completed.

8) <u>Massive IoT</u>

A large portion of time of international transport is wasted at European border crossing in South East Europe (SEE), significantly raising the cost and delivery time of goods and contributing to the segmentation of international logistics. The use of 4G/5G networks in combination with advanced cooperative connected and automated mobility (CCAM) functionality can significantly contribute to the mitigation of the border control delays by providing customs agents with advanced functionalities enabling inspection preparation, enhanced flow of information and instant status verification and which can under the right circumstances realize a "zero-touch" border crossing.

As trucks approach the border crossing an exchange of information is commencing towards the border authorities via 4G+/5G network from the cargo which will be equipped with relevant sensors facilitating border inspection and prepare custom agents for the appropriate checks. Additional information can be exchanged over the 5G networks of the neighbouring countries facilitating the acquisition of relevant information about specific truck (e.g. driver's information, travel history, cargo inventory) which could speed-up the control process.

Ericsson proposes the use of internet of things (IoT) technologies to support the exchange of information among sensor data or road infrastructure and cloud application servers facilitating border inspection and prepare custom agents for the appropriate checks. NB-IoT, being a narrowband system, can be used to provide low-cost, low-power, wide area cellular connectivity for the IoT applications. NB-IoT has been designed to have excellent coexistence performance with LTE technology and be compatible with NR.

NB-IoT Access: In-band deployment mode

NB-IoT requires 180 kHz minimum system bandwidth for both DL and UL, respectively.

For the 5G-MOBIX project, in-band deployment will be considered, which means that the presence of an LTE 800 MHz cell is assumed. The NB-IoT carrier will be located within the PRBs of the existing LTE 800 system, the anchor PRB. The middle 6 PRBs of the LTE system will never be considered for NB-IoT deployment since they contain synchronisation signals and system information broadcast for LTE.

To provide coverage for NB-IoT services, the following network equipment will be needed in the access site:

- LTE 800 MHz (B20) layer.
- NB-IoT SW enabled.
- NB-IoT compatible devices at 800 MHz.
- SIM cards for NB-IoT devices.

Core network c-SGN support, 3GPP Rel.13.

Annex 5 – DE 5G architecture

Figure 55 illustrates the overall communication infrastructure in German trial site, which consists of three main segments: cloud infrastructure, mobile broadband network infrastructure and road infrastructure (including road and road side deployment).

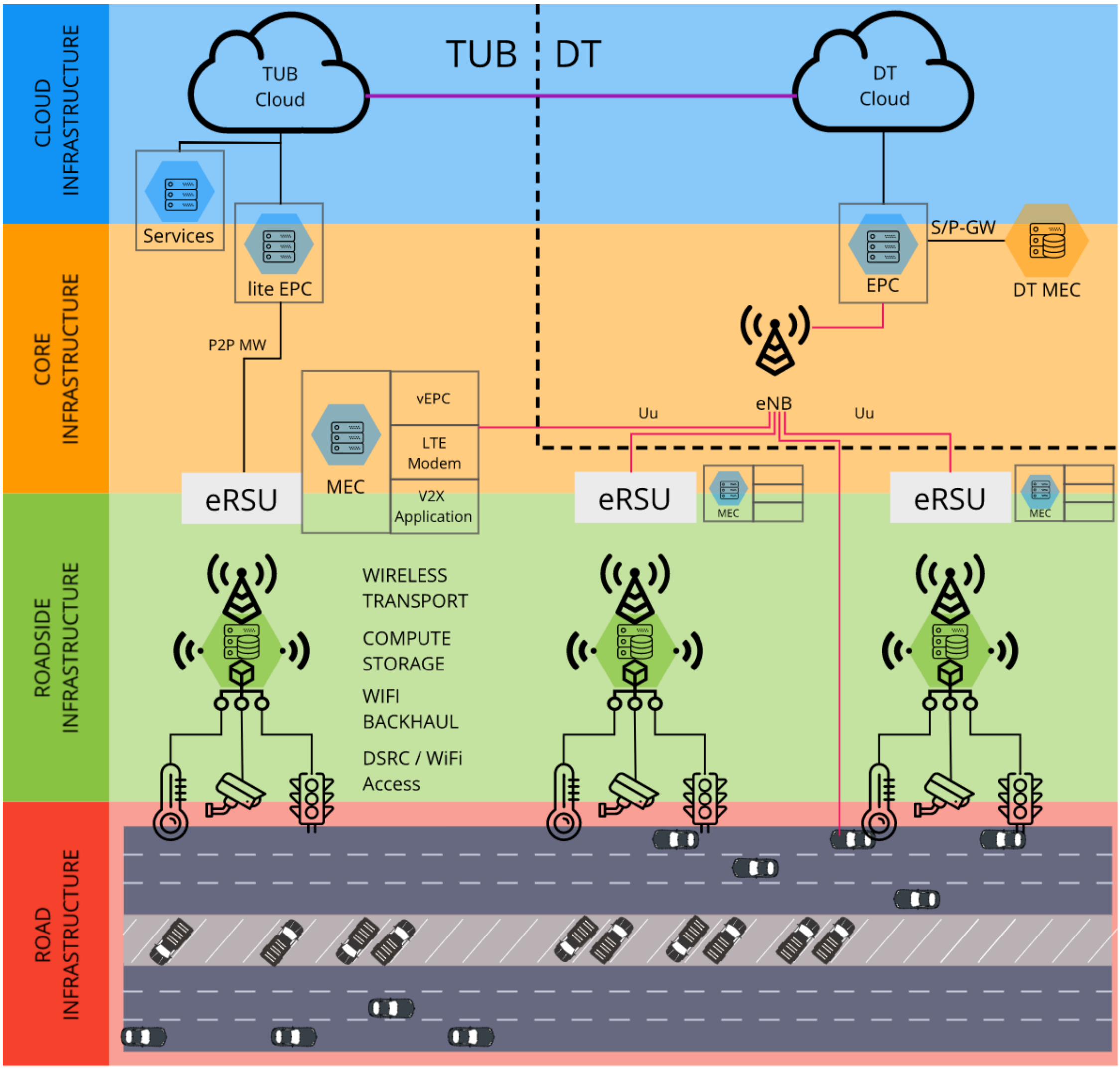


Figure 55: End-to-end network architecture of German trial site.

The road and roadside infrastructure comprise sensors and roadside units. The details are available in deliverables D2.3 [2] and D2.4 [3]. Important for the scope of this document is that the roadside units are directly connected to the sensors and contain compute resources that are referred to as near edge component. The eRSUs are also connected to the data centre through P2P and P2mP Microwave links besides mobile network interface.

A mobile network core is provided by TUB with several options. Two core network implementations, virtual EPC and virtual lite-EPC, can be deployed globally in datacentre or locally in near edge infrastructure. The lite-EPC implements the necessary functions for the management of the current infrastructure and will also support the functions necessary to implement the user stories and to integrate the DTs network infrastructure. Another MNO infrastructure is going to be provided by Deutsche Telekom (DT) and will be rolled out in Phase 2, which integrates the DT MEC and MN infrastructure with TUBs infrastructure.

Radio network requirements

The focus of the German trial site test facility is on extending vehicle perceptions with high definition data about road infrastructure to support the user stories "SAE L4 platooning" and "Cooperative driving with HD-maps and surround view". The different layers of road digitalisation of German trial site, i.e., vehicle layer, road infrastructure layer and cloud layer, are seamlessly integrated to provide a complete digital world for AVs and enable coordinated decision making in different system levels. Therefore, the radio network must meet the challenging requirements for enabling interactions between AVs, road sensors, distributed application on MEC nodes and cloud infrastructure. Figure 56 shows a general picture of the data generation and consumption flows at different layer of the German trial site.

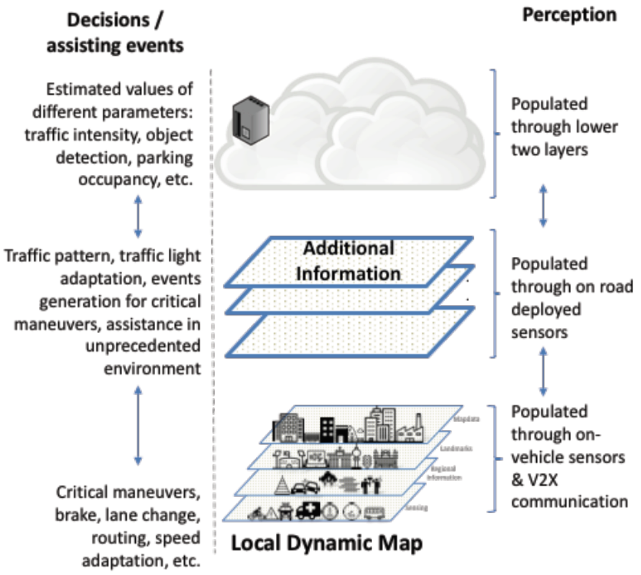
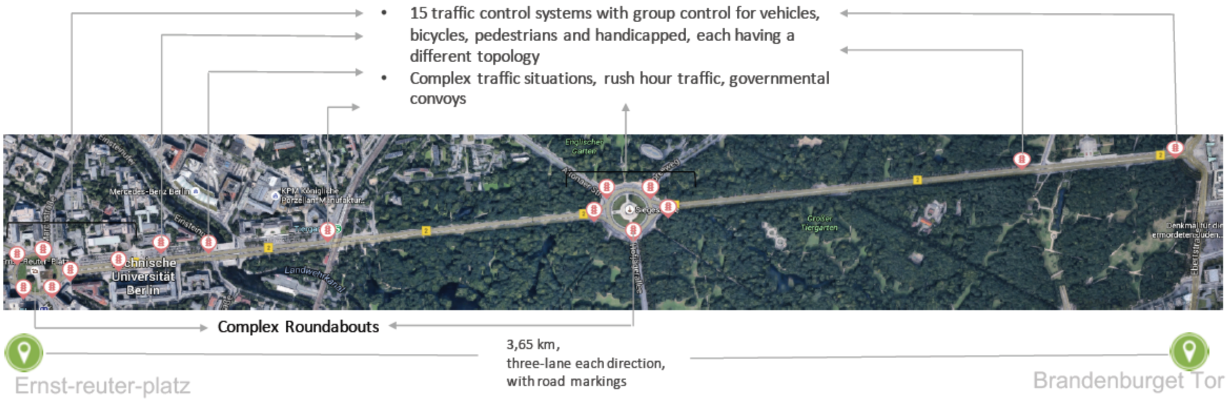

Decisions / assisting events
Perception
Estimated values of different parameters: traffic intensity, object detection, parking occupancy, etc.
Populated through lower two layers
Traffic pattern, traffic light adaptation, events generation for critical maneuvers, assistance in unprecedented environment
Additional Information
Populated through on road deployed sensors
Critical maneuvers, brake, lane change, routing, speed adaptation, etc.
Populated through on-vehicle sensors & V2X communication
Local Dynamic Map

Figure 56: Data generation and consumption flows at different layer of the German trial site

Network infrastructure requirements

Radio network infrastructure plays an important part the German trial site's road infrastructure, which enables the connectivity of all IoT devices, CCAM applications and ITS services on cloud, road infrastructure and AVs. Consequently, the design and deployment of the access network are driven by challenges and requirements, e.g., full network coverage, massive amount of data, high mobility, high availability, heterogeneous device and application types, efficient management, among others.

Figure 57 represents the ground truth of the German test site. There are two roundabouts with 5 ins and 5 outs with three lanes in each direction. There are 5 traffic lights at each roundabout. Coexistence of an autonomous vehicle with traditional vehicles in these roundabouts requires efficient control and precise information. The test road consists of a densely populated area and an unpopulated area. Such geographical setting results in different traffic patterns that affect CCAM user stories' trial. Moreover, in these two areas with different existing transport network deployment, suitable radio access networks technologies and deployment must be considered to meet feasibility and cost requirements.



15 traffic control systems with group control for vehicles, bicycles, pedestrians and handicapped, each having a different topology
Complex traffic situations, rush hour traffic, governmental convoys
Complex Roundabouts
3,65 km, three-lane each direction, with road markings
Ernst-reuter-platz
Brandenburget Tor

Figure 57 Complexity of German test road as ground truth for radio network requirement analysis.

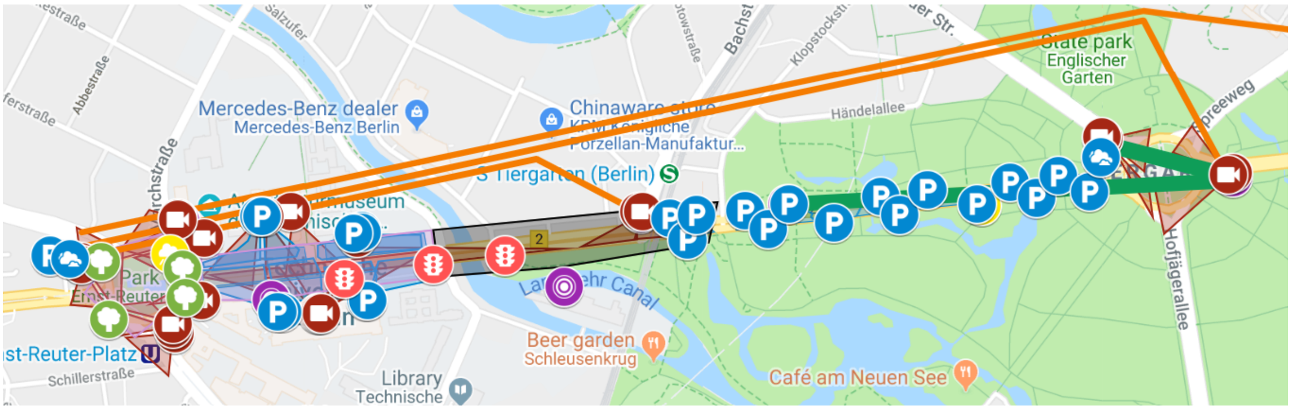


Figure 58 Overview of sensors deployment on German test road in phase 1.

Table 20 provides an analysis of data communication requirements of each type of sensor deployed in the German trial site, shown in Figure 55. A rough estimation results in around 3 GB of aggregated sensor data generated per minute.

Table 20 Sensor data generated in radio access network of German trial site.

Dense Deployment	Sensors/km²	Raw data generation kB/minute	Description
Environmental	4	192,00	Populated Areas, high resolution measurements

Road Condition	8	2.880,00	High-risk areas (bridges, parks, boulevards)
Weather	1	3.600,00	
Parking	50	720.000,00	No high buildings, only 6-15m building or street light height
Traffic	30	2.178.000,00	Large intersections, dense traffic
Vehicle	4	161.297,70	
Sum		**3.065.969,70**	**Kilobyte/Minute**

Beside the large amount of data generated, the available and optimal communication interfaces of the sensors are different. While wireline interfaces are preferred, a large part of the trial site can only be covered with wireless technologies. Depending on the type of sensor and data requirements, Wi-Fi-, Bluetooth, DSRC and broadband 4G (and future 5G) interfaces are required for the communication of sensor data. This results in a heterogeneous radio access network, which requires efficient management.

Near edge infrastructure deployed on eRSUs enables large amount of data to be consumed on the road infrastructure by instances of CCAM applications deployed there. This eliminates the transfer of raw sensor data to data centres. This makes eRSU coverage a good complement to 5G for V2X communication requirements. However, it requires an efficient management and orchestration of both type of networks and CCAM services.

To achieve high mobility, the radio network is required to provide full wireless coverage, high availability and low delay. Depending on the deployment location of the IoT devices, different radio technologies (Bluetooth, Wi-Fi, 4G/5G) are deployed to provide coverage to all network devices. The connectivity quality of wireless technologies is subject to device mobility and operation environment. In order to achieve high availability, radio network is required to have self-healing capability. This allows data to be transferred through interrupted wireless links to be rerouted through alternative redundant paths. The devices and eRSUs are therefore equipped with multiple radio interfaces allowing constant connectivity to infrastructure networks.

Core network requirements

Core options

With the intended mobile broadband networks in German trial site, core networks will be available with a commercial deployment using physical and virtual 5G core function and a virtual 4G/5G core deployed in far edge infrastructure/testbed. For both core network options, a set of APIs must be defined which are required to meet the above-mentioned functional requirements, especially mobility management, flexible data flow control and cross provider network orchestration.

MEC deployment

Given the high mobility nature of autonomous vehicle applications, mobile broadband network has been the baseline infrastructure for the design of their MEC enabled architecture. The ETSI MEC reference architecture [17] components are required to be flexibly placed in the 4G/5G infrastructure of the German trial site. We extend the mobile network with small cell (SC) segments covered by eRSUs. Mobile Edge Host (MEH) is the eRSU component that provides computing, storage, network capacity for edge applications. Depending on how close the applications are required to be placed towards UEs and AVs, they must be dynamically deployed on MEHs available in different mobile network segments.

A Small Cell network segment includes densely deployed RSUs with multiple short-range network interfaces, i.e., DSRC, Wi-Fi, WSN, which cover a road segment. AV applications are especially delay-sensitive, e.g., intersection collision warning, real-time situation awareness and see-through applications. The data locally generated by AV sensors and roadside components are combined with downstream data from cloud services to provide AV agents context for autonomous decision-making. AVs are equipped with the same wireless interfaces for V2X communication.

Due to the wider coverage of Radio Access Network (RAN) components (eNB/gNB), mobile edge applications (MEA) are expected to aggregate situational data from AVs and road sensors and provide AVs with broader context for more strategical decision-making. Towards Core Network (CN) and Service segment, critical MEAs are increasingly concerned with the management and orchestration of mobile network provisioning, and MEC infrastructure in lower network segment. Disappearing network and computing constraints of centralized computing infrastructures allow core network and service applications to be deployed in datacentres or dedicated servers. Nevertheless, they may take advantage of management and orchestration functions for Mobile Edge Platforms (MEP).

Roaming

As there is only one MNO in the German Trial, actual roaming is not supported in the German Trial site. However, roaming scenarios can be realized by using the two separate mobile network cores of both TUB and DT through DT PLMN.

Interdependencies with other infrastructure

The communication infrastructure in German trial site consists of multiple layers serving specific CCAM infrastructure. From 5G network perspective, two main network interaction domains can be identified: core and access domains. In the core network, multiple core deployments interact for the secure, low delay forwarding of user data to the multiple core MEC platform. The interactions are realized through the configuration of the core network to expose the network functions to the different MEC services. Such interaction can be generalized for multiple core network slices. On the access network, the eRSU infrastructure relies on the 5G data plane as backhaul transport network for sensor data, traffic control messages, and V2X messages. Therefore, main interactions with 5G network involves 5G C-V2X related interface and functions.

Radio network architecture

The radio network of German trial site consists of both a small-cell network provided by eRSUs along the test road and broad band 4G/5G coverage. Radio network infrastructure provides a gapless coverage for all sensors, AVs, and roadside MEC components near to the test road (near edge). The small cell eRSUs are densely deployed and provide high bandwidth and low latency wireless communication links for V2V, V2I, and sensor data. Figure 59 shows the deployed eRSU in this phase of the project. Additional eRSUs will be deployed to increase the density of small-cell network coverage. Where wireline is not available, e.g., outside TUB campus area, dedicated Hop-to-hop Wi-Fi and microware interfaces provide high bandwidth links connecting the eRSUs to far edge and cloud infrastructure.

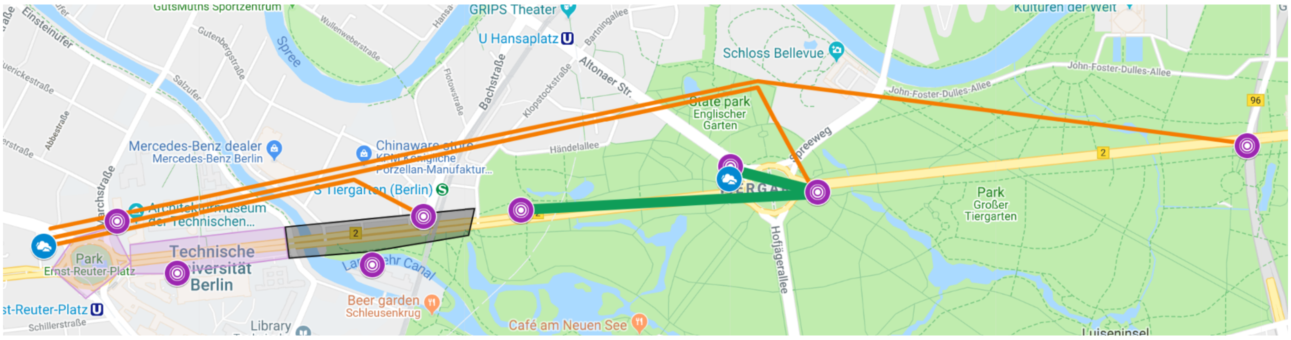


Figure 59: eRSU radio access network in German trial site.

The access network is provided by TUB and Deutsche Telekom. TUB 4G/5G testbed provides mobile broadband coverage to the TUB campus area (left part of Figure 59). DT 5G network covers the other part of the German trial site (right part of Figure 59). The mobile broadband networks serve as uplink interfaces for the eRSUs and as communication links for AVs and sensor devices depending on their communication capability and locations, i.e., where there is lack of eRSU coverage.

Network configuration and deployment options

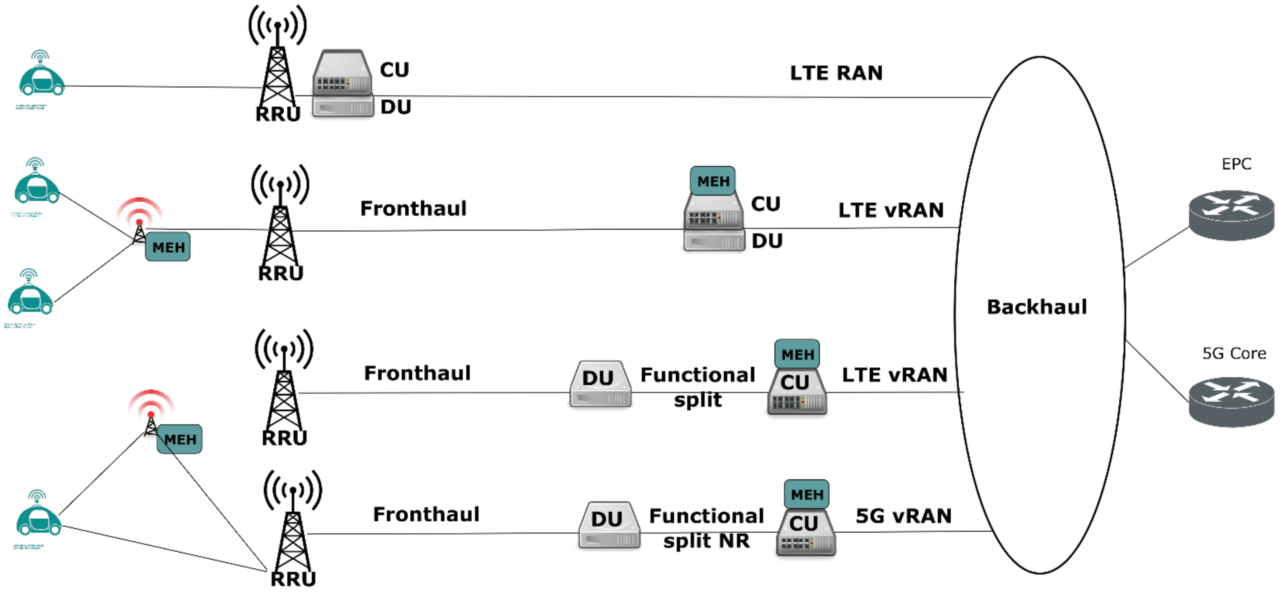


Figure 60: Network configuration and deployment options

To meet the communication requirements of the infrastructure, the small-cell and broadband networks are configured to complement each other and enable flexible control of data flows to meet CCAM services' QoS requirements. Such efficient control of end-to-end network flows is achieved by relying on edge computing capability deployed across the network segments for the placement of virtual core network or SDN control functions. This results in different network slice configurations showed in Figure 60. In current 4G network, AVs and sensor devices are connected using DT's LTE network. AVs and sensors can also be connected using eRSUs wireless interfaces. In this setting, MEC component on the eRSUs allows application-aware network control application to be deployed and direct data flow among the devices and local CCAM instances. These control applications are orchestrated by a global control application deployed in the far edge or data centre. The eRSUs rely on 4G/5G network to provide transport network for their connected devices.

Frequency bands

The small-cell networks provided by the eRSUs have overlapping coverage of different wireless technologies. For low latency V2X communication, an IEEE 802.11p based DSRC interface is deployed using 5.9 GHz band. Wi-Fi coverage is provided by dual-band interfaces. Sensors and AVs communicate with eRSU over Wi-Fi in the 2.4 GHz band. 5 GHz Wi-Fi band is used for the point-to-point links between eRSUs forming the eRSU backhaul network.

Mobile broadband networks use the licensed frequency of their respective MNOs. The new 3.6 GHz frequency band will be used for Deutsche Telekom's 5G NR networks. This will allow high data rates at significantly faster speeds and low latencies. Channel bandwidths of 100 MHz are suitable for more dataintensive applications and for the precise supply of smaller radio cells. The 2GHz frequency band continues to be used for 4G coverage.

TUB Access Network

The radio access network will consist of TUB deployed short range communication small cells (~12 small cells) and 4G/5G macro-cell covering the test-road. It is worth highlighting here that for the on-going trials, the roadside units, on-road deployed sensors, and vehicles make use of the 4G technologies. Mobile broadband infrastructure will be extended to 5G technologies during the project in alignment with German 5G roll-out. Further development of network infrastructure in the German trial site looks as follows:

Phase 1: Deployed and Functional

Since the trial site has already executed the deployment phases of the CCAM road infrastructure and roadside units, the communication infrastructure is already in place and functional. Figure 61 provides a pictorial overview of the functional communication infrastructure. However, in this section, the focus is confined to radio and backhaul.

Phase 2: Intermediate Deployment

It is planned to connect the TUB communication infrastructure with the MEC of Deutsche Telecom. The 4G (commercial deployment) of Deutsche Telecom is already used for enabling the communication of on-road deployed sensors and vehicles with the data-centre of the TUB. A test APN (Access Point Name) is used to connect to the Deutsche Telekom MEC. While the integration plan is being finalized between TUB and DT, some parts, relevant for the execution of the user stories, are described in the following.

Figure 62 shows the architecture of DT access network and MEC, Figure 63 shows the integration of TUB and DT infrastructure. TUB's eRSUs, the vehicles used in trials, as well as some of the roadside sensors are able to connect through the mobile network of DT to the MEC of DT by using the provided test APN. Vehicles and sensors may connect to the MEC of eRSUs using either Wi-Fi or ITS G5/DSRC for a direct connection. These technologies will be replaced by C-V2X once the 5G networks are deployed. LTE/5G networks provide additional connectivity through the internet. The user stories planned for this trial site require a service handover between MECs of different providers triggered by vehicle mobility. The following options are considered for this phase:

<u>Option A: Network level</u>

In this phase, DT has full control over the network stretch between the UEs and the DT MEC. Due to the configuration of the DT test APN, any L3 traffic is routed to the DT MEC. However, the DT MEC infrastructure allows for NAT/rerouting traffic to the TUB MEC. To execute the handover, a handover message is generated at either the vehicle triggered by its GPS location, or at the eRSU level based on a connect/disconnect event through V2I interfaces. This handover message is sent to the handover handling function in DT MEC, which then implements NAT/reroute flow rules and triggers the service handover of the V2X application in DT MEC to TUB MEC.

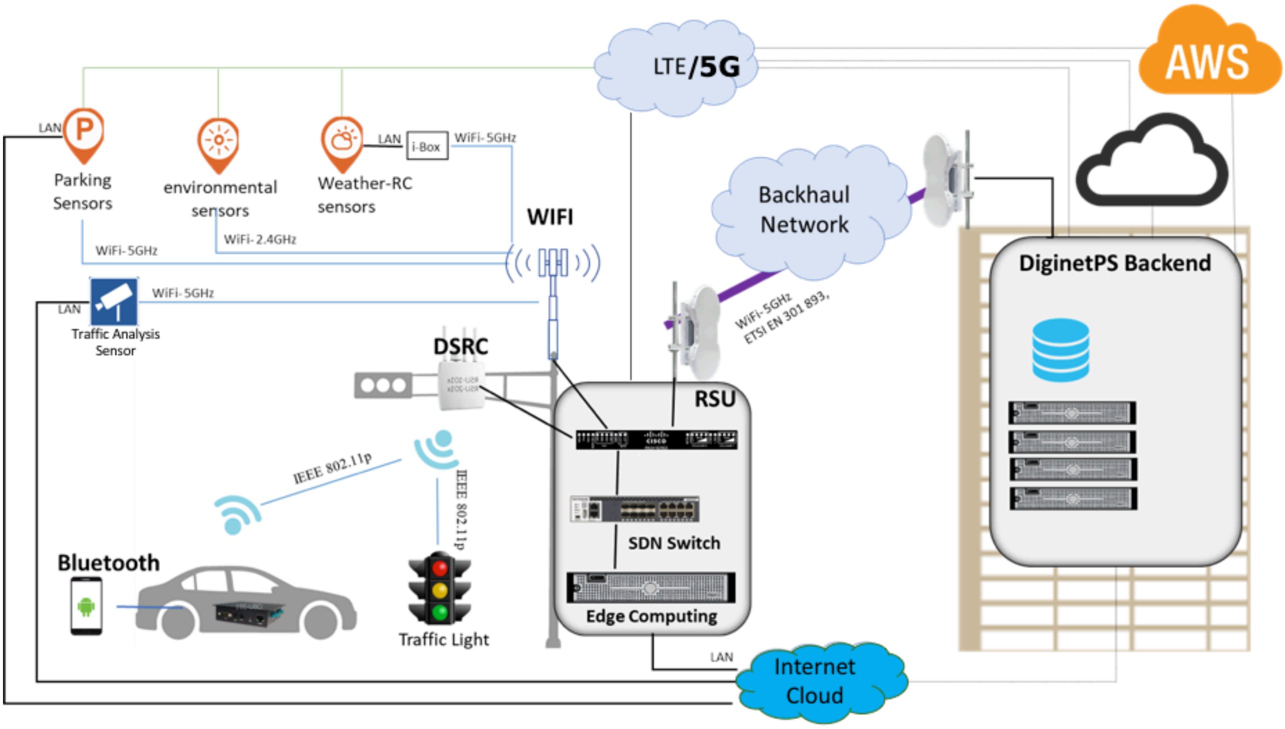


Figure 61: Functional Communication Infrastructure at DE Trial Site

Option B: Vehicle level

DT test APN routes any L3 traffic to the DT MEC, while the standard DT APN would route the traffic to TUB's infrastructure. The handover trigger is generated at the vehicle level based on the vehicles GPS location. Hence, to enable the service handover, we opt for the following two options within this phase:

i) The vehicle can quickly change its APN: Once the handover process is triggered, the vehicle reconfigures its APN from the test APN to the standard APN. Before the APN is changed, the handover trigger message is also sent to the MEC, which in turn triggers the service handover between DT MEC and TUB MEC.

ii) Two LTE modems are installed in the vehicle: One of the vehicle's modems is configured for the DT test APN, the other is configured for the DT standard APN. Once the handover process is triggered, the vehicle switches the LTE modem used. Before switching the modem, the handover trigger message is also sent to the MEC, which in turn triggers the service handover between DT MEC and TUB MEC.

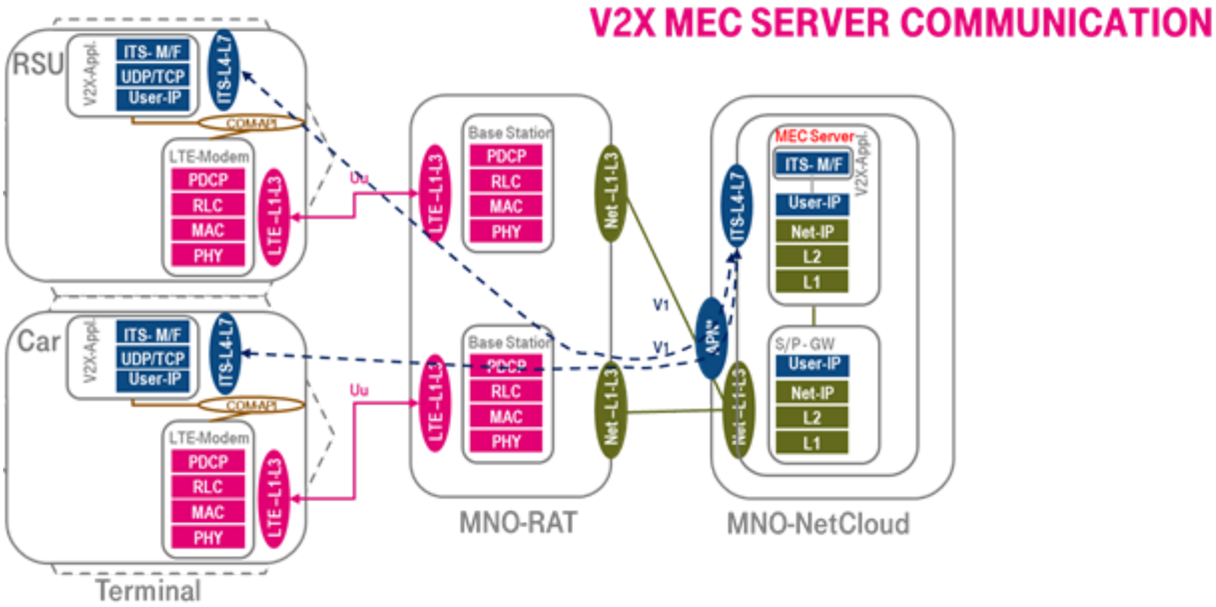


Figure 62: Deutsche Telekom MEC architecture

Phase 3: 3GPP R-15 NSA

TUB is working closely with Deutsche Telecom on the 5G network deployment plans on German trial site. The following two options are being worked out in this regard. Option 1: DT has the test deployment of 5G at the German trial site. An arrangement of using the test deployment for 5G-MOBIX (through T-Systems, as they are our partners in a project) is considered as an option and being discussed. This option also depends on DT's 5G rollout plan, as they may replace this deployment with the commercial deployment. In any case, we are planning to create a roadmap for 5G coverage with DT for 5G deployment on the German Trial site with the priority to have 5G coverage for the 5G-MOBIX trials.

Option 2: DT plans the rollout for 5G deployment at the trial site and connects with TUB core and radio parts. Due to the dependency on DT's frequency licence, TUB's gNodeB will consist of DT's NR RRH and the software DU, CU components developed by TUB and deployed in near edge infrastructure.

Core network architecture

The core network architecture for German trial site has two versions: preliminary and finalized version. These versions are inspired by the deployment phases, which will enable the trialling of the two user stories for the trial site in two stages. The preliminary version of the architecture (see Figure 62) will integrate the existing core network of TUB with commercialized 4G network and the MEC of Deutsche Telekom, which will allow the service and network handovers (basic requirements of the 5G-MOBIX scenarios for this trial site) with 4G and ITS G5.

The final version of the proposed architecture is depicted in Figure 63. This version of the architecture will mainly create the 5G core and radio network of the operator and integrate it with TUB network infrastructure. The service and network handovers are executed via 5G core and radio components.

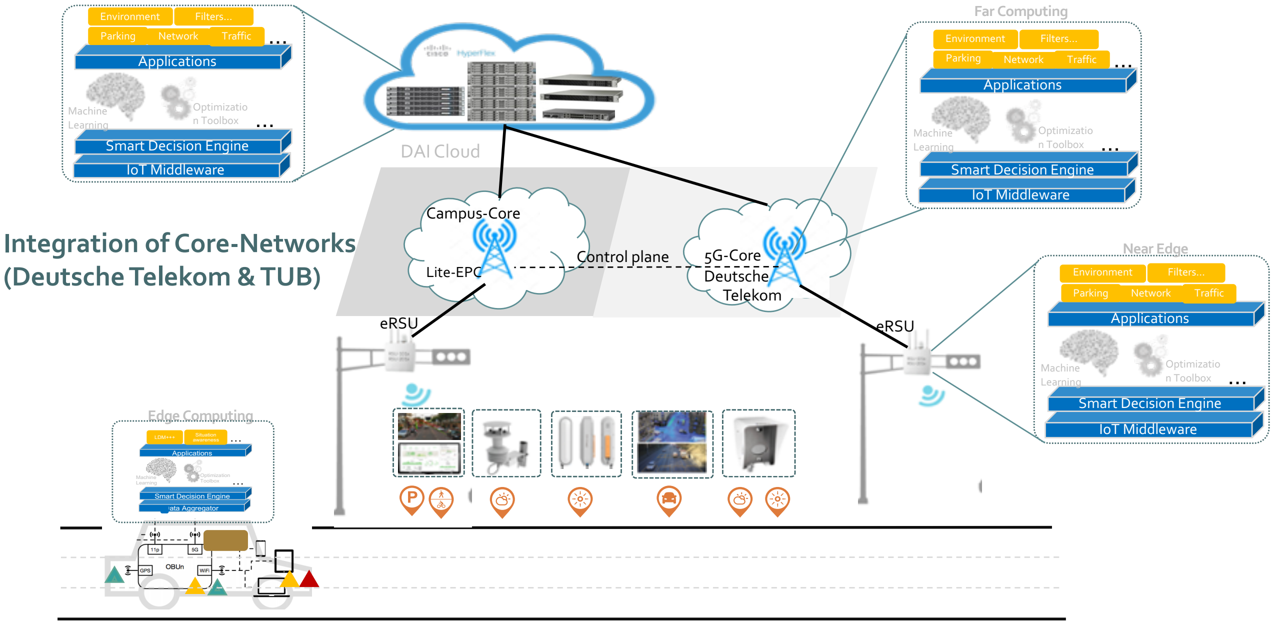


Figure 63: DT & TUB Integration Architecture

TUB & DT Core Network

For autonomous vehicle communication with the network, we are proposing an architecture as in Figure 64. In order to connect vehicles with the network, we will use a MEC and a 5G core network. TUB will provide a MEC which will be connected to TUB's virtualised 5G core network, and from there we will communicate with the Deutsche Telekom 5G network. The TUB MEC will access all the services from Deutsche Telekom.

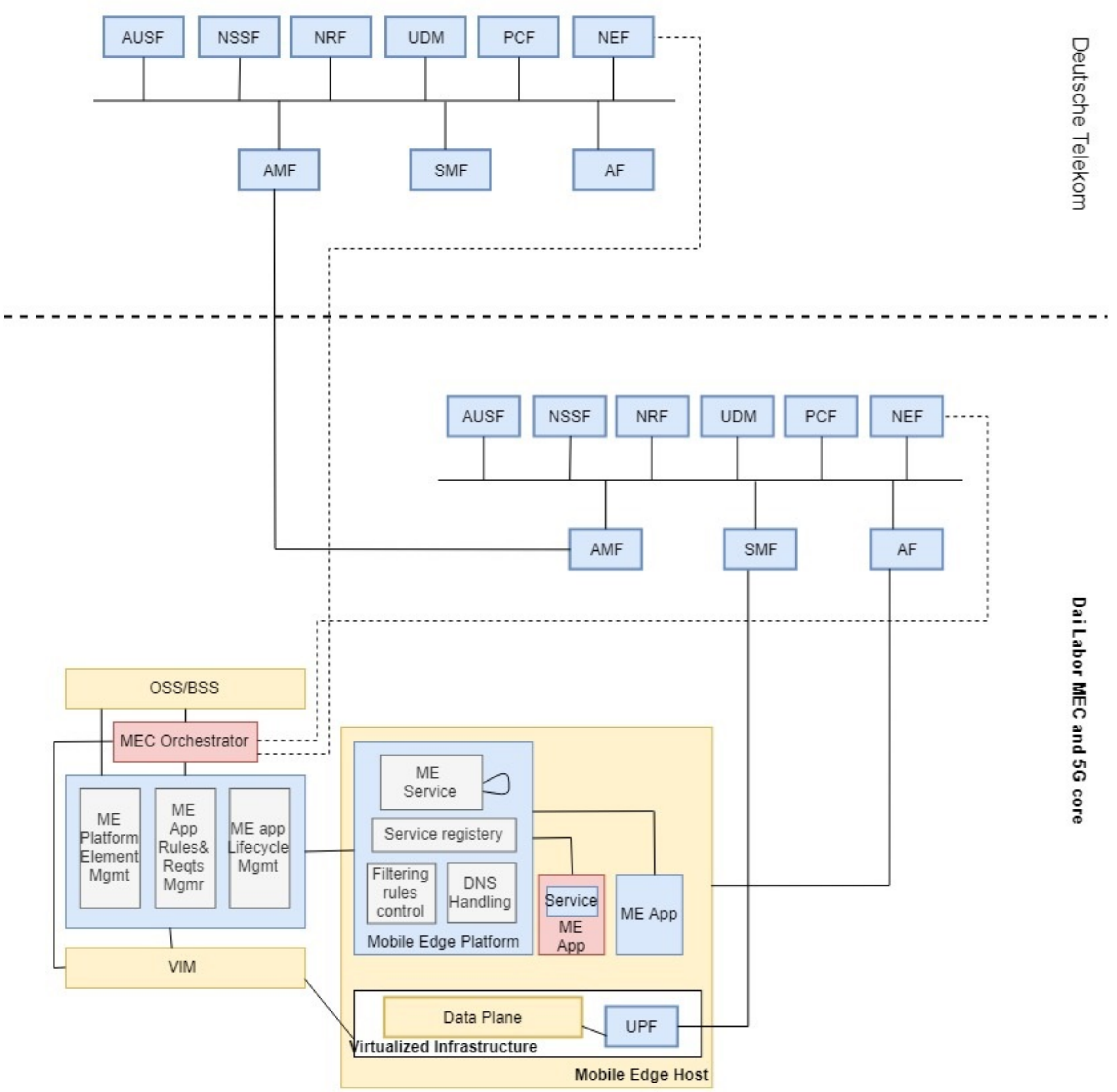


Figure 64: Architecture for interworking between TUB & DT networks

As shown in Figure 64, all the services of TUB deployed on the MEC are connected through TUB's virtualised mobile network core. If the services on MEC want to use the network services of Deutsche Telekom, then TUB 5G core will use the access mobility function to connect with the Deutsche Telekom 5G core network. Once they connect with each other, MEC orchestrator can easily access the services of the Deutsche Telekom 5G core, NEF will expose all the services to the MEC and UPF instance of the Deutsche Telekom 5G core will be in the MEC.

5G and V2X technologies to be deployed

The 5G and V2X technologies used in German trial site are summarised in the following tables.

Table 21: 5G technologies and attributes for 5G network deployed by TUB

Mobile Core	EPC/5GC
Virtualised	Yes
Virtualised infrastructure	OpenStack and Container Infrastructure
Network Slicing	Yes, Free Text for standard
Orchestrator	ONAP, Tacker
Multiple access Edge Computing	Yes
Radio Access Network	LTE and NR
# of sites	1
Vendor	Deutsche Telekom
# of cells per site	2
# of antennas per cell	2
Frequencies used	LTE 2GHz, 5G NR 3.6 GHz, 5G NR 700FDD (pending auctions)
Frequency Bandwidth	100 MHz
Carrier aggregation	Yes

Table 22: 5G technologies and attributes for 5G network deployed by DT

Mobile Core	EPC/5GC
Virtualised	No
Virtualised infrastructure	N/A
Network Slicing	N/A
Orchestrator	DT specific
Multiple access Edge Computing	Yes
Radio Access Network	LTE and NR

# of sites	1
Vendor	Deutsche Telekom
# of cells per site	TBD
# of antennas per cell	TBD
Frequencies used	LTE 2GHz, 5G NR 3.6 GHz, 5G NR 700FDD (pending auctions)
Frequency Bandwidth	100 MHz
Carrier aggregation	Yes

Cellular V2X

While 5G is not deployed in the trial site during Phase 1 and Phase2 of the 5G deployment plan, vehicles may exchange V2X messages through LTE based PC5. To ensure compatibility with the trial site infrastructure, the V2X messages sent and received must mirror the messages sent through the ITS G5 interfaces in vehicles and roadside infrastructure. Unicast communication between V2X Application and UE data shall not be supported in LTE based PC5 communication, as defined by 3GPP.

When 5G NR is available in Phase 3 of the 5G deployment plan, unicast communication between V2X Application and UE may be supported through the NR based PC5 reference point. The MEC of either TUB or DT may in this case serve as V2X application server. The existence of multiple V2X Application Servers offering the same CCAM services is described in [27].

Multi-access edge computing

Edge computing support by 5G enables core and CCAM services to be hosted close to the AV, eRSUs and road sensors' points of attachment, so to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network. Edge computing servers provided by operators in German trial site are deployed in the radio access network and in the core network infrastructure. Near edge servers are provided by road infrastructure provider and integrated in eRSUs. The different edge deployment strategies are depicted in Figure 65.

The main challenge for multi-access edge enabled CCAM use cases is to maintain UE session continuity. This can be achieved with enablers in mobile network infrastructure or at application level approaches for service continuity.

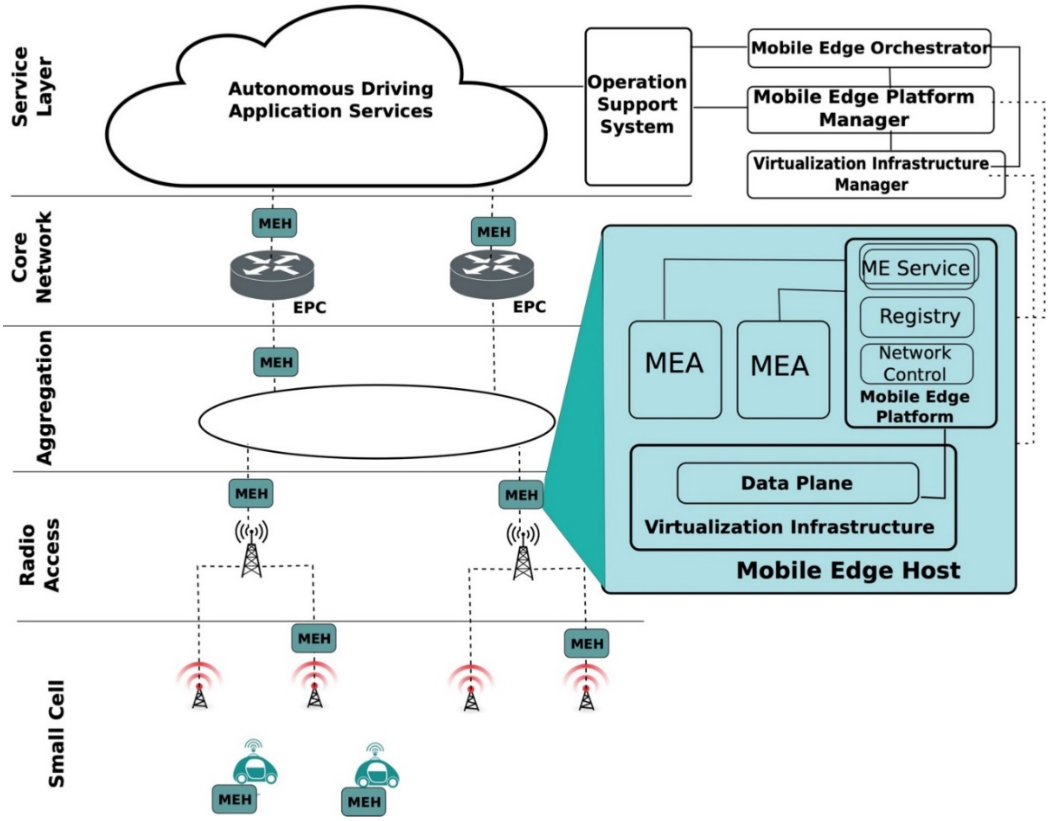


Figure 65: MEC in mobile wireless infrastructure of German trial site.

Support for edge computing in 5G networks is described in [13]. The 5G Core Network selects a UPF close to the UE and executes the traffic steering from the UPF to the local Data Network via N6 interface. This may be based on the UE's subscription data, the UE location, the information from the Application Function (AF), and the policy or other related traffic rules. Due to user mobility, the service or session continuity may be realised with the network services of the 5G network. The 5G Core Network may expose network information and capabilities to an Edge Computing Application Function by allowing certain Application Functions to interact directly with the Control Plane Network Functions or to use the external exposure framework via the NEF. Edge computing can be supported by one or a combination of the following enablers: user plane (re)selection, Local Routing and Traffic Steering, session and service continuity, network capability exposure and support of Local Area Data Network.

Network Slicing

The distributed virtualisation infrastructure of German trial site consists of data centre, far edge and near edge computing platforms. The platforms are capable of computing and hardware-based virtualisation technologies.

Multiple Network Slices may be deployed, which deliver the same features but for different groups of CCAM infrastructure components. The slicing of TUB 5G core network will support all standard slicing and service types defined in [13]: eMBB, uRLLC, MIoT. The network may serve a single UE (e.g., AV) with one or more Network Slice instances simultaneously via a 5G access network. One important component of the network slicing infrastructure deployed in German trial site is the management and orchestration platform. The AI based MANO helps realize a service delivery paradigm with highly integrated networks, computing infrastructures, and application services.

Interactions and integration between 5G networks

Two 5G network core deployments will be available for the trial of MNO handover in German trial site. To fully test cross-border settings, 5G System roaming architectures specified in 3GPP TS 23.501 [13] will be implemented/configured, i.e., with local breakout with service-based interfaces within the Control Plane or with home routed and service-based interfaces within the Control Plane. Interaction with EPC and eRSU infrastructure (in non-3GPP access mode) will also be investigated.

Complementarity and added values compared to CBC deployment

Despite being deployed at a local trialsite, the DE 5G infrastructure allows the trials of cross-border and national roaming scenarios to be carried out with two core networks. Moreover, such extensive deployment of eRSUs and sensors on road infrastructure as in DE TS is difficult to achieve due to stricter regulation at CBCs trial locations. Therefore, the trials at DE TS also enable the evaluation of the impact of RSU infrastructure and near-edge based solution approaches for CCAM scenarios. The added infrastructure components allow the trials to cover more complex interactions between CCAM services, cloud, MEC, and communication infrastructure, as well as their respective providers' objectives. The trials can also be designed to emulate security issues and data privacy requirements that are highly restricted at CBCs.

Annex 6 – FI 5G architecture

The Finland trial site is located within the Otaniemi area of Aalto University. The 5G-MOBIX project use case categories will leverage legacy 4G/5G testbeds deployed in the Otaniemi area in past/ongoing national projects. The actual roads targeted for the 5G-MOBIX trials include the interconnected Maarintie and Otakaari roads with a total length of about 1.2 km (see Figure 66). This road test environment includes features (buildings, vegetation etc.) that will impact radio propagation.

Radio network requirements

The network deployed in Finland for supporting the 5G-MOBIX use case categories will be based on the 5G-NR NSA architecture. The radio access network will consist of two base station sites. The actual site selection will be evaluated based on several candidate site locations, which have existing 4G base stations deployments in the Otaniemi area of Espoo. The site selection criteria include the availability of necessary site facilities, including existing access to power from the grid and fibre backhauling cables.

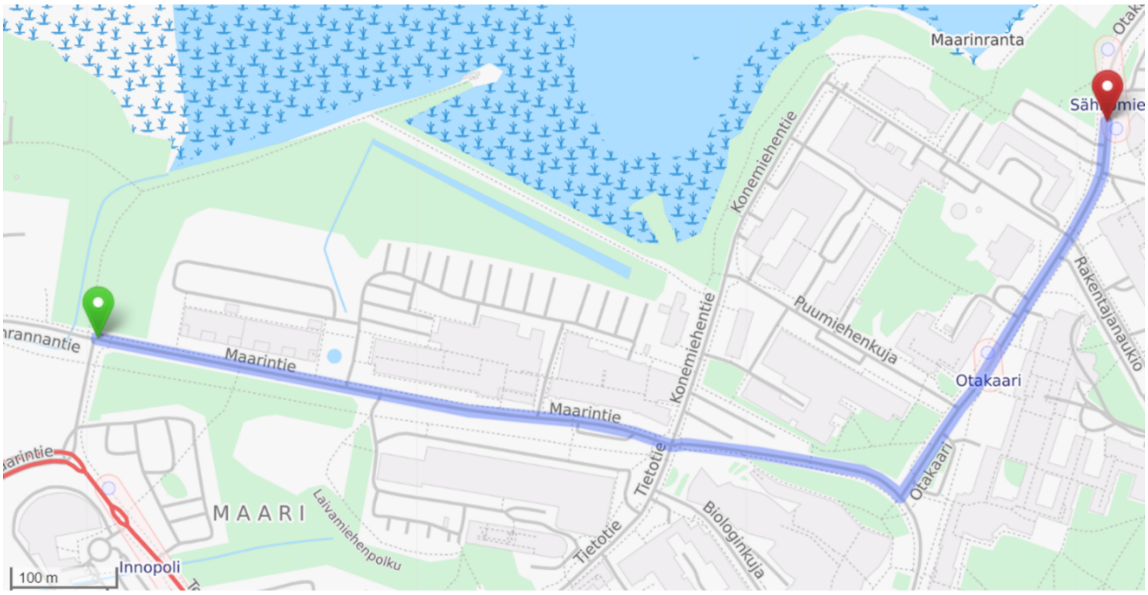
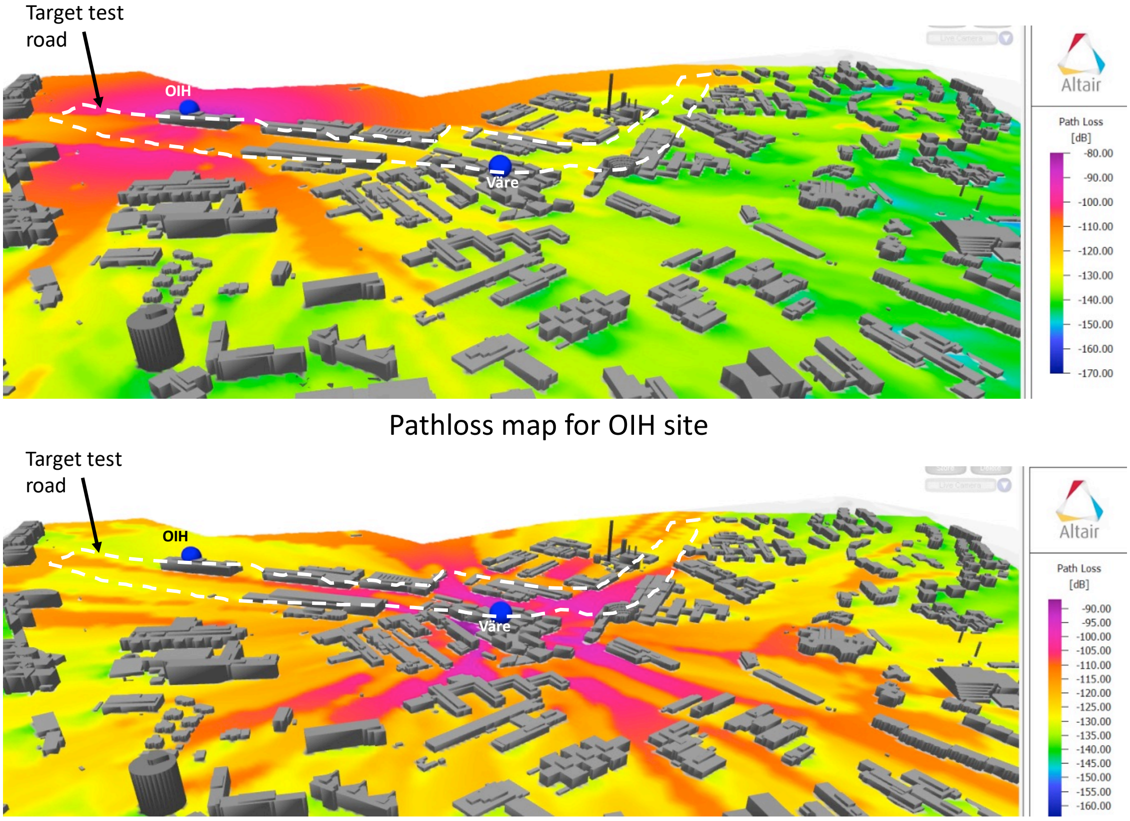


Figure 66 Espoo (Finland) trial site (the roads targeted for the trial is above in blue lines)



Pathloss map for OIH site

Pathloss map for Väre site

Figure 67: Path loss maps for the two candidate sites (OIH and Väre)

The evaluation of the candidate locations will be carried out in the pre-deployment phase utilising commercial radio propagation modelling tools. To that end, initial propagation modelling has been carried out to get initial understanding of the radio propagation environment from two candidate sites, namely: OIH (Open Innovation House) and Väre building (see respective path loss maps in Figure 67). It should be noted that these initial propagation modelling has been done with simplified specifications, by assuming each site having omnidirectional antennas operating in 3.5 GHz band, whereas, eventual deployments will employ directional antennas with sophisticated MIMO configurations and beamforming.

Core and edge network requirements

The remote driving and cooperative perception user story used in the Finland trial site are to be implemented and tested under a multi-PLMN environment. Two potential scenarios drive the motivation for this arrangement. In the first case, multi-PLMN arrangement could be used to provide connectivity redundancy for an L4 vehicle, demonstrating the potential benefits of having the vehicle maintain its services when it loses connectivity to one of the two PLMNs it is attached to. The second multi-PLMN scenario is when the vehicle roams or hands over from one PLMN to another. This scenario is implemented to emulate conventional roaming when vehicle traverses from an area covered by one network to another (as is the case in cross-border locations). The rest of this subsection outlines some of the requirements on core network deployments, MEC deployments and roaming to fulfil those multi-PLMN scenarios.

Core network deployment

In terms of the core network deployments, these multi-PLMN scenarios underline the need for usage of multiple virtualised 4G and 5G core networks. Virtualised core networks provide the necessary level of deployment flexibility and sharing of cloud infrastructure. To that end, these core network deployments require a local data centre or server farm that has, among other features: virtual machines or servers, public IP addresses, stringent security, and redundancy in powering, cooling and high-speed (1 Gbps or higher) fibre connectivity. Additionally, access to multiple PLMN IDs and SIM programming capabilities to create multiple PLMN instances is required, even in cases where common infrastructure is leveraged. Currently Aalto University has access to ten PLMN IDs (244 50 to 244 59) assigned by the local regulator, TRAFICOM.

MEC deployment

The MEC platforms will be utilised for the cooperative perception use story in the Finland trial site. The use story considers the deployment setup where different MEC platforms are associated with different PLMNs. As is the case with previously described multi-PLMN scenarios, this allows testing of the cooperative perception user story when migrating between MECs or using one MEC for redundancy. This multi-PLMN and multi-MEC scenarios presents several requirements, including ability of the MEC platforms to support interoperability in multi-PLMN scenario, enabling MEC apps in different PLMNs to communicate securely with other and synchronise operations and provide service continuity across borders of different PLMNs. The MEC platforms in the Finland trial site will be either collocated with the 5G base station sites or deployed in a data centre that is located within 1-2km of each of the planned 5G sites. At the time of writing, these different options are still under evaluation.

Roaming

The implementation of roaming in the Finland trial site is a key part of the multi-PLMN scenarios described previously. However, the fact the different test networks fall under common organisation control, allows roaming to be implemented without the complexities of securing roaming agreements (as in commercial networks). The actual technical implementation of the roaming will be determined based on the feasibility with the core network implementations available locally and the need to emulate or complement the roaming implementations in the cross-border sites.

Radio network architecture

The 5G architecture supporting 5G-MOBIX in Finland consist of a Non-Standalone setup where existing 4G/LTE eNBs will be used as anchor for the new 5G NR gNBs.

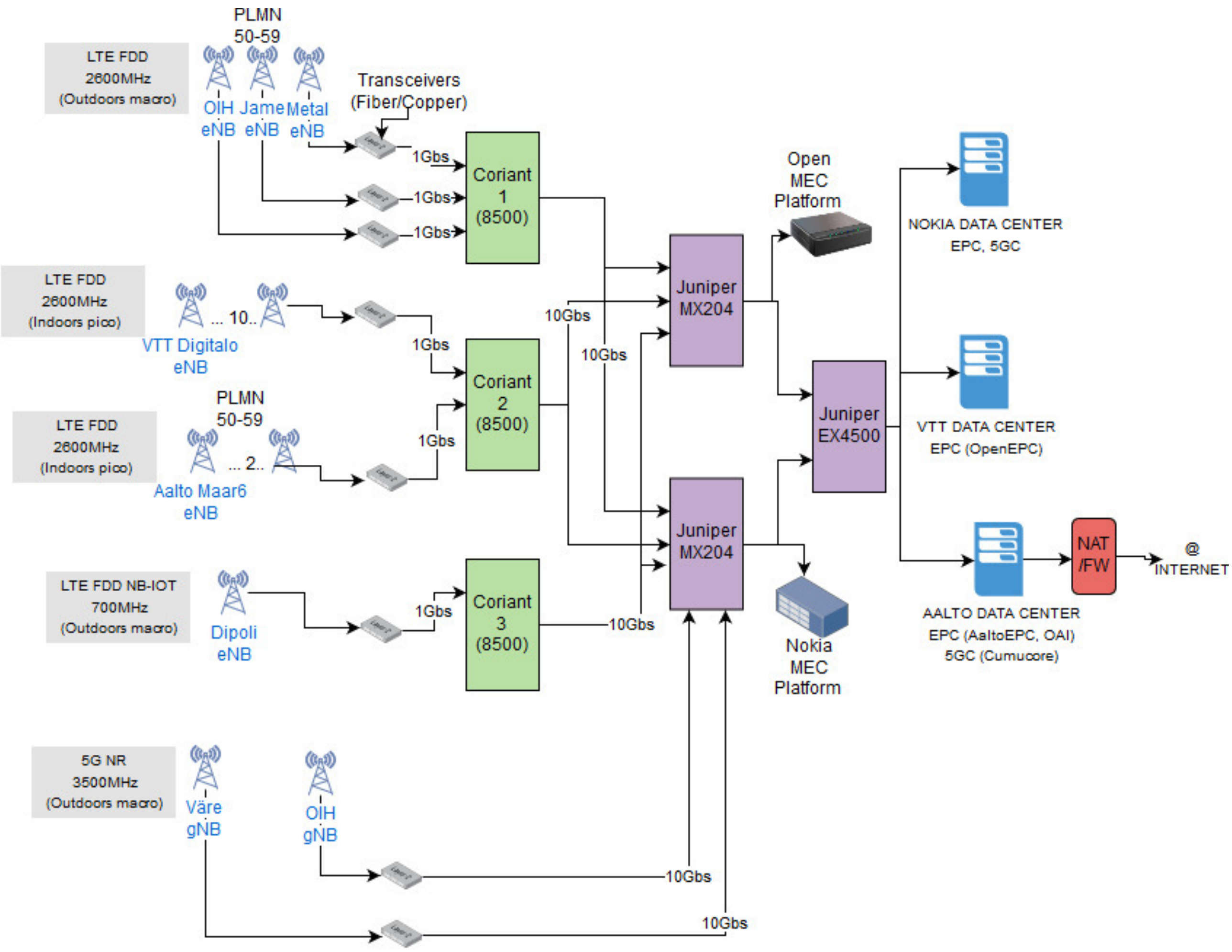


Figure 68: Alternative view of the current and planned network infrastructure deployment in the FI TS.

The overall end-to-end system will consists of a Nokia 4G/LTE eNB and 5G NR gNBs in addition to Ericsson eNBs for NB-IOT and 4G/LTE, and these are associated to Nokia 5GC, Aalto EPC and Cumucore 4G/5G Core Network platforms. The gNB antenna will be Nokia AirScale massive MIMO Adaptive Antenna (MAA) systems. The connections between eNB/gNB are based on fibre converge in SDN-ready Juniper MX204 edge routing platform with capacity up to 400Gbs where MEC platform is available. The complete system including different eNBs, gNBs, EPC, 5GC and network switches are shown in Figure 68.

Core network architecture

The Finland testbed includes several 4G/LTE EPC and 5GC from Nokia, Aalto and Cumucore. Nokia 5GC will be running from Nokia premises in a virtualised environment connected to the testbed through dedicated fibre. The testbed will utilize these PLMNs for the testing with current eNBs and with the gNB if RAN and Transport sharing is supported. The multi PLMN test cases can be demonstrated with Aalto EPC and Cumucore 4G/5GC. Figure 69 shows the core network architecture used in FI trial site and deployed at the Aalto Data Centre located in Otaniemi campus. The Aalto Data Centre, described separately in D2.3 [2], provides a multi-server environment for deployment and co-location of virtualised network functions with sufficient capacity to host multiple PLMN instances but also meet stringent core network operational requirements outlined in previously.

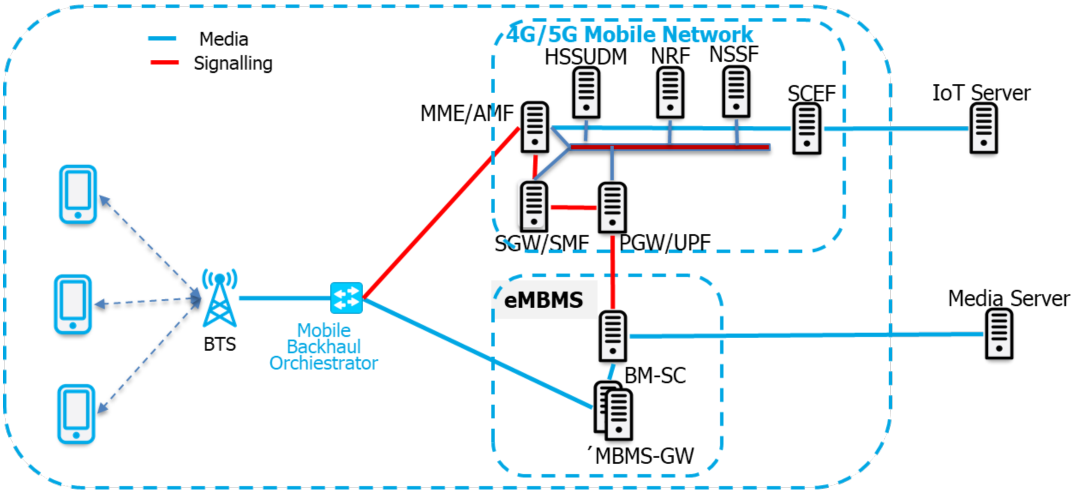


Figure 69: EPC/5GC architecture for FI trial site.

5G and V2X technologies to be deployed

Table 23 summarises the 5G radio, core and edge technologies to be deployed at the FI trial site and their main attributes.

Table 23: 5G technologies and attributes for 5G network deployed at FI trial site

Mobile Core	EPC, 5GC
Virtualised infrastructure	Virtualised Infrastructure Manager (VIM) • VIM interface (OpenStack API) • Dashboard (Horizon) • Compute (Nova)

	• Network management (Neutron) • Identity (Keystone) Dell PowerEdge compute servers SDN switch (Juniper MX and SW based OVS) SDN switch (Coriant 8500) Controller Ryu
Network Slicing	YES (based on Transport sharing and SDN managed slices)
Orchestrator	OpenStack Heat
Multiple access Edge Computing	Yes
Radio Access Network	LTE/NR
# of sites	2 NR,5 LTE
Vendor	Nokia (NR and LTE) and Ericsson (LTE)
# of cells per site	to be confirmed
# of antennas per cell	64T/64R (128 antenna elements)
Frequencies used	Band n78 (TD 3500)
Frequency Bandwidth	60 MHz (3640 to 3700 MHz)
Carrier aggregation	No

Annex 7 – FR 5G architecture

Radio network requirements

The 5G network of UTAC/Ceram test circuit is provided by Orange and Bouygues telecom operators. In case of disagreement between telecom operators on roaming contracts, seamless Handover procedure will be implemented on vehicles when crossing the border.

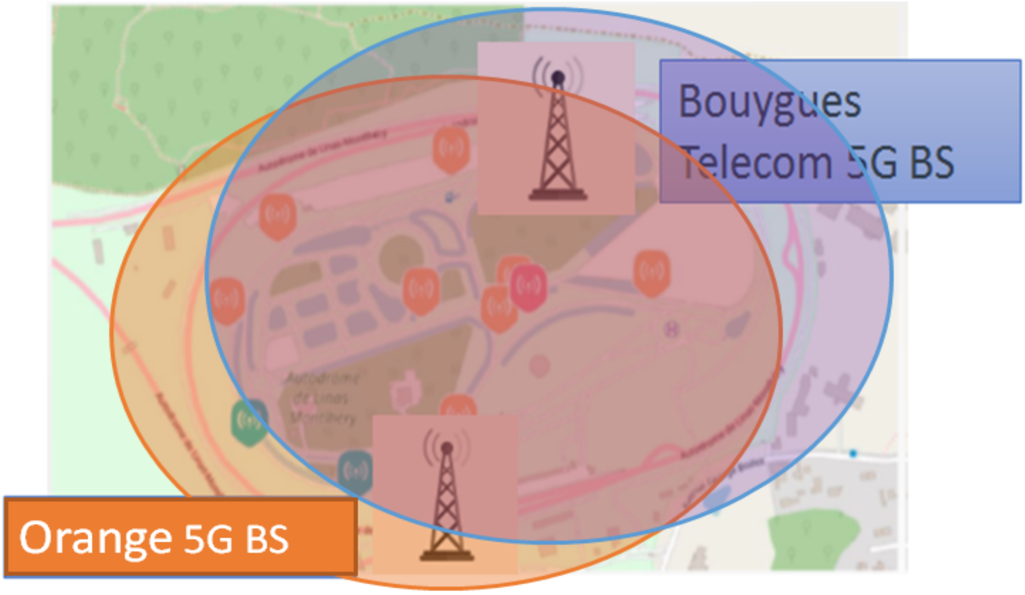


Figure 70: 5G network coverage in UTAC/CERAM Site

UTAC/CERAM test circuit has perfect coverage of 5G networks, provided by Orange and Bouygues as illustrated by Figure 70. Nevertheless, the cells sizes can be adjusted and hence allowing particularly:

- Cross-border with overlapping 5G networks.
- Cross-border with non-overlapping 5G networks.

The above mentioned terrestrial 5G radio networks will likely be supplemented by Low Earth Orbit (LEO) satellite communications. The priority of the satellite communication is to maintain the service continuity with acceptable QoS.

Particularly, we intend to test intelligent roaming/Handover supported by the satellite communication. In order to continuously benefit from the 5G technology, thanks to the satellite communication link, we ensure that the roaming/handover is made at the right timing and in a stable manner. By emulating such a situation, we intend to bridge that gap by the terrestrial and the satellite communication technology. In this case, 5G to 4G handover, and satellite communication technologies will ensure the service continuity. In doing so, the throughput degradation will happen and hence we will work on intelligent network selection and QoS control.

Core network requirements

Being a local and test facilities site, the French team is intended to simulate cross border situations targeting above mentioned different radio coverage situations with the core-network functionalities. The user stories for France trial site are "Infrastructure assisted advanced driving under hybrid traffic" and "QoS adaptation for Security Check in hybrid V2X environment" . Both are tightly related to the eMBB and URLLC 5G services. Network requirements for remote teleoperation include broad coverage, high data rate and low latency to enable continuous video streaming and to send commands between a remote operation centre and the autonomous vehicle.

For the "Infrastructure assisted advanced driving under hybrid traffic" user story, URLCC is a major requirement to enable fast and reliable communications between vehicles to share information about lane change operation. In this case, the use of Multi-access Edge Computing is foreseen at the two PLMNs installed at UTAC/CERAM test site. For both user stories, service continuity shall be supported. For this, inter-PLMNs handover must be carried out between the two 5G networks (Orange and Bouygues).

Core options

Orange and Bouygues Telecom are already deploying 5G EPC (option 3) at UTAC/CERAM facility. They are discussing interconnection possibilities to allow roaming between the two networks.

The core network of Bouygues telecom is installed in Île-de-France region, which is close to the UTAC/CERAM facility. On the other hand, the core network of Orange is currently situated in Aachen Germany.

MEC deployment

In the trial site of UTAC/CERAM, MEC will be deployed in the network of the telecom operators. Such nodes will allow faster communication at the edge of the network. These MEC locations will have different servers operated by the two telecom operators. A connection between the two MEC nodes could be envisaged. The MEC locations will be close to the base stations of the network operator.

Roaming

At the Orange and Bouygues UTAC/CERAM trial site, it is envisaged that a roaming functionality and mechanism will be required to address the cross-border scenario between the two operators. Through the manipulation of the transmission power of the base station and the UE, it is possible to stimulate different levels of cell overlapping and handover scenarios.

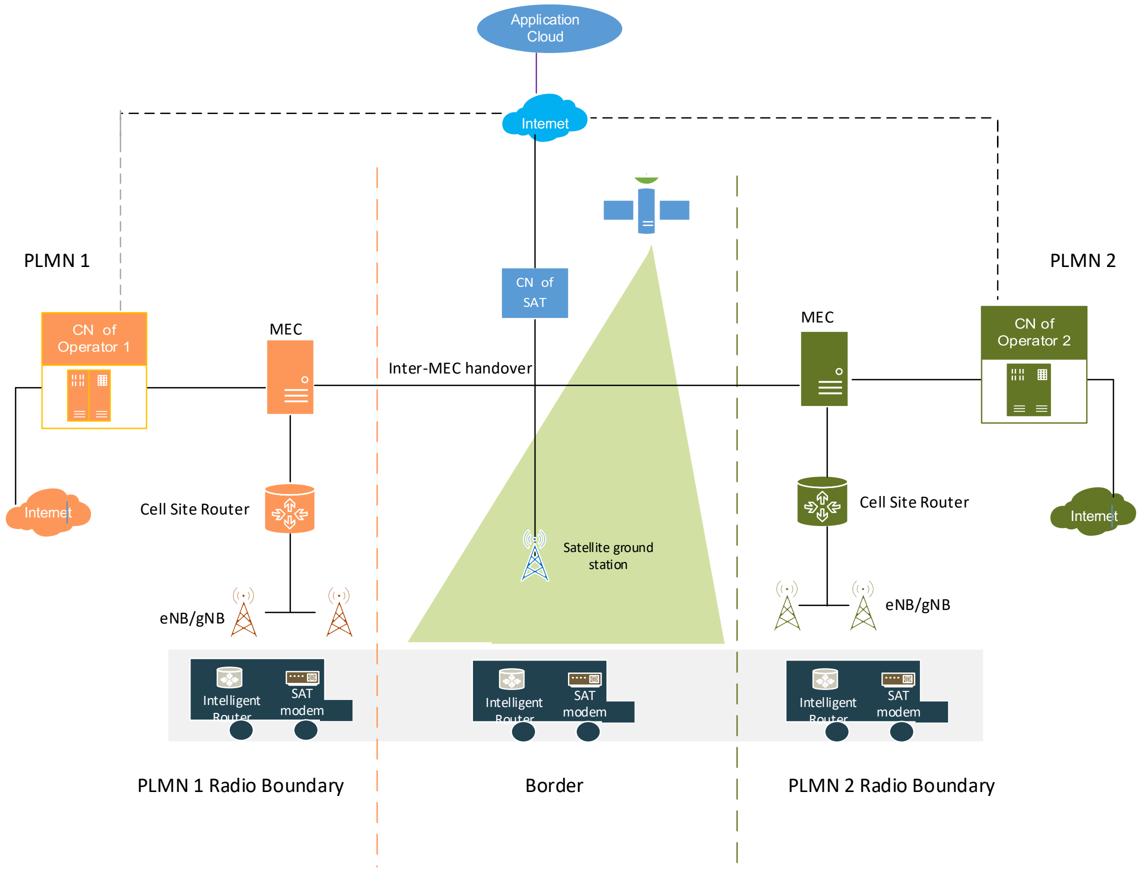


Figure 71: Cross-border deployment cases/scenarios using satellite communication

The network operators are discussing interconnection possibilities to allow roaming between the two networks. However, it should be noted that it is possible there is a "gap" where there is no radio coverage, or the radio signal strength or quality are poor, in these circumstances, satellite communication technology can be deployed to fill the "gap" with the priority to ensure the network continuity with acceptable QoS. Satellite communication can provide various cross-border deployment cases/scenarios and the functional architecture is depicted in Figure 71. The following two cases/scenarios can be envisaged based on the architecture of Figure 71.

- **Case 1:** Bridging radio coverage gap between PLMNs
- **Case 2:** Direct internet connection via satellite network in the event of poor terrestrial coverage

Interdependencies with other infrastructure

To enable the aforementioned user stories and satisfy their QoS requirements, especially in terms of low latency and high throughput, some dependencies with other infrastructures shall be taken into account. One of them, is the inevitable coexistence with the ITS-G5 systems deployed in the test site, especially on the assignment of dedicated spectrum in 5,9 GHz band for 5G NR-V2X (via PC5 sidelink).

Radio network architecture

The RAN handles the communication links between the User Equipment (UEs), On-Board Units (OBUs) and the Evolved Packet Core (EPC) network. The access links are divided into user plane and control plane. The user plane carries the V2X payload traffic while the control plane carries the control signalling for user plane traffic. Hereinafter, the RAN is described for each trial site

UTAC CERAM trial site

In UTAC CERAM trial site, both Orange and Bouygues Telecom will operate 5G networks as depicted in Figure 72. The radio access network consists of the following network components:

- 2 macro 5G cells offering 5G cell coverage;
- 4 C-V2X RSUs;
- Compute processing units (eNB, gNB) controlling the radio connections with connected vehicles as well as managing radio cell resources including connection mobility control.

The RAN network architecture for both telecom operators is implemented according to the 3GPP R15 Non-Standalone (NSA) architecture, as depicted schematically in Figure 73 (option 3). The two operators can completely cover the trial sites. To enable roaming between operators, some mechanisms like power tuning or beamforming can be envisaged.

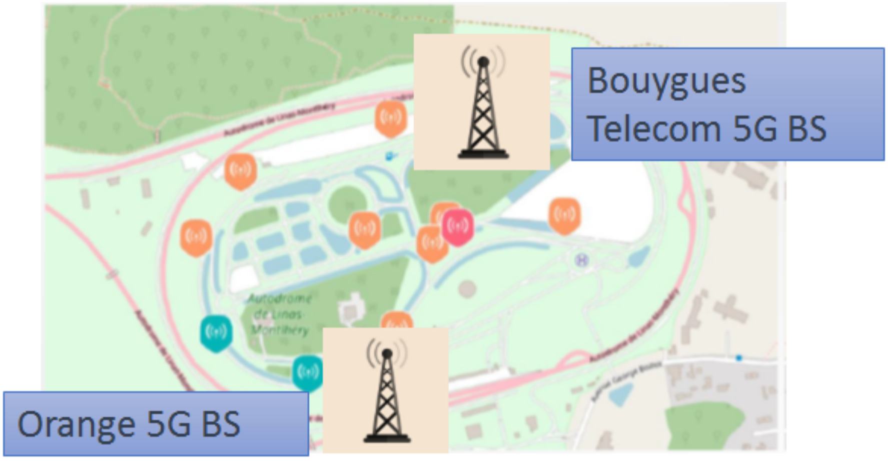


Figure 72: 5G network deployment at UTAC/CERAM trial site

Bouygues Telecom operator

In Figure 73, the RAN architecture deployment relative to Bouygues telecom is highlighted.

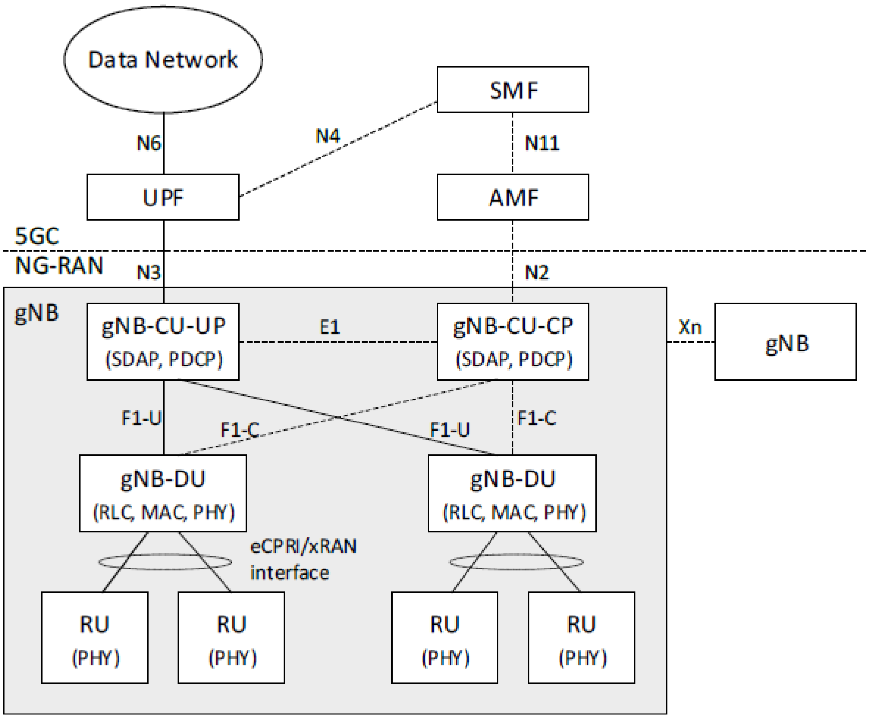


Figure 73: RAN architecture of Bouygues Telecom installation

One of the key elements of the RAN architecture design is to support centralized processing in Cloud-RAN with protocol functionality split of NR base station, namely gNB, between central units (CUs) and distributed units (DUs). Such novel architecture enhancements provide a significant opportunity to design an innovative RAN architecture for delivering multicast content in 5G. According to Figure 73, the gNB functions are split into CU and DU, where CU covers higher layer protocol functions of SDAP and PDCP, and DU covers lower layer protocol functions of RLC, MAC and PHY. The gNBs are inter-connected through an Xn interface.

8.1.1.1.1. Orange operator

Orange 5G installation will be ready by July 2019. It is implemented according to the 3GPP R15 Non-Standalone (NSA) architecture, option 3. It consists on one site deployment with three cells. The user plane will be operating at 3.5 GHz band, while the control plane will use 700 MHz band. The core network is operating in local breakout to enable the Mobile Network Operator (MNO) to break out Internet sessions into the Home network. The goal behind this is to provide inbound roamers with an ability to order data, which is provided directly by the visited network:

- Network layer: slicing with QoS profiles;
- Security layer: V2X Server interface for CP/UP;
- Application layer: logic and its split on V2X (V2N / V2V);
- MEC functionalities enabled.

Core network architecture

UTAC CERAM trial site

Bouygues Telecom operator

Bouygues core network installation at UTAC Ceram trial site is based on NSA option 3 architecture.

Orange Operator

Regarding the deployment of the core network of, it will be operated in local breakout to manage the site. The core network is operated by Ericsson and is situated at Aachen site in Germany. Flow prioritization will be supported with QoS profile. In addition, MEC functionalities will be supported during the project.

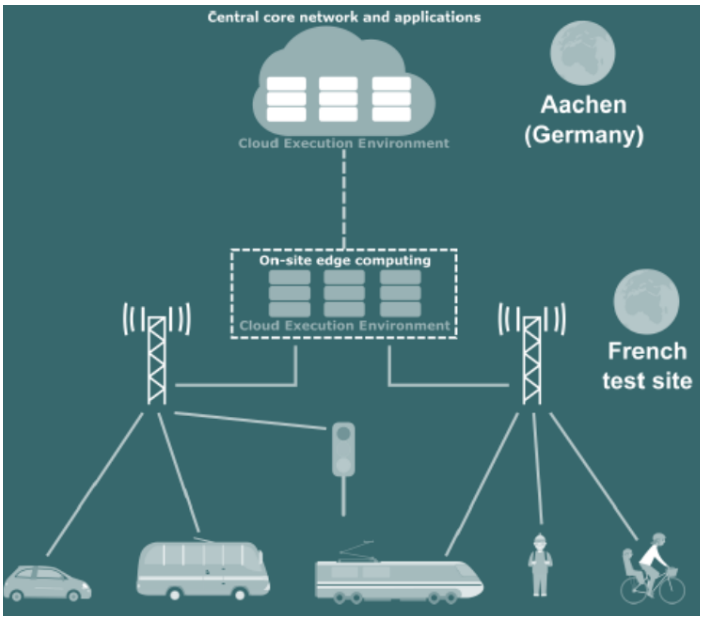

Central core network and applications
Cloud Execution Environment
Aachen (Germany)
On-site edge computing
Cloud Execution Environment
French test site

Figure 74: Orange core network set-up

5G and V2X technologies to be deployed

In Table 24, we highlight the different attributes of the 5G network that is deployed at UTAC/CERAM site by Bouygues Telecom.

Table 24: 5G technologies and attributes for 5G network deployed by Bouygues Telecom

Mobile Core	5G EPC
Virtualized infrastructure	Yes
Network Slicing	No

Orchestrator	Not yet
Multiple access Edge Computing	Could be envisaged
Radio Access Network	LTE & NR
# of sites	1
Vendor	Ericsson
# of cells per site	3 sectors
# of antennas per cell	2
Frequencies used	700 MHz (4G), 800 MHz (4G), 900 MHz (2/3G) 1800 MHz (4G), 2100 MHZ (3G/4G), 2600 MHz (4G), 3700-3800 MHz (5G test pilot frequencies, will be used until commercial frequencies are allocated, probably late 2019/2020) (licensed)
Frequency Bandwidth	100
Carrier aggregation	LTE: Aggregation of 4 frequencies in 4G Downlink, MIMO 4x4 (in 4G 1800/2100/2600), 256 QAM
Backhaul	1 Gbps from S2 2019

Cellular V2X

UTAC/CERAM site has 4 LTE-V2X RSUs and the vehicles will also be equipped with LTE-V2X OBUs. Indeed, LTE-V2X communication is to be between vehicles (V2V) and vehicles and road side units (V2X) for exchange of the standardised V2X messages (DENMs, CAMs, and CPMs).

Multi-access edge computing

Regarding Bouygues Telecom, the option of integrating Multi-Access Edge computing is examined. Different technical solutions are considered. Hosting a MEC in regional metropolitan offices could be an adapted solution if the goal is to optimize latency. On-premises, MEC could be an adapted solution if the goal is to keep content on-site. Hosting HW solutions (for compute) supplied by a centralised cloud server is an option that we have identified, but not planned as for now.

ETSI MEC reference architecture proposes the use of MP3 interface for interconnecting MEC but the specification of MP3 is still in early draft at the time of writing. The background IPR for interconnecting MEC through satellite communication to synchronize application states while inter-PLMN handover is in progress, is jointly owned by 5G-MOBIX partner SA Catapult. The interconnecting MECs for cross-border deployment scenarios can be summarised as follows:

- The UE (the car) is initially connected to a local MEC application on MEC PLMN 1.
- As the UE moves towards PLMN 2 and that the radio signals are deteriorating
  - Before the UE moves into the coverage area of PLMN 2, the "intelligent router" will switch the radio connection to the satellite network to main the application connectivity (Figure 75)
  - At the same time, when MEC detects UE is about to perform a handover, a notification is sent both for the source and the target MEC applications
- The source and target MEC platforms will subsequently allow the MEC applications to communicate (over MP3 interface), so the UE state can be updated in the target application (Figure 75)
- Finally, when the UE reaches the coverage area of PLMN2, the "intelligent router" detects the signal strength/quality changes, it will switch the radio connection to the terrestrial network in the PLMN 2 (Figure 76).

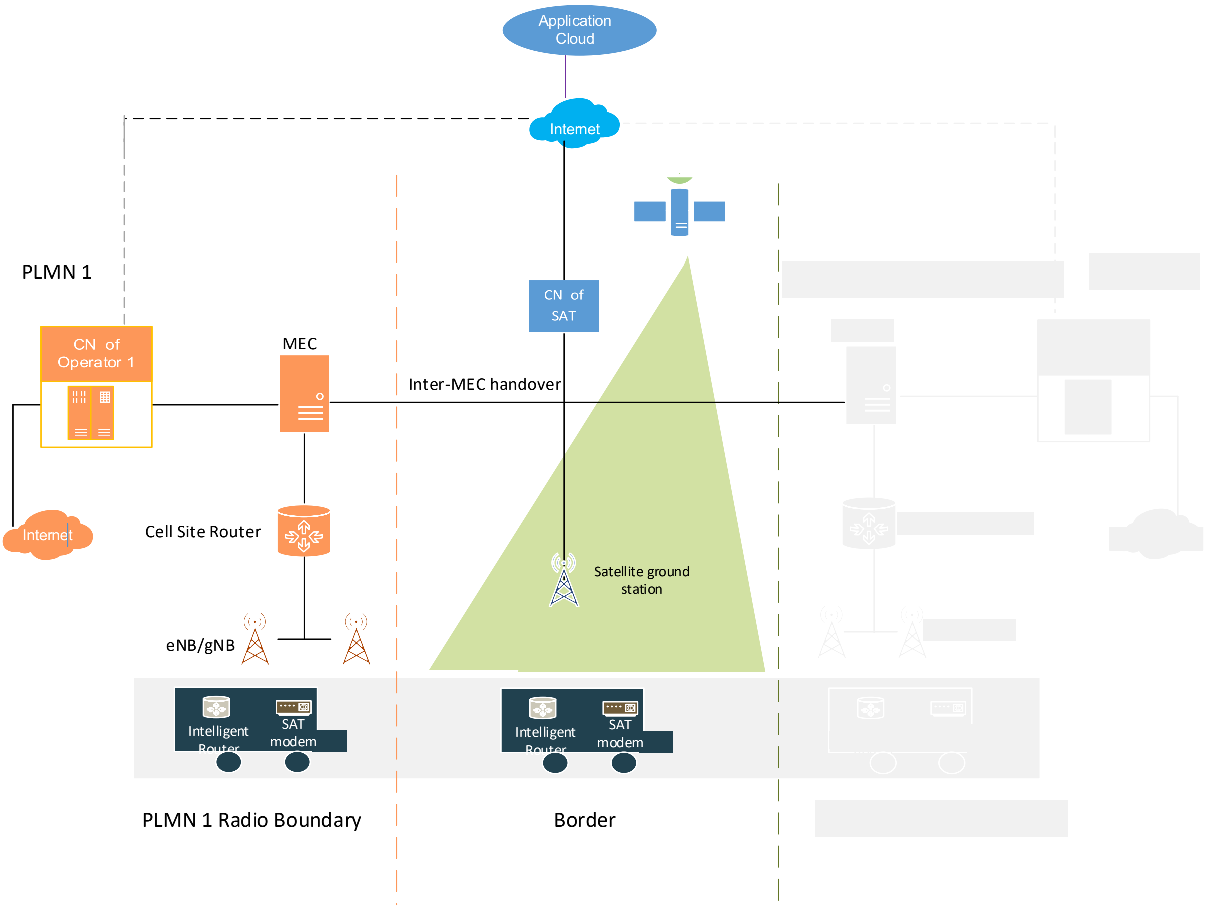


Figure 75: Interconnecting MECs Cross-border deployment scenarios using satellite communication (stage 1)

This innovative approach can be tested at the trial site prior to possible deployment at one of the cross-border trial sites. The implementation of the inter-MEC interface (MP3) on commercial MEC platforms is dependent on the supplier and the progress and maturity of the ETSI MP3 specification, therefore consideration will be given to the feasibility of using suitable MEC platforms within operator network and within private network to support this functionality. The testing results could provide useful inputs to considerations of solutions for deployment across Europe (in WP6) – beyond the test sites considered within the project. It will also provide input to the existing working group within 5G-PPP on the Integration of Satellite communication within 5G Phase 2 release.

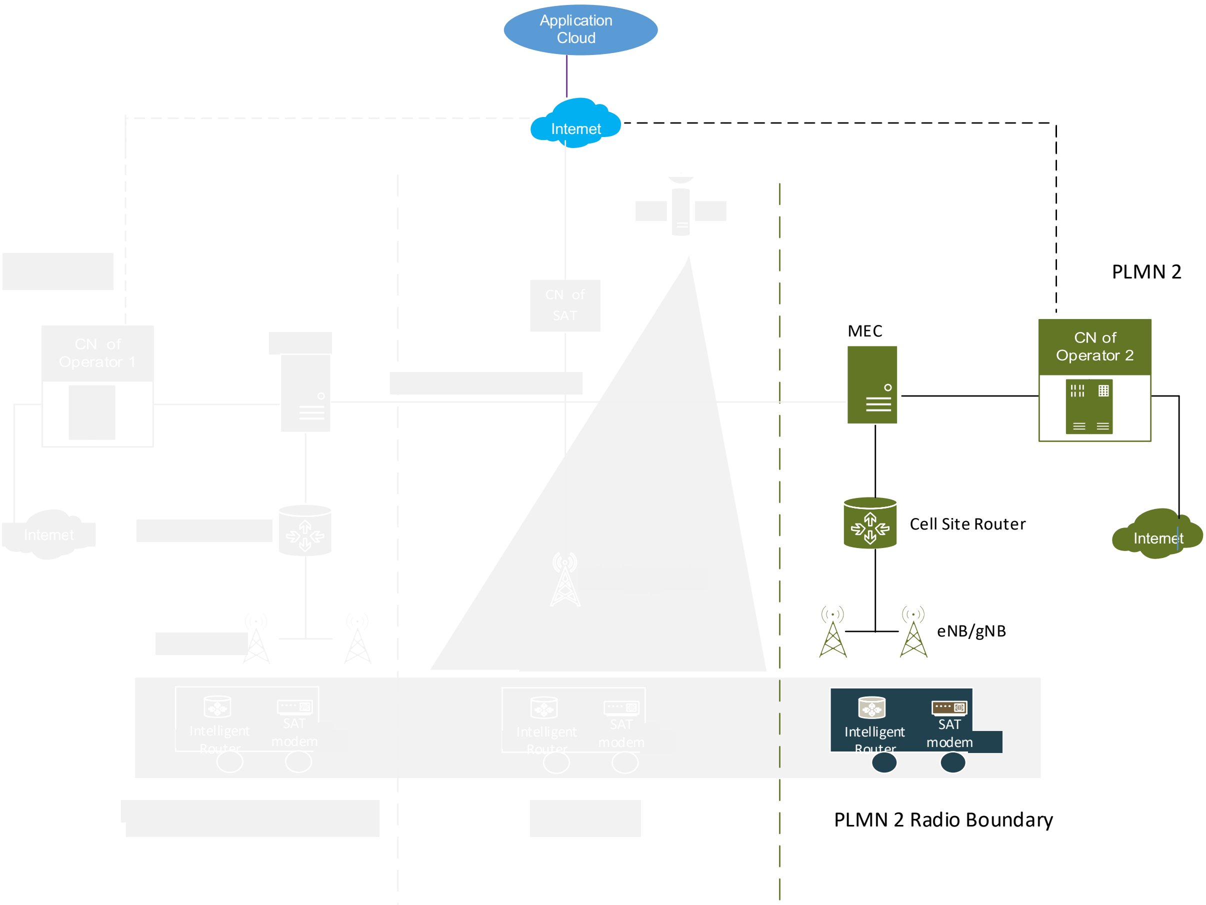


Figure 76: Interconnecting MECs Cross-border deployment scenarios using satellite communication (stage 2)

Network Slicing

NW Slicing needs the use of 5GC which will not be available during the timeframe of the experimentation. Nevertheless, different kinds of prioritization techniques can be used before slicing.

Roaming

Roaming is going from one network to another when crossing a country-border. Changing network from one operator to another in the same country is not a real-life use case (due to regulation), however it can occur in the case of an MVNO who has agreements with two or more operators in the same country. Alternatively, if a device is equipped with two SIM cards of two different networks, in the event where the coverage of the first network is poor, the device would move from the first network to the other network in the same country provided that the second network coverage is better than the first.

As discussed previously, for the purposes of the trial, the coverage scenario could be simulated by adjusting the transmit power of the base station of one of the networks with the collaboration of Orange and Bouygues.

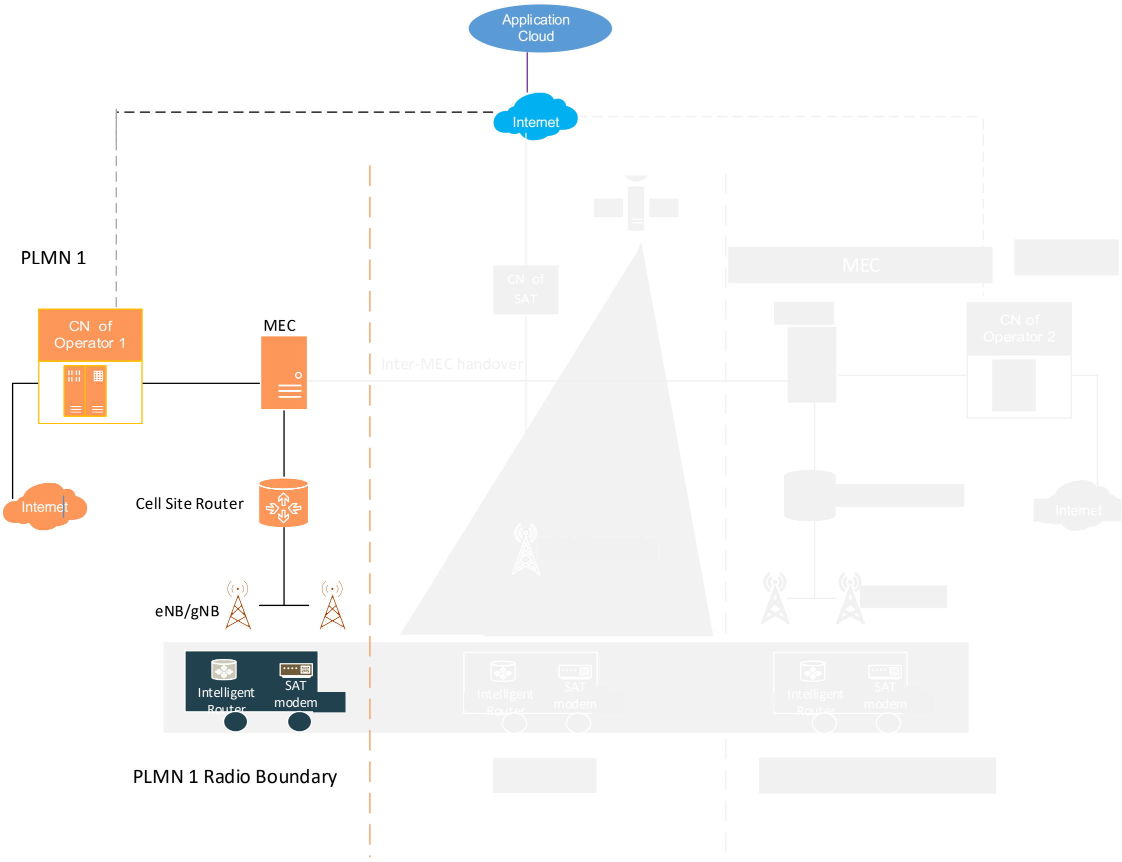


Figure 77: Bridging Radio coverage gap between PLMNs (stage 1)

From mobility perspective, when UE moves from one network to the other, the device will lose radio connection temporarily from the first network and is then reconnected to the second network when the radio condition is established. For data connection, this "radio gap" may not have impact on data connection due to error detection/recovery mechanism is in place as per the 3GPP specification. For voice call connection, it is possible that the call would be dropped due to lack of coverage from either network.

In order to maintain the network connectivity and provide the acceptable QOS services, the radio gap could be addressed by the satellite communication and the following cases are proposed:

- **<u>Case 1 – Bridging radio coverage gap between PLMNs</u>**
  - The UE (the car) is initially connected to PLMN 1 (Figure 77)
- As the UE moves towards PLMN 2 and that the radio coverage from PLMN 1 is deteriorating and hence a radio gap is created. Before the UE can move into the coverage area of PLMN 2, the "intelligent router" will switch the radio connection to the satellite network and the radio connectivity and application sessions are retained (Figure 78);
- As the UE moves closer to the edge of the PLMN 2 coverage area, the intelligent router detects the presence of radio signal in PLMN 2, it will switch the radio connection to the terrestrial network in PLMN 2 (Figure 79) and the UE will resume terrestrial network services.

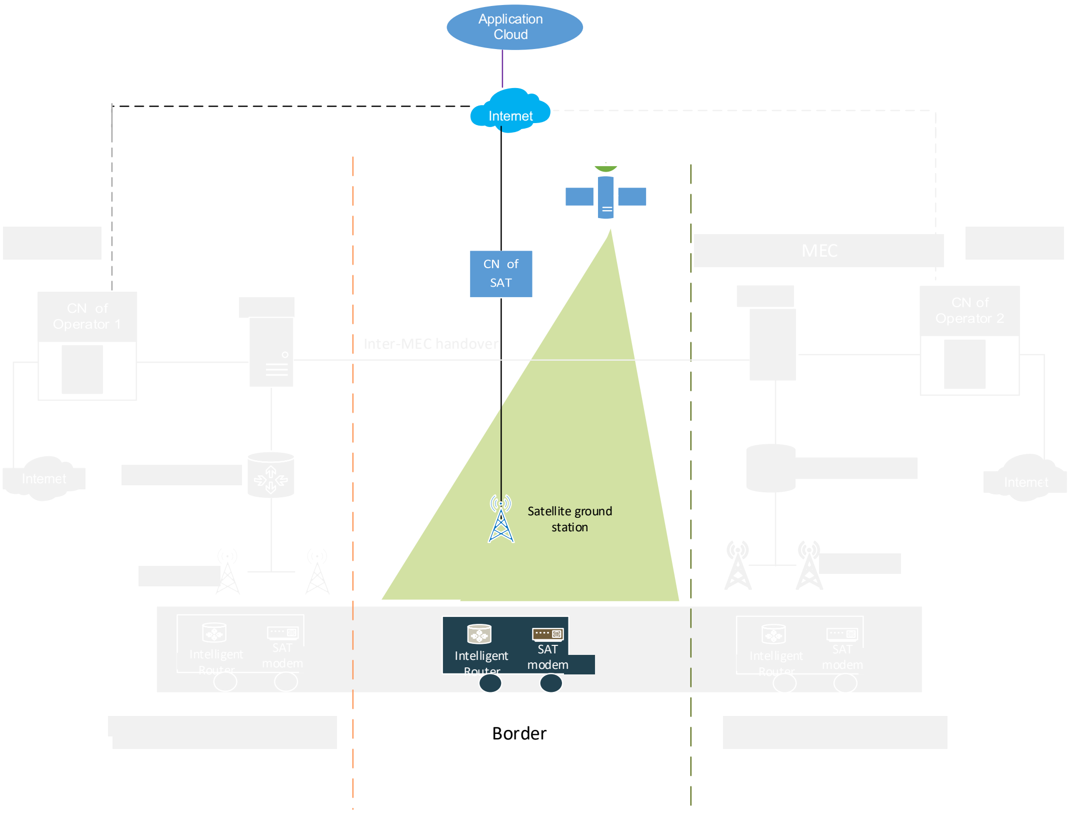


Figure 78: Bridging Radio coverage gap between PLMNs (stage 2)

- **<u>Case 2 – Direct internet connection via satellite network in the event of poor terrestrial coverage</u>**

There is scenario where the user wanting or expecting their applications (e.g. car navigation map, car manufacturing settings) to get live update from cloud services/applications anywhere and anytime. Hence there is case where the car or user is in a poor terrestrial coverage area and would not be able to connect to the cloud server to get the services as expected.

Figure 80 shows that the user is connected to both the Cloud application server via satellite connection and terrestrial connection. The intelligent router will detect the signal condition of both the satellite and terrestrial radio condition. In the case where the terrestrial network coverage is poor, the satellite connection could be deployed to obtain the cloud application service. In the case where the terrestrial is good, the terrestrial network will provide the connectivity for the cloud service and the satellite connection will be idle. The satellite communication can further be exploited to work with N3IWF and/or ePDG and this is still in discussion at this stage.

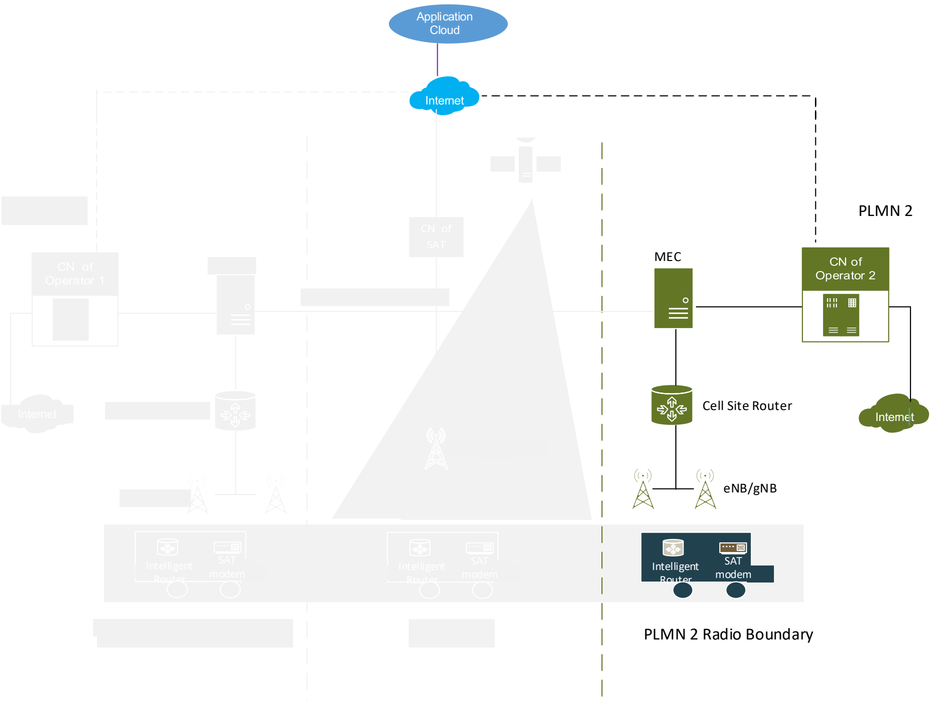


Figure 79: Bridging Radio coverage gap between PLMNs (stage 3)

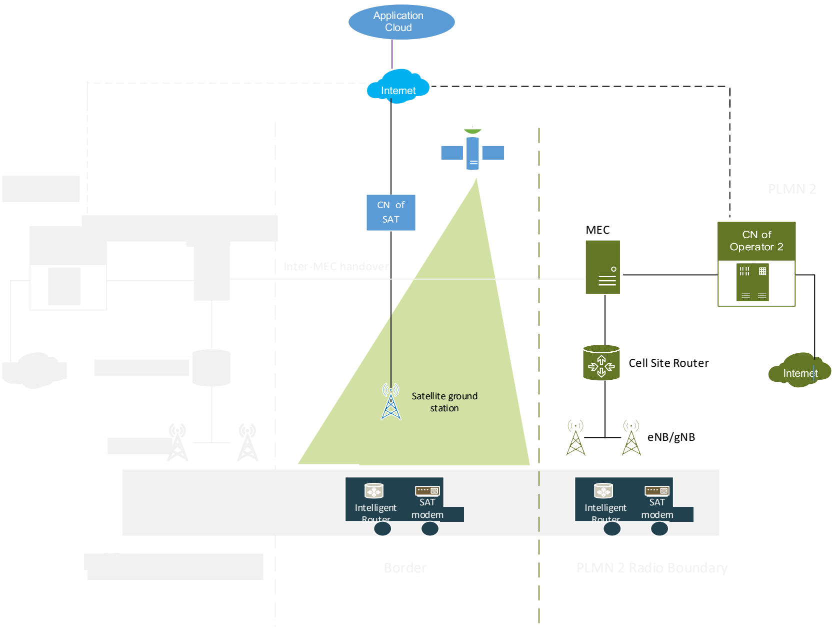


Figure 80: Direct internet connection via satellite network

Annex 8 – NL 5G architecture

Radio network requirements

The design of the three networks deployed in the south of the Netherlands in the region Helmond/Eindhoven is such that each use case category can be handled by at least two neighbouring networks. Figure 81 shows the three neighbouring networks in the Netherlands with a coverage map of KPN. Below it is described how the design considers various key requirements which can be derived from these use case categories.

Ability to exchange raw sensor data between vehicles and between vehicles and network (e.g. 10-20 Mbps per flow)

Use of 5G NR in both 3.5 GHz and 26 GHz spectrum which provides adequate bandwidth. Use of 5G NR in 3.5 GHz in NL is constrained to specific regions and possible via temporary licence via regulator, but feasible for the trial site.

Ability to reduce V2N latency down to 10-15 ms range

Use of 5G NR in both 3.5 GHz and 26 GHz spectrum which provides adequate bandwidth. Use of 5G NR in 3.5 GHz in NL is constrained to specific regions and possible via temporary licence via regulator, but feasible for the trial site.

Each PLMN provides adequate coverage within its service area

The KPN network with 6 planned gNBs (LTE800+1800=>NR700(+NR1800/NR2100)) in the trial area (N270/A270) will provide the largest coverage area of over 50 km^2. The TNO network (LTE 1800

MHz=>NR@3.7 GHz) is much smaller and closely aligned with the N270 road, but partially overlaps with the KPN network within the trial site area which creates options to verify inter-PLMN connectivity scenarios. The third network from TU/e (NR26 GHz) will be more localized on the TU/e Campus covering the parking lot and exit road, with 3-4 sites considered.

QoS (particularly latency) can be maintained, also under heavy traffic conditions
QoS needs to be supported for time critical ITS message flows (e.g. 5QI value 84; see (3GPP TS 22.261, n.d.)), either using the standardised QoS mechanisms (Rel.16), or using slicing. All partners prefer slicing, the feasibility and how to evaluate the performance of multiple slices will be investigated. Unclear yet to what extent modems will be able to support QoS (5G grade) and how end-to-end slicing could be realized (including the RAN).

Service continuity should be provided at inter-PLMN handover (roaming)
Currently the 3GPP standards lack solutions for inter-PLMN handover in 5G networks. It will be investigated during the project how service continuity can be achieved.

Table 25 provides a brief overview of attributes of projected sites of each of the individual networks (KPN, TNO and TU/e) in the area to accommodate the three use case categories. In Figure 81, a geographical layout is depicted using the KPN coverage plan as a basis and showing the intended "borders" between the three networks.

Table 25: Overview of attributes of the projected NL sites.

Network attributes	KPN	TNO	TU/e
Determine cell coverages and hand-over location	Hand-over: - TU/e exit road - On ramp A270 Overall coverage: - A270/N270/Campus	A270/N270	Parking lot TU/e Campus + exit road
Sites in scope	- Campus (exit road) - A270/N270 (6 sites)	1-2	3-4
Cells per site	3	2	1
Antenna's per cell	2	1	2
Frequencies and bandwidth	First LTE800+LTE1800; later Option 2: NR700 (+NR1800 or NR2100)	Option 3x or 2 LTE1800 (20 MHz) NR 3.5-3.7 GHz (100 MHz)	26.5 GHz (100 MHz)

Carrier aggregation (and anchor point)	First LTE 800; later NR700	First 1800, then 3.5-3.7 GHz	26.5 GHz

With respect to the application of short range V2X technologies LTE and 5G NR Sidelink connectivity (Mode 4) are in scope of UC1 (Collision Avoidance). ITS-G5 is included in UC3. Short range V2X technology is not considered in scope of UC2 (Remote Driving). Timing of implementation will be subject to availability (particularly 5G NR Sidelink).

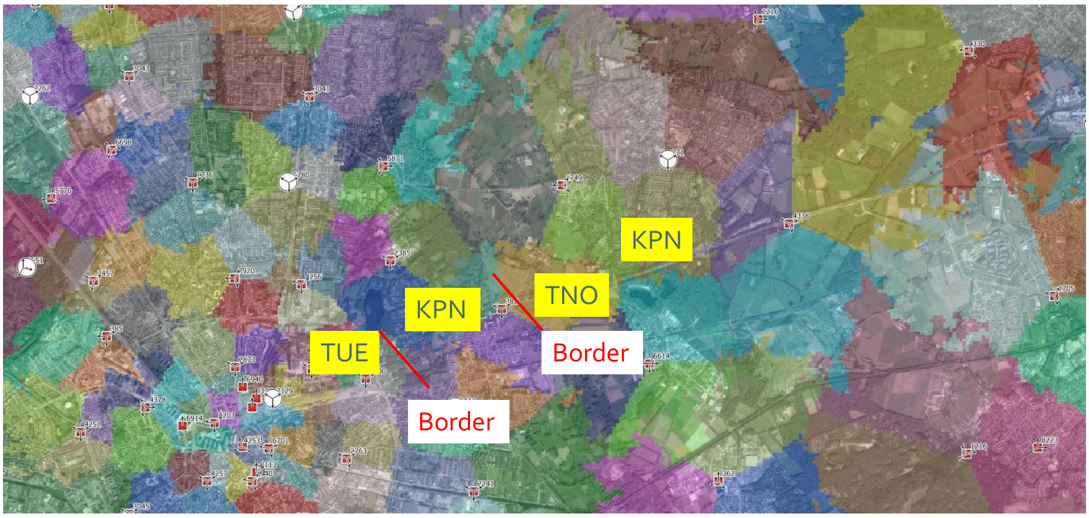


Figure 81: Coverage map KPN network with additional network presence of TNO and TU/e annotated. Network borders (emulating cross-border settings) are shown by red line sections.

Core network requirements

See also table above which also contains aspects which relate to the Core Network functionality.

Core options

Full leverage of 5G grade end-to end connectivity requires 5G Core solutions. KPN considers initiating with 5G EPC (Option 3x) which can be extended to a dual core solution (5G EPC + 5GC) later. TNO and KPN are considering starting their research networks with 5GCore functionality. The availability of a 5GC is under discussion with the provider of this Core Network capability (Fraunhofer).

An important core network requirement in this trial (and in others) is the support of inter PLMN-handover. Currently no solution exists yet for cross-border handover. We will investigate the feasibility of inter-operator handovers with session continuity in UC3 (Collaborative Perception Environment).

To support QoS requirements in all three use case categories, the implementation of slicing is considered in Core and RAN, in accordance with TS 23.502 section 5.15. Slicing allows separation of time critical ITS data (messages and video) and other generic data. During the trial, the generic slice will be used for logging data.

MEC deployment

The application of MEC technology is relevant to all three use case categories and is expected to be supported in at least two of the three networks. Table 26 identifies the most important MEC related attributes and their application for this trial site.

Table 26: MEC related requirements and compliance.

MEC Requirement	Compliance/solution
LADN (Local Area Data Network) (23.501 §5.6.5)	Supported by KPN, TNO and TU/e
Application Function influencing traffic routing	To be decided during the project
Session and Service continuity mode 2 or 3 (23.501 §5.6.5)	KPN will implement different edges and test service continuity
Compute orchestrator	All partners will implement container technology
See also edge computing (23.501 §5.13)	-

In the trial site two MEC locations are considered, which will be operated by two different network operators. These MEC locations will have servers where a Kubernetes cluster is running. There will be a direct network connection between the two different MEC locations. The MEC locations will be near the base stations of the network operator. Figure 82 shows the different MEC locations currently being considered.

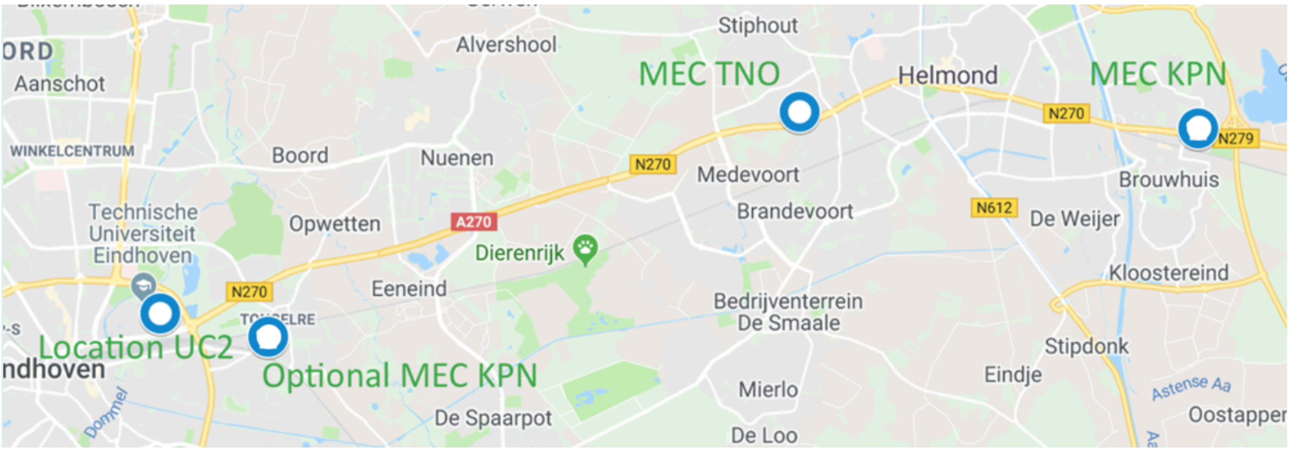


Figure 82: Planned locations for the deployment of MEC in the Dutch trial site.

Network Slicing

Network slicing (as discussed in Section 2.3) will implement DÉCOR for UC1 and UC3 using log or generic data and ITS messages. The scope of the network slicing will be across the RAN and Core for all the use case categories with Slices expected to be implemented for generic and log data and a separate slice for ITS messages. UC2 will require an additional slice for Video data. Per slice performance will be evaluated as these use case categories are studied. It is expected that with several slices, traffic will also be generated in a slice to setup, maintain, and evaluate the slide performance.

Roaming

Roaming is relevant in all three UCs. The emphasis is expected to be on implementation of solutions in UC2 (Tele-operation) and UC3 (Collaborative Perception Environment). A particular focus will be put on achieving interworking between the MEC-nodes of neighbouring networks. No details yet on priorities handling.

Interdependencies with other infrastructure

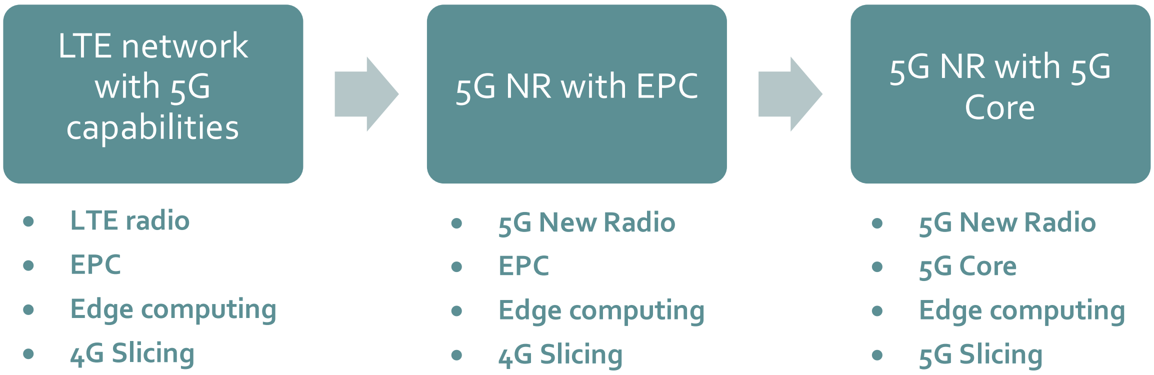
To meet the end-to-end performance requirements on communication of the use case categories, especially on high throughput and low-latency, special attention is needed on other elements:

- Roadside and cloud systems that process raw (video-based) data to events;
- Roadside systems that collect and forward information (in time or spatial);
- Use of roadside systems that support direct communication at locations with poor 5G coverage
  - 5G as backhaul connection from roadside systems to cloud systems;
- Coexistence with non-5G systems
  - Support of use case via 4G radio network (fall-back or when out-of-range);

Coexistence with ITS-G5 systems deployed for safety-related applications, especially on the assignment of dedicated spectrum in 5,9 GHz band for 5G NR-V2X (via PC5 Sidelink).

5G Architecture implementation

Deployment of the 5G mobile network will evolve as technology becomes available. Starting with the current 4G setup, adding 5G NR to this and later also adding a 5G Core. Timing will depend on the appropriate modems and software becoming available. In general, we see three major steps to be taken going from a current LTE network to a 5G network, see Figure 83.



LTE network with 5G capabilities

- LTE radio
- EPC
- Edge computing
- 4G Slicing

5G NR with EPC

- 5G New Radio
- EPC
- Edge computing
- 4G Slicing

5G NR with 5G Core

- 5G New Radio
- 5G Core
- Edge computing
- 5G Slicing

Figure 83: Rollout sequence 5G technology in Dutch trial site.

Within the Netherland test site, three 5G networks will be setup with a different focus area. Below, the general steps and setup are detailed but per 5G network different emphasis will be placed, depending on the focus area.

1) LTE Network with 5G capabilities

All base stations are equipped with LTE Radio's and a Base Band Unit. This is connected to an edge facility and the central core network. At the Edge facility, a MEC (Multi-access Edge Computing) is set up and user plane traffic will be split from control signalling to the central core location. For the splitting of user and control data EPC Control and User Plane Separation (CUPS) can be used. For the 4G slicing and latency reduction different technologies can be used in parallel such as:

- Radio:
  - Advanced Subscriber Group Handling (ASGH), together with prescheduling reduces latency.
  - Prescheduling reduces latency for a select group of UE's.
  - Instant Uplink Access (IUA) reduces latency for a select group of UE's.
  - Radio resource partitioning, slicing in the radio for a select group of UE's.
- Core:
  - DECOR (Dedicated Core), slicing in the core.
  - Split for each slice user plane traffic towards separate EPC network functions and virtual networks.

This way different subscribers (SIM cards) can get different resources assigned. It is not yet possible to bind a single subscriber to multiple slices using a single UE. During this stage, QoS might be used to further differentiate between data streams and give priority to those.

2) 5G NR with EPC

In addition to the EPC and LTE bands, 5G NR is added. Control signalling will still go over the current LTE bands. 5G NR with EPC is referred to in section 4.1.1 as Option 3x and as Non-Standalone (NSA) NR. Modems that support deployment Option 3x and support the correct frequency bands are required. With this step the advantage of 5G NR in terms of latency and bandwidth can be determined. Other more core related 5G features like 5G slicing are not yet available.

3) 5G NR with 5G Core

The EPC will be replaced by a 5G Core. Control signalling will be transmitted over 5G NR. Ideally, multiple 5G NR bands are available for carrier aggregation (currently already possible with LTE) or a larger bandwidth band is used to be able to show a performance gain over the current LTE setup. This will make it possible to have a 5G Core signalling over 5G NR. Modems that support deployment option 2 and support the correct frequency bands are required. With the 5G core it is possible to add 5G slicing and to setup edge computing based on LADN (Local Area Data Networks). In addition, QoS can be used with 5QI values assigned corresponding to the desired QoS characteristics.

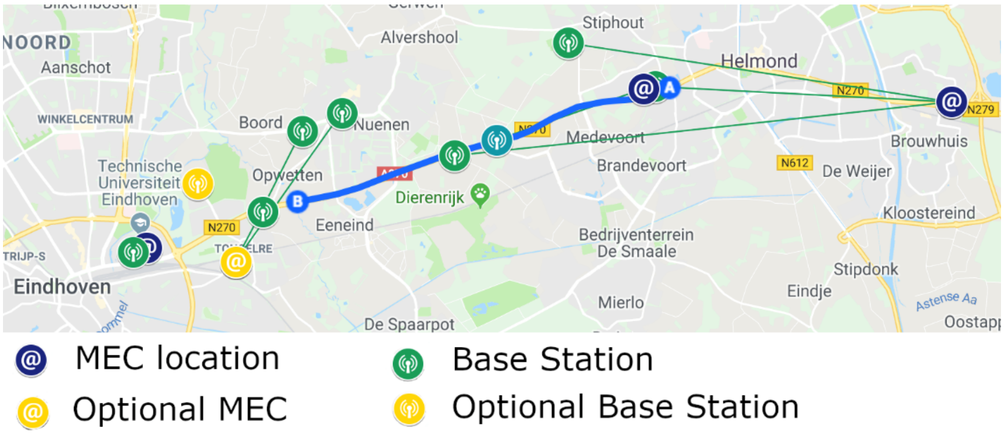


Figure 84: Dutch trial site infrastructure overview.

The specific deployment options chosen for each of the 5G networks at the Netherland trial side are described below. Three 5G networks are setup, each with a specific emphasis:

- **KPN**: with a focus on testing out possible future 5G deployment scenarios with automated driving vehicles. Emphasis for 5G-MOBIX is focussed on three different aspects: First, possible service levels for specific trial side user stories. Secondly, on edge computing scenarios with multiple edges deployed and thirdly Interoperability between different PLMN's.
- **Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)**: with a focus on applied research and an emphasis for 5G-MOBIX on two aspects: First 5G technology applied to automated driving user stories and secondly Interoperability between different PLMN's.
- **Technische Universiteit Eindhoven (TU/e)**: with a focus on 5G millimetre wave applications and an emphasis for 5G-MOBIX on two aspects: Firstly, on larger bandwidth applications needed with remote driving user stories and secondly, on positioning of the UE with 5G millimetre waves.

The Dutch trial site in total will consist of 8 or more base stations, 2 or more MEC's and 3 core networks. They are divided over three different networks. The infrastructure will be deployed in Eindhoven, Helmond and the road in between. Figure 84 gives an overview of all the base stations, MECs and transmission in between.

Radio network architecture

At the Netherlands trial site three 5G radio networks will be set up. TUE will provide a network with coverage at the TUE campus, TNO will provide a small network along the A270/N270 road and KPN will provide a wide network covering the A270/N270 road between Helmond and Eindhoven. The KPN network can provide a corridor between both TUE and TNO and will overlap the TNO network making different testing scenarios possible, e.g. border crossing and multi operator scenarios.

The RAN will be deployed in three different steps, going from a current LTE network to a 5G NR network. The frequencies in mentioned in this section might vary depending on the available licences (licenses still to be requested) and availability of handsets. See Figure 85 with the different deployment stages. In the sections below the specific setup for each 5G network will be specified.

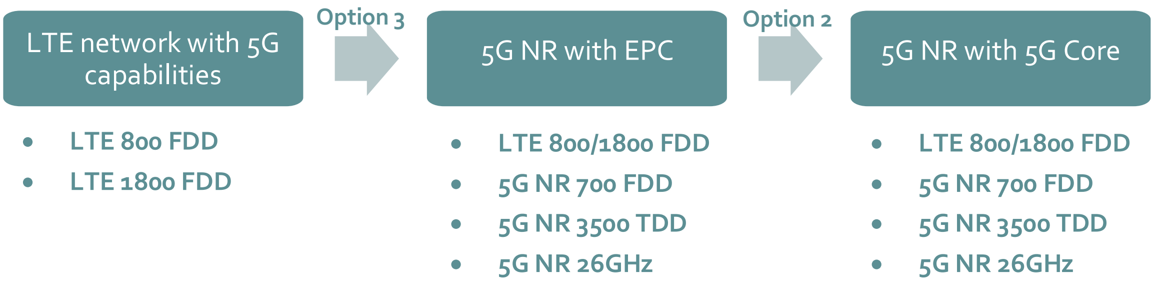


Figure 85: Deployment stages for the RAN.

KPN

This section describes the future KPN 5G radio network setup. The KPN network will cover the A270 and N270 between Helmond and Eindhoven. This in total consists of around six to seven base stations. KPN will equip its current production base stations such that they can be used for a test network in 5G-MOBIX.

The KPN network will consist of six base stations to be extended to seven base stations, if needed, see Figure 84. One MEC facility will be located at the Metro Core[3] in Helmond with an option to add an extra MEC facility to the Metro Core[3] in Eindhoven. The core will be at a remote location.

All sites are connected using direct fibres to either the Helmond or Eindhoven Metro Core location[3]. The sites including the transmission is currently used for production purposes and will be used during the tests to serve both production customers and the tests in 5G-MOBIX. This will be done with a shared RAN feature

[3] Metro Core: part of the KPN access network to offer nationwide connectivity. Metro core locations are connected to one of the four core locations in the Netherlands. In total 168 metro core locations are present in the Netherlands.

Multi Operator Core Network (MOCN). This way only the radio resources are shared as there is a dedicated core network for the 5G-MOBIX tests.

Deployment options

The radio network will evolve in different stages, depending on available spectrum, national deployment of operator network and available user equipment.

1) LTE Network with 5G capabilities

The current KPN LTE network is used with shared RAN to enable a dedicated core for the test network. Different technologies provide enhancements for automated driving usages. These incorporate:

- ASGH with prescheduling to be enhanced with IUA at a later stage when available.
- QoS.

2) 5G NR with EPC

5G NR is added as an extra band next to LTE providing deployment Option 3x. For reduced latency, the following technologies can be used (depending on availability in gNB and UE):

- Grand free uplink.
- QoS.

3) 5G NR with 5G Core

5G NR is used without LTE using deployment option 2. Enhancements are mainly expected at core level.

TNO

The network deployed by TNO for supporting the 5G-MOBIX use case categories will be aimed at using 5G in deployment option 2. However, first COTS UEs and network equipment will only be based on the 5G NR deployment Option 3x. It is expected that during the 5G-MOBIX project 5G NSA and SA equipment will become available. The current radio network architecture is based on LTE technology and will be upgraded during the project when 5G equipment becomes available. First, the current architecture shall be discussed, secondly, the NSA option shall be discussed and lastly the SA option will be discussed.

TNO will build the 5G NR system next to the current deployed LTE system. The current LTE system and the envisioned modifications to support 5G NR in NSA and SA mode will be described. TNO has one site deployed with two LTE cells for coverage along the A270 and N270 motorway. During the 5G-MOBIX project the site will be upgraded with 5G NR equipment. The mobile core network is in the TNO The Hague location. From the TNO The Hague location an encrypted VPN connection is created towards Siemens in Helmond. Siemens offers computing and storage capacity to support Edge applications. From the Edge location, there is a fibre ring connection towards the radio network site of TNO.

The current deployed LTE base station is an eNB from Ericsson (RBS 6501). This is an integrated baseband and radio unit and has 2 antenna ports for cross-polarized antennae. The unit is designed for a small cell single antenna deployment but has support for extra external radio units. The RBS 6501 is extended with a micro Radio 2203 from Ericsson via the CPRI interface. Both the RBS 6501 and the radio unit have a maximum transmit power of 5 W. The RBS 6501 and the 2203 radio are connected via Coax cables to directional antennas from Welotec. The antennas have two antenna connectors for cross-polarization. The two antennas are directed in the direction of the motorway to achieve maximum coverage on the motorway. The frequency band used for LTE is an FDD band 1780-1785/1875-1880 MHz. This specific band is unlicensed in the Netherlands and can be used within certain transmit power limits for private networks.

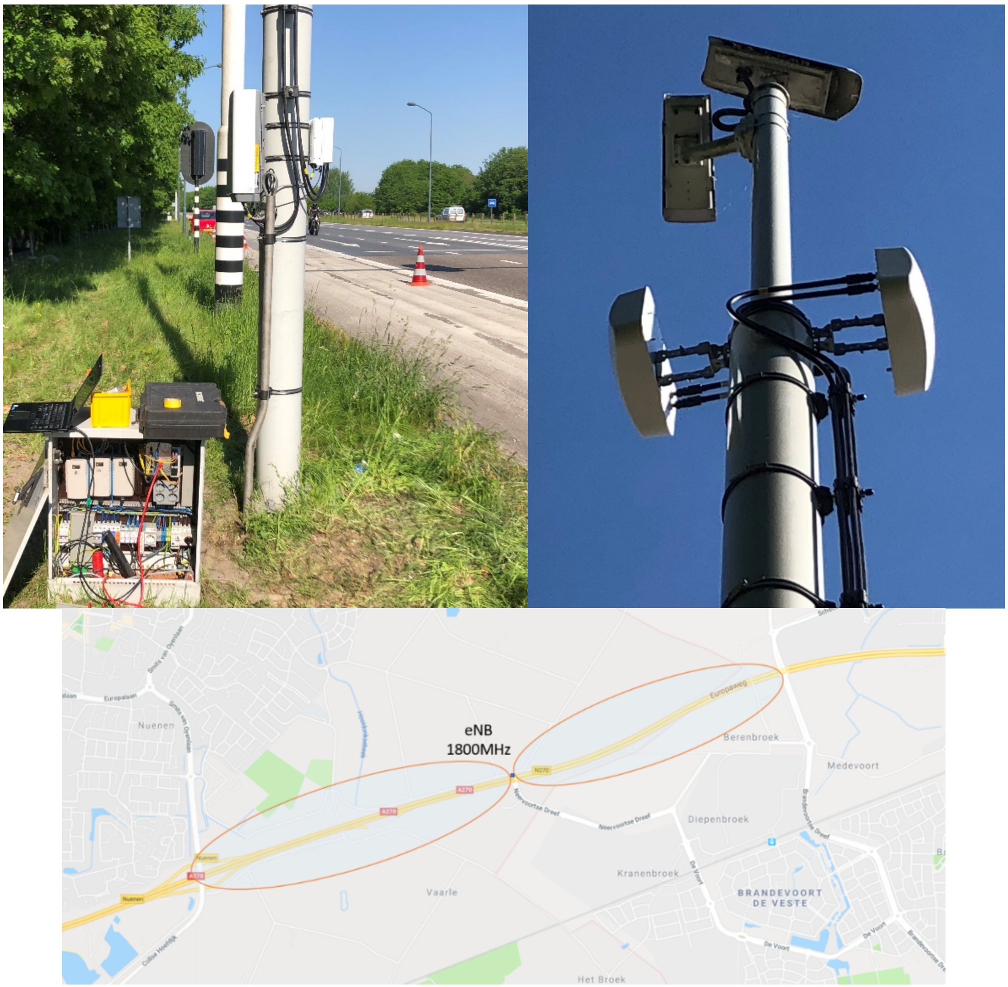


Figure 86: TNO LTE radio network deployment.

For the 5G-MOBIX project this site will be upgraded with 5G NR and possibly an extra 5G NR site will be setup alongside the A270/N270 motorway depending on coverage requirements. For 5G NR bands 42 and 43 are considered. Ericsson Radio 4422 is considered together with a Baseband 6502. The Baseband and Radio modules will be installed next to the current LTE infrastructure. To support early 5G NSA UEs the new equipment will be configured in NSA mode and will work together with the LTE system. When 5G SA is available, the equipment will be configured to support SA mode.

TU/e

KPN 5G NR 3.5 GHz cells overlap the TU/e campus network. Within the TU/e, 3 micro cells operating in the 5G NR millimetre wave bands between 26.6 and 26.7GHz will be employed. Based on reference architectures, TU/e will employ option 2, Standalone 5G NR.

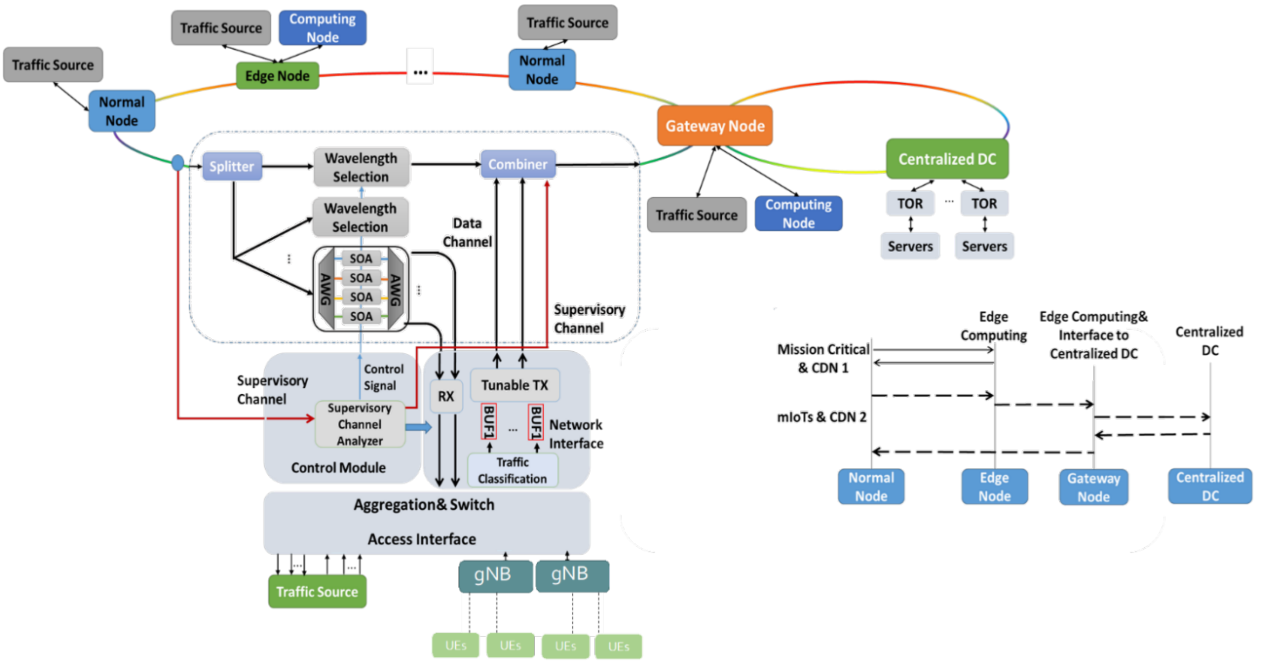


Figure 87: TU/e Campus Network Architecture.

In addition, the onboard UEs in the vehicles are connected to the baseband units via the radio network architecture shown in Section 4.7.2.3. The baseband units (BBUs) are interconnected via a campus-wide optical fibre network infrastructure. Each optical network based on fast reconfigurable optical nodes enables fast provisioning of optical light paths in support of the end-to-end high capacity video slice required. The functional interaction between edge computing resources and the centralized data centre on campus is also illustrated in Figure 87.

Core network architecture

For each of the three 5G networks a core network will be deployed. KPN will initiate with 4G EPC, to be extended to use with 5G NR (Option 3x) and, at a later stage, to a 5G Core (option 2). TNO and TU/e will leverage further their research networks with added 5GCore functionality. The availability of a 5GC is under discussion with the provider of this Core Network capability. The core will be adapted in different stages, going from a NSA to a SA deployment. Figure 88 gives an overview of the different steps that are taken. More information about the three core deployments can be found in the sections below.

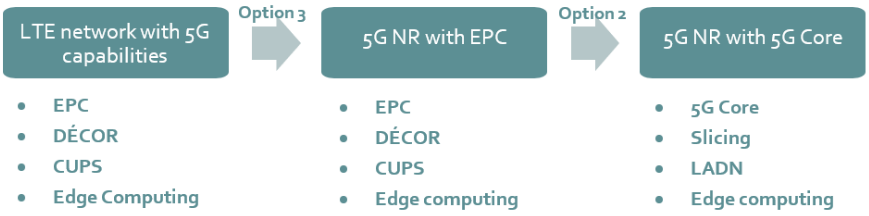


Figure 88: Deployment stages core network.

KPN

The KPN core network architecture will evolve over time within 5G-MOBIX to offer state of the art capabilities depending on available technology. At first, a regular EPC is used, which will evolve to a NSA core after which it will evolve to a 5G SA Core. During the first two stages CUPS and DECOR will be used. With CUPS the traffic stays local at the MEC. With the 5G Core deployment LADN is used to connect the vehicles to the closest edge location.

Edge facilities will be located at the KPN Metro Core location in Helmond and possibly Eindhoven. The Core will be situated at a central location, currently in Aachen. All V2X functions are provided over the top from an edge cloud at the metro core location.

TNO

TNO uses the Open5GCore from Fraunhofer as mobile core network solution. This is a research mobile core network which is software implemented. The core is fully virtualised and can run on any virtualised infrastructure. The current core architecture is EPC based but has an enhanced control, user plane separation and some early 5G functionalities.

Next to the EPC core, a 5GC version of the Open5GCore will be also deployed. The 5GC version will support the minimum required control signals to support SA mode. This ensures maximum flexibility in the UE and radio equipment selection. The subscriber database for the HSS and the UDM will be connected.

The virtualised network functions are deployed on a virtualised infrastructure provided by OpenStack. OpenStack is running on bare metal servers in our main data centre in The Hague. The OpenStack cloud consists of several high-end computing nodes and storage nodes based on a Ceph Storage Cluster which ensures data replication. The virtual networks of the core connect to a physical Secure Gateway (SeGW) that allows authenticated external connections to be made to the core network. Edge location and external RAN connections are connecting to the SeGW to have encrypted and secure access to the core network.

TU/e

Like TNO, TU/e will also use the fully virtualised Open5GCore from Fraunhofer FOKUS described above. TU/e plans to focus on deployment of the 5G version of Open5GCore, avoiding deployment and use of its

4G LTE version if possible and will further optimize according to the nuances of using in millimetre wave frequencies. Further availability of future releases of the Open5GCore from Fraunhofer FOKUS will be evaluated during the project.

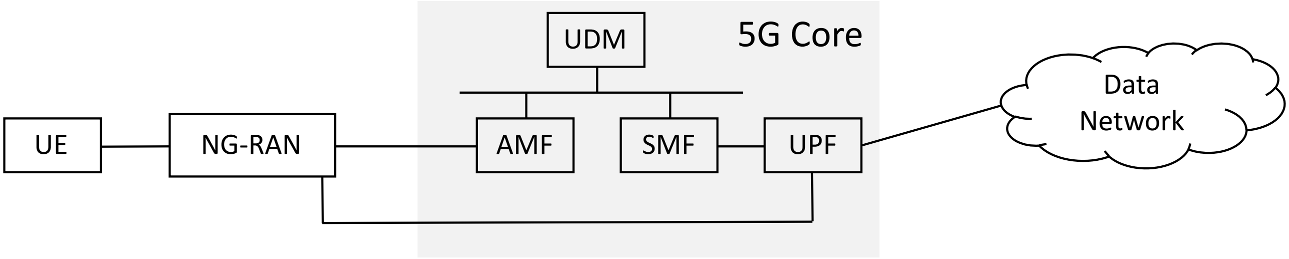


Figure 89: 5GC architecture at TU/e [13].

At TU/e site, an important core network requirement in this trial, and others, is the support of inter PLMN-handover. Solutions are under investigation within the NL trial site. The 5G network at TU/e is introduced with respect to the following principles: the 5G core being implemented with access and mobility management functions, session management and user plane functions, all supported by the unified data management for handling the user identification handling, access authorisation and subscription management of the user equipment and on-board units. At TU/e, the user plane will be designed and optimised to run Slices optimised for Video and the ITS/log messages whilst the control plane carries the control signals user plane traffic.

5G and V2X technologies to be deployed

Table 27: 5G technologies and attributes for 5G network deployed by KPN.

Mobile core	Starting with EPC Following with 5GC
Virtualised	Yes
Virtualised infrastructure	Openstack
Network Slicing	Yes
Orchestrator	TBD
Multiple access Edge Computing	Yes, applications deployed in a Kubernetes Cluster
Radio Access Network	LTE and NR
# of sites	6 or 7
Vendor	Ericsson for first stage
# of cells per site	3
# of antennas per cell	2
Frequencies used	LTE 800FDD, LTE 1800FDD, 5G NR 3.5GHz (pending auctions)

Frequency Bandwidth	60 – 90 MHz depending on auctions and deployment setup
Carrier aggregation	Yes

Table 28: 5G technologies and attributes for 5G network deployed by TNO.

Mobile core	EPC and 5GC
Virtualised	Yes
Virtualised infrastructure	Openstack
Network Slicing	Yes
Orchestrator	Open Source Mano
Multiple access Edge Computing	Yes, applications deployed in a Kubernetes Cluster
Radio Access Network	LTE and NR
# of sites	1 or 2
Vendor	Ericsson
# of cells per site	2
# of antennas per cell	1
Frequencies used	LTE B3 1800MHz, NR B43 3700 MHz
Frequency Bandwidth	B3 - 5 MHz, B43 - 100 MHz
Carrier aggregation	No

Table 29: 5G technologies and attributes for 5G network deployed by TU/e.

Mobile core	5GC
Virtualised	Yes
Virtualised infrastructure	Openstack/Opendaylight
Network Slicing	Yes
Orchestrator	Open Source Mano
Multiple access Edge Computing	Yes, Applications deployed using Kubernetes or Docker Swarm
Radio Access Network	mm-wave NR
# of sites	2-3
Vendor	Experimental/Proprietary
# of cells per site	1
# of antennas per cell	1 (multi-element)
Frequencies used	NR FR2 n258, 26.65 GHz (licensed/test-licence)

Frequency Bandwidth	40 MHz (100 MHz max)
Carrier aggregation	Possible (if needed, not initially foreseen)

Cellular V2X

For direct communication between vehicles LTE Sidelink will be used in use case category one. This will be based on mode 4 without coordination of the cellular network. V2X services from the cellular network will be provided over the top from edge locations. Pending available technology Application Functions can be used to influence traffic routing to V2X applications at the edges.

The test network at TU/e will focus entirely on communication between the vehicle and a remote operator and consequently will only employ V2N functionality. As TU/e plans to not deploy a 4G or enhanced 4G core, rather aiming to directly deploy the 5G version of the Open5GCore (as shown in Figure 89), TU/e will focus on the experimental 5G V2X technology as specified in [14].

Multi-access edge computing

Edge computing is offered from different mobile networks. This to provide V2X services in close vicinity to the road infrastructure, thus making them available with low latency. Each edge computing facility will be set up using a Kubernetes cluster, a solution that simplifies exchange workloads and deploy microservices. Different technologies will be deployed to break out local traffic to the edge. At first, CUPS is deployed to split user plane and control plane traffic. With the availability of the 5G Core this can evolve to either a local UPF or by employing LADN.

With a 5G Core setup both roaming and home traffic will be routed to the edges of the local operator. With scenarios, it is expected that subscribers are subscribed to different operators with different edges, possibly in different countries. This will add extra complexity to the user stories since information needs to be shared across operators and edges to offer subscribers up to date information of the surroundings. Edge locations will be interconnected, please refer to Figure 84 for the MEC locations of the Dutch trial site.

Network Slicing

Network slicing is enabled following a multi-step approach. The scope of the network slicing will be across the RAN and Core for all the use case categories with slices expected to be implemented for:

- Generic and log data.
- ITS messages for all user stories.
- Video data (if needed).

With 4G and 5G different technologies will be employed to enable slicing (see Table 30). Slicing will be enabled on all three networks. One of the networks is a production network were production traffic is mixed with test traffic.

Table 30: Slicing technologies.

Slicing technologies	4G	5G
ASGH with radio prescheduling and IUA	X	
Radio Resource Partitioning	X	
DECOR	X	
5G Slicing (3GPP, 2019)		X

Slicing will become available with 5G but pre 5G different technologies are available to employ slicing. In general, it is possible to define different SPID values for different slices. This way for each slice a separate SIM is deployed and installed in the vehicle. With 5G slicing, defined in TS23.501, a single UE can handle different slices. Three use case categories will be addressed in the Dutch pilot site for which in total three slices are needed. Table 31 shows an overview of the slices per use case category.

Table 31: Slices per use case category.

Slices per UCC	UC1	UC2	UC3
Slice 1	ITS Messages	Vehicle control data and ITS Messages	ITS Messages
Slice 2	Generic - and log data	Generic - and log data	Generic - and log data
Slice 3		Video Data	

Interactions and integration between 5G networks

Subscribers are expected to connect to different 5G networks, each with its own edge location. Information needs to be shared such that all subscribers are receiving up-to-date information needed for the automated driving user stories tested at the trial site.

With cross-border handovers between separate operators we see currently that the subscribers are disconnected for up to a minute or even more. For automated driving vehicles, a disconnect for more than one second means that it cannot rely on the mobile network. On the other hand, currently we don't see that technology has evolved enough for 5G Core networks to offer a solution to this problem. For 4G Core networks solutions do seem to exist using the S10 interface (although no network operator has implemented this yet). As technology evolves for 5G core networks this should be tested when becoming available. There is a direct fibre connection between the edge locations of KPN and Siemens/TNO. This fibre connection is used to allow communication between different operators which use different edge locations.

Annex 9 – CN 5G architecture

Radio network requirements

The specific use case categories for the China trial are Automated Driving and Road Safety and Traffic Efficiency Services, as described in D2.1 [1]. The two cases are deployed through the vehicle-road collaborative overall architecture, which is mainly composed of the control centre (or ITS-centre), automated vehicles and a variety of communication technologies. The main requirements for Radio network are to eMBB, mMTC, and uRLLC. These requirements can be used to enhance the communication capacity in autonomous applications and enable the control centre to access to mass terminals, and finally realize more reliable applications of autonomous applications.

Regarding the above UCCs, radio network requirements are described, in the following subsections.

Network infrastructure

To efficiently support the diverse user stories related to the Automated Driving UCC and Road Safety and Traffic Efficiency Services UCC, more flexible and optimized exploitation of network infrastructure is necessary. Network slicing is the provisioning of network resources into multiple virtual networks to support more services. The advantage of network slicing is that it allows network operators to choose the features required for each slice, such as low latency, high throughput, connection density, spectrum efficiency, traffic capacity and network efficiency, which can help improving the efficiency in creating products and services, and on the customer experience. The eMBB slice has been adapted for the high bandwidth information service applications such as video road condition sharing, HD map update, HD map acquisition, high precision positioning, remote control, business promotion and passenger entertainment. The uRLLC network slicing has been adapted for the low delay safe and efficient applications, such as front vehicle collision prevention, lane change assistance, abnormal vehicle alarm, pedestrian collision prevention, fleet formation, signal light reminder, front stationary vehicle reminder, among others.

As shown in Figure 90, the above network slicing can be employed in the V2X scenario. Multiple services of the Internet of vehicles can be realized through the multi-level deployment of edge computing. For the high bandwidth information service applications, there can be a mobile broadband slice for the Automated Driving UCC which provides high-quality video streaming or Internet access to in-vehicle passengers. The network resources can be flexibly allocated according to the bandwidth demand variation. Also, the cache usage in the edge cloud can be maximally utilized. And for the low delay safe and efficient applications, there is a mission-critical slice for the remote driving UCC, which can support ultra-reliable and low-latency (URLL) traffic by the dedicated usage of network resources for its mission.

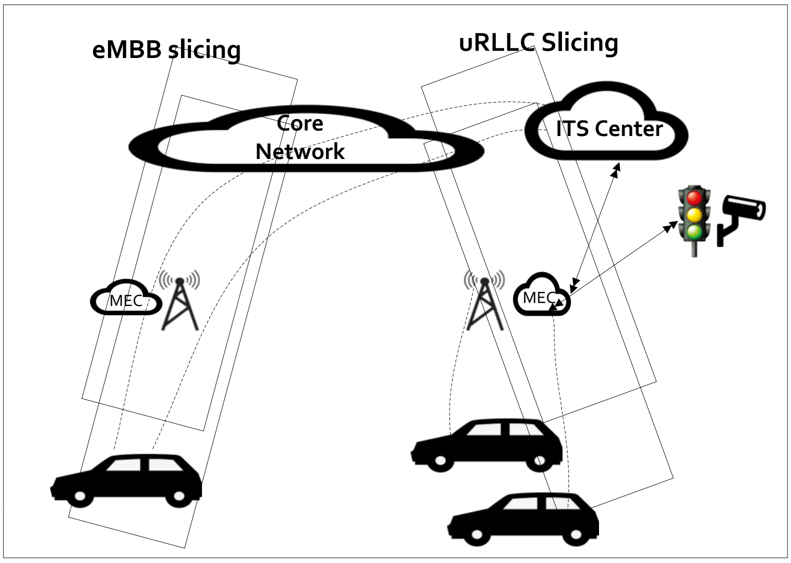


Figure 90: Network slicing example for V2X scenario

The following basic requirements apply to the Chinese UCs:

- *Basic connection*: such as high-precision map download, information interaction between vehicle and central control platform, etc.;
- *Cost reduction*: such as Sensor Data Sharing, network high-precision positioning, etc., to reduce the cost of vehicle radar, Sensor, positioning system, etc.;
- *Improved reliability*: autonomous driving under conditions of smaller safety distance and higher vehicle speed, including the fleet management function; improve the effectiveness, reliability and robustness of visual identification of traffic lights, etc.;
- *Improved intelligence*: such as collaborative control, vehicle priority game at intersections, etc.;
- By integrating low power consumption, edge computing, vehicle-road collaborative multi-mode intelligent roadside unit and vehicle-mounted communication unit, the fusion application of multi-perception technology in intelligent network road and autonomous vehicle will be realized.5G edge cloud computing is used to research the autonomous driving road management and service platform based on big data and intelligent decision-making;
- 5G autonomous driving evaluation currently facing complex test scenarios, weather and other environmental factors are complicated, the problems such as driving behaviour are also difficult to evaluate by traditional techniques, so we need to build technical indicators, reaching 5G autonomous driving business needs from systematic, completeness and scientific aspects.

Core network requirements

Core options

Compared with 4G, the architecture of 5G core network has undergone great changes. In order to distribute and deploy core network functions as multiple virtual network elements, core network cloud, forwarding and control separation, virtualisation slicing technology based on software defined network/function virtualisation (SDN/NFV) technology can be applied.

To meet different service application scenarios, the core network and radio access network of 5G adopt the network slice architecture. Slicing deployment is conducive to the new business development of 5G. For example, the core network slice of uRLLC's business will focus in the location near the base station, to meet the network demand for low latency.

MEC deployment

Due to the associated end-to-end latency, reliance on the cloud can affect the performance of data analysis for autonomous vehicles. Therefore, to reduce end-to-end delay, we consider multi-access edge computing (MEC) as a technology suitable for edge analysis supporting autonomous vehicles. MEC servers are deployed on the edge network, as shown in Figure 91.

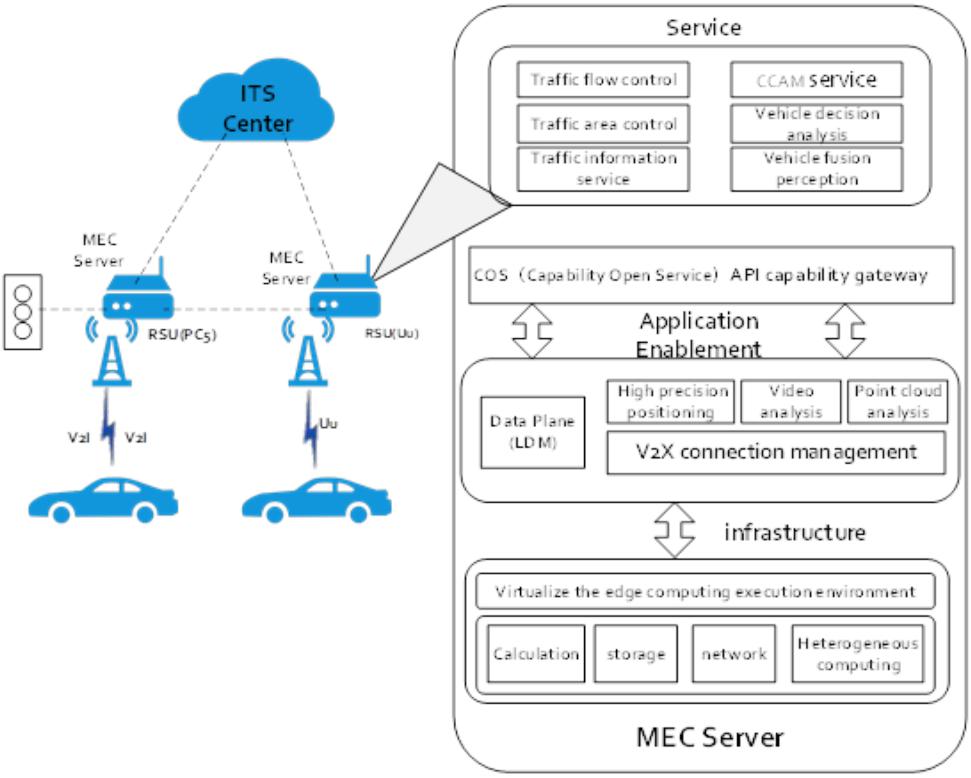


Figure 91: MEC deployment diagram in CN

The MEC server integrates several businesses, such as traffic flow control, CCAM service, traffic area control, etc. Besides, it can enable many applications, which are data plane, high precision position, video analysis, point cloud analysis and V2X connection management. In order to virtualize the edge computing execution environment, MEC server should realize calculation, storage, network and heterogeneous computing at the infrastructure layer.

Interdependencies with other infrastructure

Direct communication mode can work within the network coverage and can work without network coverage, using ITS specially near 5.9 GHz spectrum for direct communication between terminal equipment,V2V communication, roadside infrastructure, such as pedestrians around nodes of low delay, high reliable communication. Direct communication mode can satisfy the forward collision warning, intersection collision warning and emergency vehicle warning safety applications requirements. In terms of technical performance, LTE-V2X has obvious advantages in coverage, reliability, and capacity compared with other currently optional V2X wireless communication technologies. Also, LTE-V2X technology system will continue to evolve, including LTE-v2x enhancement and standardisation of V2X wireless communication technology based on 5G new port (NR), to further support the richer and more advanced Internet of vehicles applications.

In addition, MEC servers are deployed on the edge of the connection network, as shown in Figure 92. Figure 92. For this work, MEC servers have been deployed on Roadside Units (RSUs) for edge analysis and content caching near self-driving cars.

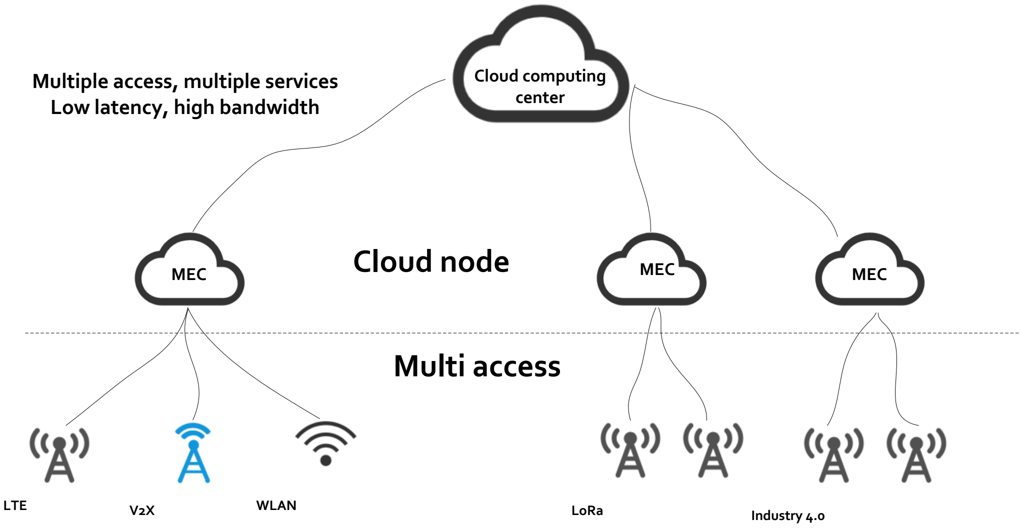


Figure 92: MEC interconnection and coexistence

5G Architecture implementation

China trial site will deploy a state-of-the-art V2X network infrastructure in Jinan City, Shandong Province, China, as seen in Figure 93, will be an ideal test site to test diverse V2X networks such as DSRC， LTE-V, 5G NR, and Wi-Fi. China trial site Supports C-V2X direct communication (V2V/V2I/V2P), GNSS, QDR3.0, SIM-less operation and so on. It has roadside and vehicle data acquisition devices, such as RSU, OBU, RT-RANGE, VBOX, etc. China trial site adopts two road scenarios, urban roads and highways (optional), which include intersections, t-junctions, uphill and downhill, toll stations, and freeway ramps.

Figure 94 shows that the main test point in Jinan adopts the network architecture of C-V2X and uses the direct connection mode and the network mode. The PC5 direct connector works in ITS 5.9g frequency band through the roadside unit to realize low-delay communication of V2V, V2I, and V2P. As shown in Figure 95, V2V can provide early warning. V2P ensures pedestrian safety. V2I can provide traffic lights, traffic signs, parking location, etc., and the vehicle communicates with the cloud through the mobile network (V2N). Through all the communication above, the user stories will run well.

Figure 93: China trial site area

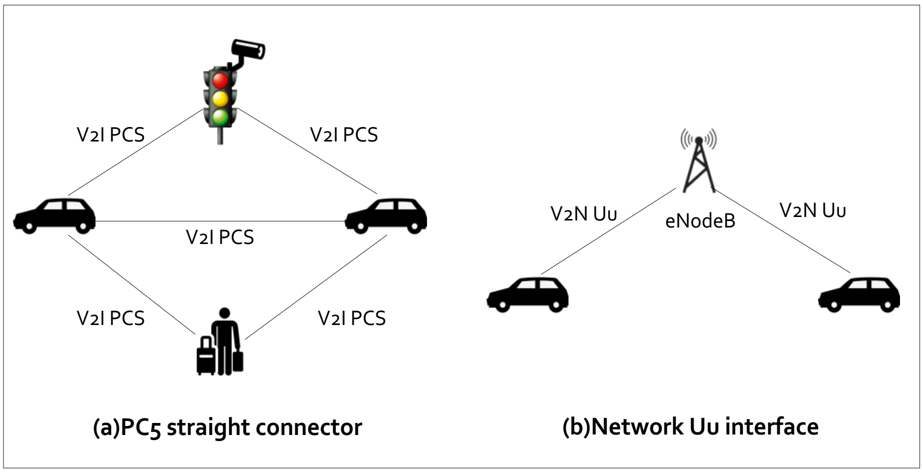


Figure 94: Radio network type descriptions: a) PC5 Straight connector; b) Network Uu interface

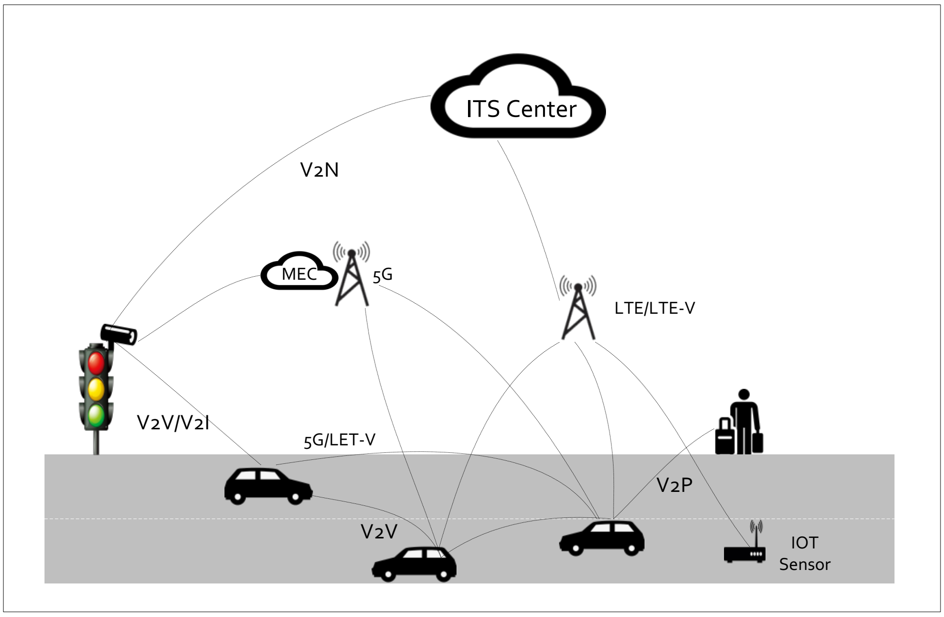


Figure 95: C-V2X network architecture

Radio network architecture

As illustrated in Figure 96, the radio network architecture adopts the ITS control centre.

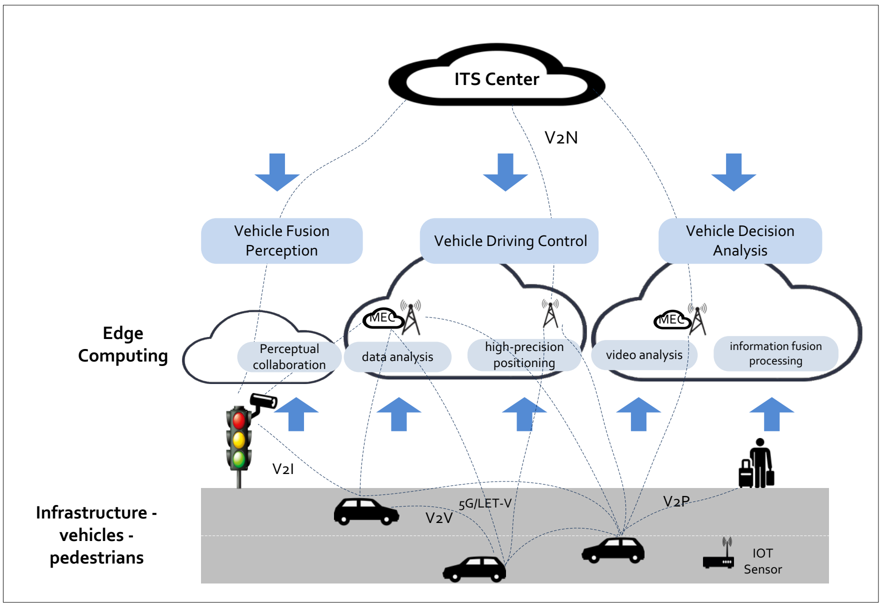

ITS Center
V2N
Vehicle Fusion Perception
Vehicle Driving Control
Vehicle Decision Analysis
Edge Computing
Perceptual collaboration
MEC
data analysis
high-precision positioning
MEC
video analysis
information fusion processing
V2I
Infrastructure - vehicles - pedestrians
5G/LET-V
V2V
V2P
IOT
Sensor

Figure 96: Radio network architecture.

The three-layer architecture of ITS control centre, edge computing and some terminals (roadside facilities, vehicles, and pedestrians, etc.) is adopted. The control centre realizes vehicle hybrid perception through V2N. The radio architecture can be used to implement vehicle fusion perception, vehicle driving control, and vehicle decision analysis. Edge computing includes perceptual collaboration, data analysis, high-precision positioning, video analysis, and Information fusion processing. The V2I, V2V, and V2P transmit the information to the Edge calculation and then transmit the calculated data to the ITS Centre. The ITS centre then feeds the processing decisions back to the Edge computing, and then controls V2I, V2V, and V2P. Through eNB, the network mode runs in the licensed frequency band of the operator to realize V2N communication of vehicle-to-network.

Core network architecture

Station scale: one S1, covering the trial site.

Networking framework: vehicle controller & vehicle video stream -> front-end router -> CPE-5G NR -> Jinan core network -> 100M Internet private line -> control centre -> vehicle control & video decoder (fixed public network IP) -> display screen.

Scheme of the video streaming transmission: five cameras are used in the front end (front, rear, right and left + in the car) and fixed IP (192.168.2.x) is adopted. After setting up the Video decoder with fixed public network IP, the front end can ping the video decoder, and then the front-end pushes the video stream to the video decoder to realize the video stream playback.

Scheme of the control signal transmission: the front-end vehicle and the rear end driving hall both have a controller which adopts fixed IP and fixed configuration so that the driving control room can send control commands to the vehicle.

5G and V2X technologies to be deployed

Network slicing is the process of cutting a physical network into multiple independent, logical slice sub-networks that share physical infrastructure and provide different service types to cope with different scenarios. eMBB network slicing has been adapted to high-bandwidth information service applications such as video road sharing, high-definition map update, high-definition map acquisition, high-precision positioning, remote control, business promotion, and passenger entertainment. uRLLC network slicing has been adapted to low-latency, safe and efficient applications such as front-vehicle collision prevention, lane change assistance, abnormal vehicle alarms, pedestrian collision prevention, formation, signal light reminders, and front vehicle stationary reminders.

The physical configuration of China's wireless network can be composed of LTE-V2X (also known as C-V2X), a global solution for vehicle-to-everything (V2X) communications, designed to improve vehicle safety, autonomous driving and traffic efficiency. The LTE-V2X has a powerful 5G NR evolution path and is widely supported by the global communications and automotive ecosystem including the 5G Automotive Alliance (5GAA). The 5GAA supports V2V, V2I and V2P communications in the 5.9GHz Intelligent Transportation System (ITS) band. There are some other performances in the following:

- support GNSS;
- QDR3.0;
- support sim-car-free operation;
- longer communication range and greater reliability;
- optimize density traffic flow scheduling;
- enable vehicles, VRUs, RSUs.

Annex 10 – KR 5G architecture

Radio network requirements

The selection of radio network structure should consider processing capability and delay sensitivity of the traffic as well as deployment cost. For example, the radio network can be deployed either in a centralized RAN (C-RAN) or a distributed RAN (D-RAN) for providing flexible user services. In a C-RAN structure, main baseband and higher layer processing are performed at the centralized DU pool (Figure 97a). The interface between DU and RSUs require higher bandwidth connectivity such as optical fibre. On the other hand, in a D-RAN structure (Figure 97b), baseband and higher layer processing capability are distributed to each RSU.

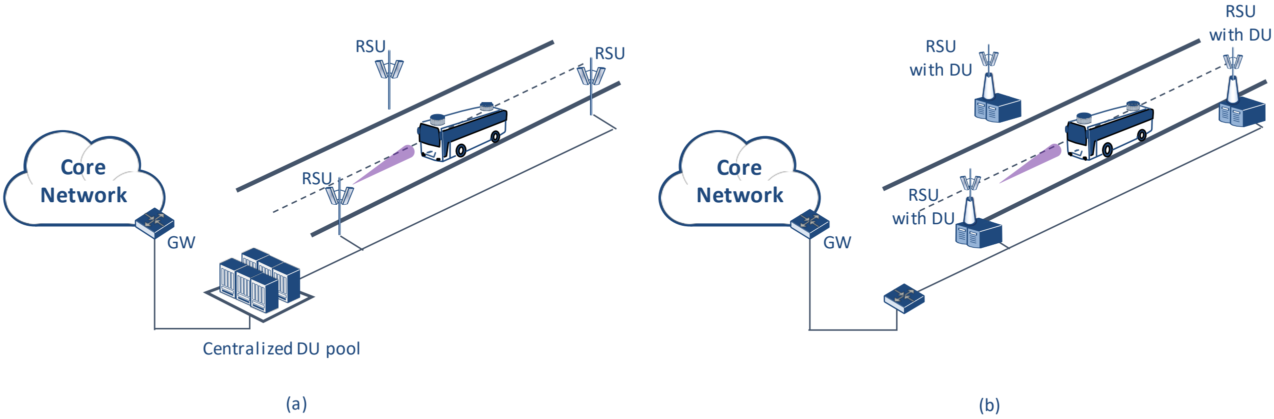


Figure 97: radio network type descriptions: a) C-RAN; b) D-RAN

In order to efficiently support the diverse user stories related to the Tethering via Vehicle and Remote Driving UCC, more flexible and optimized exploitation of network infrastructure is necessary. Thus, network slicing enables coexistence of diverse service verticals based on the common physical network infrastructure with software-defined and highly virtualised network functions [33]. By network slicing, separate and independent logical networks (a.k.a. called network slices) are created, each of which is specifically tailored for each user story having a unique QoS requirement. Network slicing has been adapted to the high mobility applications such as high-speed train scenario where several different service verticals can be supported efficiently [34].

The following additional radio network-related functional requirements should be considered for the design of South Korea trial connectivity:

- *Seamless handover*: To support enhanced V2X services, seamless handover is needed. Meanwhile, 5G NR targets to support near-zero or zero handover interruption time which can provide seamless eMBB or uRLLC service to vehicle applications through techniques such as RACH-less handover or make-before-break schemes.
- *Beam switching*: When using mm Wave bands, the effects of blockage is significant due to the high directivity of the mm Wave signals. As a possible solution to avoid such blockage effect is fast beam switching which enables to detect any signal blockage situation and to switch the transmit/receive beam to one of the unblocked beams.

Core network requirements

Core options

The South Korean site will make sure to take Slicing into account when designing the core for its trials, as this feature is expected to play a significant role in the KR trials.

Interdependencies with other infrastructure

The V2X infrastructure for South Korea trial site will be deployed and operated in Standalone mode. However, it is designed to coexist with the 5G NR system. More specifically, numerology, frame structure, reference signal, and physical channel structure are designed to be compatible with the 5G NR. Hence, in the future, there will be a potential to reuse 5G NR infrastructure with minimum migration efforts.

5G Architecture implementation

In the near future, 5G built-in to connected vehicle systems will enable remote control of vehicles by human pilots, and within the vehicles, various types of infotainment services will be provided to onboard passengers. Thus, at the Yeonggwang trial site in South Korea, a field trial with a 5G NR-based V2X prototype system providing two relevant V2X UCCs as illustrated in Figure 98, *tethering via vehicle* and *remote driving*, will be carried out.

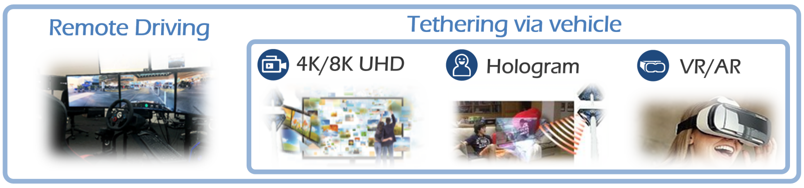


Figure 98: target V2X use cases.

The most remarkable feature of the system is using mm Wave band that can provide a high-bandwidth connection between vehicle UEs (V-UEs) and network. In addition, since the system operates at mm Wave band, it is designed to comply with 5G NR specification with numerology of $\mu \in \{2,3\}$, which can effectively reduce the end-to-end latency for the targeted UCCs, by reducing transmission time interval (TTI) as compared with numerology of $\mu = 0$. Through the field trial, it is expected to demonstrate the feasibility and superiority of mm Wave-band NR V2X system for offering the two targeted V2X UCCs.

Radio network architecture

As illustrated in Figure 99, the radio network architecture for the targeted V2X system consists of mm Wave-band NR V2I link (or NR Uu) between vehicle and network and onboard access link (e.g. NR V2P link, Wi-Fi link), where Uu is air interface between base station and user equipment.

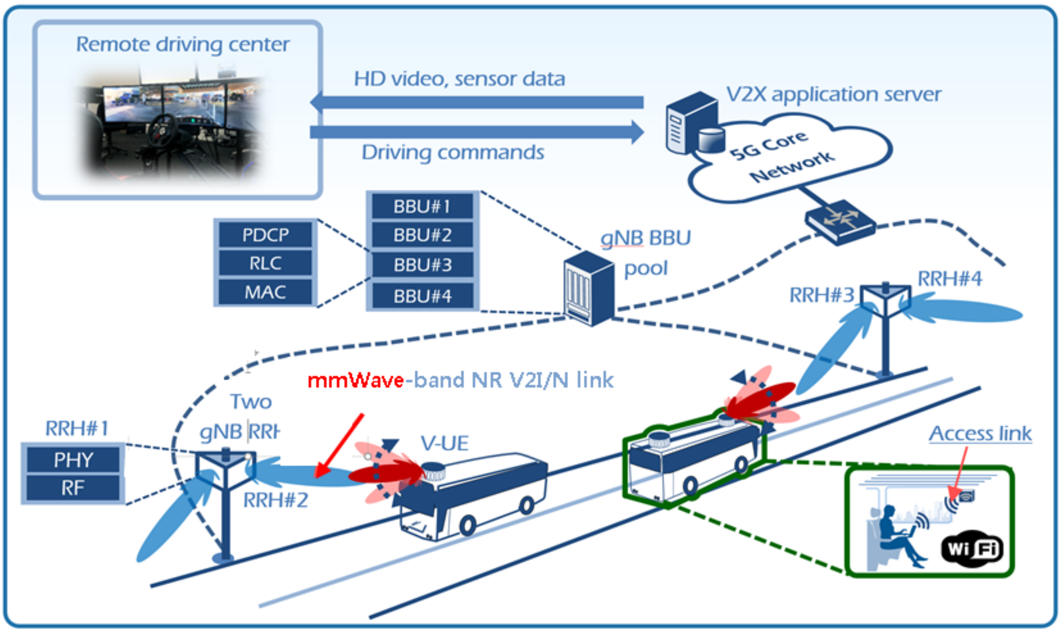


Figure 99: mm Wave band 5G NR V2X network architecture.

Thanks to a vast amount of bandwidth available in the mm Wave, V-UE enables to establish a high-bandwidth connection with network and onboard users (e.g. passengers) can connect their devices to the access link (e.g. Wi-Fi) connected to the V-UE. Meanwhile, vehicles with onboard cameras and/or sensors periodically transmit necessary data (e.g. HD video with H.265/ HEVC) to a remote driving centre. Based on the information, a human driver at the driving centre using an interface like today's car-driving simulators can operate the car remotely by sending the driving commands to the car through the reliable and low-latency V2I link.

In addition, by adopting C-RAN architecture to the network, a base station (BS) is functionally split into a remote radio head (RRH) and a baseband unit (BBU). A RRH independently interconnected with corresponding BBU is composed of RF/antenna for transceiver and baseband (BB) module for physical-layer processing, and two RRHs covering sectors (cells) in opposite directions are located at a same site. Generally, in highway environments, the RRHs are installed along the road side at regular intervals, while in urban environments, they can be installed on the roof of a building or in a street structure. For the field trial, however, it is most likely to demonstrate a simplified scenario where vehicles move in one direction. In this case, one RRH pointing the opposite direction of the moving direction will be installed at each site. Each BBU is connected to the data network (e.g. public Internet) or V2X application server via 5G core (5GC) network, which is responsible for higher-layer functionalities.

For the prototype system, mm Wave band, namely Flexible Access Common Spectrum (FACS), is utilized for the NR V2I link between RRH and V-UE. The FACS is an unlicensed spectrum that has been allocated by Korean government and ranges from 22 GHz to~23.6 GHz. Since the FACS is close to NR FR2 band (i.e. n258), the prototype system for NR V2X is designed to comply with numerology of μ ∈ {2,3}, where μ is sub carrier spacing, i.e. when μ=2, sub carrier spacing is equal to 60kHz, and μ=3 equal to 120kHz, respectively. The detailed physical-layer parameters supported in the prototype system are listed in Table 32. Also, V-UE equipped with three antennas creating beams in different directions is mounted on top of the vehicle, which allows the V-UE to perform beam switching to align its TX/RX beam with beam transmitted from the serving RRH.

Table 32: Physical-layer parameters

Parameter	μ=2	μ=3
Frequency allocation for V2I link	22.1~22.7 GHz	
Max. number of CCs per gNB	6	6
Max. number of CCs per V-UE	3	3
Bandwidth per CC (MHz)	100	100
Subcarrier spacing (kHz)	60	120
Number of PRBs per CC	132	66
FFT size	2048	1024
Sampling rate (MHz)	122.88	122.88
TTI (μs)	250	125
OFDM symbol duration (μs)	16.67	8.33
Cyclic Prefix duration (μs)	μ=2	μ=3

OFDM symbol including CP (μs)	22.1~22.7 GHz	22.1~22.7 GHz

Core network architecture

The Core Network Subsystem (CNS) interfaces with the Moving Network-Radio Access Subsystem (MN-RAS), which acts as a base station through the external interface N2/N3. CNS consists of CPS (Control Plane Subsystem) and UPS (User Plane Subsystem. CPS provides signal processing for providing Attachment and Mobility of UES (User Equipment Subsystem) based on NAS protocol, UPS processes media transmission, acts as an endpoint of GTP tunnelling and works with MN-RAS.

The CPS functionally includes AMF and SMF functions, processes signal messages received in NGAP messages, and provides functions to create, modify, and delete User Data channels through the UPS and IPC interworking. The UPS consists of a Session Manager, a Traffic Controller, and a DPDK module, providing a function for processing user data between the MN-RAS and the DN. UPF is developed using NIC cards and multi-core processes that support DPDK, connected to MN-RAS via Ethernet. The overall 5G core network architecture is depicted in Figure 100.

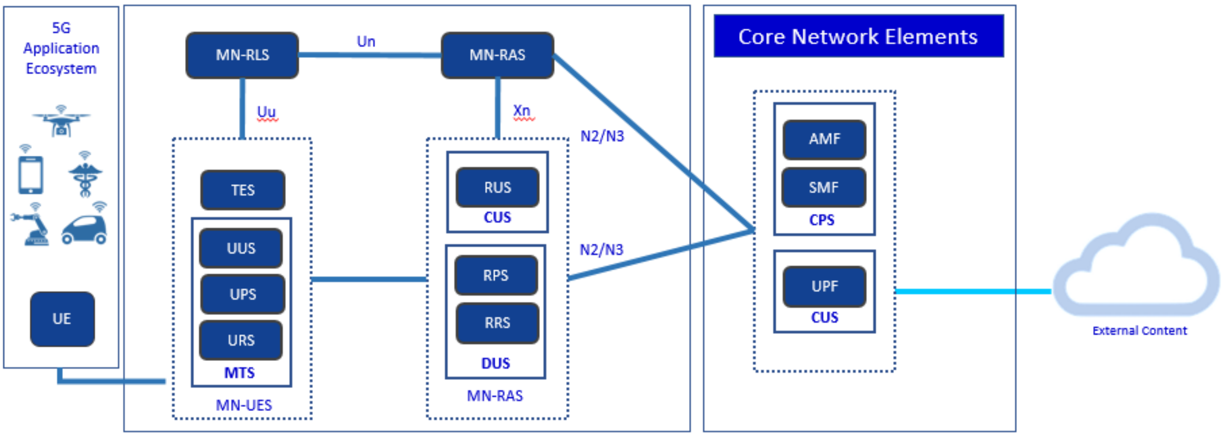


Figure 100: 5G Core network architecture

5G and V2X technologies to be deployed

In the Korean trial site, YeongGwang PG, a 5G trial network will be deployed. The 5G technologies included are listed below.

Table 33: 5G technologies and attributes for 5G trial network deployed by ETRI and Snet ICT

Mobile Core	5GCN

Virtualised	Yes
Virtualised infrastructure	N/A
Network Slicing	Yes
Orchestrator	N/A
Multiple access Edge Computing	N/A
Radio Access Network	NR based network
# of sites	2-3
Vendor	Prototype system developed by ETRI
# of cells per site	1-2
# of antennas per cell	2T2R
Frequencies used	22-23.6 GHz (unlicensed)
Frequency Bandwidth	600 MHz
Carrier aggregation	6 x 100-MHz carriers

Cellular V2X

Experimental 5G C-V2X technologies will be developed and deployed to support the Korea local trials. The Korea site user stories will use a kind of V1 interface between an application server and applications in a UE. The V1 interface adapted in the deployment may reuse established service and application layers by automotive community, e.g. SAE. Furthermore, the 5G V2X will take advantage of 5G Uu interface features such as low latency, large bandwidth, and high mobility support, where Uu is air interface between base station and user equipment. Specifically, a large bandwidth of 600MHz will be exploited to expand data pipeline between gNodeB and vehicles into ~1Gbps per vehicle. Low latency is also crucial factor for enhanced vehicle applications, e.g., remote vehicle controlling, and technologies to attain low latency will be deployed.

Frequency bands

Traditionally, ITS band around 5.9 GHz has been used for the V2X systems, such as IEEE 802.11p-based dedicated short-range communication (DSRC), which mainly targets safety-related applications. The DSRC technology is now mature but it can only provide the data rate on the order of 10 Mbps due to the relatively narrow bandwidth and the inefficiency of the distributed multiple access scheme namely carrier-sense multiple access (CSMA) [35]. LTE V2X can utilize licensed spectrum which is wider and can be much more efficiently allocated to each vehicle, achieving data rate in the order of 100 MHz [35]. However, it is still not satisfactory to support 5G V2X user stories especially South Korean trial connectivity requiring multi-Gbps data rate.

These multi-Gbps data rate can be best achieved using very wide bandwidth in the order of Gbps, which can be attainable in the mm Wave frequency bands. Hence, in the South Korean trial, mm Wave band around 23 GHz is employed for the V2I links for the Tethering via Vehicle and Remote Driving UCCs. The use of mm Wave band may suffer increased path loss which can potentially reduce the coverage. However, if we fully utilize the beamforming capability, we can confine and concentrate the desired signal along the road, potentially extending the coverage area and providing better connectivity to the vehicles of interest. In addition, if the RSUs are properly deployed, the blockage effect can be minimized.

Annex 11 – Security Architecture Overview

1) Domains

The basis for the security architecture is the use of domains. Figure 101 illustrates an instance of a 5G network and depicts the domains defined so far.

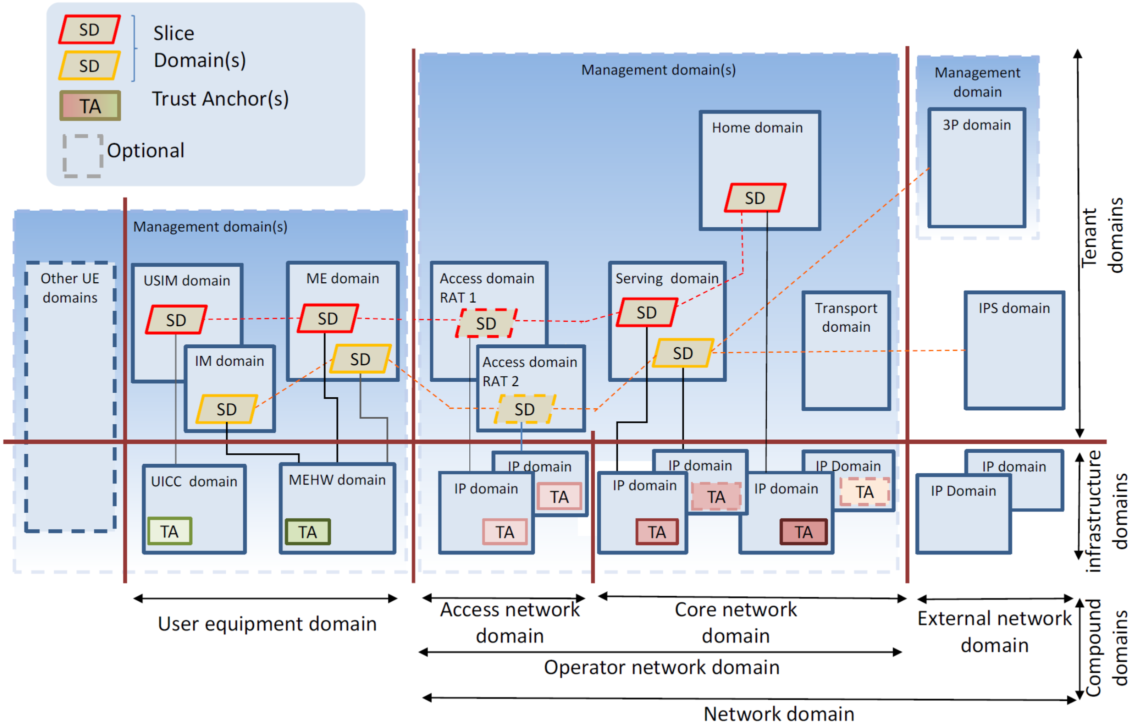


Figure 101: 5G Security Architecture

The domain concept is a cornerstone in the security architecture as it enables the definition of different types of domains used to represent a 5G network's different functionalities, services and actors. The defined domains may occur in multiple instances, and belong to different actors taking on different roles and responsibilities in the network, which provides flexibility for the modelling of different 5G network configurations and describing their inherent multi-party trust aspects. By observing interdependencies and required interactions between domains, it becomes a relatively straightforward task to analyse and model their trust relationships and their need for different security controls.

We use three different types of domains. Firstly, there is the Infrastructure Domains focussing on the relevant physical network aspects, i.e. they contain the "hardware" in the network. Then, there are Tenant Domains which are logical domains executing in infrastructure domains. By this division into infrastructure and tenant domains, it is easy to map and handle virtualised environments onto the architecture as these types of domains give a clear division between the physical platform offering an execution environment and the logical functions and services in the tenant domain.

To capture higher order groupings of entities and/or functionality we have defined a third type of domains, namely Compound Domains. Such domains consist of a collection of other domains, grouped together according to some 5G relevant aspects, e.g. ownership, joint administration or the like. With this concept, we can map 3G/4G defined domains onto our security architecture in a simple way.

Slice Domains are of particular importance. They are compound domains used to capture network slicing aspects. A slice can cover only some parts of the network, e.g. parts of the Core Network domain, but are in general defined end-to-end. In this way, slicing is explicitly handled. The use of slice domains also highlights the trust issues appearing between actors controlling a domain and other actors controlling concurrently operating slices in that domain. The requirement on strict isolation between domains and slices belonging to different actors is also made clear. We note that slicing may be implemented without relying on a virtualised system, but in most 5G systems it is.

The domain figure depicted above also shows so called Trust Anchors (TAs) in the infrastructure domains. These trust anchors are used to capture trust issues appearing in virtualised systems, e.g. how to get assurance of tenant domain integrity and that a tenant domain executes on a designated and trusted infrastructure. The trust anchors can also be used to verify infrastructure domains' integrity and to bind tenant domains to infrastructure domains. We only have three types of infrastructure domains. They are:

i. UICC Domains containing the conventional tamper-resistant module offering protected storage and processing of long-term subscriber credentials and other security critical information.

ii. Mobile Equipment Hardware (MEHW) Domains containing the hardware support for the Mobile Equipment (ME). The MEHW domain may include Trusted Execution Environments (TEE) supporting e.g. other forms of credentials such as certificates.

iii. Infrastructure Provider (IP) Domains containing the hardware platforms for the compute, storage, and networking resources required by both the network/telecom functionality and the access (radio) specific hardware.

At present, there are 10 tenant domains defined. They are:

1. Mobile Equipment (ME) Domains containing the logical functionality required for using access to the network services, for the operation of access protocols by users and for user applications.

2. USIM Domains containing the logical functionality for USIM operation together with other hosted security services (it is analogous to the USIM domain of TS 23.101 [40], but only contains the logical functionality).

3. Identity Management (IM) Domains containing the functionality to support alternatives to USIM-based authentication, i.e. for industry automation use cases (the IM Domain may contain for example public key certificates). The IM domain preferable obtains security support from a UICC or from a TEE in the MEHW as discussed above.

4. Access (A) Domains containing the logical functionality that manages the resources of the access network and provides users with mechanisms to access the core network domain.

5. Serving (S) Domains containing the logical functionality that is local to the user's access point. It also routes calls and transports user data/information from source to destination. It can interact with the home domain to cater for user specific data/services and with the transit domain for non-user specific data/services purposes.

6. Home (H) Domains contains the logical functionality conducted at a permanent location regardless of the location of the user's access point. The USIM is related by subscription to the home network domain. The home network domain therefore contains at least permanently user specific data and is responsible for management of subscription information. It may also handle home specific services, potentially not offered by the serving network domain.

7. Transit (T) Domains containing the logical core network functionality in the communication path between the serving network domain and external remote parties.

8. 3rd Party (3P) Domains containing functionality for use cases where a (semi-)trusted third party such as a factory/industry vertical provides its own authentication services for e.g. M2M devices like industry robots and IoT-devices.

9. Internet Protocol Service (IPS) Domains representing operator-external IP networks such as the public Internet and/or various corporate networks. Such networks may be partially or fully non-trusted.

10. Management Domains containing the logical functionality required for management of specific aspects of a 5G network. Management domains may cover security management, traditional

network management, orchestration of SDN and virtualised environments, management of user equipment domains, etc.

Finally, the compound domains defined are:

1. Slice domains (described above).

2. User Equipment (UE) Domains defined by MEHW, ME, UICC, USIM and IM domains included, i.e. it consists of the equipment used by a user to access network services. The "Additional UE Domain" in Figure 90 is added to capture the so called direct-mode, UE-to-UE communication.

3. Access Network (AN) Domain defined by the A and IP domains included, i.e. it consists of the entities that manage the resources of the access network and provides the user with a mechanism to access the network. It may comprise of different types of accesses, e.g. both WLAN and 5G-radio accesses.

4. Serving Network (SN) Domain include the S and corresponding IP domain and correspond to the same concepts defined in TS 23.101 [40].

5. Home Network (HN) Domain include the H and corresponding IP domain and correspond to the same concepts defined in TS 23.101 [40].

6. Transit Network (TN) Domain include T and corresponding IP domain and correspond to the same concepts defined in TS 23.101 [40].

7. Core Network (CN) Domain defined by the HN, SN, TN and IP domains included, i.e. it consists of the entities that provide the network features and telecommunication services. The support provided includes functionality such as user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information.

8. Operator Network (ON) Domain defined by the AN and CN domains included, i.e. it consists of the physical nodes together with their various functions required to terminate the radio interface and to support the telecommunication services requirements of the users.

9. External Network (EN) Domain defined by the 3P, IPS and IP domains included.

10. Network (N) Domain defined by the ON and EN domains included.

2) <u>Strata</u>

Figure 102 shows the strata of 5G security architecture. The definitions of the strata are analogous to the definitions given in TS 23.101 [40] except for the management stratum which is added in the 5G security architecture. The management stratum is graphically drawn to be behind and cover all other strata because the management stratum will perform management operations on network functions in all the other strata. For instance, it will comprise protocols like OpenFlow for configuring network components. Obviously, there will also be dedicated protocols, data, and functions related to managing NFVs and network slices.

The strata provide a high-level view of protocols, data and functions that are related in the sense that they are exposed to a common threat environment and exhibit similar security requirements. The use of strata thus helps structuring by purpose and where different security controls are needed.

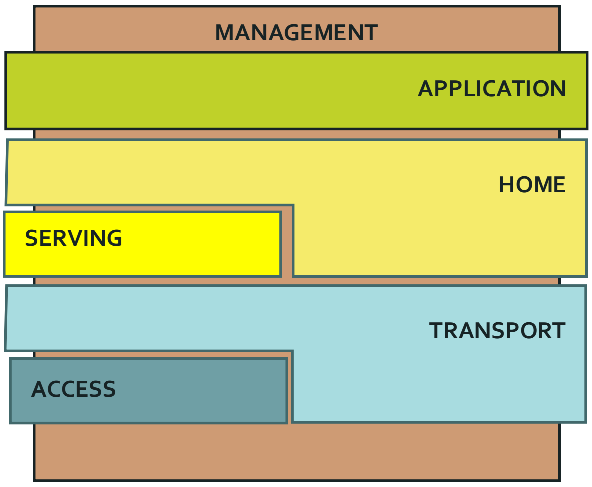


Figure 102: Illustration of the strata

The Application Stratum represents the application process itself, provided to the end-user. It includes end-to-end protocols and functions which make use of services provided by the home, serving and transport strata and infrastructure to support services and/or value-added services. End-to-end functions are applications that are consumed by users at the edge of/outside the overall network.

The Home Stratum contains the protocols and functions related to the handling and storage of subscription data and home network specific services. It also includes functions to allow domains other than the home network domain to act on behalf of the home network. Functions related to subscription data management, customer care, including billing and charging, mobility management and authentication are in this stratum when end-users are at home network. When end-users are roaming, then serving network domain can do mobility management at serving network level.

The Serving Stratum consists of the protocols and functions to route and forward data/information, user or network generated, from source to destination. The source and destination may be within the same or different networks. Functions related to telecommunication services are located in this stratum.

The Transport Stratum supports the transport of user data and network control signalling from other strata through the network. It includes consideration of the physical transmission, e.g., physical transmission format, error correction/recovery, data encryption, resource allocation, to name a few. The Access Stratum is a sub-stratum of the Transport Stratum. It is located between the edge node of the serving network domain and the UE Domain. It provides services related to the transmission of data over the radio interface and the management of the radio interface.

The Management Stratum comprises aspects related to conventional network management (configuration, software upgrades, user account management, log collection/analysis, etc.) and, particularly, security management aspects (security monitoring audit, key and certificate management, etc.). In addition, aspects related to management of virtualisation and service creation/composition (orchestration, network slice management, isolation and VM management, etc.) belong to this stratum.

3) Security control classes

The structure of the Security Control classes was inspired by the security dimensions found in ITU X.805 [43]. Several of the X.805 security dimensions were adopted, some with minor modifications, and then complemented with a few new Security Control classes relevant for 5G networks. The exact functions and mechanisms to enforce a specific security control are left for consideration in the detailed design phase. The different security control classes are listed below:

i. Identity & Access Management: A collection of security functions and mechanisms addressing access control (authorization), management of credentials and roles, etc.

ii. Authentication: A collection of security functions and mechanisms serving to verify the validity of an attribute, e.g. a claimed identity.

iii. Non-repudiation: A collection of security functions and mechanisms serving to protect against false denial of involvement in a specific action.

iv. Confidentiality: A collection of security functions and mechanisms protecting data against unauthorized disclosure.

v. Integrity: A collection of security functions and mechanisms protecting data against unauthorized creation or modification.

vi. Availability: A collection of security functions and mechanisms serving to ensure availability of resources, even in the presence of attacks. Disaster recovery solutions are included in this category.

vii. Privacy: A collection of security functions and mechanisms serving to the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact and share it personal information with its environment.

viii. Audit: A collection of security functions and mechanisms providing review and examination of a system's records and activities to determine the adequacy of system controls and detect breaches in system security services and controls. The necessary data collection to enable audit (e.g. logging) is also included.

ix. Trust & Assurance: A collection of security functions and mechanisms serving to convey information about the trustworthiness of a system. For a trusted party such information constitutes a claim that may or may not persuade them to trust the system, while a trustee would see such information as evidence of the security level achieved.

x. Compliance: A collection of security functions and mechanisms provided to allow an entity or system to fulfil contractual or legal obligations.

4) Security Realms

The domains and slices in the security architecture provide boundaries between different network functions and services and the strata provide information on required security needs for domain interaction and communication. A joint analysis of domains and strata will thus enable identification of required security control points for groups of protocols.

i. The Access Network (AN) SR captures security needs of the access Network domain and access stratum as part of the transport stratum - in particular, aspects related to users securely accessing 5G services over 3GPP (5G radio) and certain non-3GPP (e.g. WLAN) access technologies.

ii. The Application (App) SR captures security needs of the application stratum. That is, end-user applications/services provided over the 5G network, either as operator provided services (from HN or SN Domain), or provided from External Network Domains (3P or IPS Domain with associated IP domains). Note that when the service is hosted by an External Network Domain, the services may not always be fully trusted by 5G network operators. Examples of applications/services include: VoIP, VoLTE, V2X, ProSe, HTTP-based services.

iii. The Management (Mgmt) SR captures security needs of the Management Stratum and Management Domains, including secure management (secure upgrades, secure orchestration, etc.) and management of security (monitoring, key and access management, etc.). Thus, Management Security is either a concern related to communication between a Management Domain and some other (semi-)trusted Domain, or, related to security of the Management Domain itself.

iv. The User Equipment (UE) SR captures security needs of the user equipment (UE) domain comprising the ME, MEHW, UICC, USIM, and IM domains and other UE domains, e.g. visibility and configurability and security aspects related to communication between these domains.

v. The Network SR captures security needs of communication in core network domains and between the core network domains and external network domains - including aspects related to securely exchanging signalling and user data between nodes in the operator and external network domain.

vi. The Infrastructure and virtualisation (I&V) SR captures security needs of IP Domains, e.g. for attestation, secure slicing/isolation, and trust issues between tenant domains and between tenant domains and infrastructure domains.

The defined security control classes provide a structured way to prevent or answer to a risk identified regarding specific data, functions and services in a network. The defined security realms capture needs of one or more strata or domains and are there to group different network aspects with different but area specific security concerns. Bringing these two concepts together by analysing which security controls are required in each security realm will provide a detailed and structured view of the required security mechanisms to ensure that the security requirements are fulfilled. The security realms should be subdivided with respect to functionality, domains, strata and end-points of protocols and for each such subdivision a security control mechanism should be selected. In this way, it is possible to get a detailed overview of the security mechanisms needed in a 5G network.

Annex 12 – Additional security aspects

1) GDPR regulation overview

GDPR has 99 articles, grouped in 11 chapters. Each chapter is focussed to different important parts of the law, as summarized below.

- **Art.1-4: General provisions**
  - Definition of the main actors in this law: Dad subject, Controller and Processor.
- **Art 5-11: Principles**
  - Principles, purpose limitation, data subject consent and how to be managed by controllers.
- **Art 12-23: Rights of the data subject**
  - List the rights that the data subject has in order to control its personal data, and how controllers have to inform them when the data is collected, allow them to access/manage/update/delete the data, set restrictions on the processing, etc…
- **Art 24-43: Controller and Processor**
  - Data protection by design and by default is supposed to be performed by controllers, and other obligations like recording all the processing activity and specifying which mechanisms are being used to protect personal data (pseudonymisation and encryption). In case of data breach, if there is a high risk to the rights and freedoms of natural persons, the controller has to notify it to the supervisory authority within 72 hours after having become aware of it.
- **Art 44-50: Transfer of personal data to third countries or international organisations**
  - This chapter is especially interesting regarding x-border vehicular scenarios where a vehicle is going to pass from one country to another and one of them does not belong to the EU. Transfer of personal data

to a third country or an international organization is only allowed if compliant to some conditions like that the third country has an adequate level of data protection.

- **Art 51-59: Independent supervisory authorities**
  - This chapter describes the roles and minimum structure of the supervisory authorities in the individual member states.
- **Art 60-76: Cooperation and consistency**
  - In order to facilitate the adoption of this normative, the "European Data Protection board" will monitor and ensure the consistent application of the law issuing guidelines, recommendations and best practices. Also cooperates with the different supervisory authorities.
- **Art 77-84: Remedies, liability and penalties**
  - This chapter defines how data subject complaint with a supervisory authority and how to compensate them. Also, it is defined penalties that could reach 4 million euros or the 4% of the annual turnover of the preceding financial year of the denounced company. Those penalties are very serious and should be into consideration by 5G operators.
- **Art 85-91: Provisions relation to specific processing situations**
  - This chapter is focused in processing of personal data in special and delicate situations like employment context.
- **Art. 92-93: Delegated acts and implementing acts**
  - In this chapter it is defined what power the Commission gets with respect to the GDPR.
- **Art 94-99: Final provisions**
  - Here it is established the applicable date of the law (May 25, 2018) and how to replace 95/94/EC.

2) Requirements templates 5G-MOBIX per use case category

Specific security solutions for Advanced Driving

Advanced Driving		Requirements priority with complementary information								
		Requirement ID	ES-PT	GR-TR	DE	FI	FR	NL	CN	KR
Generic	Automation	Sec-auto								
	Monitoring	Sec-mon								
	Management	Sec-mgn								
3GPP networks	4G-LTE									
	5G-NA	.								
C-V2X										
ETSI MEC										
Slicing	Isolation	Slice-isolation								
	liability	5G-liability								
	Schemes	Liability-scheme								

Data Protection & Privacy		Sec-Privacy								
		Sec-Regulation								
		Sec-Encryption								
		Sec-Privacy-3GPP-PC5-law								
		Sec-Privacy-3GPP-PC5-pseudonymity								
		Sec-Privacy-3GPP-PC5-transparency								
		Sec-Privacy-3GPP-PC5-legitimity								

Specific security solutions for Vehicles Platooning

Vehicles Platooning		**Requirements priority with complementary information**								
		Requirement ID	ES-PT	GR-TR	DE	FI	FR	NL	CN	KR
Generic	Automation	Sec-auto								
	Monitoring	Sec-mon								
	Management	Sec-mgn								
3GPP networks	4G-LTE									
	5G-NA	.								
C-V2X										
ETSI MEC										
Slicing	Isolation	Slice-isolation								
	liability	5G-liability								
	Schemes	Liability-schem								
Data Protection & Privacy		Sec-Privacy								
		Sec-Regulation								
		Sec-Encryption								
		Sec-Privacy-3GPP-PC5-law								
		Sec-Privacy-3GPP-PC5-pseudonymity								
		Sec-Privacy-3GPP-PC5-transparency								
		Sec-Privacy-3GPP-PC5-legitimity								

Specific security solutions for Extended Sensors

Extended Sensors		Requirements priority with complementary information								
		Requirement ID	ES-PT	GR-TR	DE	FI	FR	NL	CN	KR
Generic	Automation	Sec-auto								
	Monitoring	Sec-mon								
	Management	Sec-mgn								
3GPP networks	4G-LTE									
	5G-NA	.								
C-V2X										
ETSI MEC										
Slicing	Isolation	Slice-isolation								
	liability	5G-liability								
	Schemes	Liability-scheme								
Data Protection & Privacy		Sec-Privacy								
		Sec-Regulation								
		Sec-Encryption								
		Sec-Privacy-3GPP-PC5-law								
		Sec-Privacy-3GPP-PC5-pseudonymity								
		Sec-Privacy-3GPP-PC5-transparency								
		Sec-Privacy-3GPP-PC5-legitimity								

Specific security solutions for Remote Driving

Remote Driving		Requirements priority with complementary information								
		Requirement ID	ES-PT	GR-TR	DE	FI	FR	NL	CN	KR
Generic	Automation	Sec-auto								
	Monitoring	Sec-mon								
	Management	Sec-mgn								
3GPP networks	4G-LTE									
	5G-NA	.								
C-V2X										
ETSI MEC										
Slicing	Isolation	Slice-isolation								
	liability	5G-liability								

	Schemes	Liability-scheme								
Data Protection & Privacy		Sec-Privacy								
		Sec-Regulation								
		Sec-Encryption								
		Sec-Privacy-3GPP-PC5-law								
		Sec-Privacy-3GPP-PC5-pseudonymity								
		Sec-Privacy-3GPP-PC5-transparency								
		Sec-Privacy-3GPP-PC5-legitimity								

Specific security solutions for QoS Support

QoS Support		**Requirements priority with complementary information**								
		Requirement ID	ES-PT	GR-TR	DE	FI	FR	NL	CN	KR
Generic	Automation	Sec-auto								
	Monitoring	Sec-mon								
	Management	Sec-mgn								
3GPP networks	4G-LTE									
	5G-NA	.								
C-V2X										
ETSI MEC										
Slicing	Isolation	Slice-isolation								
	liability	5G-liability								
	Schemes	Liability-scheme								
Data Protection & Privacy		Sec-Privacy								
		Sec-Regulation								
		Sec-Encryption								
		Sec-Privacy-3GPP-PC5-law								
		Sec-Privacy-3GPP-PC5-pseudonymity								
		Sec-Privacy-3GPP-PC5-transparency								
		Sec-Privacy-3GPP-PC5-legitimity								