5GMOBIX

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

D2.3

Specification of roadside and cloud infrastructure and applications to support CCAM

Dissemination level	Public (PU)
Work package	WP2: Specifications
Deliverable number	D2.3
Version	V2.0
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]

www.5g-mobix.com

Editors

Editors in alphabetical order		
Name	Organisation	Email
Marcel van Sambeek	TNO	marcel.vansambeek@tno.nl

Authors

Authors in alphabetical order		
Name	Organisation	Email
ES-PT		
João Almeida	IT	jmpa@ua.pt
Joaquim Ferreira	IT	jjcf@ua.pt
Antonio Serrador	ISEL	aserrador@deetc.isel.ipl.pt
Nuno Cota	ISEL	ncota@deetc.isel.ipl.pt
Nuno Cruz	ISEL	ncruz@deetc.isel.ipl.pt
Grazielle Teixeira	ISEL	gteixeira@deetc.isel.ipl.pt
Nuno Datia	ISEL	datia@deetc.isel.ipl.pt
Diego Bernárdez	CTAG	diego.bernardez@ctag.com
Carlos Rosales	CTAG	carlos.rosales@ctag.com
Diana Blanco	CTAG	diana.blanco@ctag.com
Daniel Jáuregui	CTAG	2jibri.jauregui@ctag.com
João Moutinho	CCG	joao.moutinho@ccg.pt
João Peixoto	CCG	joao.peixoto@ccg.pt
Fernando Correia	NOKIA-PT	2jibrill.correia@nokia.com
Mateus Mazzeo	NOKIA-PT	mateus.mazzeo@nokia.com
José Santa Lozano	UMU	josesanta@um.es
Pedro J. Fernández Ruiz	UMU	pedroj@um.es
Antonio F. Skarmeta Gómez	UMU	skarmeta@um.es
Jorge Gallego Madrid	UMU	jorgegm@um.es
GR-TR		
Kostas Tsoumanis	WINGS	ktsoumanis@wings-ict-solutions.eu
Eleni Giannopoulou	WINGS	nellygiannopoulou@wings-ict-solutions.eu
Ioannis Tzanetis	WINGS	gtzanettis@wings-ict-solutions.eu
Aspasia Skalidi	WINGS	askalidi@wings-ict-solutions.eu
Stefania Stavropoulou	WINGS	sstavropoulou@wings-ict-solutions.eu
Nazlı Güney	TURKCELL	nazli.guney@turkcell.com.tr
Tahir Sarı	FORD	tsari1@ford.com.tr
DE		
Manzoor Khan	TUB	manzoor-ahmed.khan@dai-labor.de
Xuan-Thuy Dang	TUB	xuan-thuy.dang@dai-labor.de

Tobias Dörsh	TUB	tobias.doersch@dai-labor.de
FI		
Edward Mutafungwa	AALTO	edward.mutafungwa@aalto.fi
Jose Costa Requena	AALTO	jose.costa@aalto.fi
Oussama El Marai	AALTO	3jibril.elmarai@aalto.fi
Tapio Taipalus	S4	tapio.taipalus@sensible4.fi
Jussi Suomela	S4	jussi.suomela@sensible4.fi
FR		
Ahmed Soua	VEDECOM	ahmed.soua@vedecom.fr
Oyunchimeg Shagdar	VEDECOM	oyunchimeg.shagdar@vedecom.fr
NL		
Chetan Belagal Math	SISSBV	chetan.belagal_math.ext@siemens.com
Igor Passchier	SISSBV	igor.passchier@siemens.com
Emi Matthews	TNO	emi.mathews@tno.nl
Marcel van Sambeek	TNO	marcel.vansambeek@tno.nl
Jos den Ouden	TUE	j.h.v.d.ouden@tue.nl
Aki Lumiaho	VTT	aki.lumiaho@vtt.fi
CN		
Yanjun Shi	DUT	syj@ieee.org
Zihui Zhang	SDIA	zhangzh@sdas.org
Qiangmei Han	DUT	hqmdut@163.com
KR		
You-Jun Choi	KATECH	ychoi@katech.re.kr
Heesang Chung	ETRI	hschung@etri.re.kr
Cybersecurity & Data privacy		
Djibrilla Amadou Kountche	AKKA	djjibrilla.amadou-kountche@akka.eu
Marwane EL-Bekri	AKKA	marwane.el-bekri@akka.eu

Control sheet

Version history			
Version	**Date**	**Modified by**	**Summary of changes**
0.1	14/03/2019	Marcel van Sambeek (TNO)	Final Table of Contents
0.8	27/05/2019	All authors – Trial sites	Initial draft for internal approval
0.9	03/06/2019	All authors – Trial sites	Final draft for review 1
1.0	15/07/2019	All authors – Trial sites Marcel van Sambeek	Version 1; update based on review
1.01	25/07/2019	Marcel van Sambeek (TNO)	Update Table of Contents
1.1	04/10/2019	All authors – Trial sites Marcel van Sambeek	Final draft for review 2
2.0	31/10/2019	All authors – Trial sites Marcel van Sambeek Sébastien Faye (LIST)	Final version 2; update based on review; quality check

Peer review		
	Reviewer name	**Date**
Reviewer 1	Gorka Vélez (VICOM)	21/10/2019
Reviewer 2	Ángel Martín (VICOM)	21/10/2019
Reviewer 3	Manzoor-Ahmed Khan (TUB)	24/10/2019
Reviewer 4	José Manuel Carreira Miguel (INFRAPT)	22/10/2019

Legal disclaimer

Table of contents

List of figures

List of tables

ABBREVIATIONS

Abbreviation	Definition
3GPP	3rd Generation Partnership Project
5G NR	5G New Radio
AD	Autonomous/Automated Driving
AGV	Automatically Guided Vehicles
AI	Application Interface
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
AU	Application Unit
AV	Autonomous Vehicles
BCP	Border Crossing Point
BS	Base Station
BSM	Basic Safety Message
BTP	Basic Transport Protocol
C2C	Cloud to Cloud
C2N	Cloud to Network
CACC	Cooperative Adaptive Cruise Control
CAM	Cooperative Awareness Message
CBC	Cross-Border Corridor
CC	Component Carriers
CCAM	Cooperative, Connected and Automated Mobility
CEN	European Committee for Standardization (French: Comité Européen de Normalisation)
CIM	Cooperative Intention Message
C-ITS	Cooperative Intelligent Transport Systems
CMR	Compact Measurement Record

CN	China
CoCA	Cooperative Collision Avoidance
CPM	Collective Perception Message
CPS	Collective Perception Service
CPU	Central Processing Unit
CU	Communication Unit
C-V2X	Cellular-V2X
D2D	Device to Device
DASH	Dynamic Adaptive Streaming over HTTP
DATEX-II	Data Exchange
DB	Database
DE	Germany
DENM	Decentralized Environmental Notification Message
DGPS	Differential GPS
DSRC	Dedicated Short-Range Communications
DT	Desired Trajectory
EC	European Commission
EDM	Edge Dynamic Map
eMBB	enhanced Mobile Broadband
eRSU	Extended Roadside Unit
ES	Spain
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Ego Vehicle / Electronic Vehicle
FCD	Floating Car Data
FI	Finland
FPS	Frames per Second
FR	France
GDM	Global Dynamic Map

gNB	5G base station
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GR	Greece
HD	High Definition
I2V	Infrastructure-to-Vehicle
IF	Interface
ITS	Intelligent Transport Systems
ITS-G5	Intelligent Transport Systems-G5 (in frequency band G5)
IVI	In-Vehicle Information
k-NN	k-Nearest Neighbour
KPI	Key Performance Indicator
KR	South-Korea
LDM	Local Dynamic Map
LEDDAR	Light-Emitting Diode Detection And Ranging
LIDAR	Light Detection And Ranging
LOS	Line-Of-Sight
LTE	Long Term Evolution
MANO	Management and Orchestration
MCM	Manoeuvre Coordination Message
MCS	Manoeuvre Coordination Service
MEC	Multi-access / Mobile Edge Computing
MIMO	Multiple-Input and Multiple-Output
M-JPEG	Motion-Joint Photographic Experts Group
MNO	Mobile Network Operator
MPEG	Moving Picture Experts Group
MQTT	Message Queuing Telemetry Transport
NI	Network Interface
NL	Netherlands

OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OV	Other Vehicle
PCM	Platoon Coordination Message
PCU	Platoon Control Unit
PLMN	Public Landline Mobile Network
PRB	Physical Resource Blocks
PT	Portugal
PT	Planned Trajectory
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality-of-Service
R2N	Roadside to Network
R2V	Roadside to Vehicle
RF	Radio Frequency
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services
RTK	Real-Time Kinematic
SAE	Society of Automotive Engineers
SD-WAN	Software Defined Wide Area Network
SIM	Subscriber Identity Module
SOMs	Self-Organising Maps
SPAT	Signal Phase And Time
SRM	Service Request Message
ToF	Time-of-Flight
TPEG	Transport Protocol Experts Group
TR	Turkey
TR	Technical Report
TS	Technical Specification

Tx	Transmission
UC	User story
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communication
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Person
V2R	Vehicle to Roadside
V2V	Vehicle to Vehicle
V2X	Vehicle to X, X = V (Vehicle), I (Infrastructure), N (Network), C (Cloud), P (Person)
VE	Virtual Entities
vEPC	Virtual Evolved Packet Core
VMS	Variable Message Signs
VPN	Virtual Private Network
VRU	Vulnerable Road User

EXECUTIVE SUMMARY

5G-MOBIX aims to showcase the added value of 5G technology for advanced Cooperative, Connected and Automated Mobility (CCAM) use case categories and validate the viability of the technology to bring automated driving to the next level of vehicle automation (SAE Level 4 (L4) and above). 5G-MOBIX will execute CCAM trials along two cross-border corridors (CBC) between Spain and Portugal and between Greece and Turkey, and four trial sites (TS) in Versailles (France), Berlin/Stuttgart (Germany), Eindhoven-Helmond (Netherlands) and Espoo (Finland) using 5G technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context. Besides the European sites, 5G-MOBIX works in close cooperation with sites in China and South-Korea. The project will also define deployment scenarios (D3.7) and identify and respond to standardisation and spectrum gaps (D6.4).

The present document 5G-MOBIX D2.3 "Specification of roadside and cloud infrastructure and applications to support CCAM" is delivered as part of WP2 and defines the roadside and cloud infrastructure to support the 5G-MOBIX use case categories and related user stories. The purpose of this deliverable is to describe the roadside and cloud infrastructure to support the CCAM use case categories as defined in D2.1. The roadside infrastructure includes e.g. sensor (e.g. video-surveillance or vehicle detection systems) and actuator systems (e.g. traffic light and variable message signs) along the physical road infrastructure. The cloud or central infrastructure includes e.g. (distributed) server or back-office systems for information exchange (collection, filtering, analyses and distribution) to support the CCAM use case categories. The document serves as a reference for design, development, deployment and test of the 5G-MOBIX use case categories. The 5G network infrastructure is specified in D2.2 and the specifications for AD vehicles are defined in D2.4. The outline of the document is:

- **Section 1** gives the **introduction** on 5G-MOBIX and the scope of this deliverable.
- **Section 2 - Reference description of roadside and cloud infrastructure** includes a reference architecture that is used to describe and align the deployment architectures of roadside and cloud systems on the 2 CBC sites and the TS. This approach was chosen to align the specifications of the CBC sites and TS on both functional systems - attached to physical systems in vehicle, roadside or cloud- and the information exchanged between AD vehicles and roadside / cloud systems. The section also includes description of cross-border application issues for the CCAM user stories.
- **Section 3 - Deployment descriptions of the roadside and cloud infrastructure per use case category**: the description of roadside and cloud infrastructure is given for each of the 5 use case categories: i) Advanced Driving, ii) Remote Driving, iii) Vehicles Platooning, iv) Extended Sensors and v) Vehicle QoS Support. The Cross-Border Corridor solution of ES-PT or GR-TR is included, together with descriptions of additional specific solutions to be developed in one of the TSs.
- **Section 4 - Cyber-security & data privacy aspects**: describes the security and privacy framework to support CCAM, with the corresponding requirements.
- **Section 5** presents the **Evaluation scenarios** specific for a TS to support the CBC sites.
- **Section 6** includes the **Conclusions**.

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 case categories and validate the viability of the technology to bring automated driving to the next level of vehicle automation (SAE L4 and above). To do this, 5G-MOBIX will demonstrate the potential of different 5G features on real European roads and highways and create and use sustainable business models to develop 5G corridors. 5G-MOBIX will upgrade existing key assets (network infrastructure, roadside and cloud infrastructure and vehicles) to realise improved performance of involved systems. 5G-MOBIX will then utilize and operate co-existence of 5G technologies within a heterogeneous environment comprised of multiple incumbent short-range communication technologies such as ITS-G5 and LTE-V2X and existing LTE networks.

5G-MOBIX will execute CCAM trials along cross-border corridors and trial sites using 5G technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context (D5.2 - D5.4). The project will also define deployment scenarios (D3.4 for roadside and cloud).

5G-MOBIX will first define critical scenarios needing advanced connectivity provided by 5G, and the required features to enable the selected CCAM use case categories. The matching of these CCAM use case categories and the expected benefits of 5G will be tested during trials on 5G corridors in different EU countries as well as in Turkey, China and South-Korea.

The trials will also allow 5G-MOBIX to conduct evaluations and impact assessments and to define business impacts and cost/benefit analysis (D5.3). As a result of these evaluations and international consultations with the public and industry stakeholders, 5G-MOBIX will identify new business opportunities for the 5G-enabled CCAM user stories and propose recommendations and options for its deployment (D6.3).

Through its findings on technical requirements and operational conditions 5G-MOBIX is expected to actively contribute to standardisation and spectrum allocation activities (D6.4) including the definition of deployment options for 5G technologies for CCAM (D6.2).

1.2. Purpose of the deliverable

The present document D2.3 “Specification of roadside and cloud infrastructure and applications to support CCAM” is delivered as part of WP2 and defines the roadside and cloud infrastructure to support the 5G-MOBIX user stories. The purpose of this deliverable is to specify the roadside and cloud infrastructure to support the CCAM use case categories as defined in D2.1. The roadside infrastructure includes e.g. video-surveillance or vehicle detection systems (sensor systems) and traffic light and variable message signs (actuator systems) along the physical road infrastructure. The cloud or central infrastructure includes (distributed) server or back-office systems for information exchange (collection, filtering, analyses and distribution) to support the CCAM use case categories. The document serves as a reference for design, development, deployment and test of the 5G-MOBIX use case categories. Figure 1 shows the scope of the specifications for tasks T2.2 – T2.4, related to the CCAM architecture with 5G network (T2.2), roadside and cloud infrastructure (T2.3) and AD vehicles (T2.4).

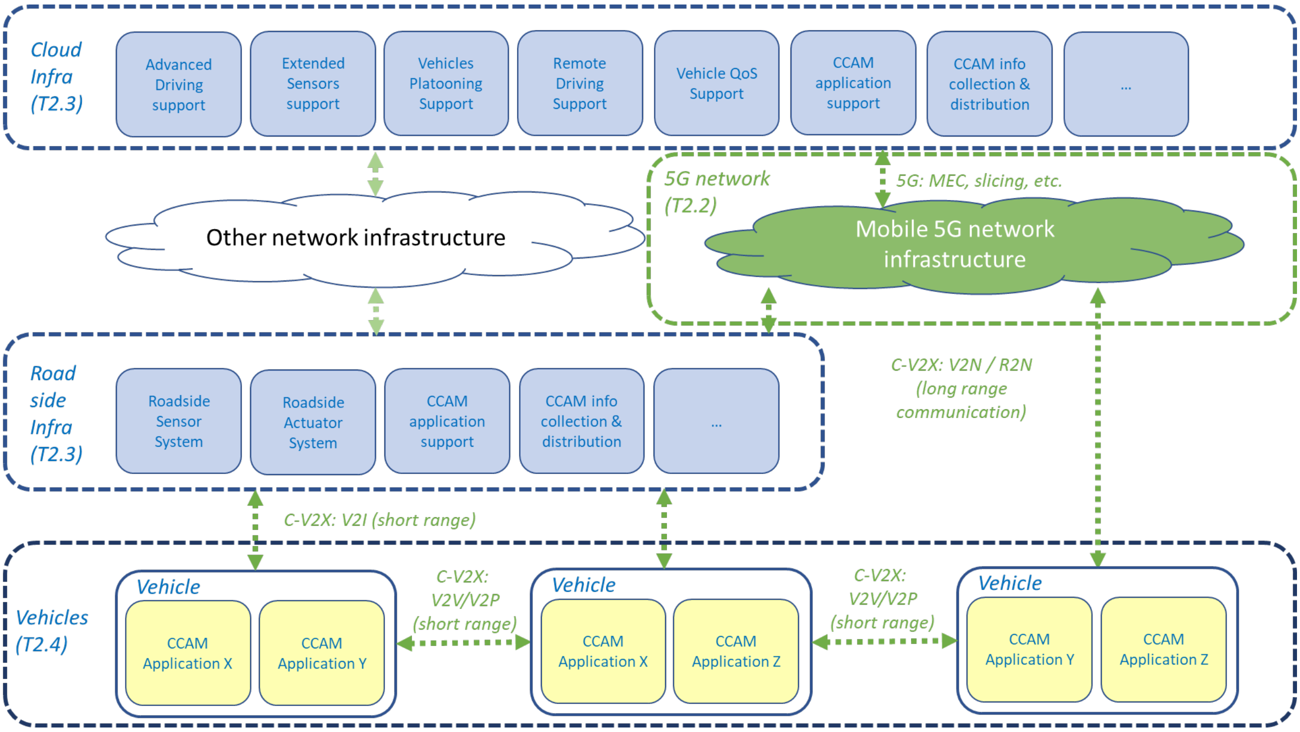


Figure 1 Overview of CCAM architecture of 5G-MOBIX and the WP2 tasks

The present deliverable is related to other deliverables in Work Package 2 (WP2):

1. D2.1 "5G-enabled CCAM use case categories specifications". This deliverable defines the 5G-MOBIX use case categories, describes the trial sites and proposes an initial set of Key Performance Indicators (KPIs). The overall purpose of the document is to serve as a reference to design, development, deployment and test of the 5G-MOBIX use case categories. The user story description with the related sequence diagrams of the information flows in time between vehicle(s), roadside and cloud-based systems are used to define the overall architecture and the interfaces for information exchange.

2. D2.2 "5G architecture and technologies for CCAM specifications". This deliverable describes the reference 5G architecture and the dedicated 5G technologies relating to the deployment of advanced CCAM user story. A reference to the interface specifications of the 5G network towards roadside and cloud-based systems is given in D2.3.

3. D2.4 "5G augmented vehicle specifications". This deliverable provides the detailed specification of vehicle enhancement using enhanced 5G connectivity for implementing the advanced CCAM use case categories.

4. D2.5 "Initial evaluation KPIs and metrics". This deliverable presents the initial KPIs and relevant metrics to be used for the evaluation, including those resulting from the specification activities.

5. D2.6 "Final set of 5G/CCAM systems and vehicle specifications". The final set of 5G/CCAM systems and vehicle specifications at M30 will collect all the final agreed specifications.

The deliverable D2.3 will be the starting point for the 5G-MOBIX activities in T3.4 on Corridor infrastructure development and integration.

1.3. Intended audience

The dissemination level of D2.3 is public (PU) and is meant primarily for (a) all members of the 5G-MOBIX project consortium, and (b) the European Commission (EC) services.

This document is intended to serve as an internal guideline and reference for all 5G-MOBIX beneficiaries, especially the trial site leaders in development, integration and roll-out.

Beyond 5G-MOBIX partners, this deliverable should guide other stakeholders to envision the required roadside and cloud infrastructures to realise a specific CCAM application. We make this deliverable public because it has an interest for CCAM and 5G research beyond the 5G-MOBIX sphere

2. REFERENCE DESCRIPTION OF ROADSIDE AND CLOUD INFRASTRUCTURE

2.1. Introduction

In this section a reference architecture of the roadside and cloud infrastructure is given to support the use case categories of 5G-MOBIX: architecture, physical and logical elements, interfaces and underlying 5G technologies. A high-level "reference" architecture is defined to align the use case categories descriptions and their sequence diagrams. The architecture is part of the specification, together with the (detailed) specifications for roadside and cloud systems and their interfaces to the 5G networks and to connected and automated vehicles. This reference architecture is used by the 5G-MOBIX partners to describe the deployment architecture of each CCAM user story in the 5G-MOBIX corridor and local trial sites in Section 3.

In section 2.2 the Use Case Categories (UCC) with the 5G-MOBIX User Stories (US) are described. The reference architecture is described in section 2.3 and the section 2.4 and 2.5 include descriptions of the specifications on network interfaces, and application interfaces, respectively. Cross-border corridor issues related to the Applications (network and service continuity) are described in section 2.6.

2.2. Overview 5G-MOBIX use case categories

During the proposal stage, the 5G-MOBIX consortium defined five use case categories pivoting around some critical manoeuvres and autonomous driving enablers. Once the project started and during task 2.1 discussions, it was concluded that it was necessary to redefine these use case categories to classify user stories. This classification enables the presentation of user stories under a common umbrella and facilitates the demonstration of their complementarity and alignment. This classification is based on use case categories in 3GPP TS 22.186 V16.1.0 (2018-12). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancement of 3GPP support for V2X scenarios; Stage 1 (Release 16).

The user stories of 5G-MOBIX are assigned to one of the five use case categories to align the specifications of the user stories of CBC and TS. Some user stories cover different scenario's and are split between different use case categories.

Table 1 Overview of 5G-MOBIX User Stories per Use Case Category and trial site

Trial site	Advanced Driving	Vehicles Platooning	Extended Sensors	Remote Driving	Vehicle QoS Support
ES-PT	Complex manoeuvres in cross-border settings (US1)			Automated shuttle remote driving across borders (US3)	Public transport with HD media services and video surveillance (US2)
GR-TK		Platooning with "see what I see" functionality in cross-border settings (US4)	Extended sensors for assisted border-crossing (US5)		
DE		eRSU-assisted platooning (US6)	EDM-enabled extended sensors with surround view generation (US7)		
FI			Extended sensors with redundant Edge processing (US8)	Remote driving in a redundant network environment (US9)	
FR	Infrastructure-assisted advanced driving (US10)				QoS adaptation for Security Check in hybrid V2X environment (US11)
NL	Cooperative Collision Avoidance (US12)		Extended sensors with CPM messages (US14)	Remote driving using 5G positioning (US13)	
CN	Cloud-assisted advanced driving (US15)	Cloud-assisted platooning (US16)		Remote driving with data ownership focus (US19)	
KR				Remote driving using mmWave communication (US18)	Tethering via Vehicle using mmWave communication (US17)

2.3. High-level reference architecture for 5G-MOBIX

In Figure 2 the high-level architecture is shown with the roadside, cloud and network infrastructure to support the 5G-MOBIX use case categories for AD vehicles.

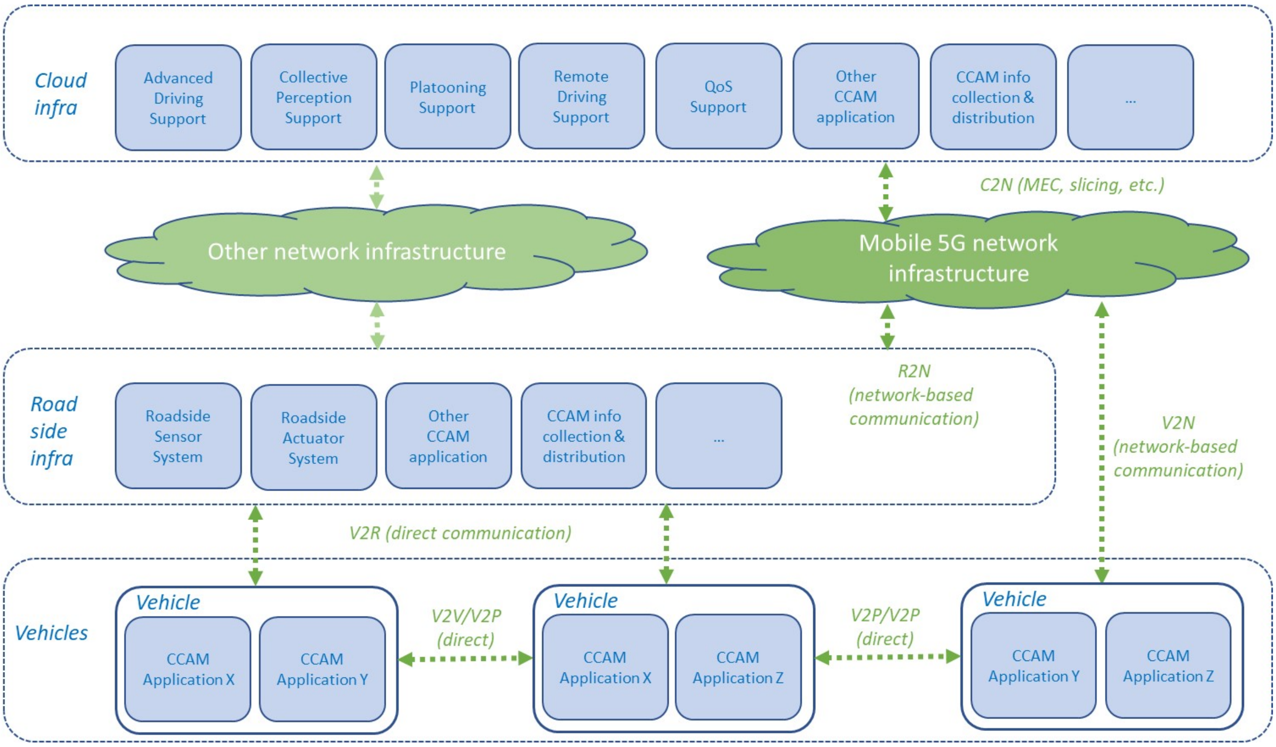


Figure 2 High-level CCAM reference architecture with network, roadside and cloud infrastructure

The high-level architecture combines different "views" of an architecture:

A. **Infrastructure view**: in Figure 2 three CCAM layers are shown: cloud infrastructure, roadside infrastructure and vehicles. Roadside systems are e.g. traffic lights and variable message signs along the road connected to (central or local) control systems and/or connected to local road sensors.

B. **Functional view**: the functional elements are shown (blue boxes) in the three different layers:
- Vehicle layer: vehicles are equipped with on-board sensors (HD camera, radar, lidar, etc.) to monitor the environment within the field-of-view and sensors from the vehicle (status, etc.), and a CCAM application / control systems and actuators to control the steering and braking functions of the vehicle. These systems are described in detail in D2.4. The architecture only shows the **CCAM application X/Y/Z**, which exchange information to support the 5G-MOBIX use case categories. Information is exchanged with roadside systems (via direct communication) or with central cloud systems via 5G networks. Vehicles have On-board Units (OBU) which contain an Application Unit (AU) to support the CCAM application and a Communication Unit (CU);

- Roadside layer: roadside systems are physical systems along a road equipped with functional elements such as a **Roadside Sensor Systems** (HD camera, radar, lidar, road condition sensors) to monitor the road infrastructure. The roadside system also includes **Roadside Actuator Systems** for dynamic traffic control such as Variable Message Signs (VMS, with traffic signs or text) or traffic lights. The roadside systems have on-board communication modules to exchange information to either (edge) cloud systems or to vehicles directly. A Roadside Unit (RSU) may contain an Application Unit (AU) to support the roadside-based **CCAM Application** and has a Communication Unit (CU) to connect to (edge) cloud system or directly to vehicles. The RSU may host the backends of the on-road deployed sensors. In cases, where the backends are hosted in the cloud, the RSU may act as relay between on-road sensors and backends in the cloud. The RSU can also work as a relay node for the **CCAM Info Collection & Distribution** function to forward messages from (edge) cloud systems to vehicles via roadside to vehicle (R2V) communication and vice versa forward messages from vehicles to cloud systems (V2R).
- Cloud layer: systems in the cloud layer are functional elements deployed as software on dedicated servers in data centres and are referred to as cloud systems in case the software is installed on virtual systems via X-as-as-Service platforms with CPU processors, GPU acceleration, data storage and query, and connectivity. The functional elements in this layer are software systems to support AD vehicles on **Advanced Driving**, **Vehicles Platooning**, **Remote Driving**, **Extended Sensors** or **Vehicle QoS**. The central layer may also include a **CCAM Info Collection & Distribution** function to collect and forward messages between vehicles, roadside and other cloud systems.

C. **Communication view**: this view is represented by the green arrows in Figure 2 to support direct communication (short range) or network-based communications via the 5G mobile network infrastructure (long range), as described in detail in D2.2. Other (fixed) network infrastructure to interconnect roadside and cloud systems is also possible, but not in scope of the 5G-MOBIX project.

Other views like an organisational view showing the stakeholders or organizations (mobile network operator, cloud platform provider, car manufacturer, CCAM service provider, (public) road operator, government) connected to the infrastructure or functional assets as described in the architecture and their roles (owner, maintenance, support) are not shown, D6.3 will cover 5G enabled business models for automated mobility. Furthermore, external (human) actors (like end-user, driver, car owner, other road users, remote driver etc.) that interact with the CCAM infrastructure and AD vehicles are not shown, D5.4 will report on user acceptance.

The sequence diagram is related to the reference architecture. The functional elements in the sequence diagram are part of one of the infrastructure layers in the reference architecture, and the information flow is supported via the network and application interfaces in the communication view.

2.4. Specifications on communication interfaces towards 5G network

In Figure 3 the Network Interfaces (NI) are shown to connect vehicles, roadside systems and cloud systems to 5G networks: the interfaces are **NI V2V**, **NI V2R**, **NI V2N**, **NI R2N** and **NI C2N** (V=Vehicle, R=Roadside, C=Cloud, N=Network).

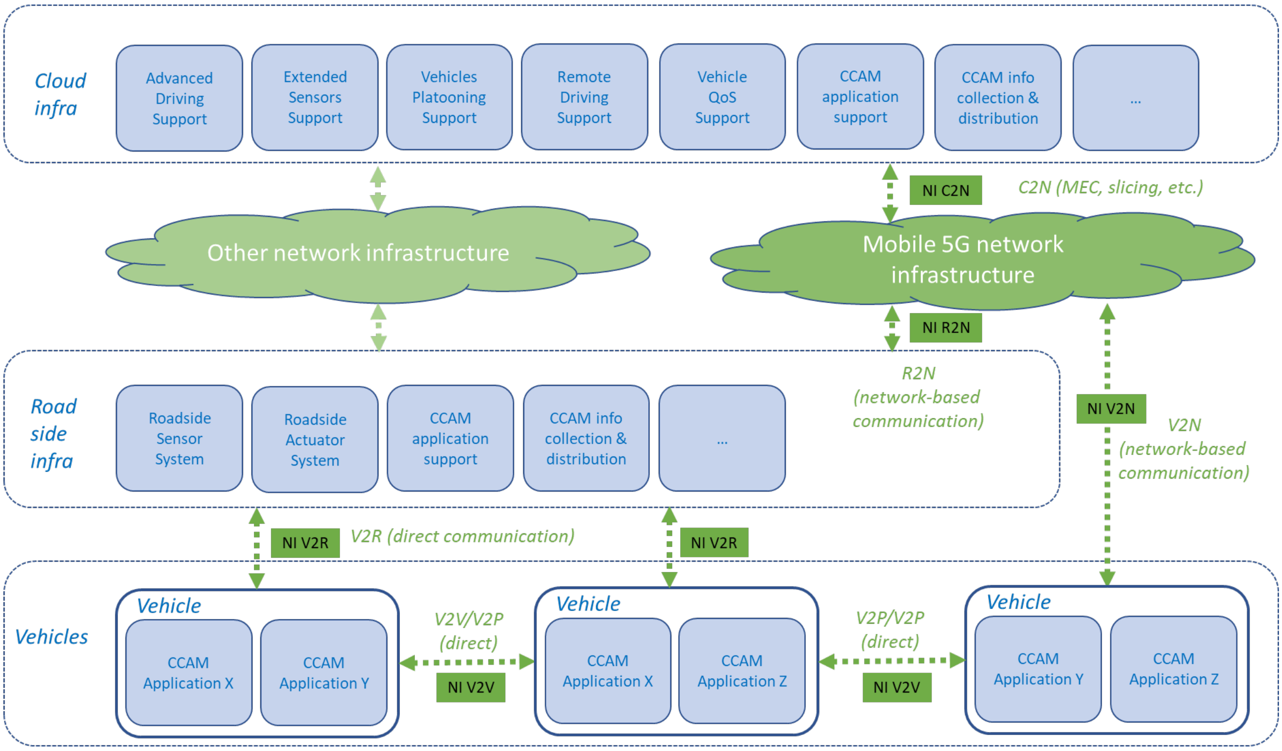


Figure 3 Network Interfaces in CCAM reference architecture

2.4.1. Network Interface NI V2R and NI V2V

The Network Interface Vehicle-to-Roadside (NI V2R) is based on direct communication (or short-range communication) between vehicle and roadside. This interface is similar for Vehicle-to-Vehicle (V2V) (vehicles with On-Board Units, OBUs) and between vehicle and roadside units, RSU (V2R with R = RSU).

The 3GPP specifications for this interface are described in section 2.1. of D2.2 for LTE-V2X (Release 14) and 5G NR-V2X (Release 15-16). This interface is named PC5 sidelink in 3GPP specifications.

Other specifications on direct communication are based on ETSI ITS-G5 and are specified in Annex II of Delegated Regulation - C(2019)1789 - for C-ITS on March 13, 2019[1]. The ETSI ITS specifications support the use of ITS-G5 and LTE-V2X as underlying communication technologies. However, at the moment LTE-V2X does not comply to regulation for radio equipment in the 5,9 GHz band. ETSI is asked to investigate solutions to support this.

[1] https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf

A roadside system may be a stand-alone system equipped with application unit (sensor, actuator, processor and CCAM application) and a communication module that supports direct communication via 5G NR-V2X (via PC5 sidelink).

2.4.2. Network Interface NI R2N and NI V2N

The Network Interface Roadside-to-Network (NI R2N) is based on network-based communication via 5G networks (Uu interface in 3GPP terminology) between C-V2X communication modules and the gNB and are used to support connectivity from vehicles towards roadside and cloud / edge systems. The specifications of this interface are described in section 2.2 of D2.2 for 5G NR (Release 15-16). This interface is named the Uu-interface in 3GPP specifications and architecture. This interface is equivalent to the Network Interface Vehicle-to-Network (NI V2N).

A roadside system may be part of an overall CCAM system and equipped with a communication module that supports communication via 5G networks (via Uu-interface) to a central system. This communication module may support other types of communication e.g. 4G or the roadside unit may act as a network gateway to relay messages via direct communication via either 5G or non-5G (ITS-G5 or LTE V2X).

2.4.3. Network Interface NI C2N

The Network Interface Cloud-to-Network (NI C2N) defines how cloud-based systems can be connected to 5G networks to support V2X applications, e.g. via 5G network functions as Multi-Access Edge Computing (e.g. ETSI MEC and 3GPP TS 23.501 on Local Access Data Network) and Network Slicing (e.g. 3GPP TS 23.501). These functions are supported in mobile networks to improve the performance ('zero' latency) and meet the requirements for CCAM applications. The external interfaces to the 5G Mobile Networks may be offered by MNO's to open their networks and resources for third parties are may be included in new service offerings with enhanced service level agreements. These aspects will be covered in D6.3.

2.5. Specifications on Application Interfaces

In Figure 4 the Application Interfaces (AI) to exchange information (message formats) are shown, with labels **AI V2V**, **AI V2R**, **AI V2C**, **AI R2C** and **AI C2C**. The interface **AI C2C** is included for information exchange between cloud systems of different stakeholders.

The message formats exchanged via the Application Interfaces **AI V2V**, **AI V2R**, **AI V2C**, **AI R2C** and **AI C2C** are specific to each Use Case category and details are given in section 3.

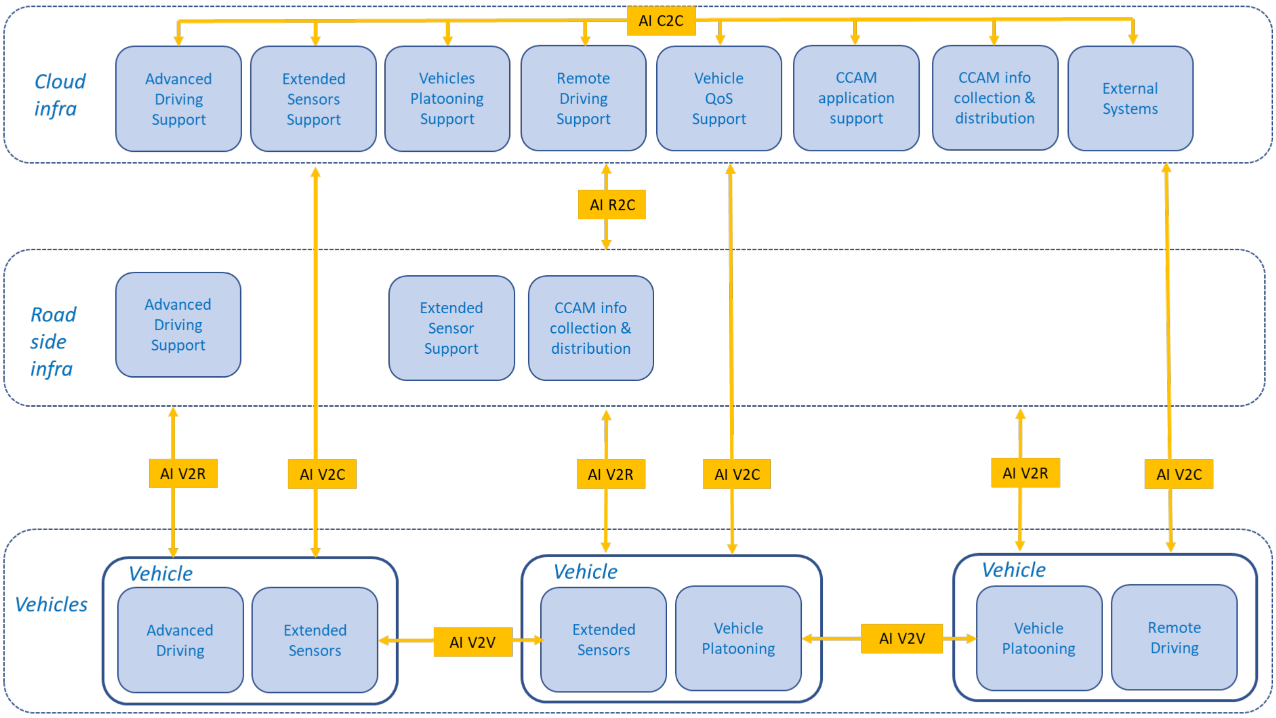


Figure 4 Application interfaces in CCAM reference architecture

2.5.1. Application Interface AI V2R and AI V2V

For the 5G-MOBIX use case categories that rely on the use of direct or short-range communication, information is exchanged via the AI V2R (or AI V2V interface). In section 3 the related **standardized** message or data sets are given per user story category.

Note: this interface is named V5 in the 3GPP V2X architecture for information exchange between V2X application and related to the PC5 sidelink network interface.

2.5.2. Application Interface AI V2C

The message sets defined for the interface AI V2R may also be exchanged from cloud systems via interface AI V2C. A distributed CCAM collection and distribution server may be used to collect and forward messages from vehicle to nearby vehicles (V2C, for V2N2V) or from roadside or cloud systems to vehicles, related to the geographical area where the information is relevant. In section 2.5.5 examples are given of these geo-messaging solutions.

2.5.3. Application Interface AI R2C

The message sets defined for the interface AI V2R may also be exchanged from cloud systems via interfaces AI R2C and V2C. A CCAM collection and distribution server may be used to collect and forward messages between vehicles and roadside/cloud systems and related to a specific geographical area.

2.5.4. Application Interface AI C2C

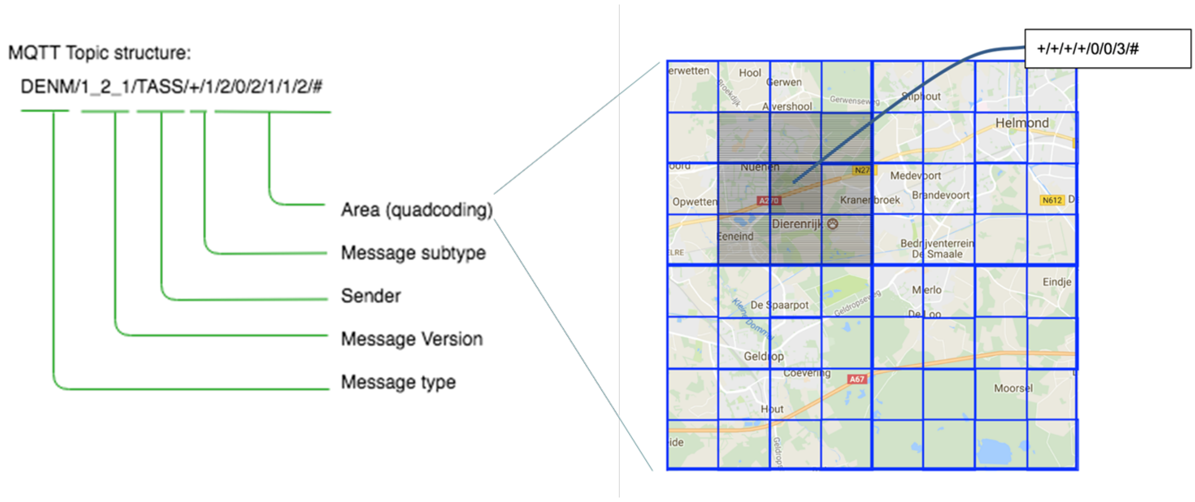
For the exchange of information between central systems existing data formats like DATEX-II or TPEG may be used. Also, the exchange of ETSI / CEN messages is possible via AI C2C. Examples are e.g. the exchange of local and global dynamic map, exchange of event-based message between OEMs, road operators and other information providers, access to live video feeds from roadside camera /radar systems etc.

Example of such interface descriptions are given in section 2.5.5. These specifications may be used for exchange of information between different stakeholders (car manufacturer, road operators, third-party providers and mobile network operators) via interface AI C2C and may also be used to collect and distribute information via interface AI V2C.

2.5.5. Geo-messaging

A 'geo-messaging' service is a service to collect messages from vehicles and other actors and distribute information to vehicles and other actors based on geographical area of relevance of the event. This service is typically deployed on a central or cloud platform. There are no standardized specifications for this service, but some specifications and implementations were developed in several projects:

- CONCORDA (Connected Corridor for Driving Automation[2]): in this project specifications for a geomessaging service via a cloud platform are developed[3]. The message exchange protocol is based on the MQTT protocol, where the topic of every published message is used to identify the type of message, geographical relevance area, and sender. The topic structure is defined as /<message type>_<messageversion>/{quadtree path}/<sender id>, see Figure 5. The quadtree path is an encoding scheme for location-based information, see http://www.maptiler.org/google-maps-coordinates-tile-bounds-projection/ for more details. In Figure 6 an example is given of the first 3 levels of Quadkeys.



[2] Reference: https://connectedautomateddriving.eu/project/concorda/
[3] Reference: CONCORDA Brabant pilot site interface definitions v0.7

Figure 5 Example of MQTT topic structure for geo-messaging with additional filters

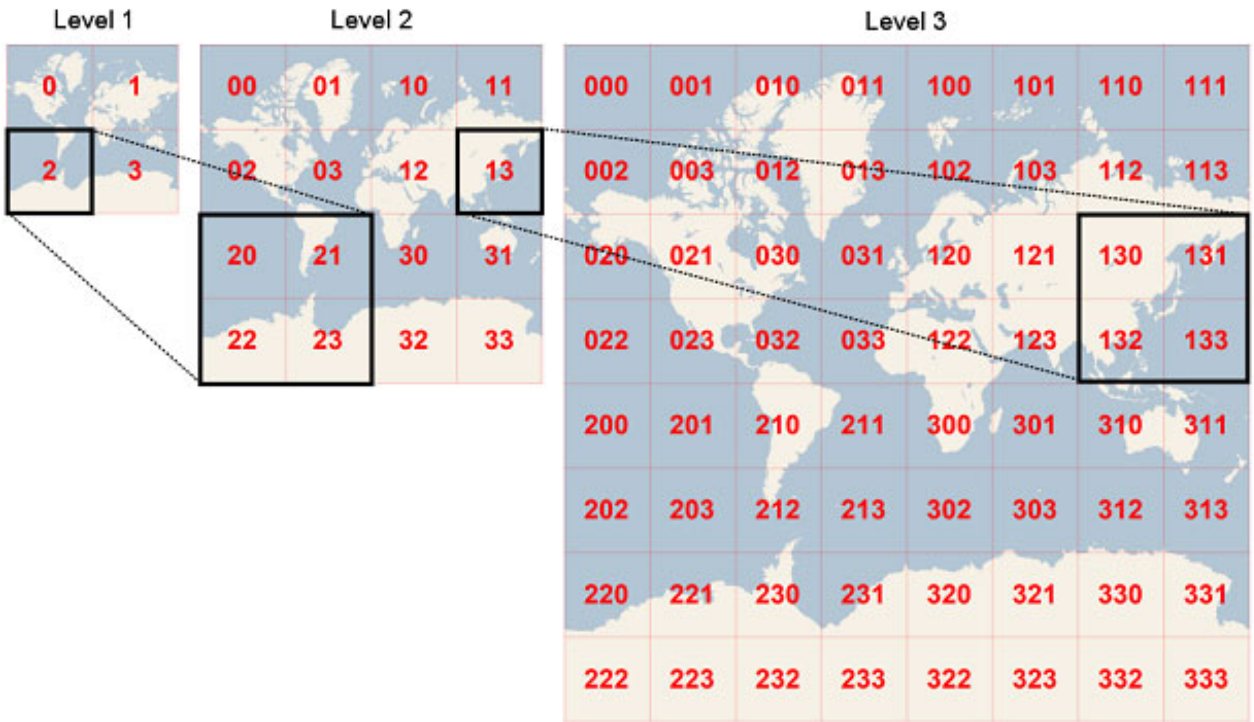


Figure 6 Using Quad keys to define a region[4]

- InterCor (Interoperable Corridors)[5]: a similar solution as developed in CONCORDA was also used in the InterCor project to exchange information between central ITS systems of the participating member states (Belgium, France, Netherlands, UK). The related specification is InterCor Milestone 4 - Common set of upgraded specifications for hybrid communication (v2.1). This specification describes an information distribution solution using message queues (based on AMPQ message broker) where clients can subscribe to 'message queues' and use criteria to filter on relevant information. Filter criteria are e.g. message type (related to a user story category), originator, geographical filtering (country or bounding box) or message rate.
- Converge[6]: in this project several architectural options are described in Deliverable D3 [Functional Requirements and Architecture Options, version 1.1, 30-09-2013] – related to the roles of stakeholders and how the geo-messaging' service can be provided to end-users of connected vehicles. The options differ where a geo-messaging server is located:
  - Geo-location Messaging Server located in MNO, as part of mobile network function

[4] Reference: https://msdn.microsoft.com/en-us/library/bb259689.aspx
[5] Reference: https://intercor-project.eu
[6] Reference: www.converge-online.de

- Geo-location Messaging Server as separate service provider: a separate role acts as service provider of the geo-messaging' service as intermediary between end-users, mobile network operators and service providers.
- Geo-location Messaging Server located at each Service Provider (SP): each SP of the geo-messaging' service offers this service to their end-users.

- NordicWay[7]: in this project a hub was defined where stakeholders (OEMs, road authorities, ITS providers) could connect and share their data / messages per geographical area (country or region). The solution uses a publish-subscribe model and DATEX-II as message format.

2.6. Application issues for cross-border corridor support of CCAM user stories

In D2.1, relevant issues at cross-border corridors are identified and grouped in four categories i.e. 1) Telecommunications, 2) Application, 3) Security & Data Privacy and 4) Regulation. In this section the issues in the category Application are described in detail, with proposed solutions to be evaluated in the 5G-MOBIX project. Figure 7 depicts different sub-categories for the identified Application issues, related to continuity (ACn), interoperability (AIn), discovery (AGn) and processing (APn). The application issues are summarized in Table 2. The last column in this table shows for which UCC and the number of User Stories (US) for which this issue was identified as relevant. E.g. the issue AC1 is identified as relevant for 11 USs in all five UCCs, so this issue should have most attention in the 5G-MOBIX development and evaluation. The other issues are applicable to specific USs (in 1 up to 3) in a specific UCC. Issue AI3 on Time Interoperability was not identified as relevant by any US but is included for completeness.

In the sections 2.6.1 to 2.6.4 the proposed solutions to be evaluated in the 5G-MOBIX project are described in more detail.

[7] Reference: https://www.nordicway.net/

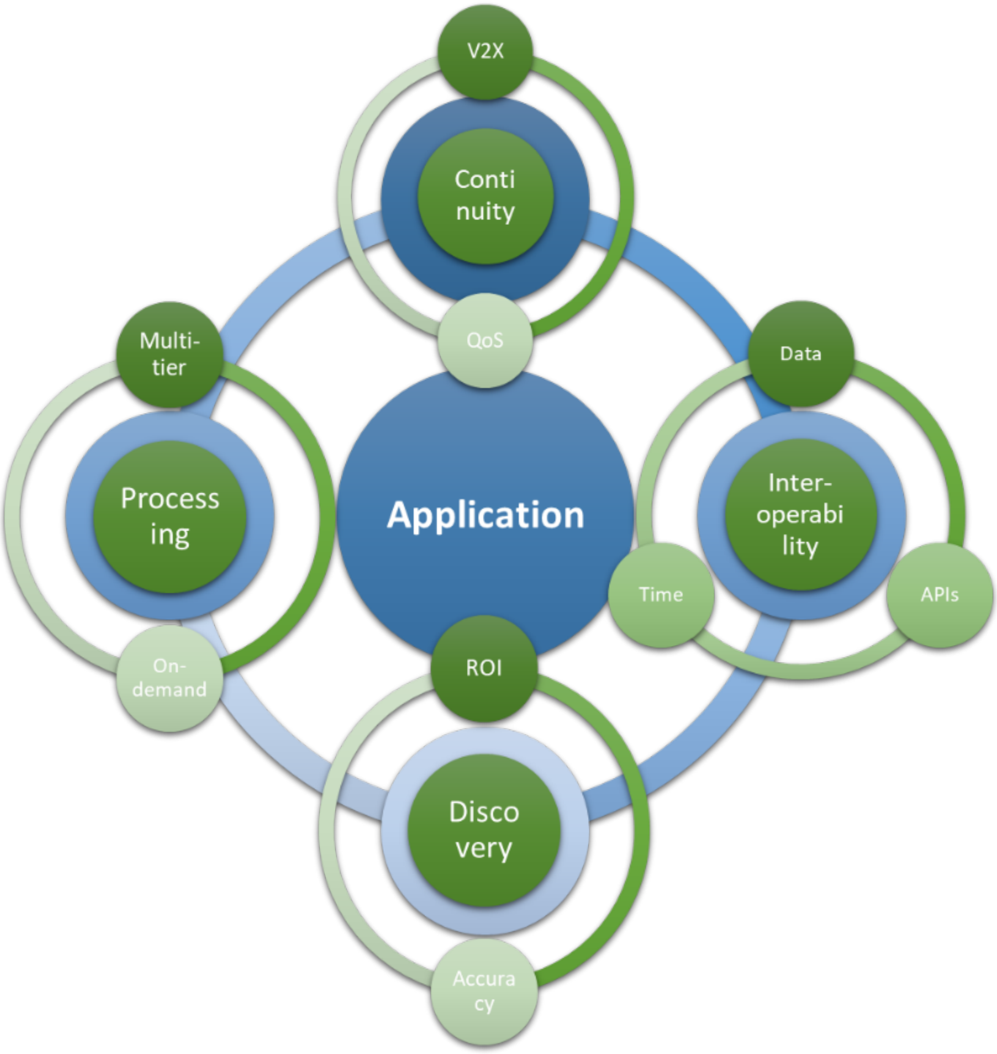


Figure 7 Application issues summary

Table 2 Issues list for Application category

ID	Issue name	Short description	UCC (no. of User Stories)
AC1	V2X Continuity	Unsteady communications performance among vehicles, servers and network functions	All UCC (11 US)
AC2	Dynamic QoS Continuity	Unsteady connectivity and changeable performance depending on network concurrency when no management of multi-resolution data	Vehicles Platooning, Vehicle QoS Support (2 US)
AI1	Data Interoperability	Inconsistent data schemas exchanged across vehicles vendors, network domains, infrastructure systems or federated service servers	Advanced Driving, Extended Sensors (3 US)
AI2	Protocol/APIs Interoperability	Inconsistent vehicle, edge or cloud protocols/APIs across different technology vendors and network domains	Extended Sensors (1 US, US8)
AI3	Time Interoperability	Inconsistent time zones management for synchronous actions with common timeline	None
AG1	Accurate Geo-Positioning	Vehicles are relying heavily on positioning. GPS positioning accuracy is not enough.	Vehicles Platooning, Remote Driving (3 US)
AG2	Geo-driven Discovery	Inefficient indexing of vehicles and attachment of data when ignoring geo-position of UEs	Extended Sensors (1US, US6)
AP1	Real-time Multi-tier Processing	Data inconsistency when data are real-time fused by AD functions hosted in different systems: data from onboard vehicle sensor processors, processed data at RSUs, the coordination data from the MEC service and the management data from the central service.	Advanced Driving, Extended Sensors, Remote Driving (3 US)
AP2	On-demand Processing	Lack of computing scalability to process the incoming volume of data with different speed and density producing bottlenecks and delays	Extended Sensors, Vehicle QoS support (2 US)

2.6.1. Issues related to V2X continuity

Table 3 Application issue and proposed solutions for V2X continuity

Issue Title	V2X continuity	Issue ID	AC1
Description	Unsteady communications performance among vehicles, servers and network functions.		

Conditions	Condition 1: One control centre for remote driving: vehicle remotely controlled by single control center for remote driving in a network handover situation from PLMN 1 to PLMN 2. Condition 2: Use of control centres in each country as for Traffic Management Centres for roadwork zones etc.: vehicle crossing the border where roadworks is located cannot send its position/status (roadwork detected, for instance) to the control center during handover. Condition 3: V2V in the collision risk area: direct V2V communication must be enabled in both (all) vehicles in the collision risk area.
Consequences & impact	1) Data loss, delay due to roaming and handover 2) Manoeuvres remain unknown and collision risk unknown 2) Collision risk high(er), performance in safety critical situations less than acceptable
Proposed Solutions	S1: Control handover delay and keep it to an acceptable value required by the application (network). S2: Have a safe strategy inside the vehicle to take back the control during handover (vehicle). S3: Implement Manoeuvre Coordination Service (MCS) between the engaged CAVs (vehicle). S4: Study the possibility to use protocols that guarantees delivery of data, with guarantee of the delivery in the same order in which they were sent (network). S5: Send information about known events in handover areas before entering them (vehicle/cloud). S6: Extrapolate vehicle position based on past trajectory to predict its potential position during handover (vehicle). S7: Have interoperability between control centres in order to allow processing in the one control center the set of data recorded during a road event in the other side of the border (cloud). S8: Improve the vehicle autonomy to mitigate the absence of data for short periods of time (vehicle, similar to S2). S9: Include sensors in the autonomous vehicle to enable continuous driving when commands are loss (vehicle). S10: Make Edge and Central servers guide in the negotiation of suitable resolution for the detected coverage (cloud). S11: Make Edge and Central servers to perform predictive discovery and handshake based on vehicles direction to boost sensor sharing (V2V) along handover situations (vehicle/cloud). S12: Enable Multicast communications to provide synchronous information at once (network). S13: Use V2V information to overcome data loss from central (vehicle).

Progressed solutions	The solutions S1-S13 need to be supported by either i) the 5G network infrastructure, ii) the connected and automated vehicle or iii) the roadside and cloud infrastructure. The solutions S5, S7, S10, S11 are related to the cloud infrastructure.

Table 4 Application issue and proposed solutions for Dynamic QoS Continuity

Issue Title	Dynamic QoS Continuity	Issue ID	AC2
Description	Unsteady connectivity and changeable performance depending on network concurrency when no management of multi-resolution data.		
Conditions	ITS Centre (in country X) needs to send to the vehicle an HD map generated by the ITS Centre in Country Y and its 5G infrastructure only supports a low bandwidth. Example: An autonomous vehicle is approaching a hazard event with an obstruction and the available 5G bandwidth is too low to transfer the detailed HD Map data regarding the event and updated road geometry with the obstruction.		
Consequences & impact	The autonomous vehicle cannot receive a map before arriving at the scene and will switch to manual mode and create a new map to be transmitted.		
Proposed Solutions	S1: Create different levels of detail of the HD Map to deliver according to the communication bandwidth available (similar to what is typically done with video streaming).		
Progressed solutions	S1		

2.6.2. Issues related to interoperability

Table 5 Application issue and proposed solutions for data interoperability

Issue Title	Data interoperability	Issue ID	AI1
Description	Inconsistent data schemas exchanged across vehicles vendors, network domains, infrastructure systems or federated service servers.		
Conditions	To avoid issues on handover between sides of the border the ITS Centres need to overlap information on the border area. Due to different information sources the two ITS Centres may have different information at a given time. Example: Country X has 3 accidents with a right lane blockage and Country Y only has one. Are the 2 accidents missing from Country Y's HD Map because they have actually ended or because Country Y doesn't include information on the location of the 2 other accidents?		
Consequences & impact	1) The vehicle won't be able to decide on which HD Map to trust 2) One of the HD Maps will be discarded		
Proposed Solutions	S1: The vehicle can use information from a single ITS Centre S2: Otherwise this C2V situation should be dealt with in the same as with different DENM messages in V2V. S3: The ITS Centres should synchronize among each other with an effective conflict resolution approach.		
Progressed solutions	S1, S2 or S3		

Table 6 Application issue and proposed solutions for Protocol/APIs Interoperability

Issue Title	Protocol/APIs interoperability	Issue ID	AI2
Description	Inconsistent Edge cloud APIs across different technology vendors and network domains		
Conditions	The extended sensors AD function requires common message formats related to the LDM, EDM and Discovery Service updates: The AD functions expect a consistent data schema to process the incoming data. The extended perception function expects a homogeneous protocol to access to and publish sensor streams.		
Consequences & impact	Incompatible solutions in vehicles for raw sensor streams or processed data (events).		

Proposed Solutions	S1: Use standard and common protocols; MEC or central service make the translation to a unique format ensuring the compatibility. As soon as possible use the standardized message sets per application, e.g. Manoeuvre Coordination Messages (MCM) for Advanced Driving, Collective Perception Message (CPM) for Extended Sensors and map message set. S2: Use same pre-standard message sets in 5G-MOBIX per UCC
Progressed solutions	S1 is preferred. S2 if S1 is not available. Follow status of ETSI ITS standardization work; agree on pre-standard message sets in 5G-MOBIX per UCC between CBC and TS. Agree on a 'profile' with minimal set of information in message set to support a UCC.

Table 7 Application issue and proposed solutions for time interoperability

Issue Title	Time interoperability	Issue ID	AI3
Description	Inconsistent time zones management for synchronous actions with common timeline		
Conditions	The vehicles in a platoon need orchestration actions with a common timeline and response time of each member. The decision for a platoon to make a manoeuvre or keep ongoing needs a deep timing for the leading vehicle triggering a cascade of actions for the rest of vehicles with an incremental delay as they end the queue. This delay depends on velocity		
Consequences & impact	Choreography integrity is not warranted so new members cannot join and the platoon must be dissolved.		
Proposed Solutions	S1: Vehicles need to use similar time referencing and accuracy. The requirements from C2C CC for vehicle ITS stations should be fulfilled by all ITS systems involved, i.e. both vehicle, roadside and edge/cloud systems.		
Progressed solutions	Solution S1		

2.6.3. Issues related to geo-driven discovery

Table 8 Application issue and proposed solutions for accurate geo-positioning

Issue Title	Accurate Geo-Positioning	Issue ID	AG1
Description	Vehicles are relying heavily on positioning. GPS positioning accuracy is not enough.		
Conditions	AD vehicles need accurate information (up to 20-30 cm accuracy) for AD functions.		
Consequences & impact	External information based on absolute position (via GPS) has to be mapped on local map with relative positions (distance to other vehicles/obstacles, lane position, etc.)		
Proposed Solutions	S1: HD maps need accurate geo-positioning, both in vehicle as in roadside/central systems S2: Vehicles need accurate geo-positioning via advanced positioning functions (e.g. differential GPS, camera/radar based (relative) positioning)		
Progressed solutions	S1 and S2		

Table 9 Application issue and proposed solutions for geo-driven discovery

Issue Title	Geo-driven Discovery	Issue ID	AG2
Description	Inefficient indexing of vehicles and attachment of data when ignoring geo-position of UEs.		
Conditions	Vehicle needs to receive all up-to-date information based on their geo-location. Roadside, MEC and central systems need to support this.		
Consequences & impact	Missing information for AD vehicles will result in road safety issues.		
Proposed Solutions	S1: Use of geo-distribution mechanism in Roadside, MEC and central systems, both between these systems in different ITS centres, or MEC systems and for vehicles to retrieve geo-location-based information of a limited area.		
Progressed solutions	S1		

2.6.4. Issues related to data processing

Table 10 Application issue and proposed solutions for real-time multi-tier processing

Issue Title	Real-time Multi-tier Processing	Issue ID	AP1
Description	Data inconsistency when are live fused by AD functions hosted in different actors, the onboard sensor processors, the processed data at RSUs, the coordination data from the MEC service and the management data from the central service. The extended sensors AD function makes real-time decisions distributed and autonomously by each vehicle based on on-board sensors (LDM), the EDM provided by the edge (MEC) and the sensor streams provided by other vehicles (V2V) indexed by the discovery service (MEC & Central).		
Conditions	The necessity of capture in real time a vast amount of sensor data and combine them to produce an EDM in real time need of high computation performance. Example: The EDM and some geo & route-based filtering must be done by MEC and central service to support the access to the appropriate external sensors. The MEC and the central service must be allocated to process a changeable density and volume of vehicles		
Consequences & impact	Information to operate the AD service is not available as an out of date information is not valid anymore.		
Proposed Solutions	S1: Use of standardized message set: Collective Perception Message; sensors need to put their information in this format S2: Use of industry wide raw data formats for video (transmission) with meta data		
Progressed solutions	S1 and S2		

Table 11 Application issue and proposed solutions for on-demand processing

Issue Title	On-demand Processing	Issue ID	AP2
Description	Lack of computing scalability to process the incoming volume of data with different speed and density producing bottlenecks and delays.		
Conditions	Roads are equipped with various types of sensors and sending the detected obstacles to the vehicle. Example: Roadworks ahead at border entrance, the vehicle has to perform a lane merge, the obstacles are provided by an RSU. The vehicle is in a handover situation.		

Consequences & impact	Information on obstacles not received/delayed from RSU or raw data formats cannot be processed in time by the OBU of the vehicle.
Proposed Solutions	S1: Enable HW-accelerated MEC processing in the edge S2: Allow on demand resources allocation at the network edge for MEC services
Progressed solutions	S1 and S2

2.7. Security and Data protection issues

From the Security and Data protection issues identified in D2.1, the issue Trusted and secure communications between vehicles from different trust domains (STS1) is described in this deliverable.

Also, cybersecurity and privacy preservation mechanisms should be implemented in order to protect the entities of the 5G-MOBIX reference architecture: the cloud, network (5G networks and the others) and the vehicles infrastructures.

Table 12 Security issue and proposed solutions for trusted and secure communications

Issue Title	**Trusted and secure communications between vehicles from different trust domains**	**Issue ID**	**STS1**
Description	Without a common trust domain between the EU, Turkey, South-Korea and China, trusted and secure communication between the vehicles could not be achieved when the vehicles from different trust domains are to communicate.ck of computing scalability to process the incoming volume of data with different speed and density producing bottlenecks and delays.		
Conditions	1. A Trust domain in the EU (a working implementation of the EU CSCMS) 2. A trust domain in China, South-Korea and Turkey		
Consequences & impact	As a consequence, the messages exchanges between vehicles from these different trust domains cannot be authenticated by the others. There these vehicles could not be allowed in the other trust domain. For example, a Turkish vehicle correctly enrolled in the Turkish trust domain will not be able to communicate with a Greek vehicle enrolled in the EU-CSMS. In general, there is an overhead related to Security and Data privacy mechanisms for CCAM messages.		

Proposed Solutions	An international collaboration between the trust domain to resolve co-existence issues (*e.g.* cross-certification between these trust domains)

3. SPECIFICATIONS OF ROADSIDE AND CLOUD INFRASTRUCTURE FOR 5G-MOBIX USE CASE CATEGORIES

3.1. Introduction

In this section the specifications of the roadside and cloud infrastructures to be deployed in CBC and TS are described in detail. The roadside and cloud architecture are based on the user story descriptions as described in D2.1. The reference description of the architecture with functional elements of the roadside and cloud infrastructure, their network connections to the 5G infrastructure and the messages formats for information exchange between and towards vehicles – via the 5G network are described in section 2.

For each user story in 5G-MOBIX a description is given:

- Description: short description of the user case category and user stories with explanation of roadside and cloud infrastructure.
- High-level deployment architecture of the roadside and cloud infrastructure of the CBC site combined with interfaces to AD vehicles
- Specific contributions of TS including detailed specifications for roadside and cloud infrastructure of the (functional) elements and systems and the interfaces towards network and applications;
- Cross-border corridor support in roadside and cloud infrastructure to support the 5G-MOBIX use case categories along EU cross border corridors;
- Others: describe other aspects

An aggregated description is included at the end of each section for each of the 5 use case categories, providing the specific details about the roadside and central systems to support the use case categories.

3.2. UC Category 1: Advanced Driving

3.2.1. Description of UCC Advanced Driving

Advanced Driving "enables semi-automated or fully-automated driving. Longer inter-vehicle distance is assumed. Each vehicle and/or RSU shares data obtained from its local sensors with vehicles in proximity, thus allowing vehicles to coordinate their trajectories or manoeuvres. In addition, each vehicle shares its driving intention with vehicles in proximity. The benefits of this user story group are safer traveling, collision avoidance, and improved traffic efficiency" (Source: 3GPP TS 22.186 R16).

The following user stories are related to Advanced Driving:

1. Complex manoeuvres in cross-border settings (ES-PT US1)
2. Infrastructure-assisted advanced driving (FR US10)

3. Cooperative Collision Avoidance (NL US12)
4. Cloud-assisted advanced driving (CN US15)

3.2.2. Deployment architecture of CBC ES-PT for Advanced Driving

The ES-PT corridor has several scenarios related with the Advanced Driving category:

- US1 (Complex manoeuvres in cross-border settings):
  - Scenario 1: Lane merge.
  - Scenario 2: Automated overtaking.
- US3 (Automated shuttle driving across borders):
  - Scenario 1: Shuttle cooperation with road users.

Description

The three mentioned scenarios follow a similar structure, in which CCAM infrastructure helps supporting automated manoeuvres. The role of the roadside and cloud infrastructure in this case is to assist the 5G autonomous vehicles in their environmental perception, planning and decision making, as well as monitoring the connected vehicles. See Figure 8.

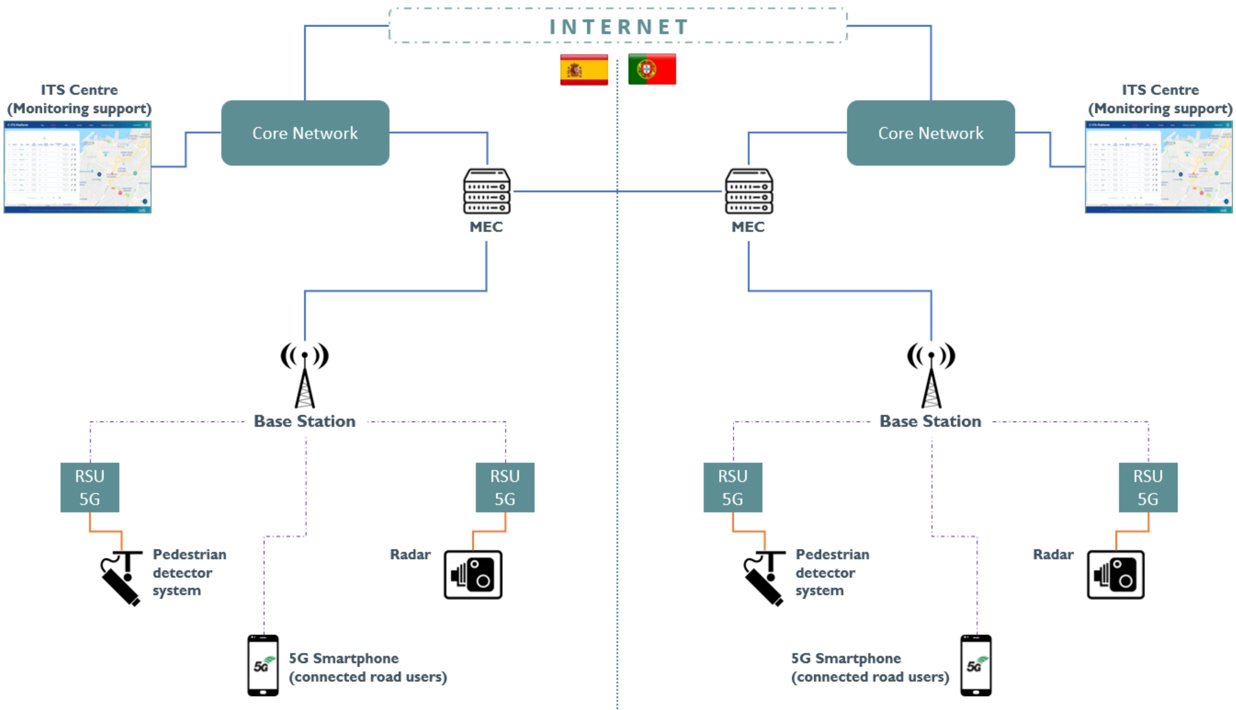


Figure 8 General CCAM infrastructure to support Advanced Driving scenarios on ES-PT CBC.

The performance of automated manoeuvres by autonomous vehicles in those scenarios are based on the information available about other road users (namely vehicles, pedestrians, etc). This information is shared simultaneously both by connected vehicles and by the road infrastructure, which is equipped with sensors (cameras and radars). The CCAM infrastructure detect vehicles and users and their attributes (position, speed, heading, …) and forward this information in real-time (via MEC node) to all relevant vehicles in the neighbouring area (geocasting).

The roadside infrastructure provides an additional source of data in those scenarios, which may be used in two different ways:

- Extend the perception layer of 5G AVs, by detecting legacy vehicles outside the range of AVs' sensors.
- Collect auxiliary data related to the pilot execution, so the evaluation is enriched with additional information that will increase the quality of the conclusions derived.

High-level architecture of the roadside & cloud infrastructure

The high-level architecture of the CCAM infrastructure for the scenarios within this category is shown in Figure 9, where functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, and the information exchange is shown in brown. The architecture does not cover the cross-border aspects.

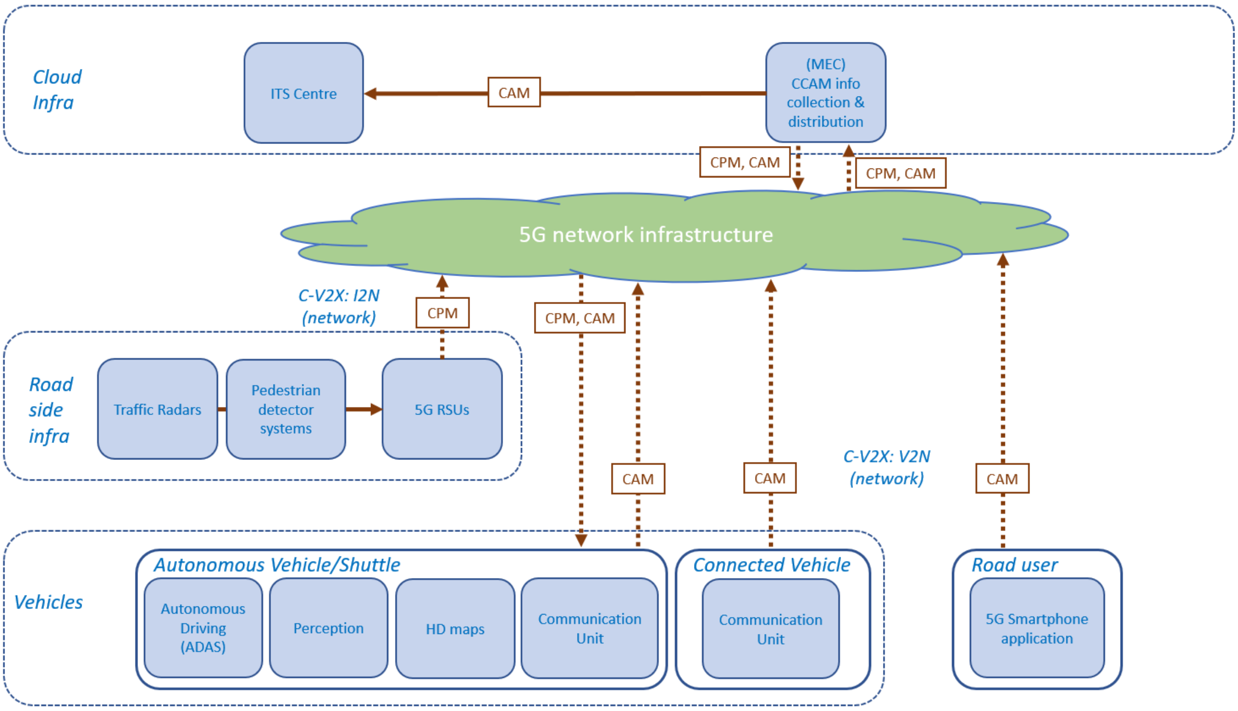


Figure 9 CCAM architecture for the ES-PT Advanced Driving scenarios.

The roadside and cloud infrastructure deployed in those three scenarios can be summarized in the following elements:

- MEC nodes: work as relay nodes where messages from vehicles and infrastructure sensors are forwarded to other vehicles in the area. Both MECs in Spain and Portugal are connected through the network, allowing one-country vehicles share information via network with vehicles in the other country.

- ITS Centers: cloud applications running on each side of the corridor. Each ITS Centre is connected to the MEC node of the same country, and consumes the data passing through this node in order to monitor vehicles connected to the regional network. Furthermore, both ITS Centres share data from vehicles of both sides, when they are in cross border areas.
- Traffic radars: static elements installed near the lane merge test sites. Those radars detect vehicles running in the main road and provide their attributes (size, speed, heading, etc). Radars are physically connected to 5G RSUs, which transform the raw outputs of the radar detections into CPM messages, that are sent to the network through the MEC nodes.
- Pedestrian detectors: like radars, pedestrian detector systems are static elements strategically located along the autonomous shuttle route. Their role is to detect any road user in problematic areas where the shuttle has limited field of view. Those detector systems are physically connected to 5G RSUs, which transform the raw outputs of the detections into CPM messages, that are sent to the network through the MEC nodes.

Lastly, even though it is not classified in roadside or cloud, there is another relevant element in the CCAM architecture:

- Smartphones: some road users in the shuttle scenario are equipped with 5G smartphones which share its attributes (location, speed, etc) to the network in form of CAM messages.

Sequence diagrams

The three scenarios considered under Advanced Driving category follow a similar working sequence:

1. Firstly, either connected vehicles or road users share their attributes to the network.
2. Simultaneously, the roadside infrastructure elements detect the presence of vehicles and road users (both connected and non-connected ones) and share their attributes to the network.
3. Finally, main vehicles in each scenario (those which perform the manoeuvre) receive the information shared in the network by the other actors, process this data and decide how to adapt their behaviour.
4. During all this procedure, the attributes sent to the network by vehicles (CAM messages) are forwarded to the ITS Centre in order to monitor connected vehicles.

In the following figures, where different kind of vehicles are depicted (AV: Autonomous Vehicle, CV: Connected Vehicle, LV: Legacy Vehicle) the sequence diagrams for the different scenarios are shown.

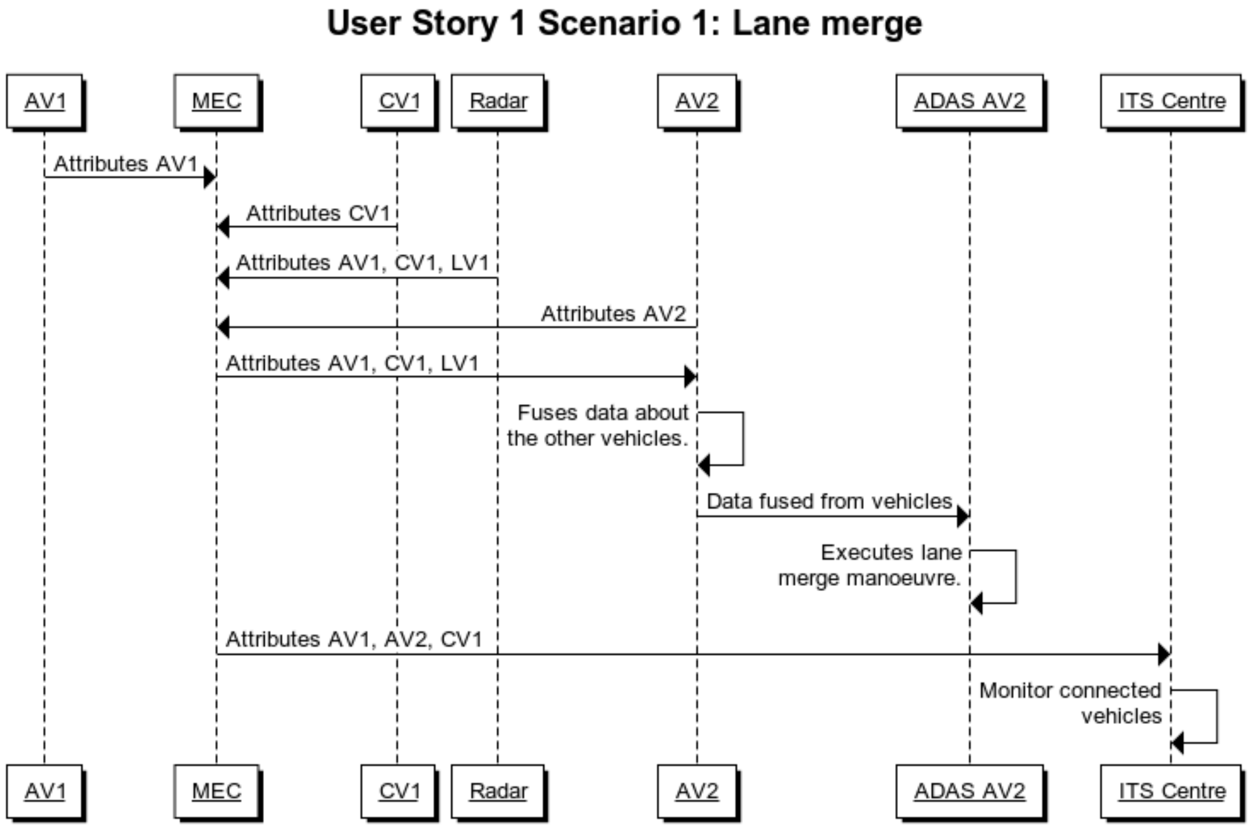


Figure 10 Sequence diagram of the lane merging scenario of ES-PT US1.

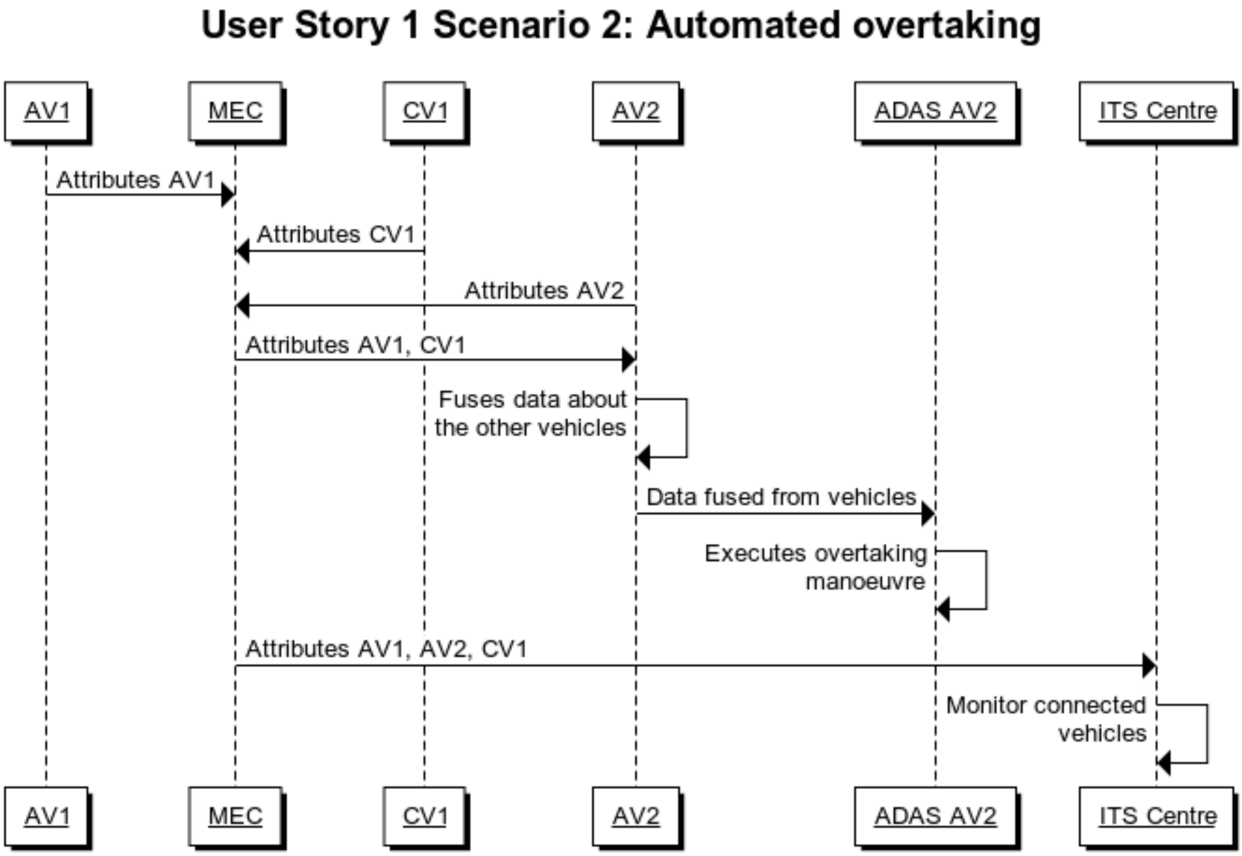


Figure 11 Sequence diagram of the automated overtaking scenario of ES-PT US1.

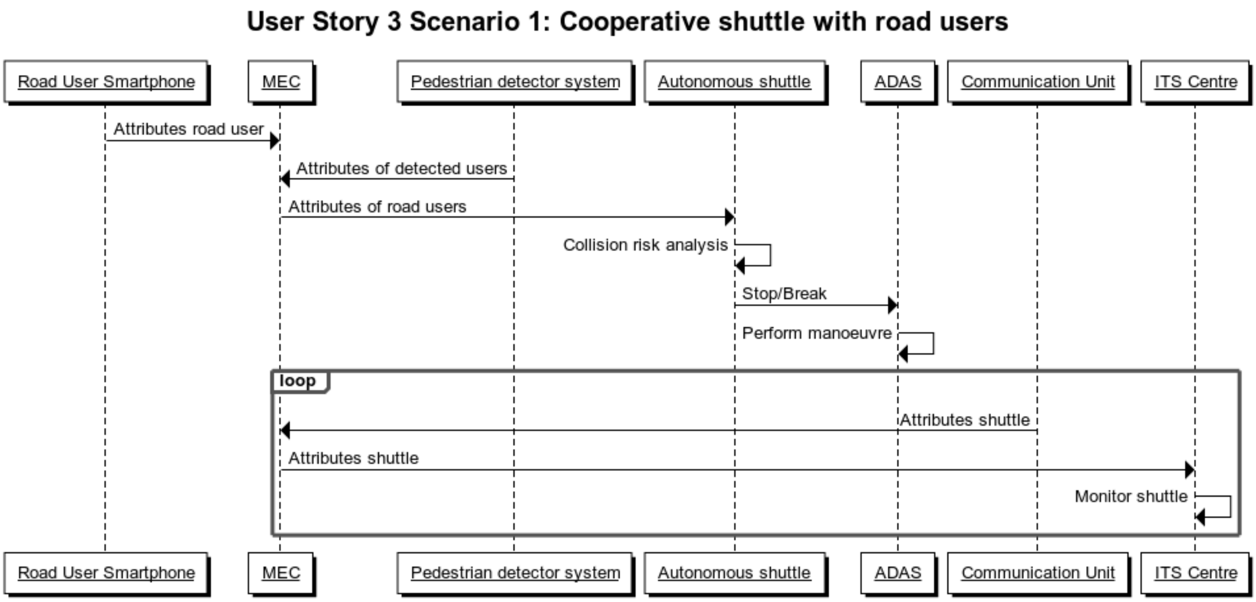


Figure 12 Sequence diagram of the Cooperative shuttle with road users scenario of ES-PT US3.

As a conclusion, the objective of those three scenarios is to test how a similar architecture and procedure can be applied to different CCAM environments with different types of roadside equipment.

Interface specifications

The Advanced Driving scenarios of the ES-PT CBC are based in the C-V2X approach, namely X2N2V (Everything-to-Network-to-Vehicle). This architecture aims to connect any kind of device through 5G cellular network. Figure 9 CCAM architecture for the ES-PT Advanced Driving scenarios. shows the communication links, technologies and type of messages used. All the interface used are briefly described below:

1) V2N (Vehicle-to-Network): vehicles send CAM messages containing their attributes (location, speed, heading, etc) to the MEC nodes (network).
2) P2N (Pedestrian-to-Network): road users' smartphones send CAM messages containing the attributes (location, speed, heading, etc) of the road users to the MEC nodes (network).
3) R2N (Roadside-to-Network): roadside devices (cameras and radars with their respective RSUs) send CPM messages containing the detections information (size of the detected vehicle, speed, heading, location, etc) to the MEC nodes (network).
4) N2V (Network-to-Vehicle): MEC nodes act as relay nodes and forward received messages from vehicles/users/roadside to other vehicles.
5) N2C (Network-to-Cloud): MEC nodes forward only CAM messages from connected vehicles to the ITS Centres with monitoring purposes.

Detailed specifications

Some of the elements mentioned in sections above are described in more detail as follows:

Traffic Radars

The road infrastructure includes traffic radars (see Figure 13) which are able to detect 7 different classes of vehicles (pedestrian, bicycle, motorbike, passenger car, transporter, truck/bus and long truck) with good accuracy. Those radars are assisted by 5G RSUs which are responsible of parsing the radar outputs into standard messages, and upload them to the network.

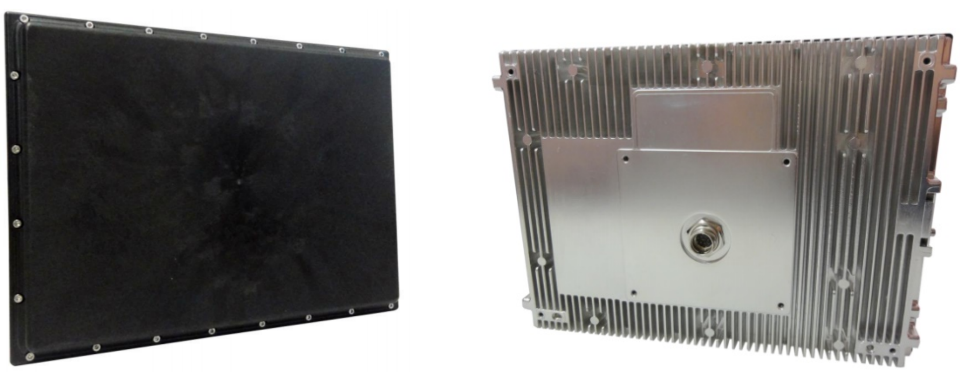


Figure 13 Road traffic radar for vehicle detection, classification and localization.

Pedestrian detector systems

The pedestrian detection system consists of a camera placed in the infrastructure who is able, with the help of the image processing application, to obtain the moving objects from an image in real time and finally to classify them as pedestrians, in case, by passing an image processing pedestrian detector over the extracted moving elements existing in the frame. The information of the detected pedestrians and their positions is passed periodically by an ethernet connection (UDP) to a road side unit placed, as well, in the infrastructure and which sends this information to the on board units placed in the vehicles so that they can make decisions in order to, i.e., brake in advance when they do not have direct vision over the scene.

The selected camera[8], having IP67 has been packaged in a box and with a lens protector in order to protect it from the adverse weather conditions that could appear in some seasons of the year. The camera is connected to a PC that processes the images coming from the camera and which sends via ethernet the above mentioned periodical UDP messages to the Road Side Unit (RSU) so that it can then send via 5G the received information to the On Board Units (OBUs), following the message standards.

ITS Centre

Regarding the cloud infrastructure, the ITS Centre will be composed by the modules and interfaces depicted in Figure 14.

The ITS Center is the control center of the cooperative ecosystem as a whole, allowing the management, monitoring and actuation of the different connected and cooperative elements. Thus, the infrastructure manager can monitor the status of the connected elements such as Traffic Managements Centers, RSUs, Vehicles post traffic events and other data to the ITS Center though the REST API. All that data is harmonized to a common data model which the Geoserver will provide the relevant information to the corresponding data consumers: other vehicles, smartphones, etc. ITS Frontend consumes also that information in order to monitor the status of the connected elements. ITS Center also allow the connection with other data sources (DATEX-II standard) increasing the possibilities of information sharing and completing a standardized.

ITS Centre application is deployed both in Spain and Portugal simultaneously, and both instances are interconnected in order to share data from vehicles near the cross border.

[8] See https://es.ids-imaging.com/store/ui-5220re-poe.html

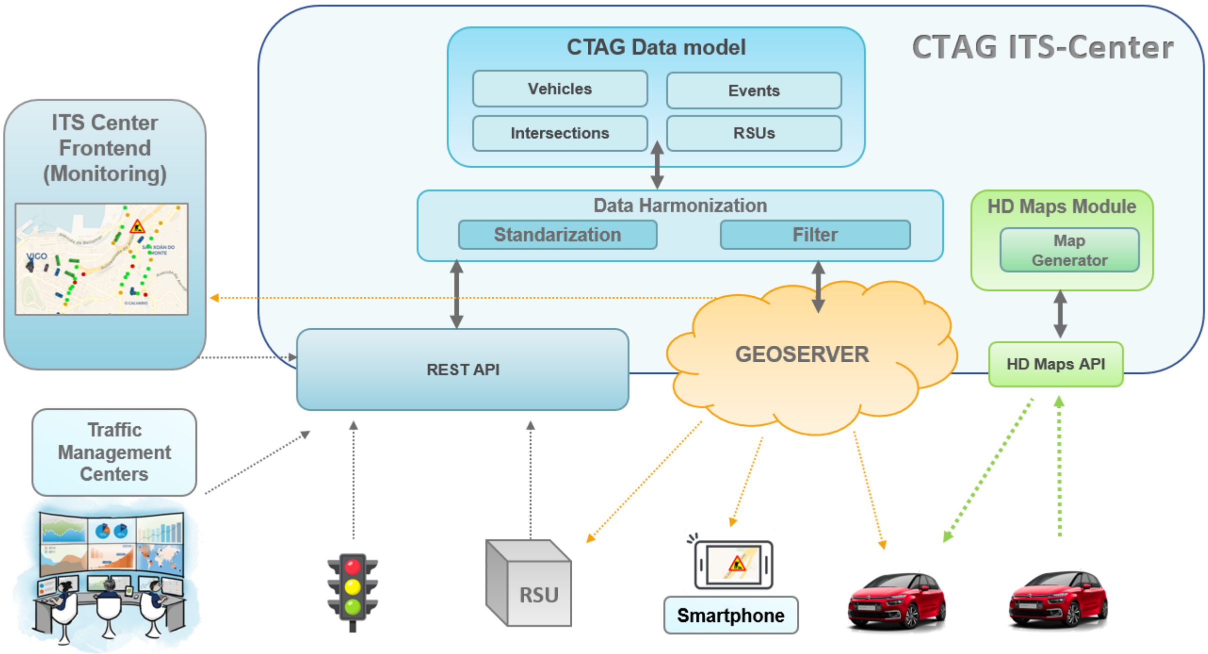


Figure 14 General architecture of the ITS Centre in the ES-PT CBC.

Connected Road Users

The connected VRU's system will be responsible for inserting connected VRUs as road agents in the challenge of assuring safety conditions in a shared environment. In this particular situation, where an EV shuttle remotely operated, it is critical to have infrastructure information that will support vehicle's decisions beyond vehicle's sensors and beyond VRU's line of sight. In short, both parties should be aware of each other.

The scenario where the UC will be developed is particular sensible as it is located in a non-open environment with several corners, VRUs (pedestrians and bicycles) walking in the same pathway as the vehicle. It is therefore important that the EV shuttle (and its remote human operator) and VRUs are aware of each other's position and intention. For that, the VRUs need to be equipped with a mobile equipment that shares relevant information (mainly position, heading and speed) about that particular UE. This will be implemented via a Smartphone (that VRUs typically have) as it is considered a pervasive equipment that can use 5G (as in the scope of this project).

The objective is to use 5G network to transmit CAM messages and receive DENM messages. The first to communicate position, heading, speed, etc.) and the latter to receive information about the collision risk warning (defined by the shuttle or the infrastructure).

Two important scenarios may be explored (see Figure 15 Explored alternatives for connected road users):

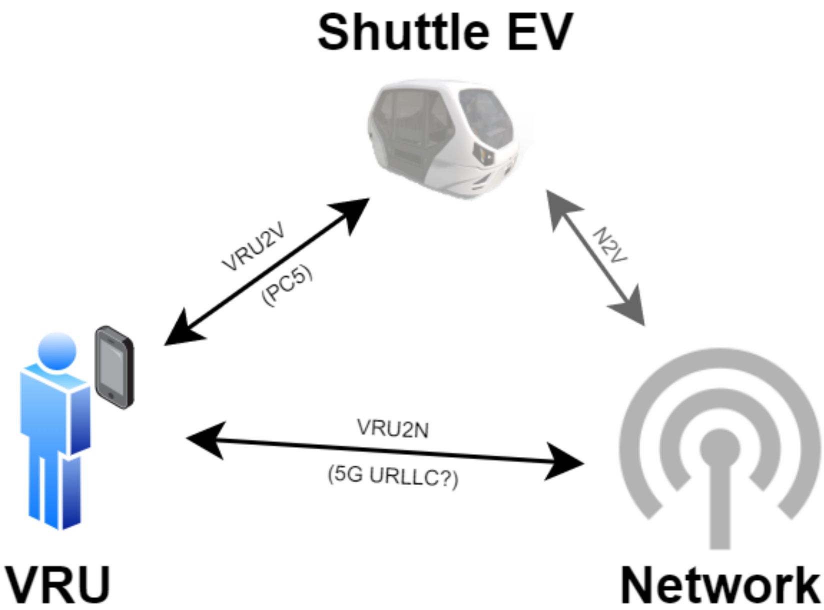


Figure 15 Explored alternatives for connected road users

- VRU2N (VRU to Network) – Using the 5G network and the MEC centralized-based approach that relays ITS messages to every pertinent road agent. This approach explores the advantages of 5G communication in the matter of assuring a low latency in data transmission (as it can be of critical importance for safety reasons). It also explores the advantages of 5G in the scenario of having a significantly larger number of connected road agents all sending and receiving messages. Yet, 5G communication via the network, even though with a lower latency than, for instance, 4G LTE, may still be insufficient for safety applications. This will be one of the key evaluations to perform. Using slicing and URLLC will depend on the commercial availability of smartphones with 5G slicing capabilities and a SA architecture. As an assured scenario, we will rely on the network's architecture 5G efficiency to provide the lowest possible latency communication.
- VRU2V (VRU to Vehicle) – This scenario is characterized by the use of PC5 (Sidelink) 5G communication. The lowest latencies, and therefore more interesting for safety reasons, are achieved using this direct communication. Yet, the lack of implementation of PC5 in actual Smartphones (due to their chipsets) may compromise the second scenario in the project's timeframe. Smartphones manufacturers have announced their will to include this feature in future the 5G equipment, but at the moment, there is not concrete information about this. Also, the Shuttle's OBU will not support PC5 communication and therefore communication would have to via the network to reach the shuttle losing its purpose. Using Rel-14 V2P (PC5 with LTE) direct communication would be a possibility (although not using Smartphones, as there are not available) but is out of scope for this project.

Considering the previous scenarios, we can therefore conclude that the VRU2N will be the one to be explored in this project in the ES-PT CBC.

Cross-border aspects

The performance of the Advanced Driving scenarios in the ES-PT CBC requires:

- Definition of standard ITS messages for common framework on both sides of the border.
- Support of the user story scenarios in inter-PLMN networks.
- 5G eMBB and URLLC support with handover between edge servers from different MNOs

3.2.3. Trial sites specific contributions to CBC for Advanced Driving

Table 13 gives an overview of the specific roadside and cloud infrastructure to support the user stories for Advanced Driving, as described in section 7.

Table 13 Overview of roadside and cloud infrastructure per user story for Advanced Driving

User story	Roadside sensors /actuators	Roadside comm. units	Cloud infrastructure
Complex manoeuvres in cross-border settings (ES-PT US1)	Road monitoring technologies (camera, radar for detection of 7 types of road users)	Yes, RSU with cellular 5G capabilities	MEC node (collect & forward) ITS center (collect recorded routes, and distribution updated HD map)
Automated Overtaking (FR US10)	Camera, lidar, other sensors for vehicle identification and localization	Yes, option for RSU for direct V2R	MEC node (raw sensor data to MEC node; collision risk at road works site
Cooperative Collision Avoidance (NL US12)	n/a	n/a	MEC node (collect & forward V2V and R2V messages)
Cloud-assisted advanced driving (CN US15)	n/a	Yes, RSU for direct V2R; forward to cloud	Cloud server and RSU with data fusion (vehicle and roadside) plus path planning from cloud server

Summary:

- Roadside perception systems are used at ES-PT and FR sites to support Advanced Driving at complex/ dangerous locations for detection and localization of (non-equipped) vehicles or other non-equipped road users.
- At all the sites information exchange for coordinated manoeuvres for lane merge, overtaking and collision avoidance are used. These specifications on coordinated manoeuvre for Advanced Driving will be aligned between the trial sites, based on the Manoeuvre Coordination Service (MCS).
- All the sites use MEC node to support Advanced Driving for local collection, processing and distribution of information. Specifications to support MEC for CCAM application, MEC hand-over in a single PLMN and interconnection of MEC solutions in multi-PLMN need to be aligned, in different configurations: inter-PLMN, multiple MEC for single PLMN, inter-MEC, and different MEC solutions (LADN, other) with 5G NSA and SA.

Table 14 shows the trial-site specific contributions to the CBC.

Table 14 Trial sites specific contributions to CBC for Advanced Driving

	FR US10	NL US12
RSU	Collective perception service (CPS) for transmission and reception of CPM via RSU	n/a
Roadside sensors	Yes, roadside system with CPS support	n/a
MEC	Data fusion to support advanced driving Geocasting for transmission of C-ITS messages over 5G	Two MEC solutions from two independent 5G telecom operators' networks, with MEC discovery, inter-MEC (multiple PLMN) and MEC-handover (single PLMN)
Cloud Systems	n/a	Collision risk detection in CAV application, alternative/backup at MEC App
Application	Use of CPS	Two schemes: In-vehicle based and MEC based application of CoCA. CoCA: Application of the Manoeuvre Coordination Service (MCS) Application of MCS in addition to CAM-based manoeuvring – to support other manoeuvring like overtaking
Other	n/a	n/a

3.2.4. Specifications on Application Interfaces for Advanced Driving

Application Interface AI V2R and AI V2V (direct communication)

1.1.1.1.1. Advanced Driving with automated vehicles supporting C-ITS basic safety services

Within Europe C-ITS has been standardized by ETSI and CEN/ISO based on 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 IEEE 802.11p. Both ETSI and CEN/ISO have 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 70+ specifications were the starting point for several pilot and pre-deployment project in Europe. These specifications were also used by Car-2-Car Communication Consortium and C-Roads Platform[9] to define 'profiles' to reach a minimum level of interoperability for vehicles and roadside systems that support C-ITS services. This work has been used as 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 [REF: https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf]. The act is based on the ITS Directive 2010/40/EU, which accelerates the deployment of these innovative transport technologies across Europe. In this act descriptions are given of the 16 safety-related V2V services and 15 I2V services, with description of the service and the triggering conditions to start sending C-ITS messages.

The list of V2V service categories with V2V services (16 V2V services in 6 categories) as described in Annex I of C(2019)1789 include:

1. Traffic jam: Dangerous end of queue and Traffic jam ahead
2. Stationary vehicle warning: Stopped vehicle, Broken-down vehicle and Post-crash
3. Special vehicle warning: Emergency vehicle in operation, Stationary safeguarding emergency vehicle and Stationary recovery service warning
4. Exchange of IRCs: Request IRC and Response IRC
5. Dangerous situation: Electronic emergency brake light, Automatic brake intervention and Reversible occupant restraint system intervention
6. Adverse weather conditions: Fog, Precipitation and Traction loss)

The list of I2V service categories and I2V services (15 I2V services in 4 categories) is:

1. In-vehicle signage: Dynamic speed limit information, Embedded VMS 'free text' and Other signage information
2. Hazardous locations notification: Accident zone, Traffic jam ahead, Stationary vehicle, Weather condition warning, Temporarily slippery road, Animal or person on the road and Obstacle on the road
3. Road works warning: Lane closure (and other restrictions), Road closure and Road works mobile

[9] See https://www.c-roads.eu/platform/documents.html

4. Signalised intersections: Green light optimal speed advisory and Signalised intersections Public transport prioritisation

In this Annex I also the relevant specifications for the message sets can be found and cover e.g.:

- ETSI EN 302 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.0 (2018-08): CAM message
- ETSI EN 302 637-3, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, v1.3.0 (2018-08): DENM message
- ETSI TS 103 301, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services, V1.2.1 (2018-08): reference to IVI, SPAT and MAP messages
- ISO/TS 19321, Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures (15 April 2015): IVI message

1.1.1.1.2. Advanced Driving with use of the Manoeuvre Coordination Service (MCS).

The Manoeuvre Coordination Service (MCS) is intended to reduce prediction errors by exchanging detailed information about intended manoeuvres between vehicles. Furthermore, the MCS provides possibilities to coordinate a joint manoeuvre if several vehicles intent to use the same space at the same time. Within ETSI ITS work has started to specify the MCS which defines an interaction protocol and corresponding messages (Cooperative Intention Message, CIM) to coordinate manoeuvres between two or more vehicles. The MSC is intended to support automatic driving as well as manual driven vehicles. The current specifications on MCS are draft versions: (i) ETSI TR 103 578 V0.0.2 (2018-10) "Intelligent Transport Systems (ITS); Vehicular Communications; Informative report for the Manoeuvre Coordination Service" and (ii) ETSI TS 103 561 V0.0.1 (2018-01) "Intelligent Transport Systems (ITS); Vehicular Communication; Basic Set of Application; Manoeuvre Coordination Service". The MCS is at early stage of standardization. 5G-MOBIX partners (e.g. VEDECOM through PACV2X project, see section 7.1.1) are actively contributing to the standardization process by participating in all the meetings and presenting the proposals for the MCS. Therefore, pre-standardized versions of CIM will be used in 5G-MOBIX.

Application Interface AI V2C, R2C and C2C

The message sets defined for the interface AI V2R and AI V2V for direct communication may also be exchanged via cloud systems via interface AI V2C and R2C and between cloud systems, AI C2C. A distributed CCAM collection and distribution server may be used to collect and forward messages from vehicle to nearby vehicles (V2C, for V2N2V) or from roadside or cloud systems to vehicles, related to the geographical area where the information is relevant. In section 2.5.5 examples are given of these geo-messaging solutions.

3.3. UC Category 2: Vehicles Platooning

3.3.1. Description of UCC Vehicles Platooning

Vehicles Platooning "enables the vehicles to dynamically form a group travelling together. All the vehicles in the platoon receive periodic data from the leading vehicle, to carry on platoon operations. This information allows the distance between vehicles to become extremely small, i.e., the gap distance translated to time can be very low (sub second). Platooning applications may allow the vehicles following to be autonomously driven" (Source: 3GPP TS 22.186 R16).

The following user stories are related to Vehicles Platooning:

1. Platooning with "see what I see" functionality in cross-border settings (GR-TR US4)
2. eRSU-assisted platooning (DE US7)
3. Cloud-assisted platooning (CN US16)

3.3.2. Deployment architecture of CBC GR-TR for Vehicles Platooning

The deployment architecture of the user story Platooning with "see what I see" functionality in cross-border settings from the CBC site GR-TR is the basis for this UCC.

Description

"See-what-I-see" streaming application

In the platooning mode, the distance between the vehicles in the platoon can become very small to obstruct the view of the followers, where only the leading vehicle has a clear view of the road in front of the platoon. The streaming application solves this problem by sharing the view of the leading vehicle with the rest of the vehicles that belong to the platoon. This means that every vehicle, which can act as a leader depending on the particular circumstances, has to have a 4K-camera installed to record and stream a high-quality image in real time.

Abstract description of the "see-what-I-see" functionality

Once the platoon is formed an information message is sent to the application. The application responds with a confirmation message to the leading vehicle of the platoon. So, there are two distinct roles, the leading vehicle and the following trucks. The platoon has a specific identifier (ID). The camera of the leading vehicle is recording the view of the road from the said vehicle. The image data is compressed by the camera itself (IP camera). The compressed data is transferred to IMEC's OBU (inside the leading vehicle), then the data is transmitted to the base station of the MNO in jurisdiction. The application server gets the compressed data and the ID of the platoon. The ID of the platoon is needed for the following vehicles to send the 4K image data back to the following vehicles of the formed platoon. The OBUs of the followers transfers the data to the respective in-car video displays. Low latency is an important requirement in this user story, the maximum latency for video transmission that the 5G network can achieve will be the determining factor (URLLC and eMBB).

Application design

Basically, peer-to-peer data traffic (the compressed 4K image data and other information such as position and velocity) is routed by the gNB (MEC server) to all the following vehicles of the platoon, once the platoon has been created. All the following vehicles are considered (realistically) to be UEs within the same gNB (X2 links within an adjacent gNB will not be considered at first).

The application server is located in the MEC to reduce network-induced delays since latency is the most crucial Key Performance Indicator to ensure the user story. The MEC server will be equipped with intelligent forwarding software. The established application Interface (API) automates the flow of the data traffic through the vEPC (one in every gNB for each MNO) directly to the UE of following trucks of the platoon. This can be facilitated by the use of the platoon ID existing in the application server hosted by the MEC of each of the MNOs. The ID of the platoon has a list of the following trucks in the form of UIDs. To support this concept an advanced traffic analyser running (pre-existing) in the MEC server is needed to identify the data streams. The UID will be injected in the TCP headers of the data streams, so these TCP headers of the traffic flow in the platoon are identified by the traffic analyser of the MEC server.

Service continuity is ensured for the application when the platoon is passing the border via Local Breakout to the MEC server. The ALTO solution to support this will be examined. ALTO, standing for Application Layer Traffic Optimization, is an IETF working group aiming to produce a protocol for optimizing peer-to-peer traffic. In ALTO, a server provided by the ISP gives clients directions to the nearest location of a requested resource. These directions can take for example pricing as well as the network topology into account.

Local Breakout enables an MNO to break out internet sessions into its own network, to provide inbound roamers with an ability to connect to internet via the visited network of this MNO. It enables inbound roamers to receive data services directly from the visited mobile network instead of tunnelling back to the home network. It offers lower latency experienced by the roaming device and has a lower GRX bandwidth requirement between the home network and visited network.

High-level architecture of the roadside & cloud infrastructure

This user stories consist of two scenarios: (1) truck platooning with "see-what-I-see" functionality and (2) truck routing in customs site. The architecture diagrams for these scenarios are shown separately in Figure 16 and Figure 18, respectively, along with Figure 17 and Figure 19 depicting an overview of these scenarios.

Truck platooning with "see-what-I-see": Once the trucks that are destined to travel on the same route for a certain amount of time (either because there are no exits from the road being traversed or this information is provided by a common application used by all vehicles) make the decision to form a platoon, the follower trucks adjust their manoeuvre based on the V2V messages shared by the leader truck which convey its heading, speed, location and intentions such as breaking and acceleration.

The leading vehicle interfaces with the "see-what-I-see" application on the streaming server in the cloud to trigger the procedures necessary for provisioning of the resources for the platoon being formed. The application is tasked with transferring the streaming video of the road view of the leading truck to the ones that follow. Hence it always needs the identities of all vehicles in a platoon (leading and following trucks) and where there might be a change of roles and members during the lifetime of a platoon. Video transmission is initiated from the leading vehicle in the uplink and continues in the downlink to the followers via the 5G network, which can support the data rates required for 4K videos. Figure 16 shows the architecture to support network handover and video streamer handover for a platoon crossing a border.

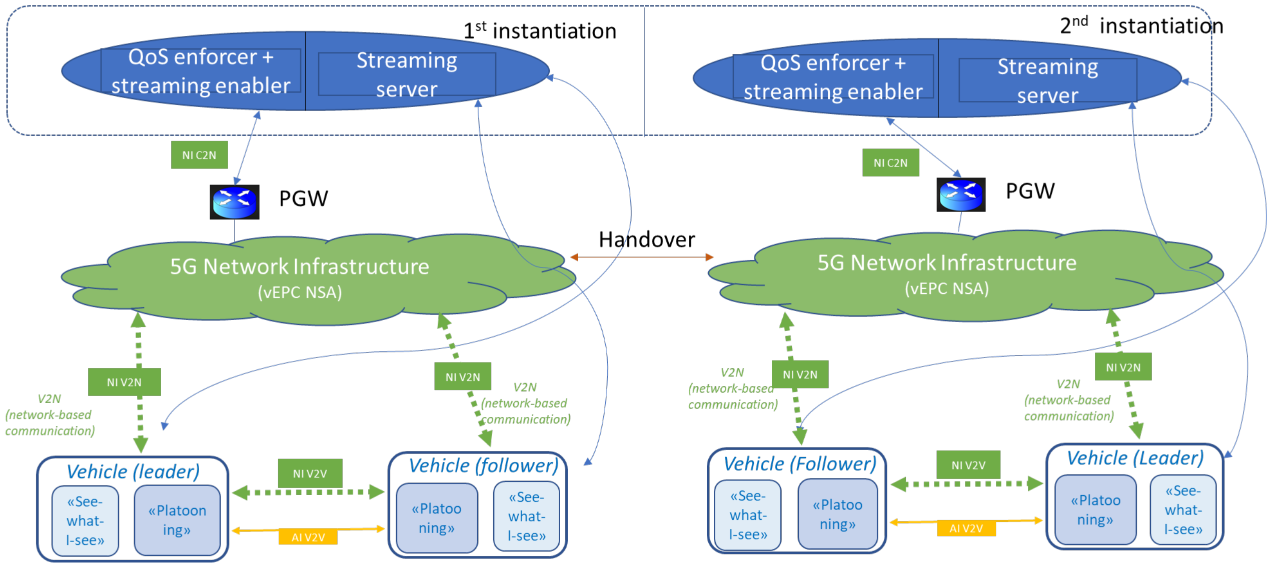


Figure 16 The high-level architecture of the cloud infrastructure for the truck platooning with "see-what-I-see" functionality user story.

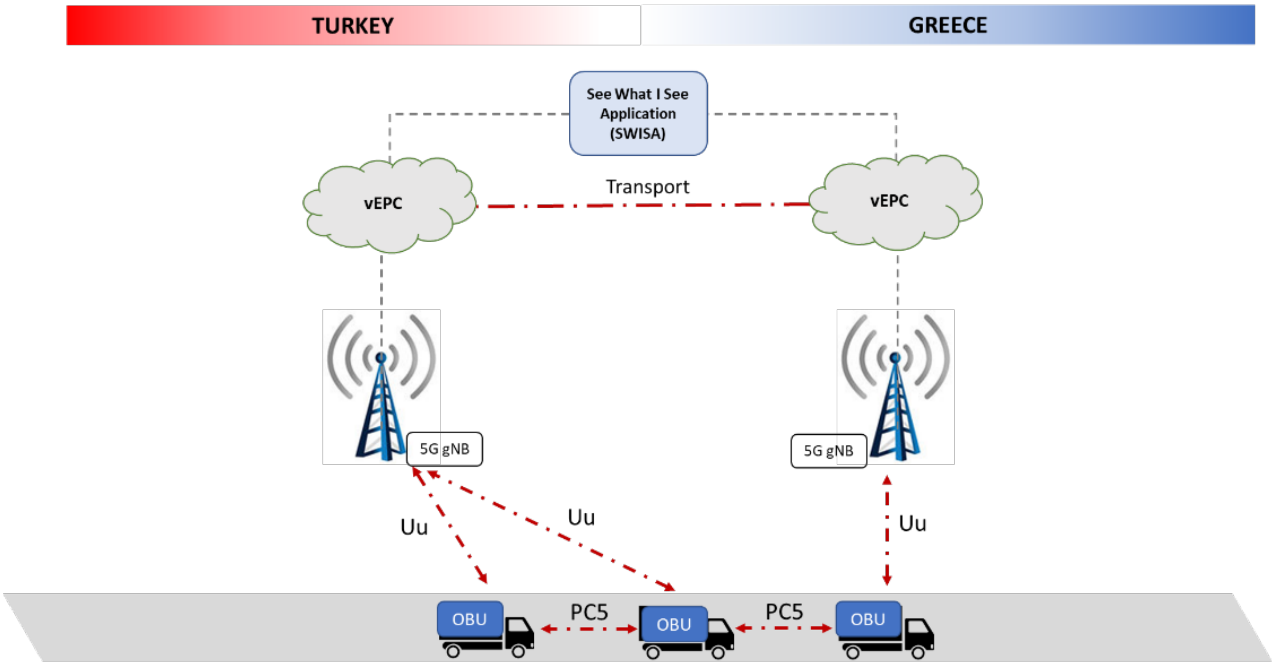


Figure 17 Overview of the truck platooning with "see-what-I-see" functionality user story.

Truck routing in customs site: The truck platoon will dissolve at the TR-side site entry gate just after getting the related message via PC5 interface of RSU located near this entry gate. The Plate Recognition System (PTS) will read the license numbers of the trucks at the gate and will register the trucks' entry to the site.

One of the trucks will be directed for the x-ray inspection and this truck will drive autonomously and without driver through x-ray inspection. After the passport check of the driver, the driver will leave the truck and the driverless truck will make its way into the x-ray building, autonomously, with the help of the sensors located between x-ray building and passport control point. Those sensors will be connected to RSUs and RSUs will send sensor data to the Cloud via a 5G base station.

Driverless entry and exit to the x-ray building will bring extra radiation safety for the drivers and operators. However, the real benefit will be the increased speed at the operations; the driver will not need to walk in and out of the radiation safety zone to leave and get back to the truck. Thus, it will be shown that a continuous flow of the trucks can be achieved through the x-ray building, resulting significant time gains which means more trucks can be scanned per day, increasing security.

The driver gets back in the truck after the scan and drives the truck to the exit. The platoon will again be formed after the GR-side site exit gate.

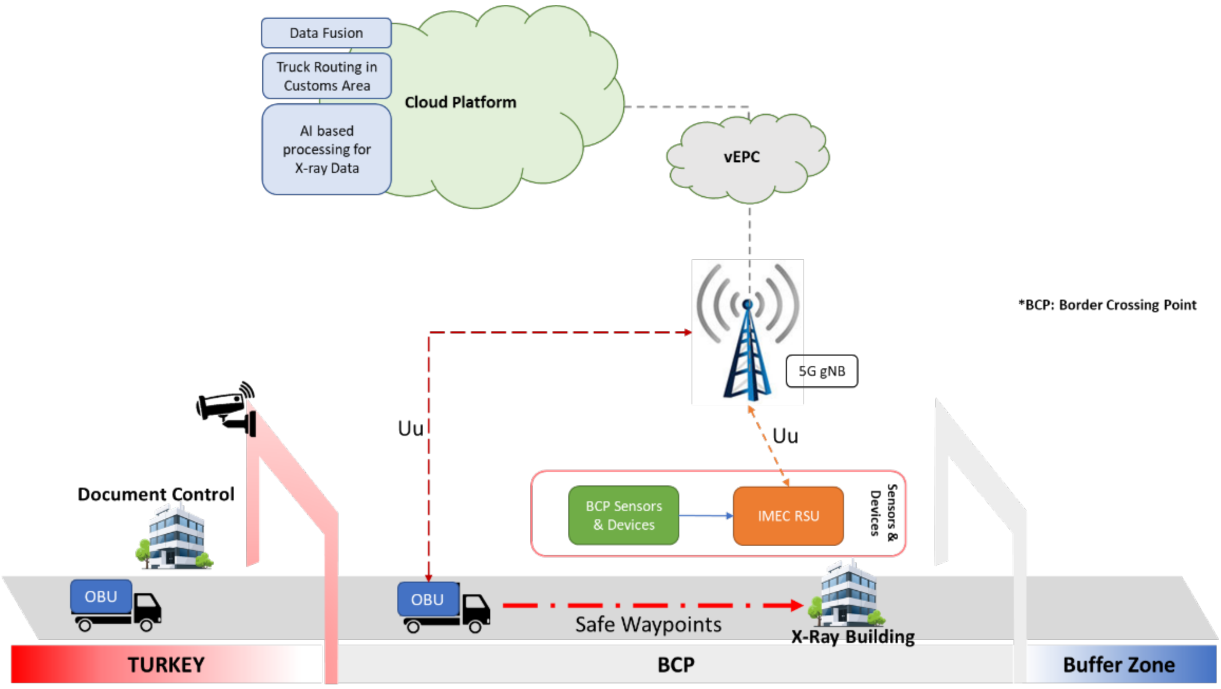


Figure 18 Overview of the truck routing in customs site use case.

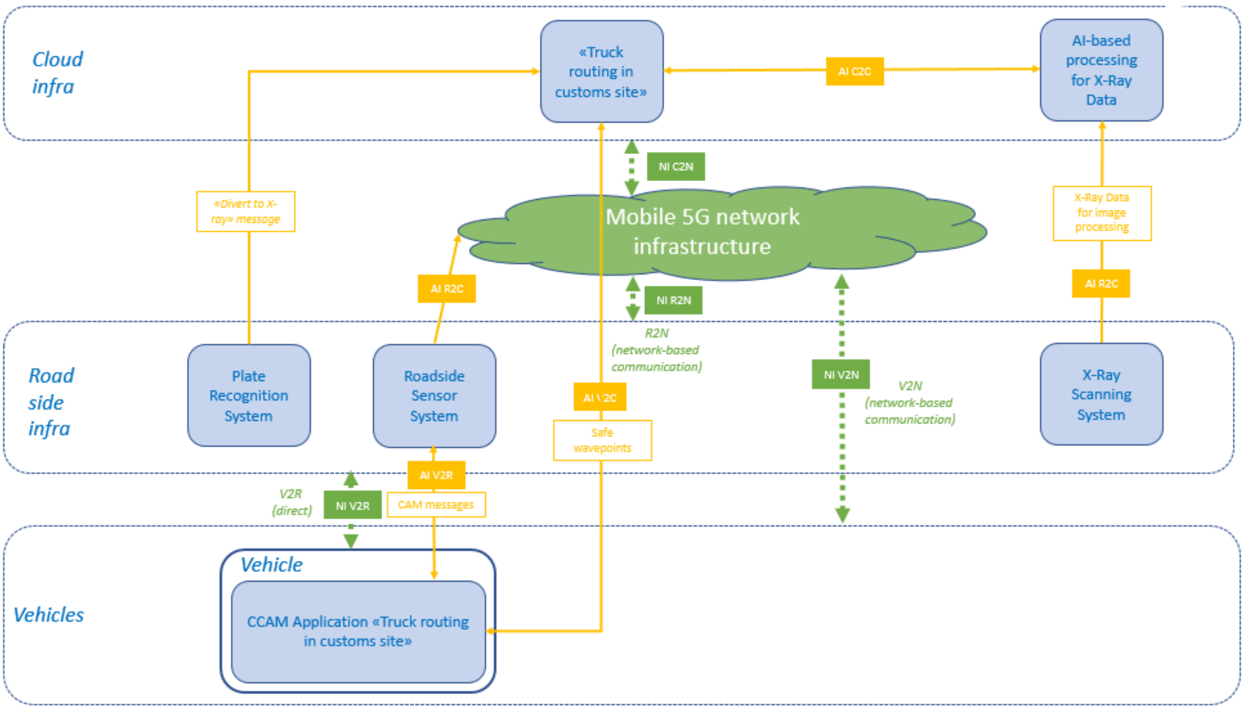


Figure 19 The high-level architecture of the roadside and cloud infrastructure of the truck routing in customs site use case.

Sequence diagrams

The truck platooning with “see-what-I-see” function user story demonstrates a close coupling between the C-V2X and 5G technologies, where the platoon members that communicate through V2V messages to operate the convoy exchange video over the 5G network. The platoon leader has a crucial role in this user story for informing the “see-what-I-see” application about the presence of a platoon and its members as well as being responsible from the manoeuvres of the platoon on the road. The sequence diagram in Figure 20 illustrates how this flow of information takes place between the relevant parties.

Interface specifications

The two sub-user stories employ a number of network and application interfaces as already represented in the high-level architecture diagrams in Figure 16 and Figure 17.

- *Platooning*: When operating in an infrastructure-less mode (see D2.2 Section 2), the maintenance of the platoon is ensured by the direct communication between the leader and the followers over the NI V2V interface. In the application domain, AI V2V interfaces should exist between the platooning applications inside the vehicles. In case a network coverage is also present, vehicles should connect to the 5G core network to receive the necessary authorization and configurations using NI V2N.

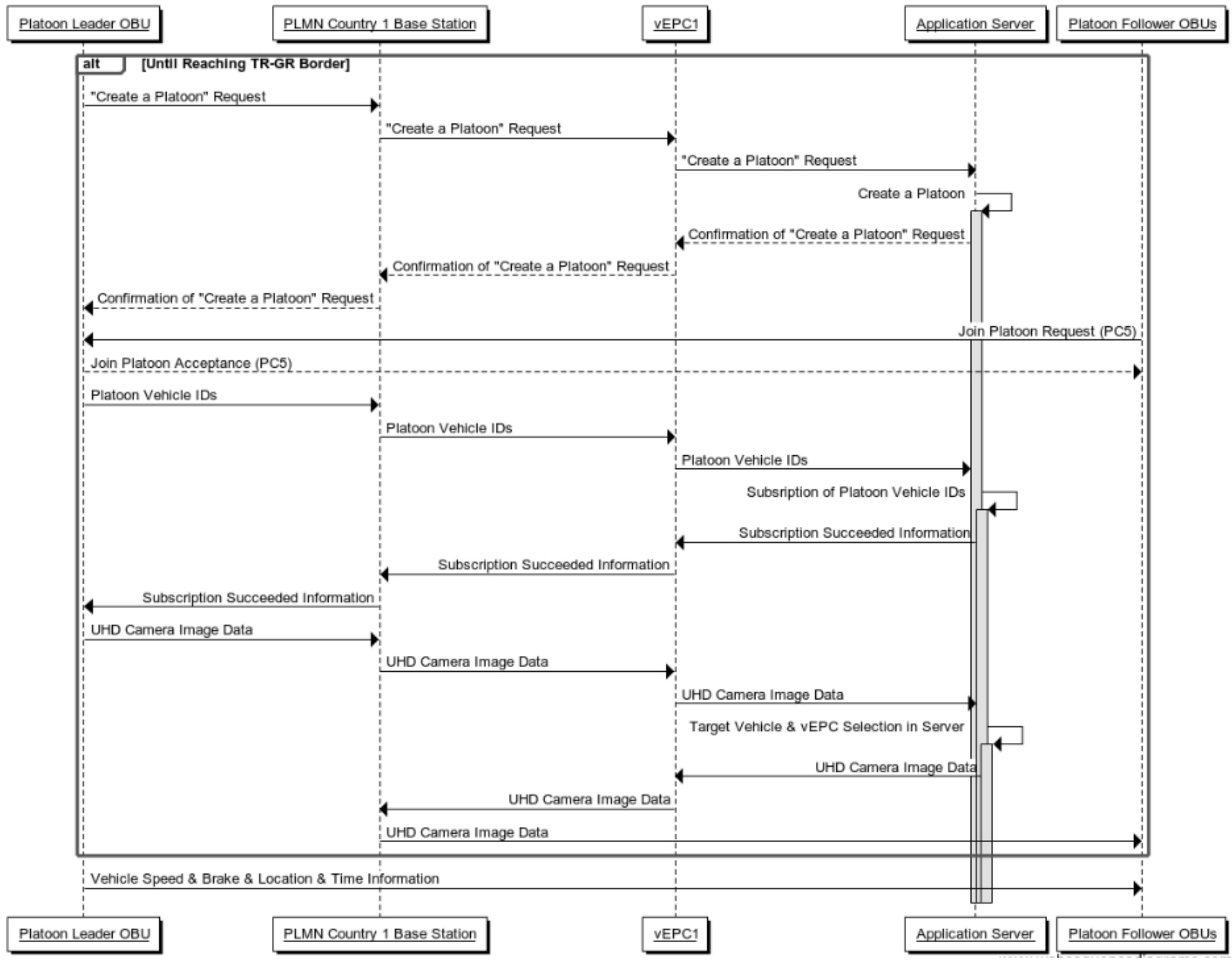


Figure 20 Sequence diagram for the platooning user story with "see-what-I-see" functionality

- *"See-what-I-see" functionality*: The application, which resides in the cloud is reached through the 5G network, and hence NI V2N interfaces and a NI C2N interface between the 5G core network and the cloud are necessary. The application interfaces are the ones that are formed between the applications on the vehicles and in the cloud: AI V2C.
- *Plate recognition system*: The plate images captured rough the camera that is positioned at the entrance of the border crossing point are sent to the application on the cloud using the NI R2N and NI C2N interfaces while an AI R2C interface is established between the systems on the roadside and in the cloud.
- *AI-based processing for X-ray data*: When the autonomous vehicle reaches the X-ray building, the images are transferred to the image processing application in the cloud with NI R2N and NI C2N interfaces. There must be an AI R2C interface between the roadside and cloud applications.
- *Truck routing in customs site*: The driver of the vehicle initiates the truck routing in customs site application after the plate recognition system grants access to the border-crossing zone to the vehicle. Thus, although the application does not interface with the plate recognition system, it has to connect to

the X-ray application in the cloud through the AI C2X interface, where the X-ray-based decision output is also fed to the truck routing application to determine the next checkpoint visit. The manoeuvres are transferred from the cloud application to the vehicle using the AI V2C interface while the roadside sensors require AI V2R and AI R2C interfaces with the vehicles and the cloud, respectively. For connectivity, NI V2R, NI V2N, NI R2N and NI C2N interfaces are utilized.

Detailed specifications

Truck platooning with "see-what-I-see": The key element of this user story is the "see-what-I-see" application, which receives the platoon information from the leader and coordinates the transmission of the video stream sent by the leader to the followers. The design will take into consideration the characteristics of the camera deployed on the leader vehicle as well as the speed and latency requirements of the user story to determine the optimum choice of codecs and interfaces as well as the positioning of the application server.

Truck routing in customs site: The plate recognition system, the X-ray image processing application and the sensor fusion-based truck routing application, which determines the safe waypoints inside the customs area are the three main pillars of this sub-user story. Also, the roadside units whose specifications are explained in more detail in Section 3.4.2. are placed in the border crossing zone to feed sensor information to the truck routing application.

Cross-border aspects

While the truck routing in customs site sub-user story is expected to take place inside the border crossing zone which is likely to be under the coverage of a single operator, the truck platooning scenario requires a "see-what-I-see" application design with roaming support.

3.3.3. Trial sites specific contributions to CBC for Vehicles Platooning

Table 15 gives an overview of the specific roadside and cloud infrastructure to support the user stories for Vehicles Platooning, as described in section 7.

Table 15 Overview of roadside and cloud infrastructure per user story for Vehicles Platooning

User story	Roadside sensors /actuators	Roadside comm. units	Cloud infrastructure
GR-TR US4 (Platooning with "see what I see" functionality in cross-border settings)	n/a	n/a	Video distribution system; platoon registration system
DE US7 (eRSU assisted platooning)	Yes, roadside sensors (cameras, other sensors) for traffic analysis, road-condition, object detection	Yes, eRSU	Edge Dynamic Map server (eRSU) with 3D map info (including traffic light status)
CN US16 (Cloud-assisted platooning)	n/a	Yes, RSU	Central system for platoon leader (path planning, etc.)

Summary:

- Roadside/cloud infrastructure is not used for (direct) information exchange to support driving during platooning (position, speed, brake)
- Cloud infrastructure is used in different ways to support platooning, e.g. via dynamic map updates, route planning, and network-based support for "see-through"

The table below shows the trial-site specific contributions to the CBC.

Table 16 Trial sites specific contributions to CBC for Vehicles Platooning

	DE User Story (US7)
RSU	Extended RSUs (eRSU) with MEC as 5G UE enable RSU assisted V2V communication (C-V2X) among AVs.
Roadside sensors	Portable sensor platform (traffic analysis, road condition, environment, weather) providing added perception to enhance platooning operations.
MEC	MEC component integrated with eRSU enables offloading of streaming services to roadside resulting in low delay V2X communication.
Cloud Systems	Microservice platform enhances CBC's cloud computing infrastructure with PaaS supporting multi-tenant resource sharing among CCAM service providers.
Application	CCAM service (360° view, LDM, EDM), Microservice platform (MEC agent, management &

	orchestration)
Other	n/a

3.3.4. Specifications on Application Interfaces for Vehicles Platooning

Application Interface AI V2R and AI V2V (direct communication)

Within ETSI a pre-standardization study on platooning is underway. The results will be published in ETSI TR 103 298 "Intelligent Transport Systems (ITS); Platooning; Pre-standardization study".

Platooning and Cooperative Adaptive Cruise Control (CACC) are enabled by adding wireless communication to already automated functionalities such as longitudinal and lateral control of the vehicle. Platooning encompasses both lateral as well as longitudinal control of the vehicle, whereas CACC usually addresses only longitudinal (brake and acceleration). Wireless communication between vehicles and smart infrastructure (V2X communication) enables a more precise control of the vehicle and it complements already existing on-board forward-looking line-of-sight (LOS) sensors such as radar, camera, and lidar. V2X provides the possibility to "see" beyond physical barriers (e.g. other vehicles) and to circumvent inherent LOS sensor delays. The idea is to receive information on the V2X sensor from vehicles in front and thereby, a smoother adaptation to for example speed differences can be made. In Figure 21 Overview of message flow for platooning from joining to leaving (source: ETSI TR 103 298) the proposed message flow for platooning is shown.

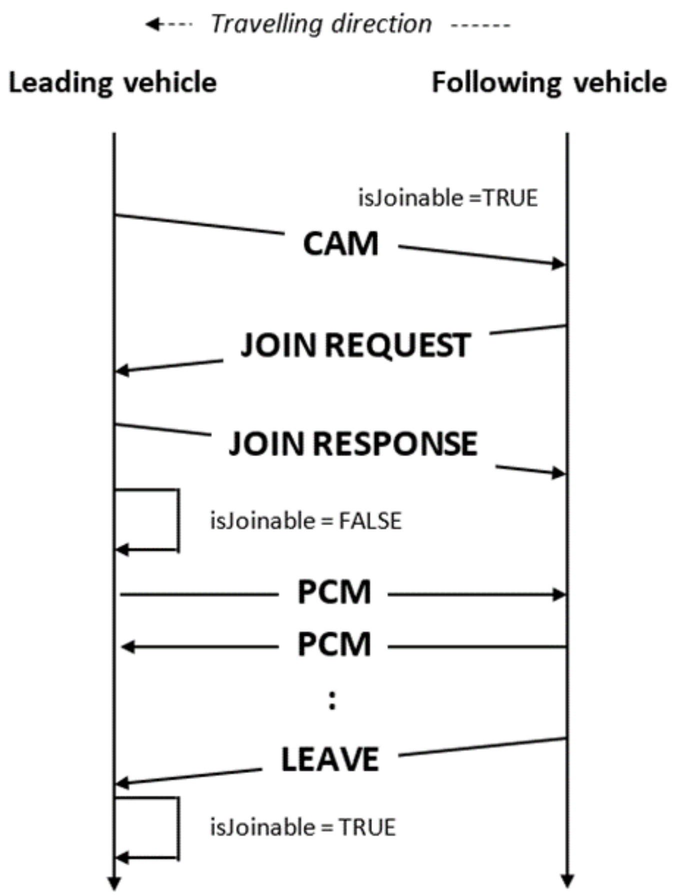


Figure 21 Overview of message flow for platooning from joining to leaving (source: ETSI TR 103 298)

The flow contains 5 types of messages that need to be specified in future work:

1. CAM extended with additional data frame on PlatooningContainer (isJoinable)
2. Join Request
3. Join Response
4. Leave
5. PCM – Platoon Coordination Message (at 20 Hz)

Within 5G-MOBIX non-standardized messages will be used.

Within ETSI a related pre-standardization study on CACC is active, see ETSI TR 103 299 V1.1.5 (2019-03) "Intelligent Transport System (ITS); Cooperative Adaptive Cruise Control (CACC); Pre-standardization study [Release 2]". This work is related to platooning, mainly on Platoon Coordination Message and the option of CACC to form a CACC string with multiple active CACC vehicles, like a platoon user story with multiple vehicles.

CACC is an in-vehicle driving assistance system that adjusts automatically the vehicle speed to keep a target time gap (in seconds) with a target vehicle (TV) while keeping a minimum safety distance with it. CACC makes use of data received from another vehicle ITS-Ss and/or from roadside ITS-Ss via ITS network. The CACC includes at least one ITS-S application (denoted as CACC application) that implements the application logic. The CACC application processes data received from other ITS-Ss and/or from on board sensors, automatically determines vehicle speed and acceleration, and accordingly transmits control commands to longitudinal control systems (e.g. brake, accelerator). In addition, the CACC application may be operating simultaneously with other in-vehicle assistance systems or with other ITS-S applications such as pre-crash system, lateral control system etc. CACC is connected to the in-vehicle network and has access to in-vehicle sensor data. The CACC can send control commands to acceleration/deceleration systems.

Multiple active CACC vehicles may follow each other, to form a vehicle group, denoted as CACC string in the ETSI TR 103 299 document. A CACC string operational environment may change dynamically e.g. a CACC string may be divided into two groups, may be combined with another CACC string to form a new CACC string, or a CACC string may be dismissed when all vehicles leave the string.

ETSI TR 103 299 describes the CACC message: CAM messages extended with additional data elements. The position and time information in CAM should be updated at minimum of 30 Hz, i.e. higher than the frequency of CAM between 1 and 10 Hz.

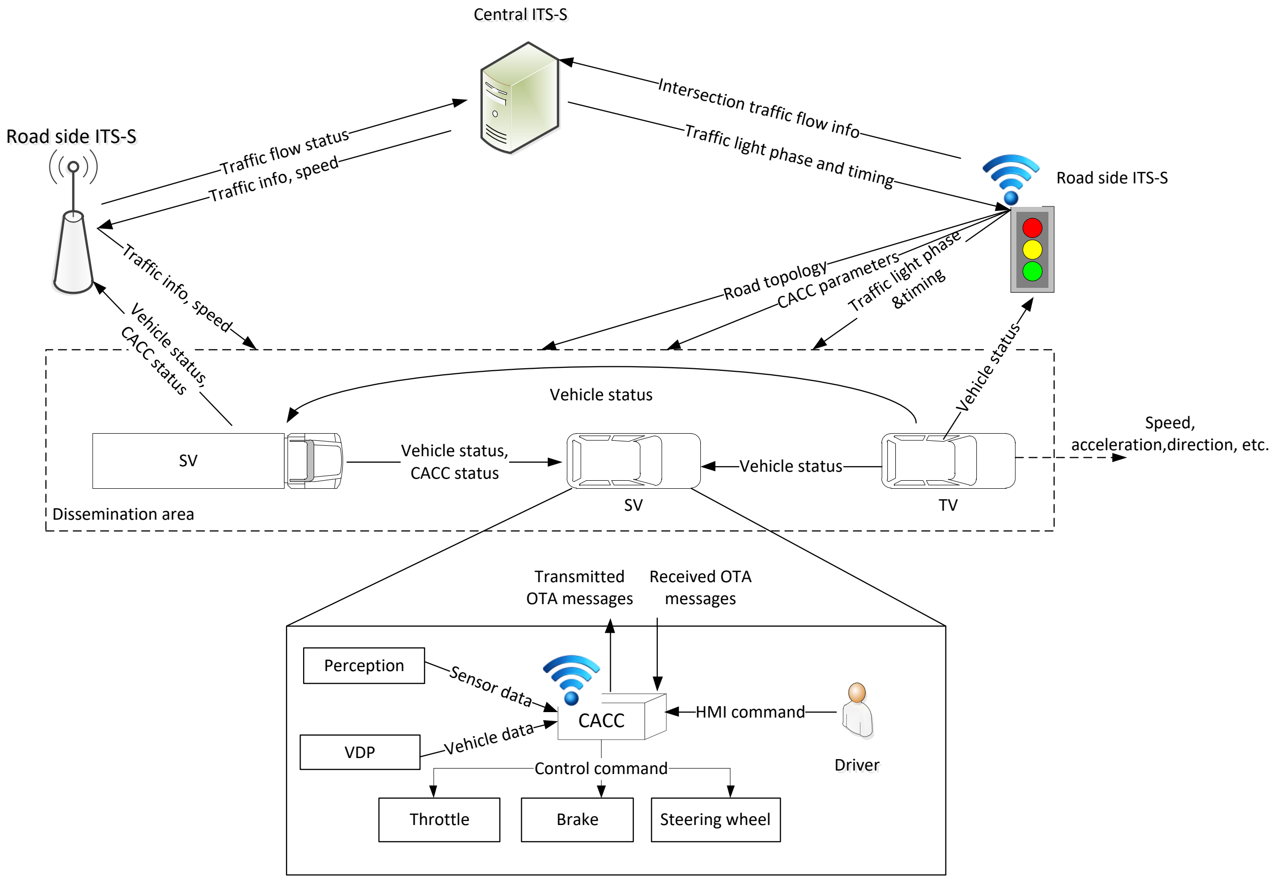


Figure 22 CACC information architecture (source: ETSI TR 103 299)

Application Interface AI V2C, R2C and C2C

The message sets defined for the interface AI V2R and AI V2V for direct communication may also be exchanged via cloud systems via interface AI V2C and R2C and between cloud systems, AI C2C. A distributed CCAM collection and distribution server may be used to collect and forward messages from vehicle to nearby vehicles (V2C, for V2N2V) or from roadside or cloud systems to vehicles, related to the geographical area where the information is relevant. In section 2.5.5 examples are given of these geo-messaging solutions.

3.4. UC Category 3: Extended Sensors

3.4.1. Description of UCC Extended Sensors

Extended Sensors "enables the exchange of raw or processed data gathered through local sensors or live video data among vehicles, RSUs, devices of pedestrians and V2X application servers. The vehicles can enhance the perception of their environment beyond what their own sensors can detect and have a more holistic view of the local situation" (Source: 3GPP TS 22.186 R16).

The following user stories are related to Extended Sensors:

- Extended sensors for assisted border-crossing (GR-TR US5).
- EDM-enabled extended sensors with surround view generation (DE US6)
- Extended sensors with redundant edge processing (FI US8)
- Extended sensors with CPM messages (NL US14)

3.4.2. Deployment architecture of CBC GR-TR for Extended Sensors

Description

The objective of the user story "assisted truck border-crossing & increased cooperative awareness" is to use the enhanced capacity, reliability and reduced latency of 5G networks in combination with advanced roadside infrastructure and vehicle intelligence to i) minimize the border crossing times of autonomous vehicles through customs inspection, ii) to facilitate the actual inspection through intelligent fusion of distributed data originating from the vehicle itself as well as from the roadside infrastructure, iii) to enhance the environmental awareness of the vehicles driver through enhanced "live" maps and iv) to increase the safety and security of customs personnel against automotive accidents. To achieve these objectives, the combination of 5G networks, roadside and cloud infrastructure and CCAM-enabled vehicles is necessary to provide Big Data collection and processing capabilities as well as reduced reaction times.

A multitude of roadside sensors varying from street cameras, smart phones and road sensors to thermal cameras and drones are capable of providing huge amounts of data, which may be combined with other sources of data (e.g., data coming from the vehicles or from third parties through the 5G network) to create a detailed image of the surroundings of the customs / border environment and to make intelligent decisions regarding potential actions to be taken, as explained in the detailed user story description in 5G-MOBIX D2.1. These intelligent decisions can be delivered within a few milliseconds to the involved parties (vehicles, customs agents) taking advantage of the 5G network's capabilities, and hence meeting the stringent requirements for CCAM operation.

In this deliverable we describe in detail the roadside infrastructure (road / environmental sensors, street / thermal cameras, smart phones, wearables, etc.) and cloud infrastructure (AI/ ML data processing and predictive analytics platform) that make the "assisted truck border-crossing & increased cooperative awareness" feasible, as well as the fashion in which they communicate between them and with the 5G network.

High-level architecture of the roadside & cloud infrastructure

The high-level overview of the CCAM infrastructure for the "assisted truck border-crossing & increased cooperative awareness", as well as its interconnection to the 5G network is shown in Figure 23 while Figure 24 depicts the high level overview of the GR-TR cloud platform, WINGS's STARLIT (**S**mar**t** living pl**a**tform powered by A**r**tIficia**l** **i**ntelligence & robus**t** iot connectivity) which will provide the assisted driving functionality necessary for the completion of the trial.

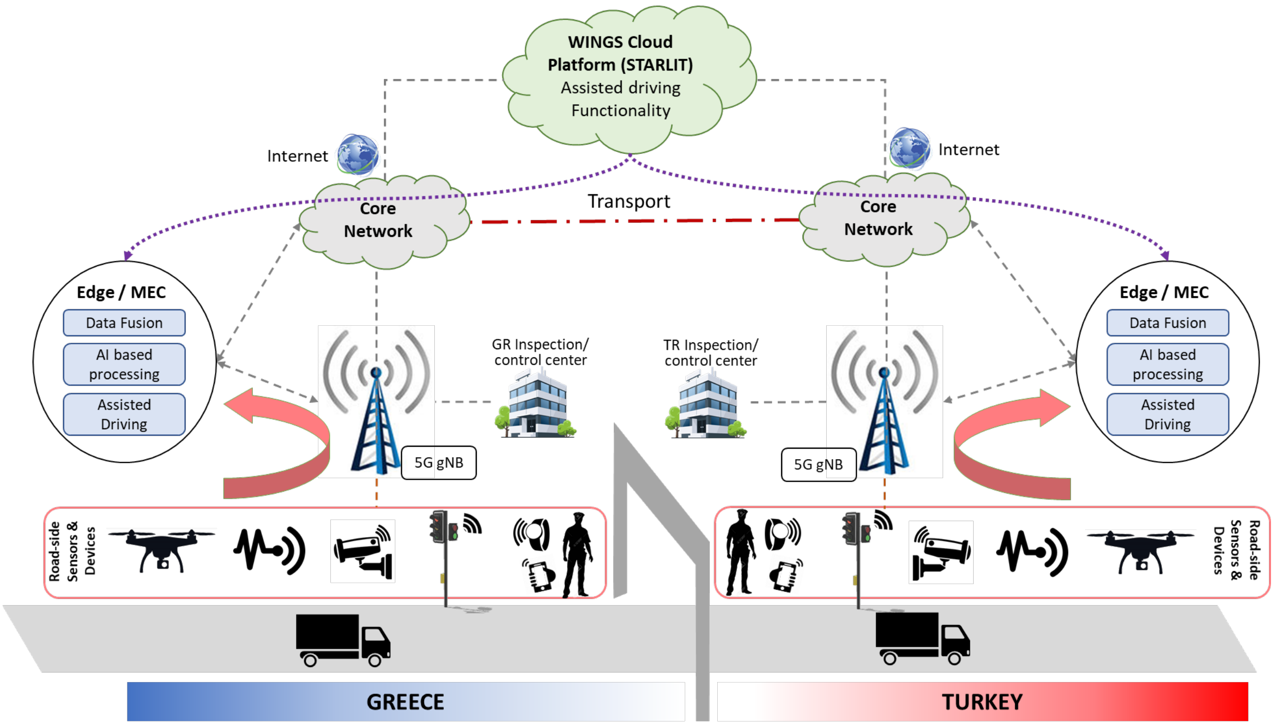


Figure 23 Overview of the roadside sensors & Cloud infrastructure for the GR-TR user story "*assisted truck border-crossing & increased cooperative awareness*".

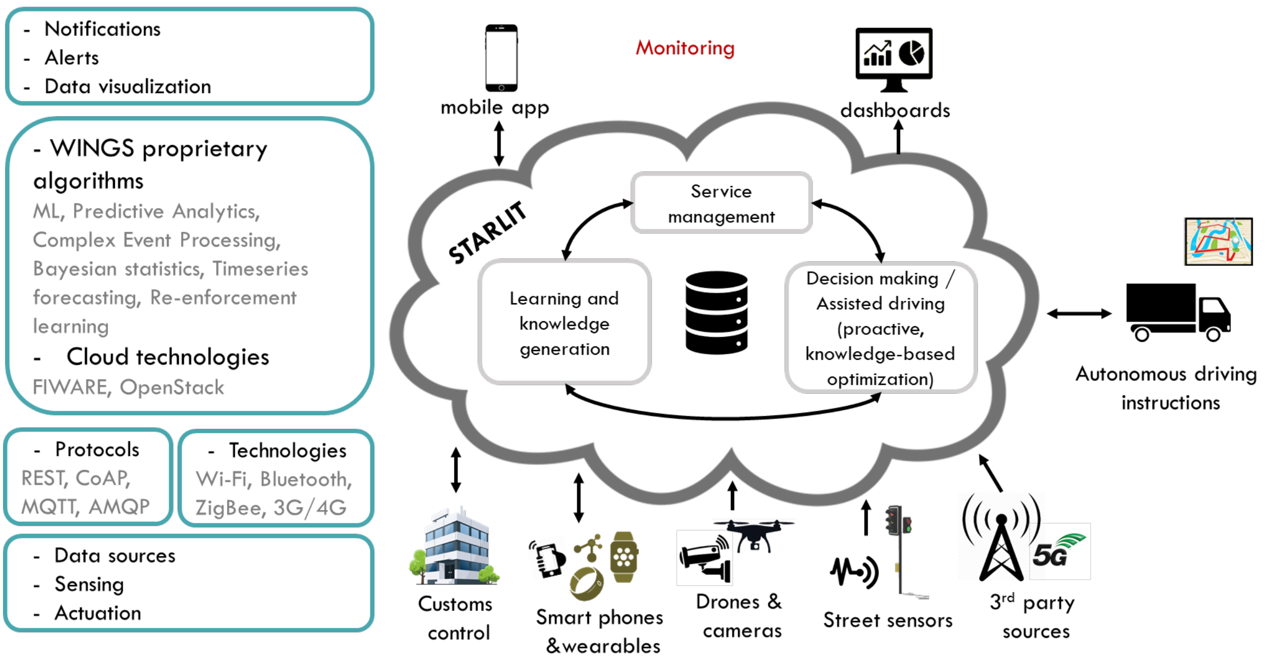


Figure 24 Assisted driving platform overview for the GR-TR user story "*assisted truck border-crossing & increased cooperative awareness*".

As can be observed from the above figures, a series of heterogeneous sensors and devices will be either statically deployed across the GR-TR trial site on both sides of the border (e.g., road / environmental sensors, traffic lights sensors, street cameras, etc.) or will be available for on-demand deployment, activated by the platform's intelligence (e.g., drones). The collected data from these sensors will be transmitted to the GR-TR cloud platform offering the assisted driving functionality and residing in the cloud. The data will be able to be transmitted via mMTC (road sensors) or eMBB (street cameras) slices once the 5G network in the trial site is operational. Based on the collected data, it can be determined that a vehicle / truck is approaching the border and that it hence will need assisted driving services as well as international hand-over preparations. In this case, partial or the complete assisted driving functionality can be downloaded from the cloud to the edge / MEC server (see Figure 25) at the border site so as to minimize the transmission and reception time of data to and from the roadside infrastructure and the vehicles, thus achieving ultra-low latencies. Once the 5G network in the trial site is operational, the decisions / autonomous driving directions of the GR-TR cloud platform will be transmitted to the vehicle / truck over a URLLC slice.

Further details regarding the exact roadside equipment to be used as well as the architecture of the GR-TR cloud platform are provided in the next sub-sections.

Sequence diagram

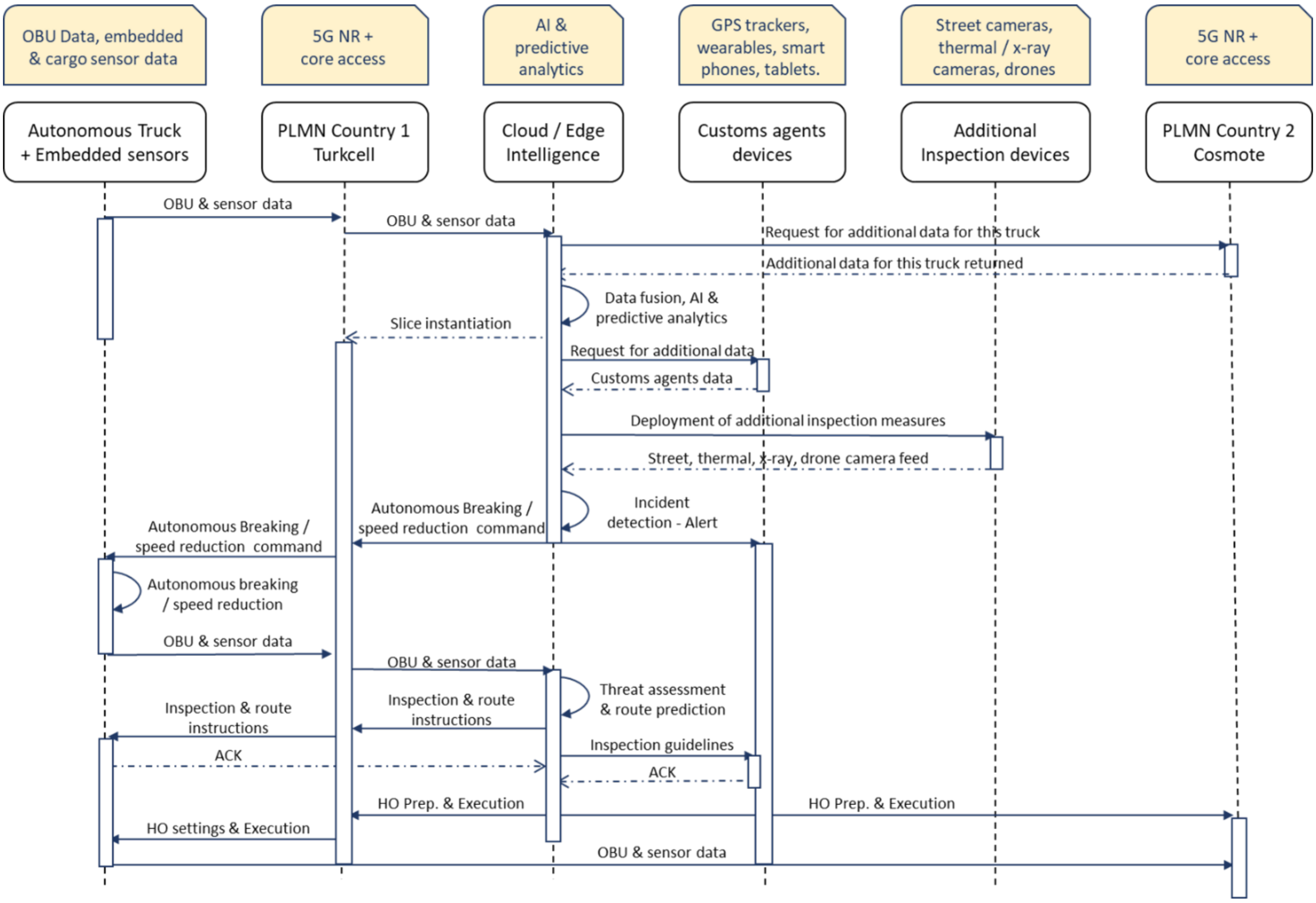


Figure 25 Sequence diagram for GR-TR US5 Extended sensors for assisted border-crossing

Detailed specifications

The GR-TR platform is a cloud-based platform focusing on smart city aspects. It interacts both with sensors and actuators and comprises of: (i) Capabilities for self-management of services/application to facilitate greater flexibility, reliability and robustness. (ii) Machine learning functionality (e.g. Bayesian statistics, timeseries forecasting, Self-organising maps) for building knowledge and predicting contextual factors (e.g., traffic, pollution, parking space availability, user's vital signs evolution, etc.). The derived knowledge can be exploited for reliable raising of alarms, efficient recommendations and application and system configuration. (iii) Decision making capabilities for the autonomous selection of the optimal application configuration actions considering current context, user profiles and knowledge. Figure 26 provides a more detailed view of the functional architecture.

The GR-TR platform can combine data from various **devices** (e.g. cameras, smartphones for crowdsourcing, sensors for monitoring temperature, humidity, luminosity, indoor and outdoor air quality, parking availability, wearables for monitoring biometric data, etc.) and automatically control different types of actuators, such as lights, heating/cooling, but also robots and Automatically Guided Vehicles

(AGVs). The GR-TR platform leverages **diverse communication technologies and communication protocols**. In terms of cloud deployment, the components can be deployed as Virtual Machines and Docker Images.

The platform's **Data ingestion and management** comprises various functionalities for deriving the data from the various devices and delivering them to any other platform components, services and applications as well as triggering actuators. **Device management** and **Virtual Entities (VEs)** enable the abstraction of the heterogeneity of the underlying infrastructure in terms of sensors, actuators and other devices and data sources to facilitate the management, addition, removal or enhancement of devices in a dynamic manner (i.e. without causing system "downtime"). The **Broker** and **Real-time stream processing** enable the efficient exchange of data between devices, other platform components, services and applications and visualisation dashboards.

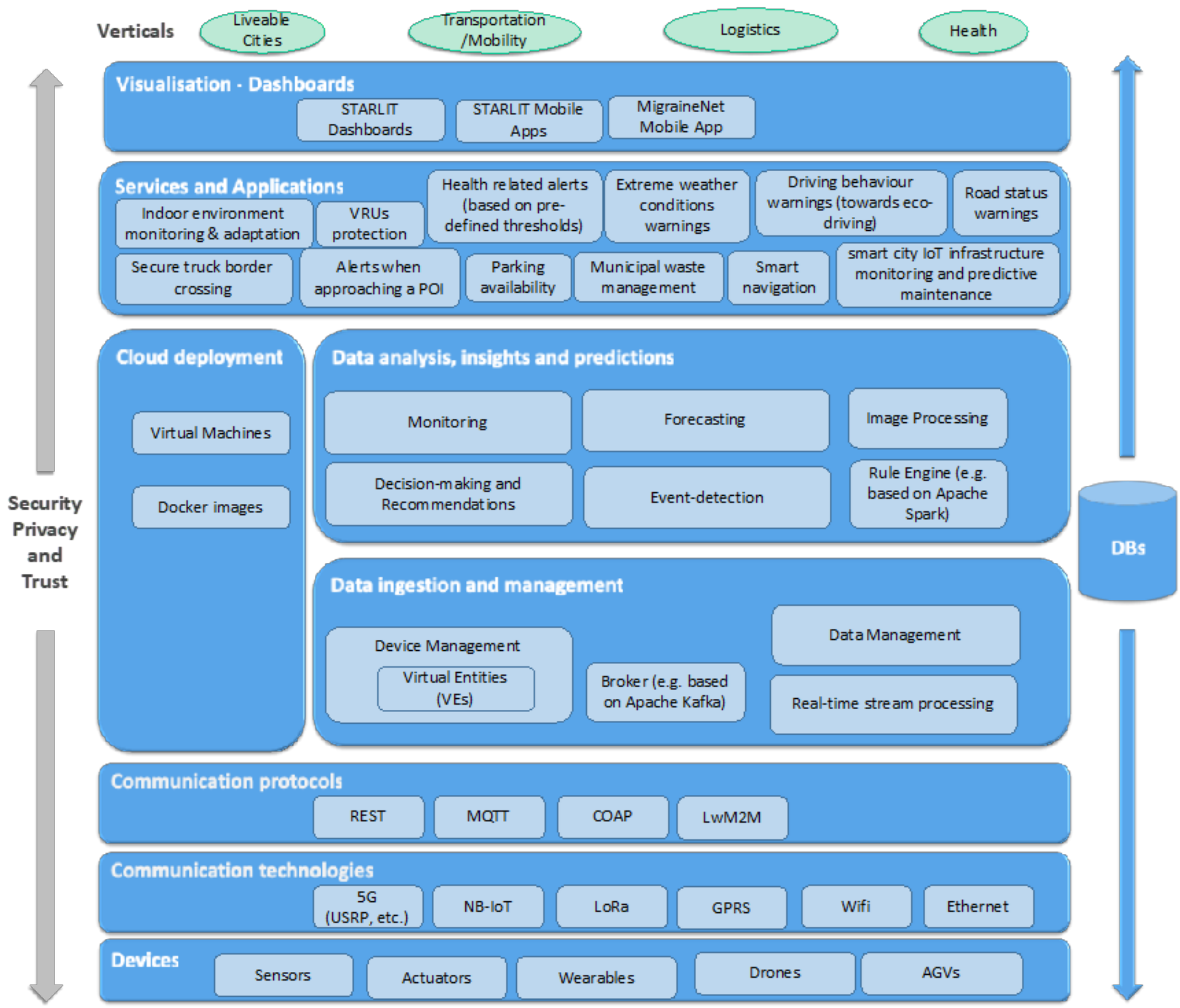


Figure 26 GR-TR cloud platform functional architecture

The data ingested into the system is processed but also stored in a hybrid database system that comprises various types of **Databases (DBs)** (e.g. NoSQL, HDFS based, etc) for various types of information, such as raw data from devices, knowledge derived through data analytics and learning mechanisms, information on available devices and services.

Data analysis, insights and predictions comprise functionalities for **monitoring, event-detection, forecasting of events and issues, large-scale data processing, image processing and automated decision making**. Specifically, it comprises artificial intelligence and functionality for data analytics, learning, knowledge inference and reasoning to support autonomous behaviour and self-adaptation of applications. The aim is to achieve a) enhanced awareness with respect to external situation(s), operational context and human/social aspects, b) learning capabilities for building knowledge and experience related to situation and past application behaviour adaptation, so as to enable faster processing of data, more efficient and reliable behaviour adaptation and control, etc. and c) reasoning capabilities to support the optimal autonomous application/system behaviour adaptation, taking into account current context, knowledge and policies. The Data analysis mechanisms run continuously, retrieving data from available data sources and applications and update the inferred data and knowledge stored in the platform databases. Methods for Artificial Intelligence and machine learning functionality for building knowledge and predicting contextual factors from data, which can be characterized (at least) by high-velocity/volume/variability), to empower decision making include Bayesian statistics, Timeseries forecasting, Self-Organising Maps (SOMs), Deep Learning, Re-enforcement learning, k-Nearest Neighbour(s) (k-NN).

On top of the various platform components and mechanisms presented above, various **services and applications** are offered to users and stakeholders, such as first responders and law enforcement agencies. As part of the GR-TR cloud platform applications **dashboards** are provided for visualization of measurements on interactive graphs and "heat-maps" that aim to present the overall city picture at a glance. This includes the visualisation of real time and historical data as well as forecasts/predictions. Dashboards are provided as a web-based UIs that can run from any tablet, smartphone or PC.

Finally, the platform integrates an OpenStack software module, namely Keystone for ensuring data **security and privacy** both at data and system level. In addition to the above, the platform communications among the services/applications/user interactions are secured and the data is transferred as encrypted payload.

In 5G-MOBIX, the platform will aggregate information from various sensors and other devices deployed or located at the broader border area. In specific, such sensors and devices involve cameras, drones, traffic lights (and ITS infrastructure in general), as well as personal devices, such as wearables and smartphones belonging to border officers and other pedestrians in the border area. These devices are expected to facilitate and significantly reduce the time needed for typical border crossing procedures or even enable "zero-touch" inspection. For instance, roadside cameras can be used to scan the vehicles' plates and keep track of the borders' load along with the support of drones; altogether they can identify a vehicle that approaches the borders and, particularly the drones, extract the load of each lane. This way, vehicles can be allocated optimally to a border lane, also considering whether they qualify for zero-touch inspection or not and proceed with automated driver and cargo checks. Traffic lights will also play their role here by sharing information like time-to-red and time-to-green. Information on the location and trajectory of borders' control officers and pedestrians in general completes the picture by ensuring that the route suggested by the platform to the vehicles takes the above into account. The aforementioned devices use appropriately instantiated 5G slices (e.g., eMBB slices for transmitting live video feeds from drones and roadside cameras, mMTC slices for transmitting traffic light signals and road users' locations) so that the captured data ultimately reach the platform, which is deployed in the cloud, and get further processed.

3.4.3. Deployment architecture of CBC ES-PT for Extended Sensors

The ES-PT corridor has two scenarios related with the Extended Sensors category:

- US1 (complex manoeuvres in cross-border settings):
  - Scenario 3: HD maps.
- US2 (public transport with HD media services and video surveillance):
  - Scenario 2: HD maps.

Description

The ES-PT CBC deploys two scenarios related with the Extended Sensors category, which consists of a real time update of the autonomous vehicle HD maps by other vehicles. The main difference between both scenarios is the vehicle in charge of the new map recording, which in the US1 is an autonomous vehicle, but in US2 is a connected bus (manual).

Those scenarios do not make use of roadside infrastructure; however, the cloud infrastructure plays an essential role in the map computing.

Figure 27 General CCAM infrastructure to support Extended Sensors scenarios on ES-PT CBC.shows a general diagram of the roadside and cloud infrastructure for those scenarios.

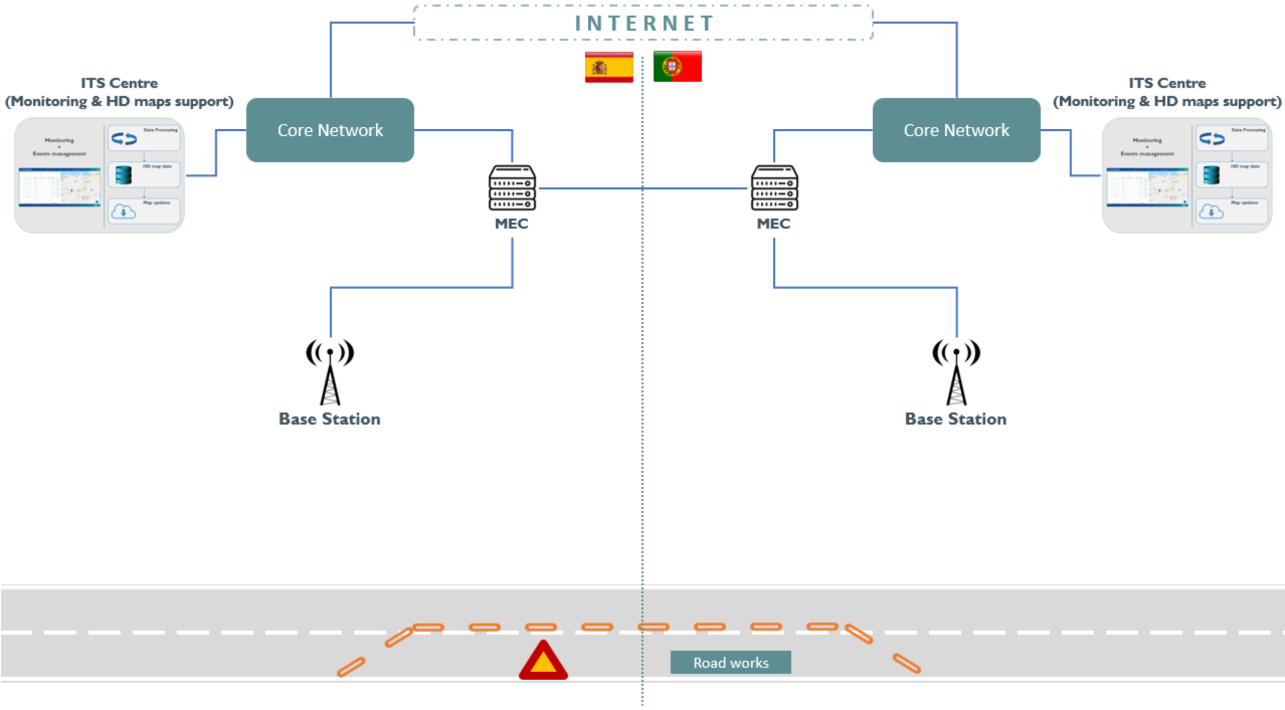


Figure 27 General CCAM infrastructure to support Extended Sensors scenarios on ES-PT CBC.

The objective of those scenarios is to take advantage of vehicles driving along a highway in order to maintain updated the internal map needed for autonomous driving in vehicles around. The procedure for this maintenance is to record an area which is outdated in the maps (i. e., due to occasional road works), then process those recordings in order to generate a new map of the area, and finally, share this map update with other autonomous vehicles.

High-level architecture of the roadside & cloud infrastructure

The high-level architecture of the CCAM infrastructure for the scenarios within this category is shown in Figure 28 CCAM architecture for the ES-PT Extended Sensors scenarios., where functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, and the information exchange is shown in brown. The architecture does not cover the cross-border aspects.

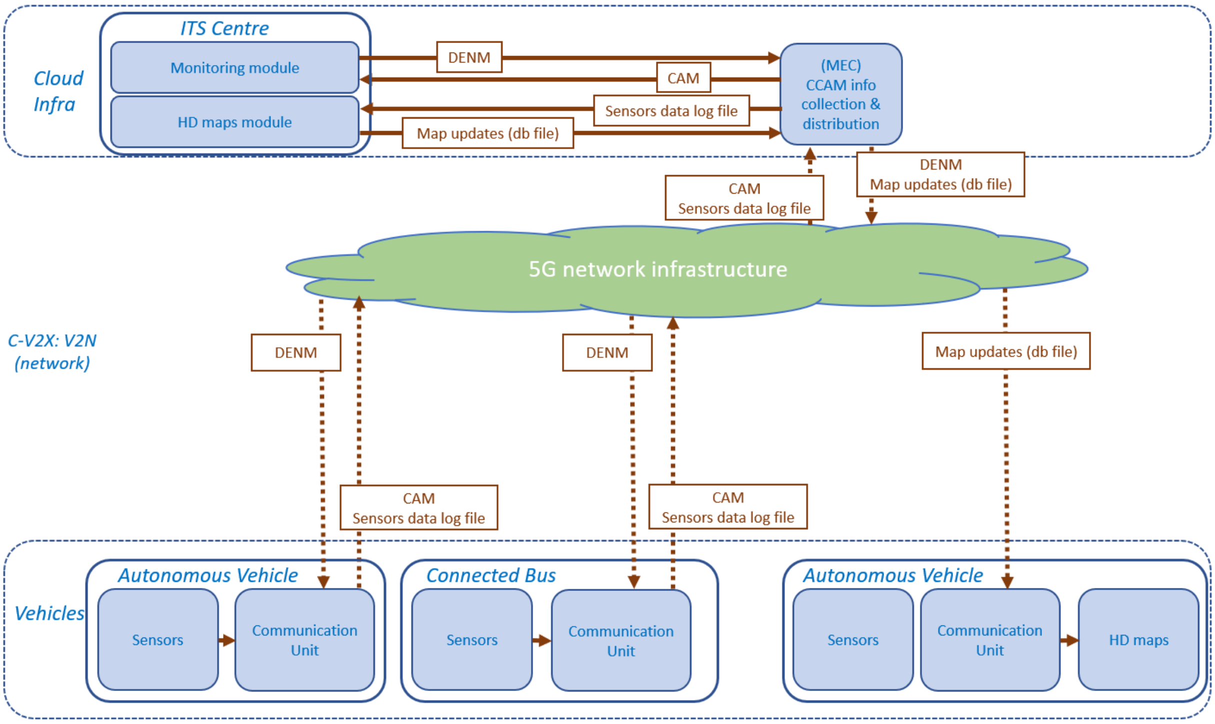


Figure 28 CCAM architecture for the ES-PT Extended Sensors scenarios.

The roadside and cloud infrastructure deployed in those three scenarios can be summarized in the following elements:

- MEC nodes: work as gateway nodes between connected vehicles and ITS Centers. MEC role is to forward both messages and sensor data packages from vehicles to the ITS Centre with monitoring or map updating purposes.
- ITS Centers: cloud applications running on each side of the corridor. Each ITS Centre is connected to the MEC node of the same country, and consumes the data passing through this node in order to monitor vehicles connected to the regional network. Furthermore, in those scenarios the ITS Centre hosts a HD map module which processes the sensor data packages from vehicles in order to update the general HD map. Then, the ITS Center shares the updated map with vehicles.

Sequence diagrams

Both HD maps scenarios considered under the Extended Sensors category are very similar, and follow this summarized sequence:

1. Firstly, the ITS Centre notify the first vehicle (AV or CV) of the existence of a road event.
2. Then, the vehicle is controlled manually along the road event, and at the same time, the vehicle records the sensor data outputs.
3. All the sensor data is packaged into a log file, and it is uploaded to the ITS Centre.

4. The ITS Centre processes the log file, fuses the sensor data and generates a new map of the area.
5. Lastly, the ITS Centre send map updates to all the autonomous vehicles near the road event.
6. Once those autonomous vehicles have updated its map, they are able to drive autonomously through the road event.

However, both scenarios have meaningful differences:

- User Story 1 Scenario 3 (HD maps): the main vehicle in this scenario is an autonomous vehicle. When it receives the road event notification, the vehicle checks if this event is already registered in its internal map. If the event already exists, it is already registered so the vehicle is able to drive autonomously along the event. Otherwise, it has to ask the driver to take the control for recording the new path.
- User Story 2 Scenario 3 (HD maps ALSA): the main vehicle in this scenario is a connected manual bus. When it receives the road event notification, it does not have maps unit for checking the existence of the event, so the bus always records the road event.

In the following figures, where different kind of vehicles are depicted (AV: Autonomous Vehicle) the sequence diagrams for the different scenarios are shown.

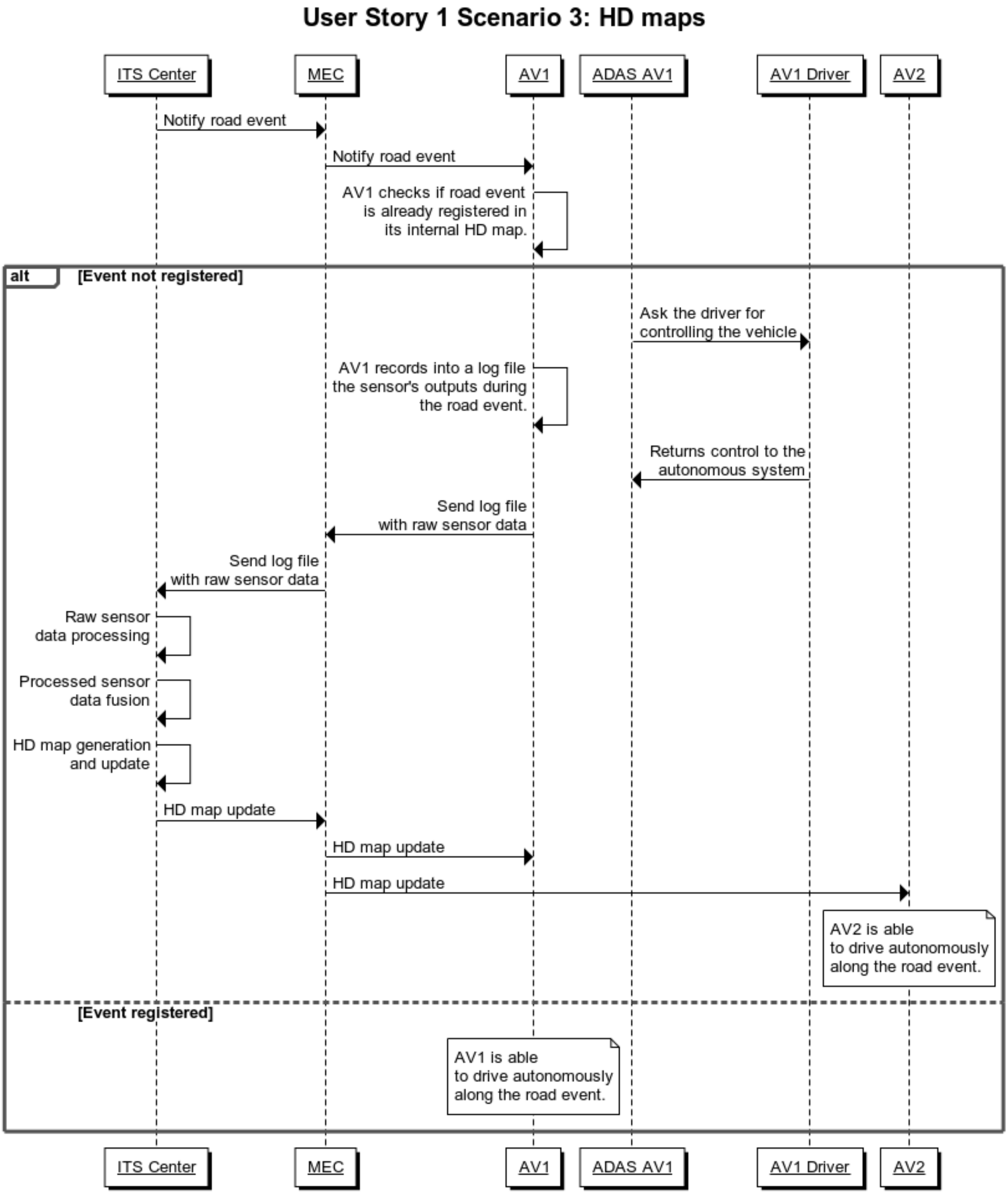


Figure 29 Sequence diagram of the HD maps scenario of ES-PT US1.

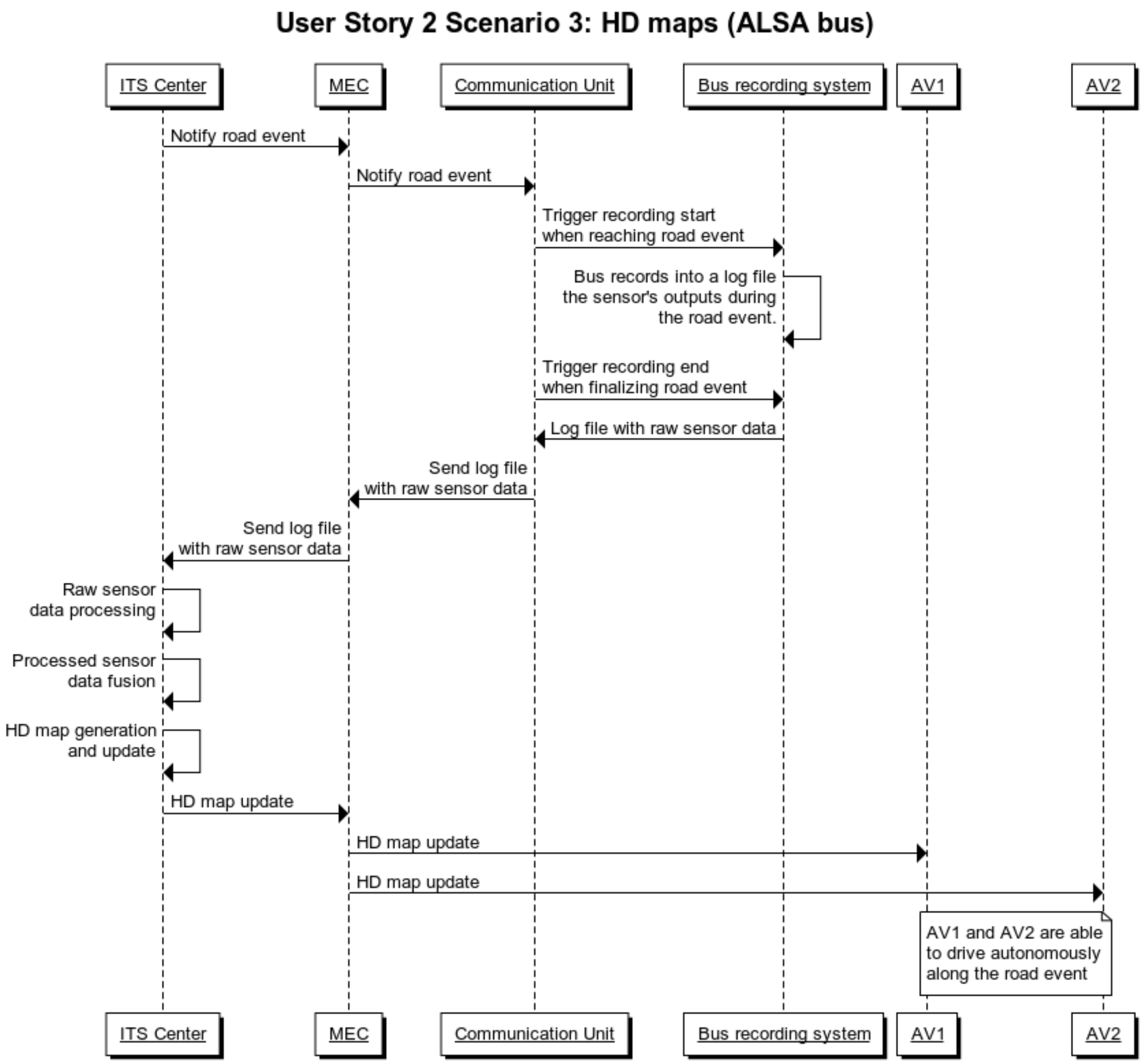


Figure 30 Sequence diagram of the HD maps scenario of ES-PT US2.

Interface specifications

The Extended Sensors scenarios of the ES-PT CBC are less focused in Vehicle-to-Vehicle communication (neither through the network, V2N2V), but are more concerned with transmitting high amounts of data on each communication. Figure 27 shows the communication links, technologies and type of messages used. All the interfaces used are briefly described below:

1) V2N (Vehicle-to-Network): vehicles send CAM messages containing their attributes (location, speed, heading, etc) to the MEC nodes (network). Furthermore, this link supports the transmission of the sensor data log files too.
2) N2C (Network- to-Cloud): MEC nodes forward CAM messages from connected vehicles to the ITS Centres with monitoring purposes. At the same time, MEC nodes act as gateways and redirect the sensor data log files to the ITS Centre in order to update the map.
3) C2N (Cloud-to-Network): ITS Centres send the map updates to the MEC nodes in order to be forwarded to the autonomous vehicles.
4) N2V (Network- to-Vehicle): MEC nodes act as gateways and forward the map updates to the autonomous vehicles.

Detailed specifications

Some of the elements mentioned in sections above are described in more detail as follows:

ITS Centre

The ITS Centre architecture overview is depicted in Figure 14, and more detailed information about the general architecture is available in section 3.2.2.

Regarding the Extended Sensors category, The ITS Centre hosts an application module for supporting HD maps scenarios. This module expects to receive data packages from vehicles containing raw sensor data. Then, the module processes this data, fuses the different sensors data and generates the updated HD maps. Finally, the module launches the map updates to the vehicles. Figure 31 shows the concrete architecture of the HD maps module inside the ITS Centre.

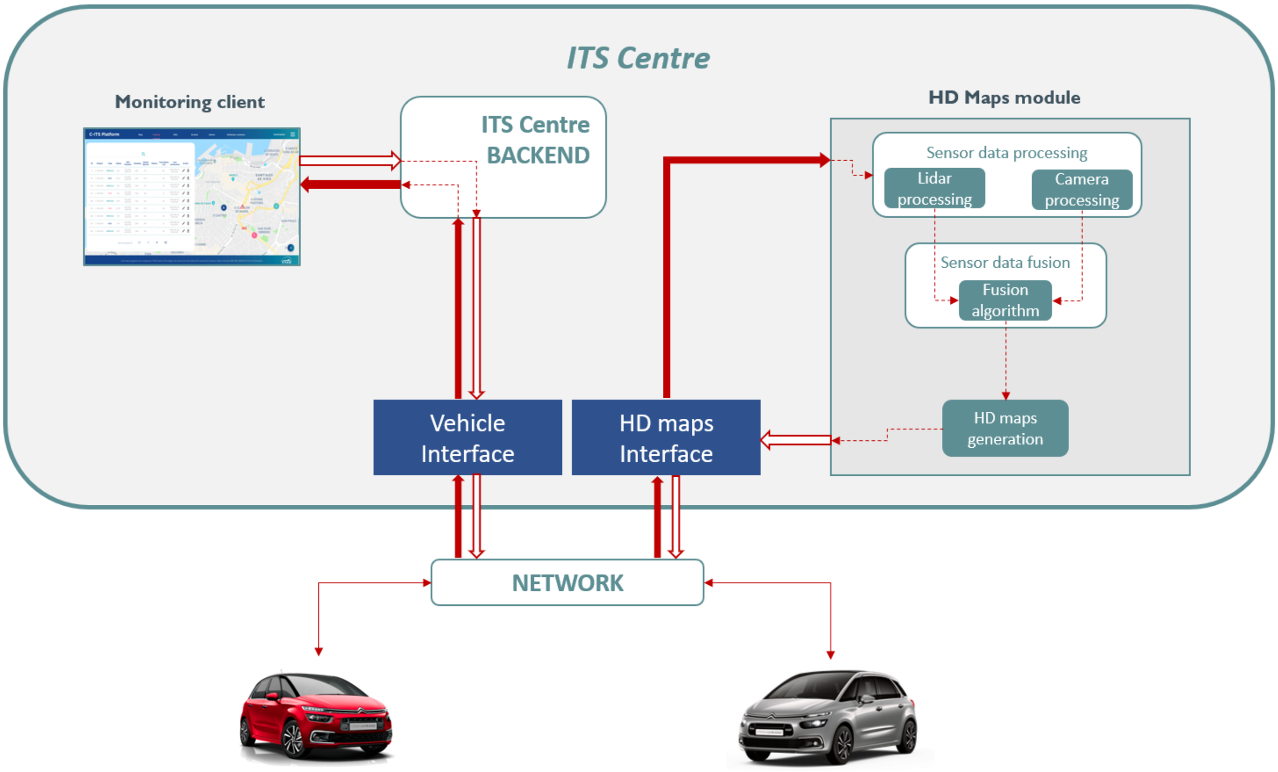


Figure 31 Architecture of the ITS Centre (HD maps support)

Cross-border aspects

The performance of the Extended Sensors scenarios in the ES-PT CBC requires:

- Interoperability between ITS Centres in Spain and Portugal, in order to share the maps in the cross-border areas.
- 5G eMBB and URLLC support with hand-over between edge servers from different MNOs.

3.4.4. Trial sites specific contributions to CBC for Extended Sensors

Table 17 gives an overview of the specific roadside and cloud infrastructure to support the user stories for Extended Sensors, as described in section 7.

Table 17 Overview of roadside and cloud infrastructure per user story for Extended Sensors

User story	Roadside sensors /actuators	Roadside comm. units	Cloud infrastructure
GR-TR US5 (Extended sensors for assisted border-crossing)	Camera for vehicle identification and localization (fixed or drone)	n/a	Cloud / Edge intelligence (collect data, data fusion, AI, predictive analysis, send inspection & route instructions)
EDM-enabled extended sensors with surround view generation (DE US6)	Camera for road monitoring	Yes (eRSU)	Edge node (eRSU) (for LDM/EDM and surround view distribution)
Extended sensors with redundant edge processing (FI US8)	n/a	n/a	Edge node with video processing and LDM distribution
Extended sensors with CPM messages (NL US14)	Camera for vehicle detection on ramp	n/a	Cloud (Collective Perception server to collect & forward)

Summary:

- The user stories on Extended Sensors use roadside systems (camera, radar, etc.) for collective perception. Also, sensor information from vehicles is exchanged between vehicles, via a network-based solution. Specifications on information exchange based on Local Dynamic Map formats and Collective Perception Service (with CPM) shall be aligned.
- Multiple trial sites use MEC node to support Extended Sensors for local collection, processing and distribution of information. Specifications to support MEC for CCAM application, MEC hand-over in a single PLMN and interconnection of MEC solutions in multi-PLMN may be aligned.

The table below shows the trial-site specific contributions to the CBC.

Table 18 Trial sites specific contributions to CBC for Extended Sensors

	DE US6	FI US8	NL US14
RSU	Extended RSUs (eRSU) with MEC as 5G UE enable RSU assisted V2V communication (C-V2X) among AVs.	n/a	n/a
Roadside sensors	Portable sensor platform (traffic analysis, road condition, environment, weather) providing added perception to enhance platooning operations.	n/a	Camera for vehicle detection on ramp, and CPM message generation
MEC	MEC component integrated with eRSU enables offloading of streaming services to roadside resulting in low delay V2X communication.	Functionality for multi-PLMN edge computing service discovery, registration, migration	Service discovery with multiple MEC's, Service & Session Continuity (SSC) and Local Area Data Network (LADN) in 5G network
Cloud Systems	Microservice platform enhances CBC's cloud computing infrastructure with PaaS supporting multi-tenant resource sharing among CCAM service providers.	Crowd-sensing platform with pub/sub-based data collection support	Providing and implementing an architecture based on MQTT where messages are published on topics specifying the geolocation using tiles Designing and implementing a dynamic architecture for message exchange between different edges optimizing volume of messages based on actual requests
Application	CCAM service (360° view, LDM, EDM), Microservice platform (MEC agent, management & orchestration)	Computer vision solution for enriching and augment videos streams received from vehicles with additional detected objects	Use of Collective Perception Service as specified by ETSI ITS; investigate practical limitations of CPM with roadside sensors
Other		n/a	Safety assurance for AD vehicle with external sensor information

3.4.5. Specifications on Application Interfaces for Extended Sensors

Application Interface AI V2R and AI V2V (direct communication)

1.1.1.1.3. Extended Sensors with use of Collective Perception Service (CPS)

Extended Sensors aim at sharing information about the current driving environment with another ITS stations. For this purpose, the Collective Perception Service (CPS) as defined in ETSI specifications provides data about objects (i.e. other road participants, obstacles and alike) in abstract descriptions. Extended Sensors reduce the ambient uncertainty of an ITS-S about its current environment, as other ITS-Ss contribute context information. This includes the definition of the syntax and semantics of the CPS and detailed specification of the data, the messages and the message handling to increase the awareness of the environment in a cooperative manner. The relevant specifications are (i) ETSI TR 103 562 V0.0.15 (2019-01) "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS)" and (ii) ETSI TS 103 324 V<0.0.12> (2017-09) "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Specification of the Collective Perception Service". ETSI TR 103 562 contains a standardized message format to exchange information on detected objects, i.e. either non-connected vehicles, or other obstacles on the road.

Extended Sensors applications may also use non-standardized data formats to share information for LDM or standard raw sensor data (e.g. video stream). These specifications are described per trial site.

Application Interface AI V2C, R2C and C2C

The message sets defined for the interface AI V2R and AI V2V for direct communication may also be exchanged via cloud systems via interface AI V2C and R2C and between cloud systems, AI C2C. A distributed CCAM collection and distribution server may be used to collect and forward messages from vehicle to nearby vehicles (V2C, for V2N2V) or from roadside or cloud systems to vehicles, related to the geographical area where the information is relevant. In section 2.5.5 examples are given of these geo-messaging solutions.

3.5. UC Category 4: Remote Driving

3.5.1. Description of UCC Remote Driving

Remote Driving "enables a remote driver or a V2X application to operate a remote vehicle for those passengers who cannot drive themselves or a remote vehicle located in dangerous environments. For a case where variation is limited, and routes are predictable, such as public transportation, driving based on cloud computing can be used. In addition, access to cloud-based back-end service platform can be considered for this user story group" (Source: 3GPP TS 22.186 R16).

The following user stories are related to Remote Driving:

1. ES-PT US3 (Automated shuttle remote driving across borders

2. FI US9 (Remote driving in a redundant network environment)
3. NL US13 (Remote driving using 5G positioning)
4. CN US19 (Remote Driving with data ownership focus)
5. KR US18 (Remote Driving using mmWave communication)

3.5.2. Deployment architecture of CBC ES-PT for Remote Driving

The ES-PT corridor has a unique scenario related with the Remote Driving category:

- US3 (Automated shuttle driving across borders):
  - Scenario 2: Remote driven shuttle.

Description

This user story scenario aims to maintain a safety control system on the shuttle in case the autonomous driving mode is not available (i. e, an obstacle blocks the shuttle path). If this situation occurs, a remote driving operator is able to take the control of the shuttle from the Remote Control Centre and help the vehicle to avoid the obstacle.

The CCAM infrastructure involved in this scenario is limited, since the main element in the remote control is the MEC node, which acts as a gateway between the Remote Control Centre and the shuttle.

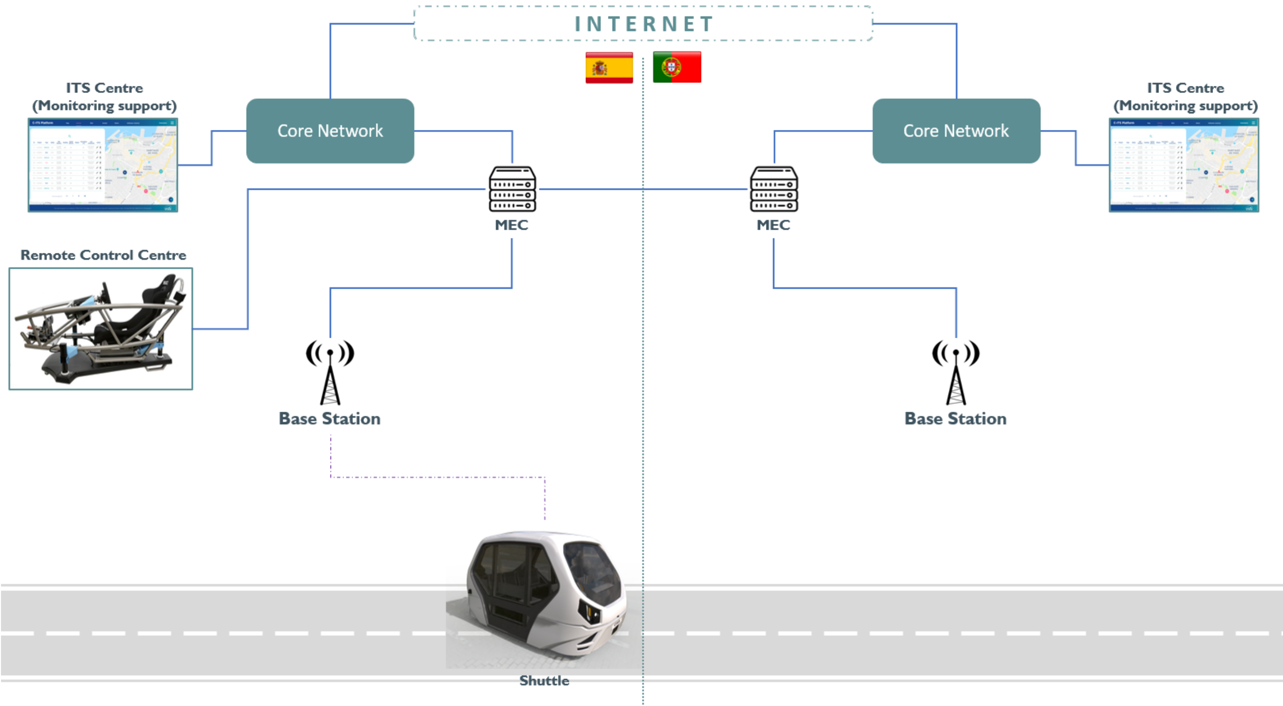


Figure 32 General CCAM infrastructure to support Remote Driving scenario on ES-PT CBC.

High-level architecture of the roadside & cloud infrastructure

The high-level architecture of the CCAM infrastructure for the scenario within this category is shown in Figure 33, where functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, and the information exchange is shown in brown. The architecture does not cover the cross-border aspects.

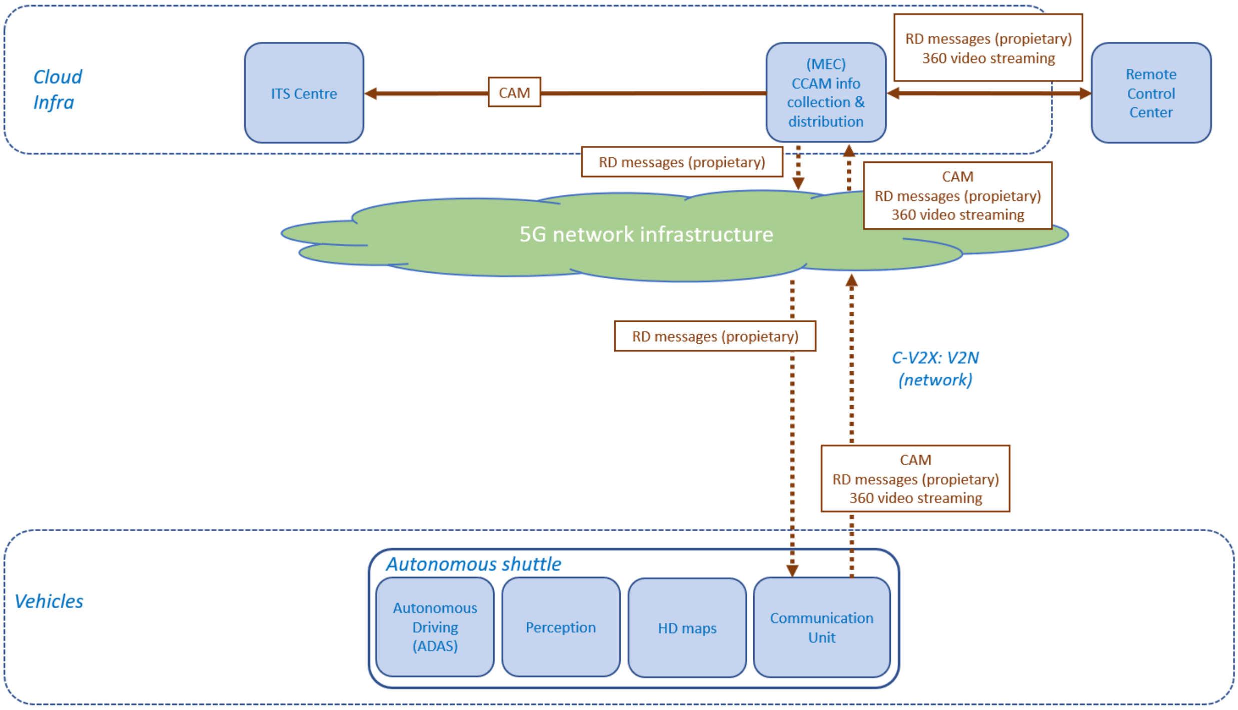


Figure 33 CCAM architecture for the ES-PT Remote Driving scenario.

This user story scenario does not make use of roadside equipment, however there are two relevant elements regarding the cloud infrastructure:

- MEC nodes: work as gateway nodes between the shuttle and the Remote Control Center. The main role is to keep the very low latency needed for driving remotely. Furthermore, MEC nodes work as relay nodes forwarding the ITS messages from the shuttle to the ITS Center, with monitoring purposes.
- ITS Centers: cloud applications running on each side of the corridor. Each ITS Centre is connected to the MEC node of the same country, and consumes the data passing through this node in order to monitor vehicles connected to the regional network.

Regarding other kind of infrastructure (neither cloud nor roadside), there is an essential element: the Remote Control Centre, which not only sends control commands to the shuttle, but receives the video streaming from a 360º camera installed in the vehicle too, as well as other data messages, in order to give the driver information about the environment around the shuttle. The operator has a set of tools (Virtual Reality glasses, a steering wheel, pedals, etc) for interacting with the remote vehicle as if the operator were driving inside the shuttle.

Sequence diagram

The remote driving ES-PT scenario follows a simple procedure:

1. The shuttle is driving autonomously along its predefined route.
2. Suddenly, the vehicle detects the presence of an obstacle blocking its route. The shuttle notifies the Remote Control Center.
3. The Remote Control Center takes the control of the vehicle and drives it remotely in order to avoid the obstacle.
4. Finally, the shuttle continues the predefined route driving autonomously.
5. In parallel with the described above, the shuttle sends CAM messages containing its attributes to the MEC node, where these messages are relayed to the ITS Centre with monitoring purposes.

Figure 34 shows the sequence diagram of this scenario.

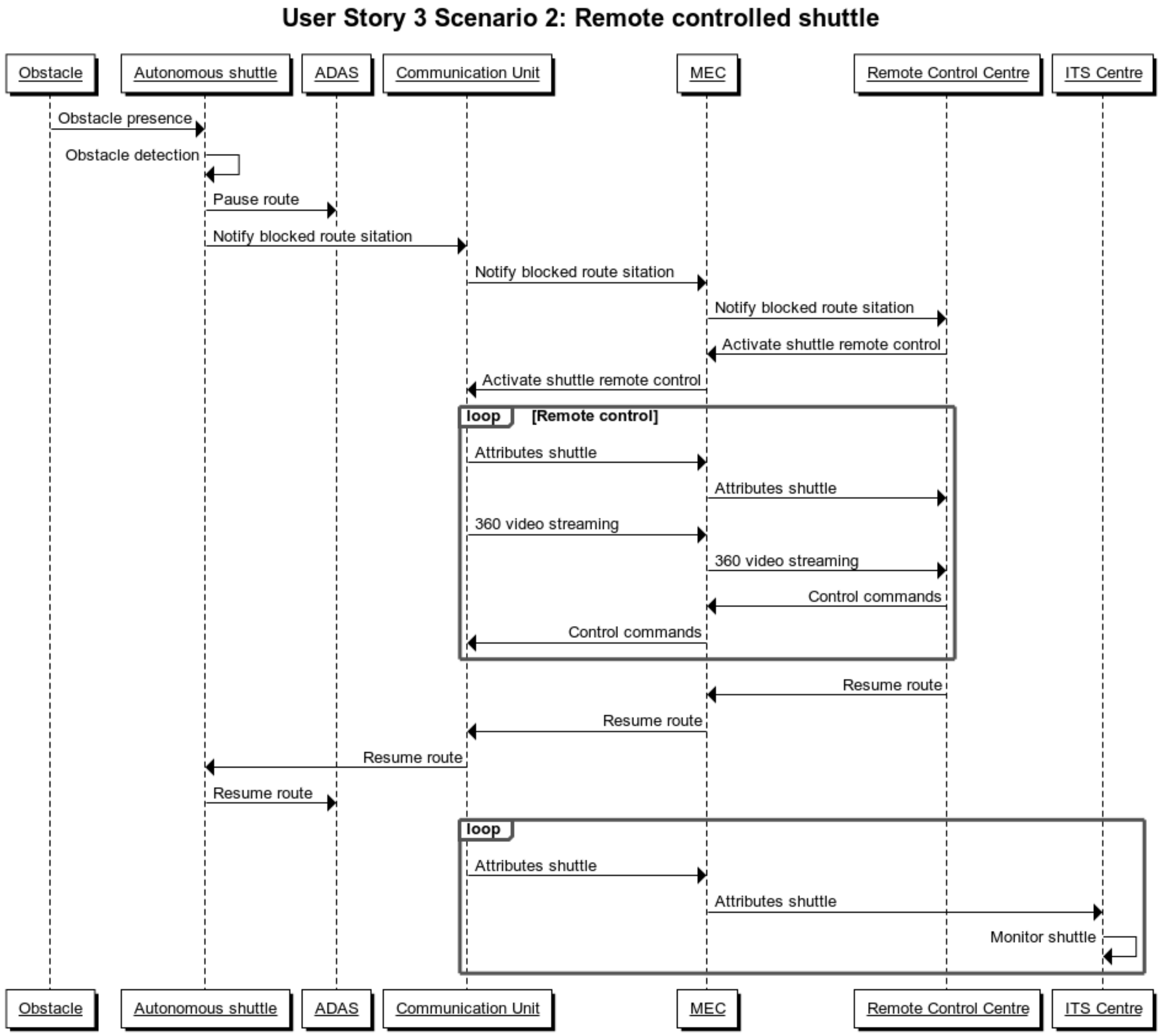


Figure 34 Sequence diagram of the Remote Driving scenario of ES-PT US3.

Detailed specifications

The specifications can be divided into two different channels: the control channel and the video channel.

For the video channel we will require to acquire raw video from a 360 or non-360 Video camera. The final decision to use one camera or the other will depend on the field tests in which the whole E2E latency will be measured.

A hardware-based video encoder is required to minimize the delay in the contribution to the E2E path. Minimal resolution to be taken into consideration is Full-HD resolution (1920x1080) and preferred codecs are M-JPEG or HEVC. We can also consider using 4K resolution using 360 or non-360 video.

For the 360-video case, the stitching post processing of the acquired video after the first compression phase will add an additional delay and extra computational power either in the car or in the MEC which might not be suitable for practical reasons in this situation.

The steering control path will be routed to MEC and the appropriate slicing is assumed to have previously been configured both in the core and radio sections. Traffic in the core part devoted to control and video ones might follow different QoS flows inside the core depending on the latency and throughput required.

Initially a single MEC will be used for other user stories concerning the rest of video processing which is not devoted to remote driving. This setup should be enough if only the video transport layer is manipulated in this piece of the network.

The diagram below depicts the E2E connection diagram which separates the control and video channels.

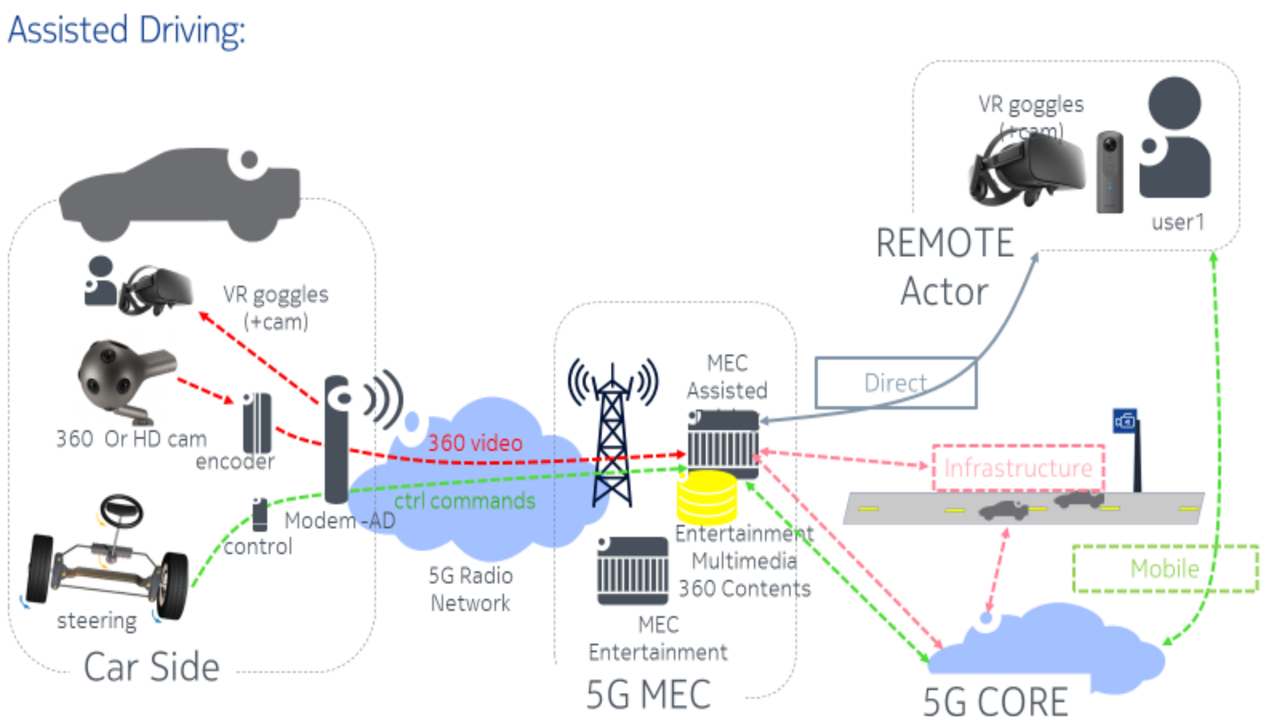


Figure 35 Assisted Driving Connection Diagram

Video Playback API Information

- Video Format:
  - M-JPEG compressed video [Primary]
  - HEVC 360 compressed video [Secondary Option]

- Video API:
  - Play/Pause/Stop/Record
  - Configure encoding parameters
  - Camera switch (if multi camera source is available)
  - Change resolution
  - Get video statistics

Control API Information

- GET Interface Section
  - Get sensors information [LIDAR, Speed, etc]
  - Get Mobile Network Info [Cell-ID, RSSI Power, SIM, Switchovers]
  - Get GPS Info (Longitude, Latitude, Height)
- ACTION Control Section
  - Take Control API (Remote driver takes control)
  - Release Control API (Remote driver releases control)
  - Steering Control API (Speed change, Break, etc ...)

Cross-border aspects

The vehicle will rely in the 5G communication continuity in the cross-border area. To increase safety, the vehicle should stop automatically in case it has lost connectivity to the network for more than n seconds. This scenario might occur in some roaming scenarios in which the UE device is switching across networks and is in the process of interchanging control messages without having the full user plane path established. Once this is established the 5G MEC connection will provide the continuity level in terms of data consistency so that remove video and related car control can be resumed normally.

Autonomous driving vehicle systems need to be aware of connection loss so that they take over the situation and pass the control situation to the remote driver.

The ability to resume video playback in the event of continuity issues also needs to be handled. Appropriate management of video timestamp information both in the server area located in the MEC and the video player located in the End User device is a topic that will be addressed. Frozen video needs to be signalled.

Initial coverage measures from existing LTE cells which will be used for anchoring the 5G connection altogether with the 5G radio simulations already taken into consideration for 3.6 GHz band will be a reference to deal in advance with handover scenarios in this area.

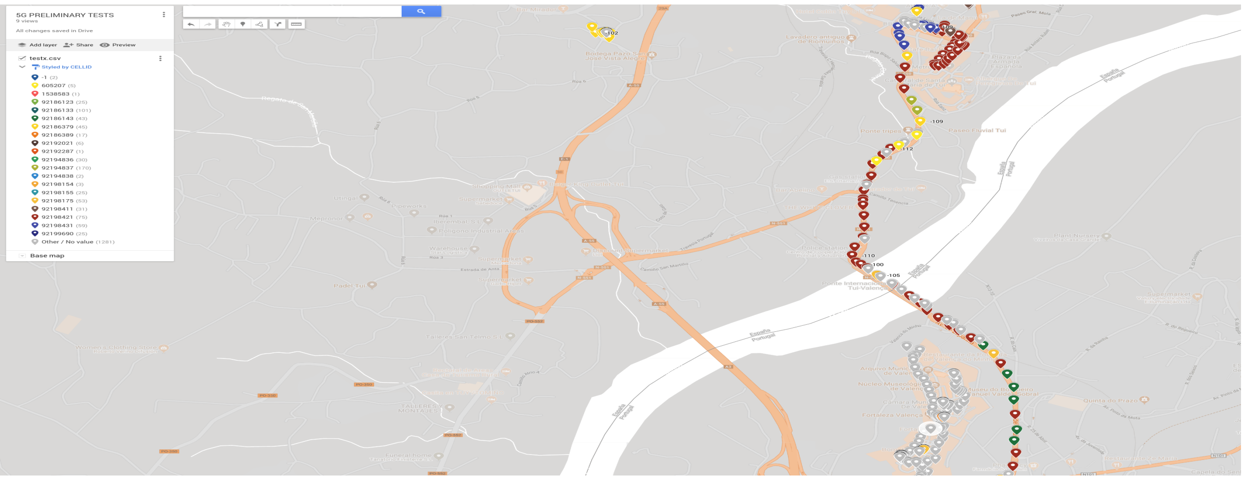


Figure 36 Anchoring LTE In the Border Measures

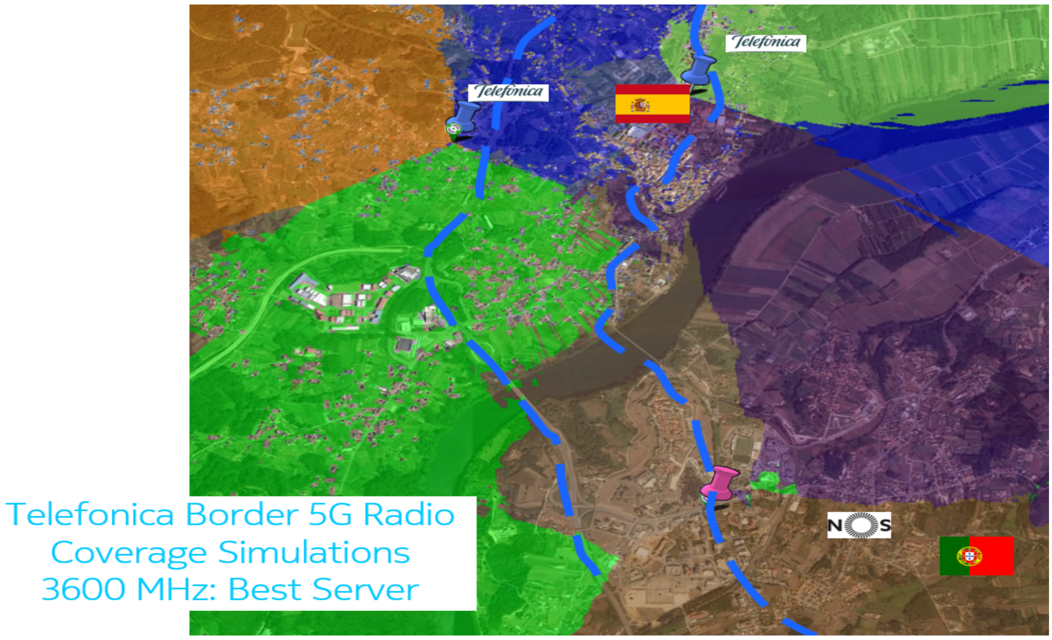


Figure 37 5G 3.6 GHz Coverage Simulation In the Border

3.5.3. Trial sites specific contributions to CBC for Remote Driving

Table 19 gives an overview of the specific roadside and cloud infrastructure to support the user stories for Vehicles Platooning, as described in section 7.

Table 19 Overview of roadside & cloud infrastructure per user story for Remote Driving

User story	Roadside sensors /actuators	Roadside comm. units	Cloud infrastructure
ES-PT US3 (Automated shuttle remote driving across borders)	n/a	n/a	Yes, MEC node + remote driving control center (with video stream)
FI US9 (Remote driving in a redundant network environment)	n/a	n/a	Yes, remote driving control center (with video stream)
NL US13 (Remote driving using 5G positioning)	n/a	n/a	Yes, remote driving control center (with video stream)
CN US19 (Remote Driving with data ownership focus)	Yes, VRU detection forwarded to update path info for remote manoeuvre	Yes, RSU	Yes, remote driving by control center (no human operator)
KR US18 (Remote Driving using mmWave communication)	n/a	n/a	Yes, remote driving control center (with video stream)

Summary:

- No roadside sensors/actuators and or roadside communication systems are used to support remote driving. CN US19 makes use of roadside sensors for VRU detection for the user story on Extended Sensors to support the user story on remote driving.

The table below shows the trial-site specific contributions to the CBC.

Table 20 Trial sites specific contributions to CBC for Remote Driving

Topic roadside / cloud	FI US9	NL US13
RSU	n/a	n/a
Roadside sensors	n/a	n/a
MEC	n/a	MEC for virtual remote control
Cloud Systems	n/a	Fleet management system to organize control of vehicle between different human and virtual operators
Application	LEVIS video streaming platform	Remote Driving with Virtual remote control
Other	Vehicle gateway for attachment to multi-PLMNs	n/a

3.5.4. Specifications on Application Interfaces for Remote Driving

Application interface AI V2R and V2V (direct communication)

For Remote Driving no messages are exchanged via the AI V2R interface.

Application Interface AI V2C, R2C and C2C

For Remote Driving no standardized C-ITS message sets are available for vehicle monitoring & control. For Remote Driving with video-streaming standardized RTP-based video streams and uplink RTCP may be used, which include a set of standard feedback messages to monitor bandwidth, packet loss ratio and round-trip-time for latency assessment.

3.6. UC Category 5: Vehicle Quality of Service Support

3.6.1. Description of UCC Vehicle Quality of Service Support

According to 3GPP TS 22.186 R16, Vehicle quality of service support "enables a V2X application to be timely notified of expected or estimated change of quality of service before actual change occurs and to enable the 3GPP System to modify the quality of service in line with V2X application's quality of service needs. Based on the quality of service information, the V2X application can adapt behaviour to 3GPP

System's conditions. The benefits of this user story group are offerings of smoother user experience of service".

The following user stories are related to Vehicle QoS Support:
1. ES-PT US2 (Public transport with HD media services and video surveillance)
2. FR US11 (QoS adaptation for Security Check in hybrid V2X environment)
3. KR US17 (Tethering via Vehicle using mmWave communication)

3.6.2. Deployment architecture of CBC ES-PT for Vehicle Quality of Service

The ES-PT corridor has two scenarios related with the Quality of Service category:

- US2 (Public transport with HD media services and video surveillance):
  - Scenario 1: 4k bus monitoring.
  - Scenario 2: Multimedia services for passengers.

Description

Those user story scenarios aim to take advantage of 5G cellular technologies for improving the quality of service in public transport, both for service managers and for passengers.

Regarding the service managers (like ALSA, for instance), the scenario of 4k bus monitoring intends to capture the inside and outside of the bus, and to display this video streaming in real time in the service manager control center.

On the other hand, the scenario of multimedia services for passengers provide a high-quality set of contents for the passengers entertainment during the trip.

The high quality of the service to be provided in those scenarios implies a great amount of data that have to be consumed in very short time, so the 5G technologies play an essential role for making possible to maintain the service.

Those scenarios depend entirely on the cloud side, since there is no roadside infrastructure involved. Figure 38 shows the general CCAM architecture deployed for QoS scenarios.

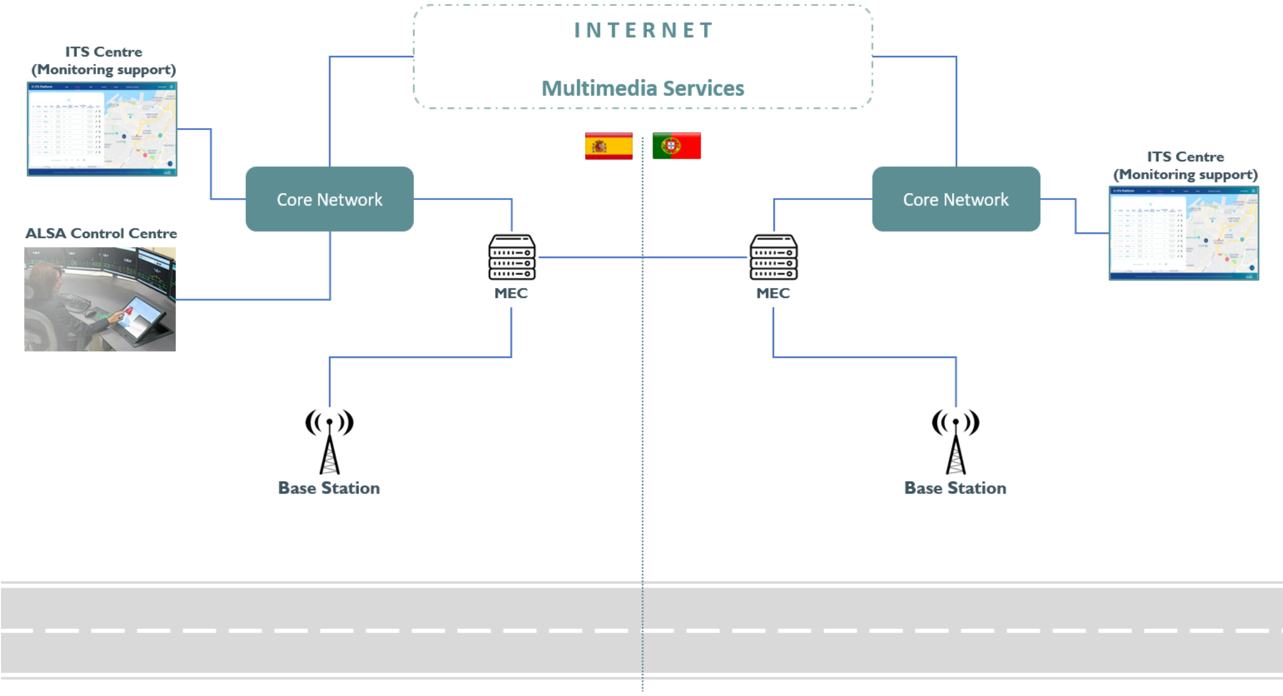


Figure 38 General CCAM infrastructure to support QoS scenarios on ES-PT CBC.

High-level architecture of the roadside & cloud infrastructure

The high-level architecture of the CCAM infrastructure for the scenarios within this category is shown in Figure 39, where functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, and the information exchange is shown in brown. The architecture does not cover the cross-border aspects.

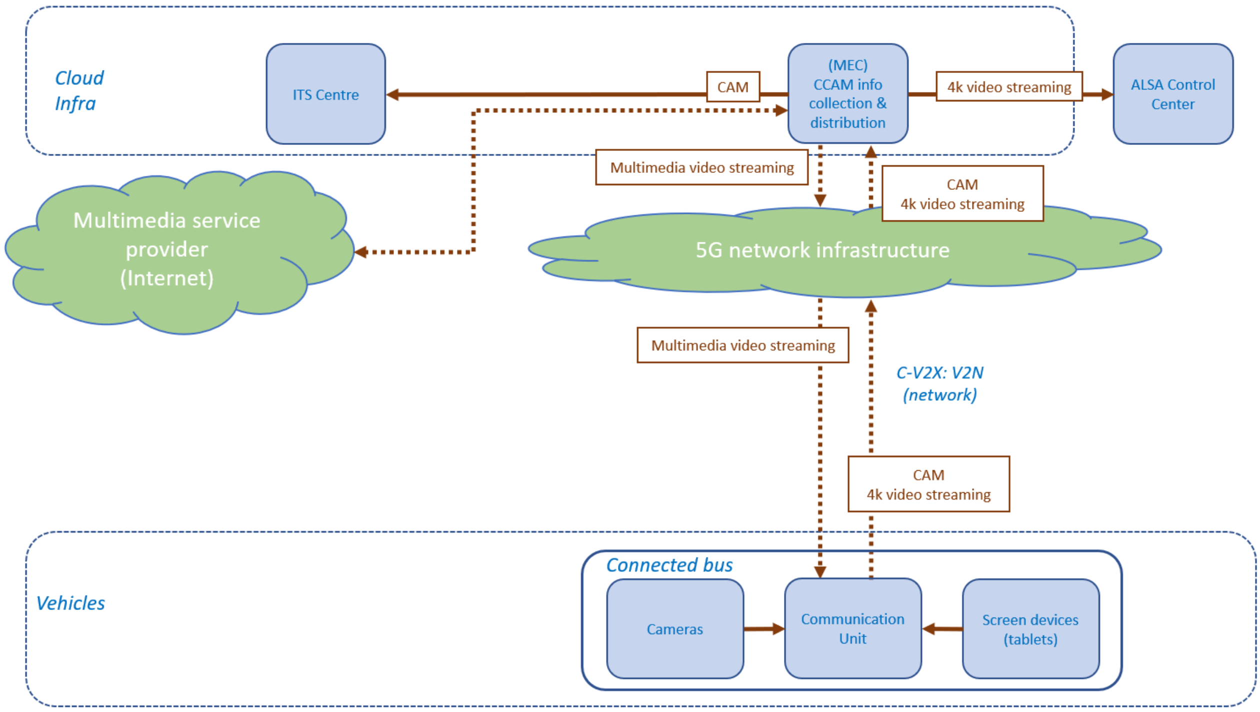


Figure 39 CCAM architecture for the ES-PT Quality of Service scenarios.

As the figure above shows, the absence of roadside infrastructure gives the importance to the cloud infrastructure elements in those scenarios, which can be summarized as follows:

- MEC nodes: work as gateway nodes between the bus and the Internet. Through this link, the bus is able to communicate with ALSA control center to send the camera streaming, and also to retrieve the multimedia content requested by passengers in the bus. Furthermore, MEC nodes work as relay nodes forwarding the ITS messages from the bus to the ITS Center, with monitoring purposes.
- ITS Centers: cloud applications running on each side of the corridor. Each ITS Centre is connected to the MEC node of the same country, and consumes the data passing through this node in order to monitor vehicles connected to the regional network.
- ALSA Control Center: the physical control center of the bus service managers counts on specific equipment which connects through the 5G network with the bus, so that the video streaming from the 4K cameras can be displayed in the control center.

Sequence diagram

The following figures depict the sequence diagrams of each one of the QoS scenarios deployed in the ES-PT CBC.

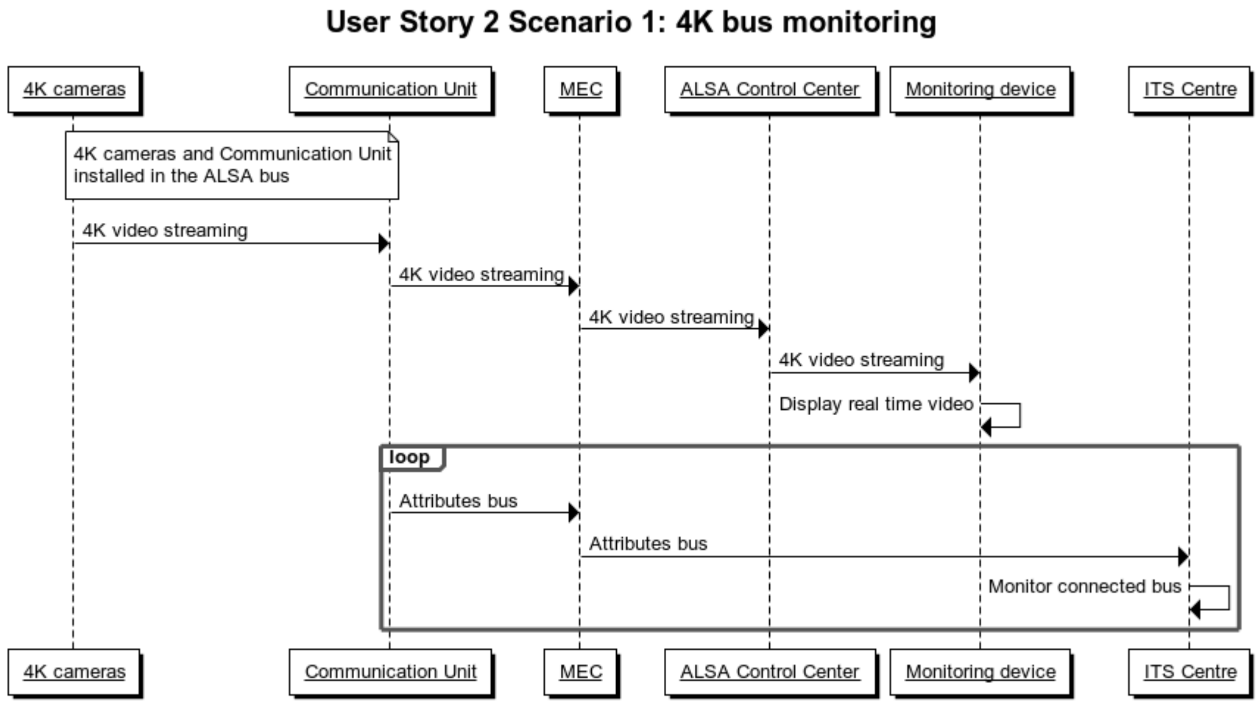


Figure 40 Sequence diagram of the 4k bus monitoring scenario of ES-PT US2.

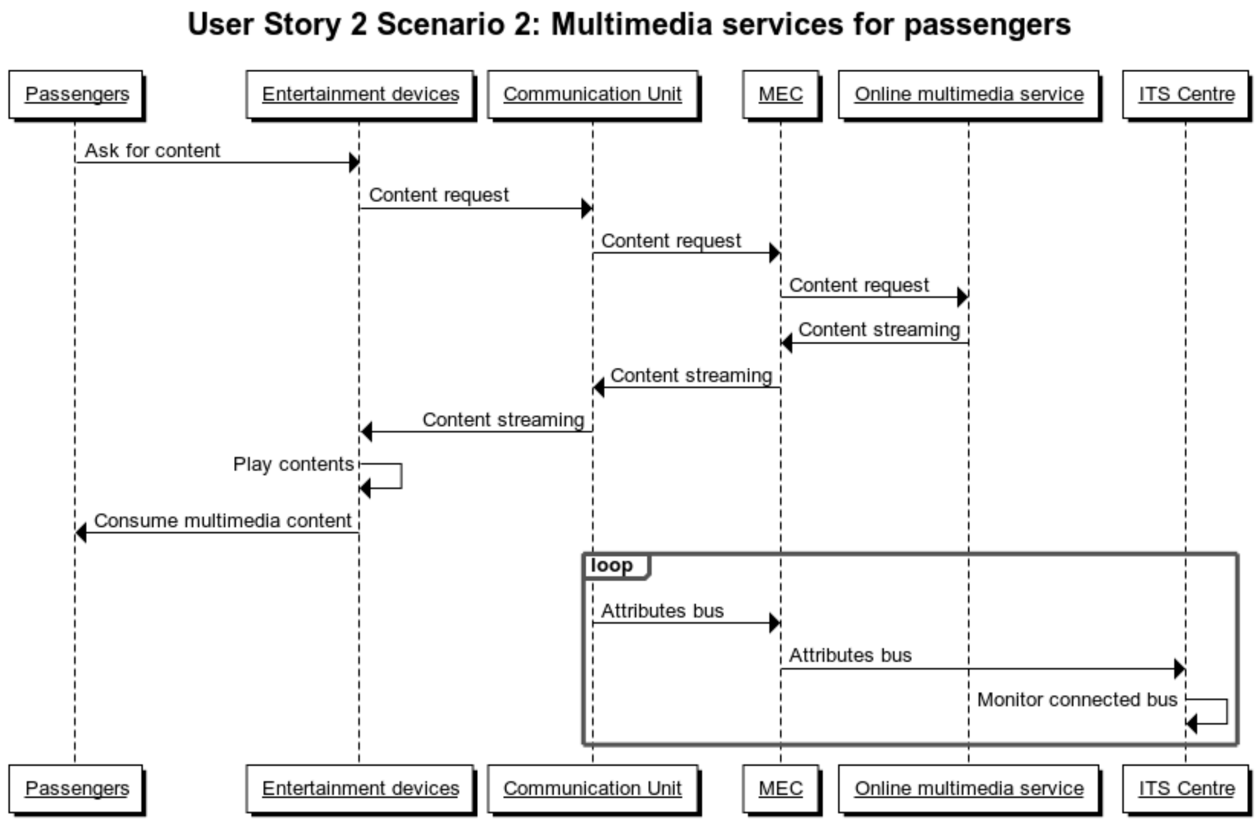


Figure 41 Sequence diagram of the multimedia services for passengers scenario of ES-PT US2.

Interface specifications

The Quality of Service scenarios of the ES-PT CBC make use of the following interfaces, briefly described:

1) V2N (Vehicle-to-Network): vehicles send CAM messages containing their attributes (location, speed, heading, etc) to the MEC nodes (network).
2) N2C (Network- to-Cloud): MEC nodes forward only CAM messages from connected vehicles to the ITS Centres with monitoring purposes.
3) N2V (Network-to-Vehicle): multimedia contents from the multimedia service is transmitted from the multimedia service to the vehicle, through the MEC node.

Cross-border aspects

- Interoperability (roaming) between Spain and Portugal cellular network assures the Internet connection in cross-border areas.

3.6.3. Trial sites specific contributions to CBC for Vehicle Quality of Service Support

Table 21gives an overview of the specific roadside and cloud infrastructure to support the user stories for Vehicle QoS Support, as described in section 7.

Table 21 Overview of roadside & cloud infrastructure per user story for Vehicle QoS Support

User story	Roadside sensors /actuators	Roadside comm. units	Cloud infrastructure
ES-PT US2 (Public transport with HD media services and video surveillance)	n/a	n/a	Control Center for remote video monitoring (4K content); MEC node for HQ multimedia streams for passengers
FR US11	n/a	n/a	MEC node with QoS adaption mechanism (adaption based on network QoS)
KR US17 (Tethering via Vehicle)	n/a	Yes, RSU (mmWave) with backhaul link to mobile core /internet (relay node)	n/a (basic internet access)

Summary:

- Vehicle QoS Support does not rely on roadside sensors / actuators and cloud infrastructure.
- KR US17 uses RSU with mmWave for communication to vehicles.

The table below shows the trial-site specific contributions to the CBC.

Table 22 Trial sites specific contributions to CBC for Vehicle QoS Support

	FR US11
RSU	n/a
Roadside sensors	n/a
MEC	QoS prediction and GeoNetworking
Cloud Systems	n/a

Application	n/a
Other	n/a

3.6.4. Specifications on Application Interfaces for Vehicle Quality of Service Support

Application Interface AI V2R and V2V

For Vehicle Quality of Service Support sensors data are exchanged via the AI V2V interface.

Application Interface AI V2C, R2C and C2C

For Vehicle Quality of Service Support no standardized C-ITS message sets are needed. In the case of Vehicle QoS when accessing to OTT-like services, no messaging is used but effective measures done at the player side from HTTP responses and remote gaming servers use the RTT to take QoS decisions

4. CYBER-SECURITY & DATA PRIVACY ASPECTS

4.1. C-ITS Security Premises in CCAM

Transportation systems are becoming increasingly interconnected and so across different countries. This implies the coexistence of people and systems of unknown trustworthiness. These systems depend on the proper functioning of their sub-systems which might have serious vulnerabilities whose exploitation could cause massive disruptions. Those vulnerabilities are due to many reasons among which:

- Security requirements are not being met with sufficient warranty in the CCAM infrastructures that are available with flaws some of which are potentially serious. Vulnerabilities in the existing infrastructure and the risks that can results from them tend to be underestimated. Also, the lack of awareness of the stakeholders can result in critical problems
- Resiliency (cyber-resiliency) of complex systems require intelligent, well-trained, and experienced workforce, especially for critical infrastructures.
- Privacy of users in a CCAM infrastructure (vehicles, roadsides, and cloud) is undermined by the data (different identifiers or quasi-identifiers) that could be harvested on them and lead to monitoring and surveillance activities[10]. Therefore, it is desirable to minimize the information that is collected and to control strictly who has access, and also to ensure the correct identity of all individuals engaged in risky activities.

Desires for privacy are generally incompatible with the desire for accountability as attempts to create completely anonymous services tend to run against practical notions of authenticity, integrity, revocability, or non-repudiability. A trade-off should be found between privacy and accountability.

Security requirements (security-by-design[11] [12]) should be properly addressed at the early stages of the CCAM infrastructure specification in order to avoid malicious actions during the deployment and exploitation phases. Furthermore, other important aspects such as privacy (privacy-by-design[13]), resiliency, reliability, system survivability and safety are to be considered at the requirement phase. Thus, it is necessary the understanding of a complete set of requirements in advance, embracing security, privacy, resiliency, safety, survivability and the interactions among them.

[10] https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D5.1-Deployment_Issues_Report_V1.pdf

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf

[12] https://www.owasp.org/index.php/Security_by_Design_Principles

[13] https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

4.1.1. Threats, vulnerabilities and risks in C-ITS

This section summarises, some threats specific to CCAM infrastructures[14]. The column (Affected interfaces) describes the interfaces in the 5G-MOBIX high-level reference architecture concerned by the threat.

Table 23 Security threats and risks related to CCAM

Threats	Description	Affected interfaces
Masquerading	Ensuring the authenticity of the information received and processed by an CCAM systems involves the protection of the system from masquerade attacks that insert false messages into the network, the identification of unplanned replay of legitimate message interchanges, the exposure of false GNSS signals and the protection against illusion and Sybil attacks.	All
Identification or de-identification of a vehicle owners, tracking	These threats are related to undermining the privacy protection mechanisms and are strengthened due to the types of messages that are used in the CCAM infrastructure (See section 2 for more details). These messages are mainly broadcasted in plaintext over an unprotected short-range radio channel and contain sensitive information about the users. In consequence, this **information is easy to intercept and leaks sensitive information** about travel itineraries and driving habits. An attacker may construct a profile of a given vehicle by observing which services are used regularly, at what times and at which location. Such analysis might be used to gain information on private vehicles and enabling the performance of masquerade attacks and location linking. **Lack of transparency** is another major privacy risk. Users will become continuous broadcasters through their vehicles, they must be aware of the other peers with whom they exchange data and how it is processed. The choice of broadcast to distribute messages poses another challenge: they can be received by an unrestricted number of entities, whose intentions cannot be known.	V2X using ITS-G5

[14] https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

Denial of Service (DoS)	Threats to the availability of CCAM infrastructures are mainly related to DoS attacks performed by introducing malwares or transmitting a high volume of messages (spamming, flooding, etc.). These attacks are difficult to protect against and may result in CCAM (Vehicles, Roadside and Cloud) systems failing to function properly.	All
Unauthorized access	Threats to the **confidentiality** of information include the illicit collection of transaction data by eavesdropping and the collection of location information through the analysis of message traffic. Restricted information may be accessed and tampered with (on the different interfaces or within the CCAM systems) by means of masquerade attack or malwares leading to the compromise of the integrity of the CCAM systems.	V2X interfaces using ITS-G5

Analysis of applicable security areas

For each of the identified threats it is necessary to consider what measures could be implemented to reduce the risks. In [4], an evaluation of potential **ITS countermeasures** are made, presenting a set of general techniques that can be used to avoid or reduce the impact of the aforementioned attacks. Some of these countermeasures are listed in the Table 24.

Table 24 Security solutions organized by the Security Control Classes

Security Control Class	Countermeasures
Identity & Access Management	• Provide remote deactivation of misbehaving CCAM vehicle system to avoid the disruption of other vehicles and protect against masquerading and unauthorized access.
Confidentiality	• Implement the security mechanisms for 3GPPP RATs (LTEV2X and 5G NR V2X) for CCAM infrastructures to provide link layer confidentiality and certificate management and secure routes for keys. This comprises the usage of symmetric and asymmetric cryptography.
Integrity	• Messages emitted by a CCAM vehicle can contain checksums, message authentication code (MAC), timestamps (UTC or GNSS) and sequence number in order to protect their integrity from misbehaving vehicles. • Inertial Navigation Systems or dead-reckoning can be used by a CCAM vehicle to determine its position from purely internal sources in order to protect against

	unauthorized messages
Privacy	• Beacons and other repeated messages, which generate considerable background radio traffic can be lowered to reduce the problem area of intrinsic high density due to broadcasting and beaconing • Pseudonyms (in all the OSI layers) that cannot be linked to the true identity of the user can be used. Most research in the ITS security and privacy during the last years has been focused on the **pseudonymization** field, in order to maintain the privacy of individual vehicles and drivers. Therefore, each vehicle is provided with a set of pseudonymous certificates used to sign the messages.[15].
Audit	• Maintain an audit log of the type and content of each message sent to and from an ITS-S. Machine learning algorithms could be used in order to detect misbehaving vehicles and also ongoing DoS attacks.
Trust & Assurance	• The trustworthiness of the system can be improved by digitally signing each message using a Public Key Infrastructure approach • Certified software authenticity and integrity to ensure that only authorized updates and extensions can be downloaded to the ITS-S • A source addresses included into a V2V message should be identifiable by the receiver, so that it can trust that source has not been modified over time
Availability	• High availability mechanisms such as using redundant cloud servers and proxies are to be considered to avoid DoS and DDoS attacks. Also, at the link layer frequency change on pseudo-random basis to make jamming attacks more difficult and costly.
Compliance	• GDPR, NIS Directive, Delegated Regulation on C-ITS. For more details see the 5G-MOBIX deliverable D1.4 and Other regulation are described in
Network Management	• Different tools, such as SIEM and SoC, could be used to manage the deployment in a CCAM infrastructure of the mechanisms presented in this table. These tools could embed Machine learning approaches to support the detection and the mitigation of the attacks listed in Table 23.

[15] https://ieeexplore.ieee.org/document/6873216

4.2. CCAM cybersecurity and privacy ecosystem

4.2.1. ETSI ITS Security framework

Overall security architecture

In ETSI[16] EN 302 665 [17], Security is presented as a vertical layer adjacent to the ITS layers. However, security services are provided on a layer-by-layer basis so that security is subdivided into the four basic ITS processing layers. In Figure 42 the security services[18] defined by ETSI which may be supported by an ITS station are presented inside the ITS architectural layers.

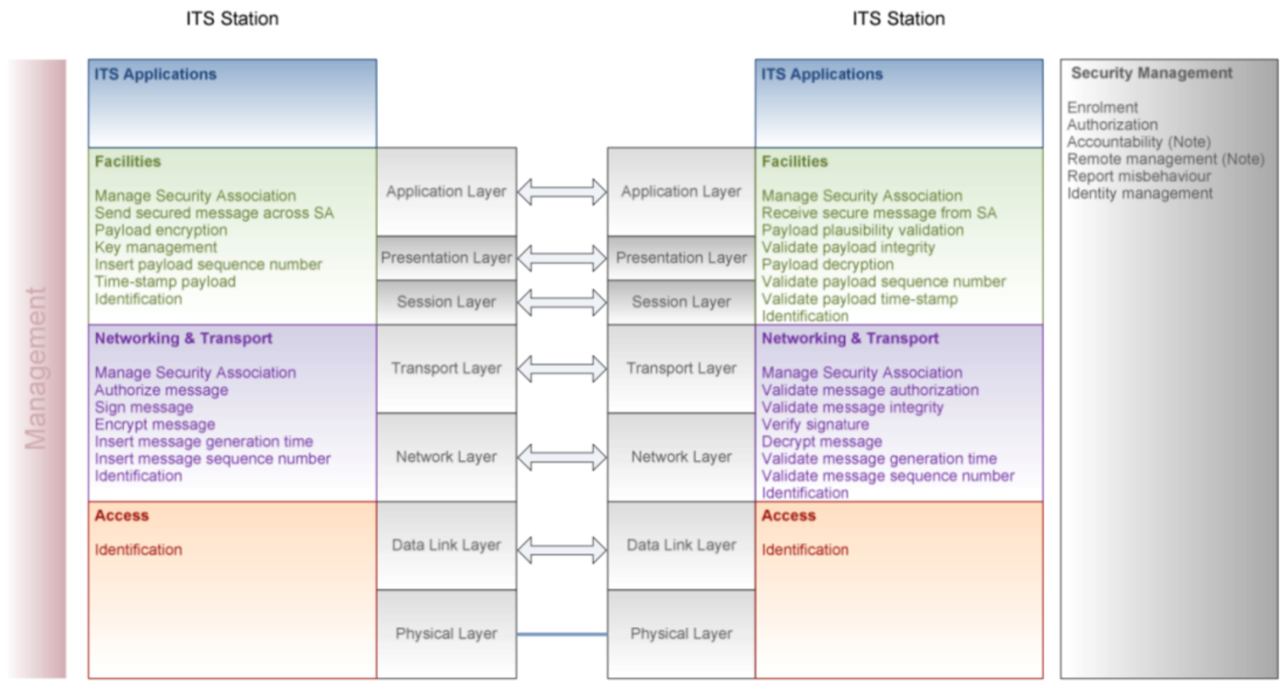


Figure 42 ETSI security services

These services are summarized in Table 25.

[16] Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs) The ETSI ITS committee (TC ITS) is working to achieve global standards for C-ITS and develops:

- Standards related to the overall communication architecture, management, security as well as the related access layer agnostic protocols.
- Standard defining the security framework for cooperative ITS including a Public Key Infrastructure (PKI). This security framework will support PKI trust model requirements from the EU C-ITS deployment platform and bring privacy protection mechanisms for users and drivers.
- Conformance test specifications which are crucial for the commercial deployment of the technology.

[17] https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf
[18] https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf

Table 25 Summary of ETSI security services

Service	Description
Confidentiality	The confidentiality of personal, or commercial, information is protected primarily by the establishment of a security association between the two implied parties independently from the broadcasting of ITS messages (CAM, DENM, etc.). Confidentiality procedures can be carried out on the: • application layer, depending on the type of application; • network layer (*e.g.* using Encapsulated Security Payload (ESP) in IPv6); • link layer (*e.g.* using the specific services for 4G and 5G).
Access control	An ITS station (ITS-S) must obtain specific credentials from the authorization authority in order to make full use of the ITS applications, services, and capabilities. To obtain the authorization certificates, an ITS-S must follow a comprehensive procedure composed of three stages: initialization, enrolment, and authorization. More details are provided in Section 4.3.1.
Trust and privacy management	Trust and privacy management requires secure distribution and maintenance of trust relationships[19], which may be enabled by enrolment credentials that provide certificates of proof of identity and pseudonym certificates. A PKI is used to establish and maintain trust between the ITS station and other ITS stations and authorities. Separation of duties for enrolment and for authorization has been shown as an essential component and provides protections against attacks. When the same operational authority manages both the enrolment and the authorization authorities, it shall guarantee privacy providing all the measures needed to ensure the separation of the identity information from the pseudonym certificates.

4.2.2. C-Road Task Force Security Aspects

C-Roads tasked the work group number 2 with describing the overall security solution for secure and trustful communications between C-ITS stations in a pilot phase[20]. This working group aims at implementing the European C-ITS Certificate Policy and Security Policy. *To ensure EU-wide interoperability of C-ITS services, it is widely accepted that C-ITS in Europe is working within one trust model based on a PKI*

[19] https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf
[20] The work of the task force constitutes an important input to the EU delegated regulation.

infrastructure comprising all C-ITS stations, both vehicles based or road infrastructure-based ones under the same certificate policy[21]..

4.3. Towards a Common Trust Domain

4.3.1. The European C-ITS Credential Management System

Overall view

The European C-ITS Credential Management System means the European Union C-ITS framework for the provision of trusted and secure communication using a public key infrastructure (PKI). It constitutes a milestone towards the deployment of CCAM and has been achieved after many EU funded cooperative projects, the work of the C-ITS platform and C-Roads. The EU CCMS is defined by these two documents:

- The C-ITS Certificate Policy for Deployment and Operation of European C-ITS [22]
- The Security Policy & Governance Framework for Deployment and Operation of European C-ITS [23].

As the EU CCMS is binding to all the entities in a C-ITS, All C-ITS stations shall be enrolled in, and comply with the rules of, the EU C-ITS security credential management system, in accordance with the specifications laid by the C-ITS Certificate policy and C-ITS Security Policy.

The C-ITS Certificate policy

The EU CCMS defines a binding certificate policy named the European C-ITS Trust model and based on a Public Key Infrastructure. This certificate policy defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. The PKI is composed at its highest level by a set of root CAs "enabled" by the Trust List Manager (TLM), i.e. whose certificates are inserted in a European Certificate Trust List (ECTL), which is issued and published by the central entity TLM[24]. This certificate policy is illustrated in Figure 43.

[21] https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/20190125_TF1_Security_report_v1.4_final.pdf
[22] https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf
[23] https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf
[24] https://webgate.ec.europa.eu/tl-browser/#/

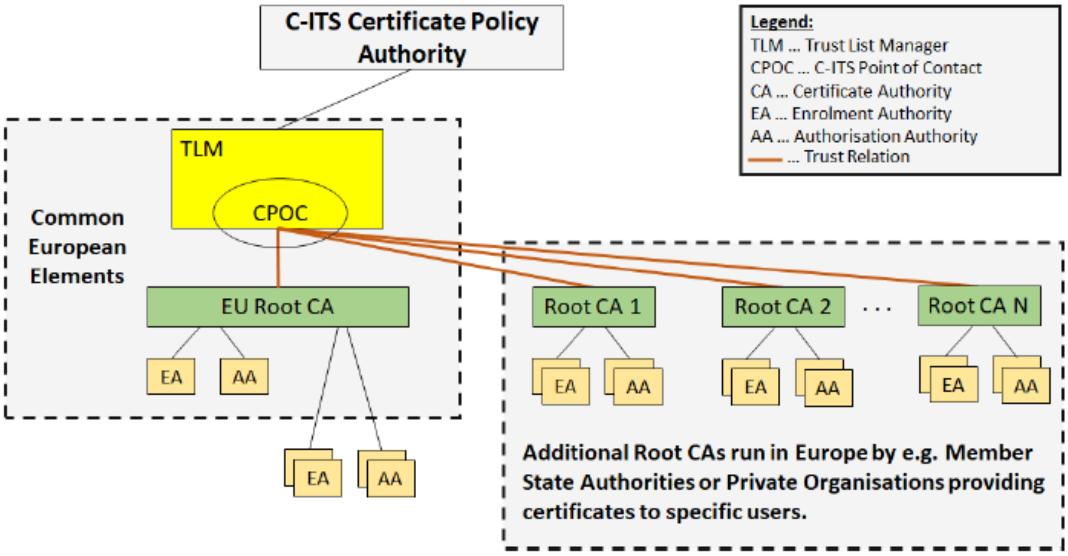


Figure 43 C-ITS Trust model architecture

The C-ITS Security Policy

The EU C-ITS security policy describes the Governance Framework and the Security policy of the C-ITS.

The C-ITS Governance framework describes the overall governance of the European C-ITS system including the following components and entities of C-ITS: the C-ITS system as a whole and its governance and management structure, the participating C-ITS Stations, the components of the trust model (e.g., PKI services) as well as the entities running them in a secure and reliable way, the trusted third parties for the trust and privacy management on which operational entities rely and which allow running them in a secure and reliable way.

The C-ITS policy defines a framework for the management of information security for the deployment and operation of the European Cooperative Intelligent Transport System (C-ITS). It defines how to manage information security including the definition of security policies for individual stakeholders and the operation of an information security management system. As such, the policy should be seen as a metapolicy. It defines the policy requirements for information security management for all organisational entities that process C-ITS data or manufacture equipment that will process C-ITS data. The C-ITS system is a distributed system with many stakeholders and many actors processing parts of the C-ITS data which makes information security not only a responsibility of the individual organisations but also a joined and shared responsibility

4.3.2. International cooperation

In the context of different trust domains between the EU, China, Koran and Turkey, an international cooperation to:

- Discuss interoperability of the others trust domains with the EU CCMS
- Address cross-certification issues that occurred when many root certificates authorities are used to support
- Harmonize the trust domains on their procedures and technical approaches of the certificates policy and security policy to improve their interoperability and enhance the security lifecycle.

PKI interoperability is also being investigated by the InterCor project[25].
Finally, a recommendation of the C-ITS platform phase II is as follow: *"It is recommended that further work should be done towards evaluating possible cross certification of the setup European C-ITS security system with other Root CAs in the international environment / other regions of the world. It is recommended that the European best practices established through the activities of the C-ITS Platform should be promoted to other regions of the world in this context, e.g. through European Standardisation Organisations"*.

4.4. Data protection & Privacy in C-ITS

ITS privacy is provided in two dimensions: the privacy of the registration and authorization tickets provisioning and the privacy of the communications between the ITS stations. ISO/IEC 15408 identifies 4 key attributes: anonymity, pseudonymity, unlinkability, and unobservability.

Pseudonymity ensures that a station may use a resource without disclosing its identity, it shall be provided by using temporary identifiers in the messages and never transmitting the canonical identifier. Unlinkability ensures that an ITS-S may make use of resources multiple times without others being able to link them together. Unlinkability can be achieved by limiting the amount of detailed information carried in the messages. In this way, both offer the appropriate protection of the privacy of a sender of ITS safety messages.

The frequency of pseudonym changes depends on the desired level of privacy, besides, in order to be effective, changes must encompass all network layers. Another important aspect is the necessity of having vehicles in the neighbourhood when changing the pseudonym, as if it is done alone, it will not confuse an observer.

4.5. Security requirements for the 5G-MOBIX CCAM infrastructure

This section describes the security requirements that apply on the different entities of the 5G-MOBIX CCAM infrastructure. These requirements are identified based on the 5G-Mobix high-level reference architecture (as defined in section 2.3 and illustrated in Figure 44) and are to be considered with the

[25] https://intercor-project.eu/pki-security-testefest/

security requirements set in D2.2 for 5G technologies and the security good practices in D2.4 for the vehicles.

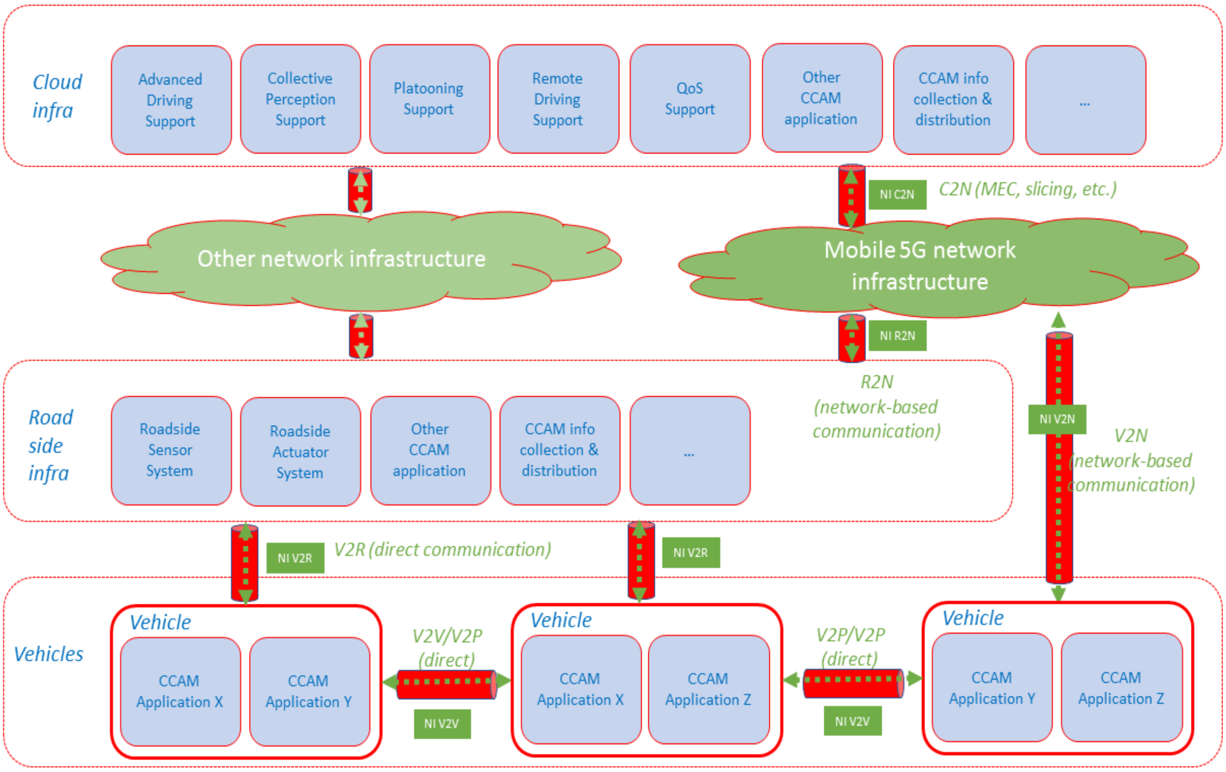


Figure 44 Secured 5G-MOBIX High-Level reference architecture.

Different set of requirements are described:

- Generic requirements related to the management of a CCAM information system are described in Table 16.
- Requirements related to network and application interfaces.

The security good practices related the vehicles used in 5G-MOBIX are given in the D2.4 and the recommendations related to cloud servers are given by ENISA[26].

Table 26 Generic security requirements related to CCAM infrastructure.

Requirement ID			Description
Sec-generic	**Methodological**	**M1**	Designate a dedicated security team. Each trial site should rely on a specialized security team, notably for

[26] https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

			secure design, penetration testing and risk management
		M2	Provide security and privacy by design. Each trial site should plan their development lifecycles to ensure that security and privacy are considered no later than at the design phase, in order to address the threats identified in the risk assessment.
	Organizational	**O1**	Define a dedicated Information Security Management System (ISMS). Each trial site should define an ISMS, possibly inspired from SAE J3061, ISO 27001 or NIST 800-53, and refine it to address the specific needs of the trial site.
		O2	Assess the threat model and use cases. Each trial site should perform a threat analysis prior to development possibly inspired from SAE-J3061 TARA approach (including EVITA, TVRA, OCTAVE and HEAVENS methods) or possible from the risk management approach of ISO 31000. Efforts in this direction are also done in the context of ISO AWI 21434.
		O3	Perform vulnerability surveys, Assess the security controls and patch vulnerabilities
	Technical	**T1**	Each trial site should consider denial of services and other risks as a real danger to the infrastructure availability, security and privacy by mitigating vulnerabilities and limitation of used libraries by patching and securing the communication between s the entities of the 5G-MOBIX high-level reference architecture.
		T2	Each trial site should use multi-factor authentication for user authentication to vehicle and cloud services, mobile interfaces and local administration sessions of devices
		T3	Each trial site should implement access control measures to separate the privileges of different users and the privileges of different applications in the vehicle, roadside and cloud infrastructures as well as to ensure traceability of access and modifications
		T4	Each trial site should rely on an expert in cryptography in

			their security team
		T5	Each trial site should follow Cryptography State-of-the-art standards in order to implement a secure communication between all the components of the 5G-MOBIX high level reference architecture
		T6	Each trial site should log security events for future audit

4.5.1. Specifications on communication interfaces towards 5G network

This section describes the security requirements on the set of network interfaces used for 5G-MOBIX uses cases in the different trial sites. These interfaces are composed of the 3GPP Radio Access Technologies (RATs) LTE-V2X and the ETSI ITS-G5. However, other RATs are considered such as Bluetooth, Wi-Fi and ZigBee.

Network Interface NI V2R (and NI V2V)

These requirements are similar for Vehicle-to-Vehicle (V2V) (vehicles with On-Board Units, OBUs) and between vehicle and roadside units, RSU (V2R with R = RSU) when applicable in the latter case.

Table 27 Security requirements on the Network Interfaces V2R and V2V

Requirement ID	Description
Sec-NI-V2R-3GPP	• Cf. D2.2
Sec-NI-V2R-ETSI-G5	• No security mechanisms have been defined at the link layer for the ETSI ITS-G5. Therefore, when non-safety messages are being sent using this RAT necessary security mechanisms should be used to guaranty the confidentiality and integrity of the messages.
Sec-NI-V2R-Others	• When other RAT is used such as Wi-Fi, Bluetooth or ZigBee, the necessary mechanisms to assure the confidentiality, integrity and authenticity of the messages should be used. Complementary information from each trial site could be provided.

Network Interface NI R2N

This section describes the requirements related to the Network interfaces NI-R2N.

Table 28 Security Requirements on the Network Interface R2N

Requirement ID	Description
Sec-NI-R2N-3GPP	• Cf. D2.2
Sec-NI-R2N-Others	• When the roadside infrastructure supports other types of RATs and acts as a gateway, the necessary mechanisms should be implemented to protect the confidentiality, integrity and authenticity of the messages.

Network Interface NI V2N

Table 29 Security requirements on the Network Interface V2N.

Requirement ID	Description
Sec-NI-V2N-3GPP	• Cf. Sec-NI-V2R-3GPP
Sec-NI-V2N-Others	• Cf. D2.2

Network Interface NI C2N

Table 30 Security requirements on the Network Interface C2N.

Requirement ID	Description
Sec-NI-C2N-3GPP	• Cf. D2.2.
Sec-NI-C2N-MEC	• CF. D2.2
Sec-NI-2N-Slicing	• Cf. D2.2

4.5.2. Specifications on Application Interfaces

This section describes the security requirements on the Application Interfaces of the 5G-MOBIX high level reference architecture with interfaces AI V2V, V2R, V2C, R2C and C2C as shown in Figure 45.

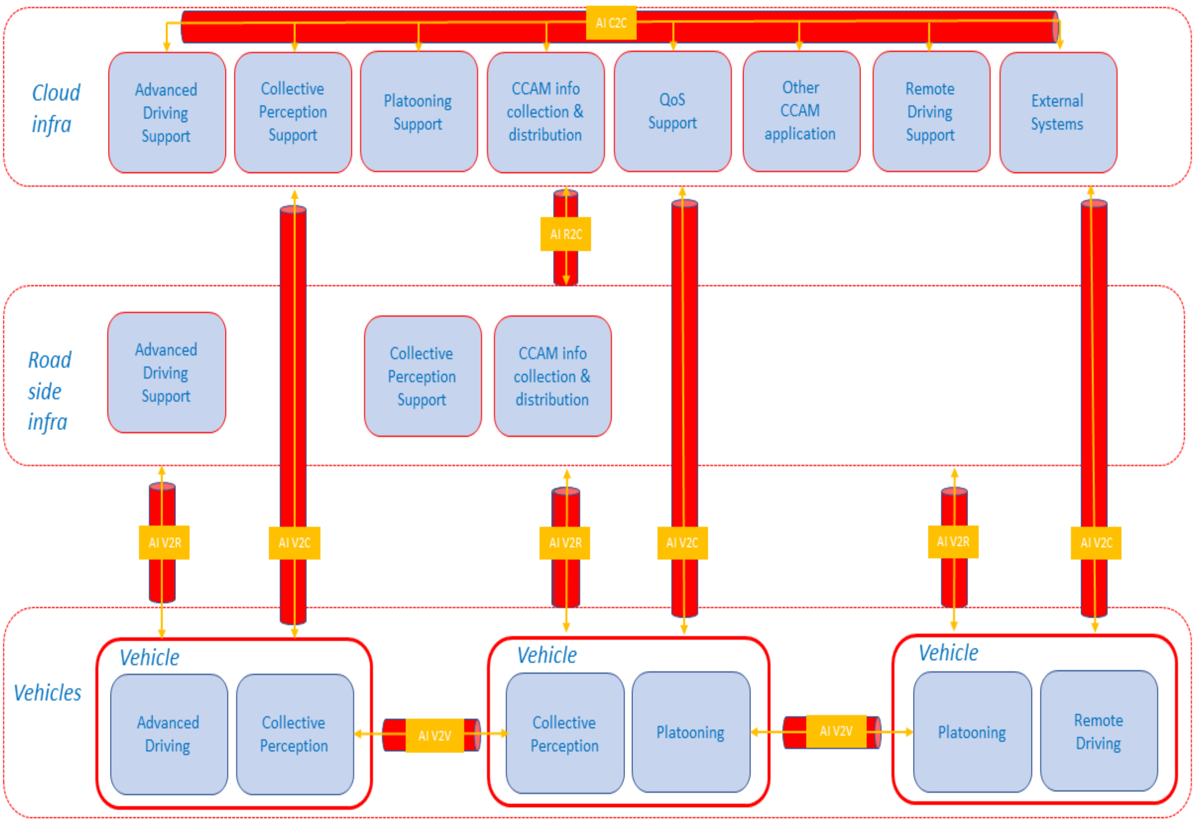


Figure 45 Secured Application interfaces in the 5G-MOBIX reference architecture

Application Interface AI V2R (and AI V2V)

Table 31 Security requirements on the Application Interfaces V2R and V2V

Requirement ID	Description
Sec-AI-V2R	• The different messages exchanged for the use case categories should be protected (integrity and authenticity) using the ETSI TS 102 941[27] and an implementation of the EU CCMS. These messages are: CAM, DENM, IVI, SPAPT, MAP, MCS, CIM, CPS, PCM, and CAAC. • Compliance with a Common trust domain should be assured when dealing with messages (CAM, DENM, IVI, SPAPT, MAP, MCS, CIM, CPS, PCM, and CAAC) from other trust domains (China, Korea and Turkey).
Sec-AI-V2R-	• For the remote driving and Vehicles Quality of service use case categories,

[27] https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v0

Others	complementary security requirements are to be provided per trial site.

Application Interface AI V2C

This section describes security requirements for the message sets defined for the interface AI V2R. These messages may also be exchanged from cloud systems via interface AI V2C for Advanced Driving (I2V), Collective Perception and Platooning. A CCAM collection and distribution server may be used to collect and forward messages, related to a geographical area.

Table 32 Security requirements on the Interface V2C

Requirement ID	Description
Sec-AI-V2C	• CAM, DENM, IVI, SPAPT, MAP, MCS, CIM, CPS, PCM, and CAAC received by the vehicle on the AI-V2C interface are protected as set by Sec-AI-V2R.
Sec-AI-V2C-Others	• For the remote driving and Vehicles Quality of service use case categories, complementary information could be provided per trial site for the non-standardized messages. • User stories specific messages might use other security mechanisms to assure the confidentiality, integrity and availability of the specific message. These security requirements are provided by trial sites.

Application Interface AI R2C

This section describes security requirements for the message sets defined for the interface AI R2C.

Table 33 Security requirements on the interface R2C

Requirement ID	Description
Sec-AI-R2C	• CAM, DENM, IVI, SPAPT, MAP, MCS, CIM, CPS, PCM, and CAAC received by the vehicle on the AI-V2C interface are protected as set by Sec-AI-V2R
Sec-AI-R2C-Others	• For the remote driving and Vehicles Quality of service use case categories, complementary information could be provided per trial site. • User stories specific messages might use other security mechanisms to assure the confidentiality, integrity and availability of the specific message. These security

	requirements are provided by trial sites.

Application Interface AI C2C

This section describes security requirements for the exchange of information between central systems of existing data formats like DATEX-II, TPEG and ETSI / CEN messages is possible via AI C2C. Examples are e.g. the exchange of local and global dynamic map, exchange of event-based message between OEMs, road operators and other information providers, access to live video feeds from roadside camera /radar systems etc.

Table 34 Security requirements on the interface C2C

Requirement ID	Description
Sec-AI-C2C	• CAM, DENM, IVI, SPAPT, MAP, MCS, CIM, CPS, PCM, and CAAC received by the vehicle on the AI-V2C interface are protected as set by Sec-AI-V2R. • The integrity, confidentiality and availability of DATEX-II and TPEG messages should be assured.
Sec-AI-C2C-Others	• For the remote driving and Vehicles Quality of service use case categories, complementary information could be provided per trial site. • User stories specific messages might use other security mechanisms to assure the confidentiality, integrity and availability of the specific message. These security requirements are provided by trial sites.

4.5.3. Other specifications

This section presents security requirements on geomessaging.

Table 35 Security requirements on Geomessaging

Requirement ID	Description
Sec-AI-Other-Geomessaging	• Pilot sites using Geomessaging should protect the confidentiality, integrity and availability of these messages.

5. EXTENDED EVALUATION

In this section the complemented and added value of the local trials to the CBC trials in ES-PT and GR-TR for each of the UC categories is described, together with the additional facilities provided. This is described for the local trials in DE, FI, FR and NL.

5.1. UC cat.1 extended evaluation on Advanced Driving

5.1.1. Complementarity & added value to CBC trials

Complementarity & added value from FR trials

Advanced driving decisions can be made solely in the vehicle or can be assisted by infrastructure. The latter case can be more efficient since the infrastructure can offer an improved perception, stronger communications and/or computing capabilities.

To this end, the FR site will evaluate infrastructure-assisted advanced driving. To do so, both the vehicle and the infrastructure need to have a complete perception of the environment. To build such a perception, vehicles and infrastructure have to exchange CPMs and fuse the data obtained from sensors, CPM and CAMs. This phase is followed by a risk analysis procedure that aims to determine if the vehicle is in hazardous situation or not, and if it have to carry out an advanced driving manoeuvre such as lane change, lane merge, etc. If it is the case, then a trajectory calculation is carried out and an MCM message exchange is required to enable the manoeuvre start.

The ES-PT corridor has considered the case where all this intelligence is located only in the vehicle. In addition, an implementation in roadside infrastructure will add an extra huge work load to their site.

On the other hand, the FR site is implementing infrastructure-assisted lane change manoeuvre where the intelligence mechanism (CPM construction, data fusion, risk analysis, trajectory guidance calculation) is made on the infrastructure side. In this scheme, the RSU will be responsible to send MCM messages to vehicles required to do an advanced driving manoeuvre.

The same observation is also made for CPM implementation in the roadside infrastructure, where the ES-PT corridor implementation is restricted to the OBU side, while the FR site is carrying this functionality in both OBU and RSU side.

Complementarity & added value from NL trials

The NL TS will develop the following functionality, complementary to the CBC ES-PT site:

- CoCA: Application of the Manoeuvre Coordination Service (MCS): Manoeuvre Coordination Service (MCS) that is still under preparation at ETSI ITS

- Seamless hand-over between two independent PLMN 5G networks to enhance ES-PT single supplier trial
- Two schemes to support CoCA: In-vehicle-based and MEC-based application of CoCA to support ES-PT scenario on overtaking
- Support of two communication schemes: network-based communication (V2N – Uu interface) and direct communication (V2V – PC5 interface): a hybrid scenario with long range (Uu interface) and short range (PC5 interface) will be evaluated
- Collision risk detection in CAV application, alternative/backup at MEC App
- Application of MCS in addition to CAM-based manoeuvring – to support other manoeuvring like overtaking
- Testing in full highway environment

Complementarity & added value from CN trials

The CN TS will develop the following functionality, complementary to the CBC site:

- Seamless connection between 4G and 5G networks to ensure network connectivity in areas not covered by 5G.
- Data type processing and conversion of MEC when the network is transferred from 5G to 4G.
- Collaborative interaction between MEC and CBC.
- Backup and management of data in CBC's cloud systems.

5.1.2. Additional facilities for UC cat.1 evaluation

Additional facilities at FR trial site

Automated vehicles have to coordinate their manoeuvres to improve the traffic safety and efficiency. To support such coordination, ETSI is currently defining the Manoeuvre Coordination Service (MCS), and The standardization process is still at its early stages. The current approach is based on a distributed solution where vehicles coordinate their manoeuvres using V2V (Vehicle-to-Vehicle) communications. This solution is based on exchanging the planned and desired trajectories using V2V communications. The proposal is divided into three steps. First, the need to coordinate a manoeuvre is detected by the involved vehicles. Second, the type of coordination is agreed between the involved vehicles. Finally, the cooperative manoeuvre is executed.

In the FR site, we propose to extend the current MCS approach to also consider for the possibility to utilize road infrastructure to support the coordination of manoeuvres under certain scenarios and conditions. This proposal exploits V2I communications and is fully complementary to the current V2V-based approach. On the other hand, the advanced driving use case in ES-PT corridor won't use MCM messages for testing.

Hence, the FR site is going to implement the MCS service in both RSU and vehicle side and then provide feedbacks and advisory on how the MCM service from roadside perspective can help in more efficient lane change manoeuvre.

Additional facilities at NL trial site

The NL assets that will be developed are:

- Specific approach of NL TS in testing of Manoeuvre Coordination Service (MCS) that is still under preparation at ETSI
- Seamless handover between two independent and different supplier 5G NWs only at NL TS to enhance ES-PT single supplier trials
- In-vehicle and MEC manoeuvring calculation integration only at NL TS to support ES-PT Overtaking
- Collision risk detection and calculation addressed only at NL TS to benefit EP-PT Overtaking
- Intelligence in the CAV addressed mainly at NL to benefit ES-PT user experience
- Testing in full highway environment to benefit ES-PT compared to border-crossing site

Based on these functions the following evaluation scenarios will be performed:

1. Applicability of MCS in Highway environment for various manoeuvring functions,
2. Applicability of CoCA
3. Manoeuvring risks calculated both in CAV and MEC
4. Cooperation among two CAV & two 5G networks, support ES-PT
5. Hybrid scenario with long range (Uu interface) and short range (PC5 interface) to determine preferences and minimum requirements for different communication protocols
6. Hand-over between MNOs with 5G Slicing enabled
7. Application integration between in-vehicle, MEC and 5G networks

Even if CoCA is not in use at ES-PT, CoCA supports various CAV manoeuvring at this cross-border site.

Complementarity & added value from CN trials

CN site will test scenes like bridge, long steep slope, ramp, toll station and some other places. At these scenes overtaking is not allowed for some safety regulations. It is difficult to place enough road 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 on dangerous situations. Also, platooning with remote driving is complementary from a single vehicle with remote driving. Not only the head of the platoon will be controlled, the rest of vehicles will be monitored as well.

5.2. UC cat.2 extended evaluation on Vehicles Platooning

5.2.1. Complementarity & added value to CBC trials

UC cat.2 "Vehicle platooning" is implemented by the CBC GR-TR with the user story "Platooning with 'see what I see' functionality in cross-border settings". Extended evaluations of the US are implemented at DE TS with "eRSU-assisted platooning" and at CN TS with "Cloud assisted platooning" user stories.

The implementation at CBC GR-TR can cover essential platooning operations with the main focus on the high-level application of zero-touch vehicle inspection and autonomous border crossing. The realization of cross border platooning scenarios relies solely on cloud and MEC platforms, which are optimally connected with two PLMNs on both side of the border for low latency and high bandwidth communication. The settings of GR-TR CBC limit the diversity of platooning scenarios that can be carried out. There is a hard border at GR-TR CBC which only allows slow and longitudinal traffic flows through the trial area (customs inspection zone). The involved vehicles are SAE-L2 trucks with limited autonomous driving capabilities. Extensive road infrastructure deployment may not be possible due to authority restriction. As the results, the following scenarios are trialled at GR-TR CBC:

- SAE-L2 longitudinal truck platooning
- "See what I see" application with 4K video streaming in platooning fleet.
- Session continuity supported by 5G based V2C communication infrastructure.
- Inter PLMNs handover with LBO solutions.
- Extended evaluations and alternative approaches for the implementation of the platooning scenarios are implemented and trialled at DE and CN TS and described next.

Complementarity & added value from DE trials

In contrast to the settings of GR-TR CBC, the test road at DE TS allows the trialling of platooning scenarios in highway setting and mixed traffic flows. The road infrastructure is fully deployed with sensors, eRSU, roadside MEC and cloud computing infrastructure. Along the 4 km straight road, various type of road sensors (traffic analysis, road condition, environment, weather) and eRSU platform are deployed and fully connected (see D 2.1 for detailed description of DE TS). 5G coverage for the test road is provided by 2 PLMNs enabling the realization of national and international roaming scenarios. Therefore, the platooning user story "eRSU assisted platooning" at DE TS can complement GR-TR CBC scenarios with more complex platooning operations and alternative solutions based on V2R and V2V communication. The platooning use case is realized with autonomous overtaking operation, which requires the AVs (SAE L-4) to coordinate to carryout longitudinal and latitudinal manoeuvres. The AVs are provided with increased situational perceptions aggregating all road sensor data and made available by EDM services deployed at eRSUs. As the result, the infrastructure of DE TS to support platooning includes a range of ITS services, distributed roadside MEC and orchestration platform to support session continuity and mobility management. Following additional scenarios are trialled at DE TS:

- Autonomous overtaking operation carried out by SAE-L4 vehicle platooning

- Pipelining vehicle data among vehicles and mainly rely on C-V2X and RSUs infrastructure for data communication and processing
- Demanding and scalable processing performed at the MEC for sensor data fusion and EDM ROI filtering
- Roaming and network handover scenarios during platooning operations requiring replication of CCAM services (states) from RSU to RSU.
- Management and orchestration of shared resources and applications deployed on distributed eRSUs.

Overview of complementary roadside infrastructure

The roadside infrastructure at DE TS consists of more than ten eRSUs along a 4 km test road. The eRSUs are connected with both large coverage of 5G networks and WLAN based direct communication. Each eRSU is also equipped with multiple radio interfaces and computing capability allowing it to serve as a near edge MEC node. The eRSUs create a digital layer at the road infrastructure for distributed and multi-access interaction models between centralized and distributed CCAM service instances deployed in the cloud, roadside and AVs. This extensive eRSUs deployment at DE TS has unique features compared to the cloud based CCAM services at other CBCs and TSs to realize complex AD operation. Platooning AVs can take advantages of the roadside infrastructure for V2X communication and added perception for autonomous decision making. The management and orchestration of distributed services and infrastructure at DE TS pose many new challenges, which require novel approaches to be developed to achieve flexibility and resource efficiency, which could provide insights for enhancement and extension of AD infrastructure at CBCs.

Overview of complementary Cloud infrastructure

Beside the centralized cloud infrastructure, a low latency MEC (far edge) platform is deployed with a direct connection to the 5GC. As a result, the far edge provides comparable computing resources for CCAM services while also guarantee low latency for high QoS requirements. Compared to other MEC deployment model, i.e., MEC hosting 5GC, the cloud infrastructure at DE TS allows 5G network to be used as transport network for distributed and centralized cloud platforms. 5G network can be sliced for each type of CCAM services with general QoS of service requirements and the management of the service instances can be focus on the application service levels given available computing and network resources.

More details of the DT TS infrastructure and interfaces to support the scenarios above are provided in Section 7.2.1.

Complementarity & added value from CN trials

CN site will test scenes like bridge, long steep slope, ramp, toll station and some other places. 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 bad situations.

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.

5.2.1. Additional facilities for UC cat.2 evaluation

Additional facilities at DE trial site

With the focus on eRSU assisted platooning scenarios in mixed traffic, the implementation at DE TS rely on fully connected eRSU infrastructure, which is managed and orchestrated by a centralized platform deployed on the cloud. Additionally, various type of sensors with specific communication interfaces are also deployed and integrated with the eRSUs providing perception data for EDM services. While a portable eRSU with sensors platform can be integrated with GR-TR CBC infrastructure for inter-operability testing, an extensive replication of DE TS deployment is not possible due to geographical setting and authority restrictions at CBC. As the results, the trialling of platooning scenarios at DT TS is needed to provide additional evaluation and assessments for possible enhancement of CBC infrastructure to fully support vehicle platooning UC. Possible evaluation results are:

- Network QoS requirements to support high-speed platooning operation in mixed traffic
- Platooning performance with V2X support
- Flexibility of CCAM infrastructure management to support multi-tenancy, on-demand deployment and service mobility
- Security and privacy enforcement in various configurations of roaming and handover scenarios.

Additional facilities at CN trial site

Platoons in CN site can past safely when in such scenes like bridge, long steep slope, ramp, toll station. The experiment of this scenario has to 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.

5.3. UC cat.3 extended evaluation on Extended Sensors

5.3.1. Complementarity & added value to CBC trials

Complementarity & added value from DE trials

The CCAM infrastructure of the DE TS with extensive roadside components deployment as highlighted in Section 5.2.1.1 also enable the trials of the use story "dynamic map with surround view" with alternative solution approaches compared to other CBCs and TSs. The scenarios involve a highly demanding 360° and HD digital map, which are constructed by distributed services from various roadside and vehicle sensor data. Moreover, such services must attain a constant QoE for AD trials along the whole test road. Such requirements beyond basic AD operations require solution approaches that can complement other TSs implementation as summarized below:

- Distributed cloud native infrastructure spanning across near edge, far edge and cloud infrastructure
- E2E approach for autonomous multi-domain and multi-tenant cloud and network infrastructure management to achieve increased flexibility and efficiency
- Realization of distributed CCAM services for increased environment perception and situation awareness through ubiquitous data sources
- Realization of interaction models and platform for multi-stakeholder resource and service composition

Complementarity & added value from FI trials

The FI TS user story *US8 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. This is distinct from the static approaches is originally considered in the CBCs. However, it is noted in Section 3.4.3 that there are tentative plans to transfer and test these dynamic MEC functionalities in ES-PT CBC at a later stage.

Complementarity & added value from NL trials

The NL TS will develop the following functionality, complementary to the CBC ES-PT site:

- Slicing setup with SA core.
  - Investigate how slicing will work in a X-border scenario
  - Design slices incorporating slices for 1. Video, 2. V2X messages and 3. Other data (mostly log data)
  - Design and test out the different parameters with the requirements for latency, bandwidth, etc.
  - Performance continuity with handover to different MNO using either static or dynamic setup.
- Service discovery with multiple MEC's, SSC and LADN.
  - Goal is to have the vehicle connect to the best message exchange compared to the overall latency.
  - Integration between message exchange, in vehicle application and 5G network is expected.
- Message exchange:
  - Providing and implementing an architecture based on MQTT where messages are published on topics specifying the geolocation using tiles (similar to EU projects Concorda, InterCor and the Dutch project Talking Traffic).
  - Designing and implementing a dynamic architecture for message exchange between different edges optimizing the volume of messages based on actual requests.
  - Assess the use of Collective Perception Message with existing roadside camera system
- Handover optimizations with 5G Core

5.3.2. Additional facilities for UC cat.3 evaluation

Additional facilities at DE trial site

The same added facility of DE TS described briefly in Section 5.2.2.1 is applied for the trials of extended sensor scenarios. Full detail of the CCMA infrastructure is provided Section 7.2.1 and 7.3.3.

Additional facilities at FI trial site

The evaluation scenarios leverage the multi-MEC multi-PLMN environment provided at the FI TS. 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 test dynamic MEC functionalities under different 4G/5G network configurations and handover scenarios.

Additional facilities at NL trial site

The NL site will develop and evaluate a dynamic architecture for message exchange between different edges – both within a single PLMN and between edges of different PLMNs - optimizing volume of messages based on actual requests. The NL site will also develop and assess the use of Collective Perception Service with the existing roadside camera system for vehicle detection and localization.

5.4. UC cat.4 extended evaluation on Remote Driving

5.4.1. Complementarity & added value to CBC trials

Complementarity & added value from FI trials

The user stories under the remote driving UCC in the ES-PT CBC 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.

However, there exists 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 have 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 "*US9 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).

Complementarity & added value from NL trials

The NL TS will develop the following functionality, complementary to the CBC ES-PT site

- Virtual remote control
- Handover for remote driving with 2 PLMN
- Fleet management system to organize control of vehicle between different human and virtual operators: a human and virtual remote driver interact trough a fleet management platform and can dynamically take control or pass control to different drivers, possibly located in different networks
- Vehicle positioning via mmWave: mmWave localization will improve Automated Driving redundancy / safety; mmWave requires an integrated hardware design of both the vehicle 5G NR OBU as well as the gNBs. TU/e deploys a mmWave 5G NR network for this reason locally in NL TS.

Complementarity & added value from CN trials

The CN trials will develop the following functionality:

- Real-time 5G-based HD video. This HD video backhaul test has been made, which employed a manned vehicle to transmit HD video back to the control centre via 5G. Meanwhile, the control screen showed road condition in real time.
- Multiple trial scenes. Especially places like tunnel, which would influence the transmission of 5G signal. Also, the topography and landform condition is essential for evaluation of 5GMOBIX 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 have to take actions according to its situation.

5.4.2. Additional facilities for UC cat.4 evaluation

Additional facilities at FI trial site

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.

Additional facilities at NL trial site

The additional facilities for Remote Driving at the NL TS are:

- Fleet management system to organize control of vehicle between different human and virtual operators: a human and virtual remote driver interact trough a fleet management platform and can dynamically take control or pass control to different drivers, possibly located in different networks
- Vehicle positioning via mmWave: mmWave localization will improve Automated Driving redundancy / safety; mmWave requires an integrated hardware design of both the vehicle 5G NR OBU as well as the gNBs. TU/e deploys a mmWave 5G NR network for this reason locally in NL TS.

Additional facilities at CN trial site

The additional facilities for Remote Driving at the CN TS are:

- 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.

5.5. UC cat.5 extended evaluation on Vehicle QoS Support

5.5.1. Complementarity & added value to CBC trials

Complementarity & added value from FR trials

To support a hybrid network configuration, a QoS adaptation is needed. This latter can be made in the vehicle as well as in the infrastructure side (MEC) in order to guarantee application continuity. In fact, this is very challenging since, even in a poor network condition status, we have to ensure that the data is sent to a remote-control entity. Since the ES-PT corridor is focusing on the OBU side, the FR site is providing QoS adaptation mechanism from the MEC perspective. In this operation, the MEC, which is receiving input data from roadside sensors, will adjust the data type, data size, date rate, etc. based on the link connectivity quality.

5.5.2. Additional facilities for UC cat.5 evaluation

Additional facilities at FR trial site

The FR site aims to extend the ES-PT QoS use case by adding a QoS adaptation mechanism on the infrastructure side (MEC). By developing the required software platform in the MEC side, the FR site can provide useful feedbacks on how a MEC-based intelligence can help in ensuring service continuity.

In addition, the FR site will develop the perception at the infrastructure side, while the ES-PT corridor is only focusing on the vehicle side. This aims to help in monitoring the automated vehicle when it's moving in the road. This will be carried out through making sensors data fusion at the MEC and sensing CPM messages from RSUs to vehicles. As previously highlighted in section 5.1.1.1, this extended evaluation will highlight the added value of the roadside infrastructure in QoS vehicle support use cases.

6. CONCLUSIONS

The document 5G-MOBIX D2.1 describes the 5G-MOBIX user stories in 5 UC categories. This document D2.3 describes the roadside and cloud infrastructure and applications for each user story in 5G-MOBIX. The descriptions are grouped per category: Advanced Driving, Vehicles Platooning, Extended Sensors, Remote Driving and Vehicle QoS Support. In this way the specifications can be aligned along the cross-border corridors and the inland trial sites.

The main observations for future work in 5G-MOBIX on development, deployment and evaluation (WP3, WP4 and WP5) are:

- Roadside perception systems are used to support Advanced Driving and Extended Sensors at complex/dangerous locations for (non-equipped) vehicle detection and localization or for localization of other non-equipped road users. The specifications on different implementations of Extended Sensors needs to be aligned across trial sites.
- Most trial sites use concepts of edge cloud or MEC with distributed data centres and close integration with 5G-network topologies. These edge cloud or MEC nodes are used e.g. to support Advanced Driving and Extended Sensors for local collection, processing and distribution of information with high-performance and minimal latency. Specifications need to be further aligned for cross-border support (i.e. inter-MNO, inter-MEC) to support the edge cloud or MEC concepts including MEC hand-over in a single PLMN and interconnection of MEC solutions in multi-PLMNs.
- Cloud infrastructure is used in several ways to support platooning, e.g. via dynamic map updates, route planning, and network-based support for "see-through". The 5G network infrastructure can be used to exchange (geo-location-based) information between vehicles (V2N2V) - in addition to direct C-V2X communication between AD vehicles to improve performance.
- Special attention will be given in 5G-MOBIX on network and service continuity of the supported CCAM use case categories along the cross-border corridors and trial sites, both from technical and business perspective. The 5G-MOBIX use case categories need to be supported for AD vehicles from multiple OEMs (inter-OEM), across multiple 5G networks (inter-MNO), across multiple MEC-providers (inter-MEC) and with multiple external information providers (e.g. local road operators, traffic information providers), external CCAM providers (e.g. companies with remote driving facilities across Europe) and or (distributed) cloud providers.
- The issues on CCAM service and network continuity for applications in cross-border corridors in Europe are explained together with the evaluation scenarios specific to the trials sites.

7. APPENDIX: DETAILED DESCRIPTION OF ROADSIDE AND CLOUD INFRASTRUCTURE PER TRIAL SITE

7.1. Category 1: Advanced Driving

In this section the roadside and cloud infrastructure are described for the following User stories:

1. FR US10 (Infrastructure-assisted advanced driving)
2. NL US12 (Cooperative Collision Avoidance)
3. CN US15 (Cloud-assisted advanced driving)

7.1.1. Roadside & cloud infrastructure for FR US10

Description

This use case deals with safe lane change manoeuvre dictated from road operator in presence on a multi-lane highway in presence of separation signs between the different lanes. The most critical factors of lane change manoeuvres comprise the following: a safe distance to the oncoming separation signs when initiating the lane change operation and a safe gap to the connected vehicle behind coming in the same direction, but on a different lane.

Consequently, such a system requires the capability to manage the speed and steering in a coordinated manner, thereby minimizing collision risk with neighbouring vehicles in a hybrid environment (connected, automated, basic vehicles).

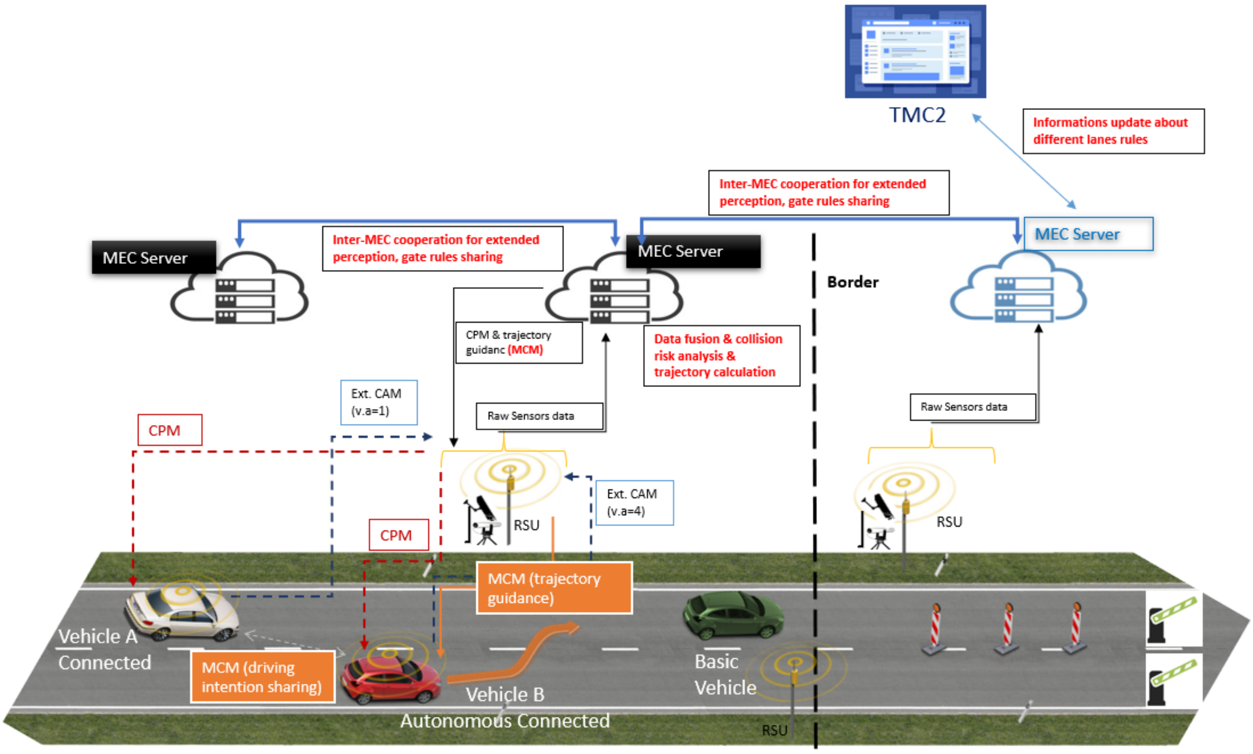


Figure 46 Infrastructure for FR US10 (Automated overtaking)

In the following, we present a high-level architecture of CCAM infrastructure that will be used for this user story. As illustrated in Figure 47, physical elements along the road infrastructure as well as cloud systems will be described hereinafter.

High-level architecture of the CCAM infrastructure

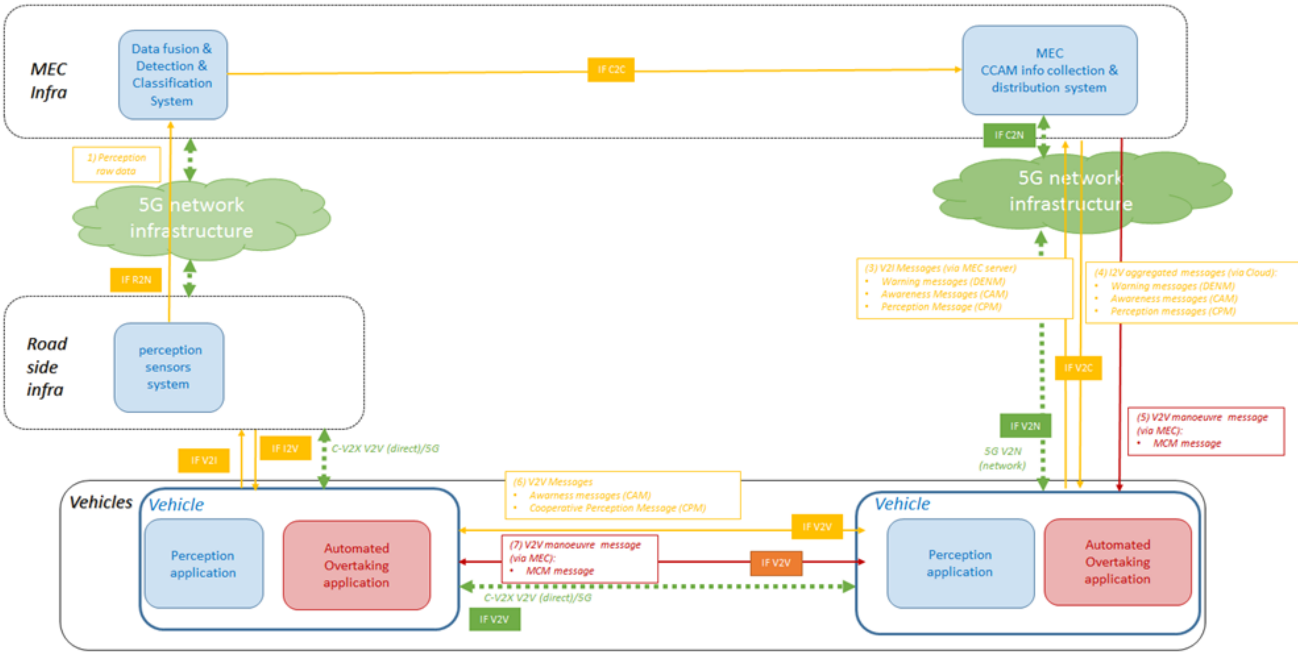


Figure 47 High level CCAM architecture of FR US10 (Automated Overtaking)

Detailed Description

The automated overtaking user story will use the following standardized/pre-standardized ITS messages:

- Cooperative Awareness Message (CAM) from vehicle-to-vehicle. These messages provide information about the vehicle characteristics. (size, type of vehicle, position, velocity, etc).
- Cooperative Perception message (CPM) is the mechanism under standardization at ETSI that allows providing, through V2X communication, the roadside perception towards the vehicles around the roadside station. At receiving station (OBU), the CPM messages are provided to the vehicles (PC-AD) on an event driven mode (each time a CPM is received by OBU it is delivered to the PC-AD).
- MCM message: The ETSI TC ITS is currently defining the Manoeuvre Coordination Message (MCM) which can be used to coordinate manoeuvres between ITS stations. The MCM is at early stage of standardization[28]. VEDECOM through PACV2X project[29] is actively contributing to the standardization process by participating in all the meetings and presenting the PACV2X proposals for the MCM. The MCM messages will be sent by the MEC and between the vehicles to negotiate the changing lane manoeuvre.

[28] ETSI TS 102 561 Intelligent Transport Systems (ITS); Vehicular Communications; Basix Set of Application, Manoeuvre Coordination Service V0.0.1 (2018-01)

[29] https://project.inria.fr/pacv2x

The message can be exchanged either via:

- Direct communication (without 5G network infrastructure) between vehicles and between vehicle and roadside infrastructure with C-V2X communication units.
- Network-based communication: the automated vehicle is connected to the MEC server through a 5G connection. The vehicle receives MCM and CPM messages when trying to change the lane and to increase its perception respectively.
    a. MEC CCAM server (connected to 5G network of operator X)
    b. Roadside-specific server connected to roadside communication units (5G UE-type supporting direct C-V2X and connected to 5G network of operator X)

Road Communication infrastructure

The deployed user story will benefit from the already installed communication infrastructure at Saclay site. The physical architecture is mainly composed of the different roadside infrastructures that will be installed along the testing area. RSUs will be installed along the road, equipped with both ITS-G5, 5G and cellular/optic fibre communications to let them communicate with distant servers.

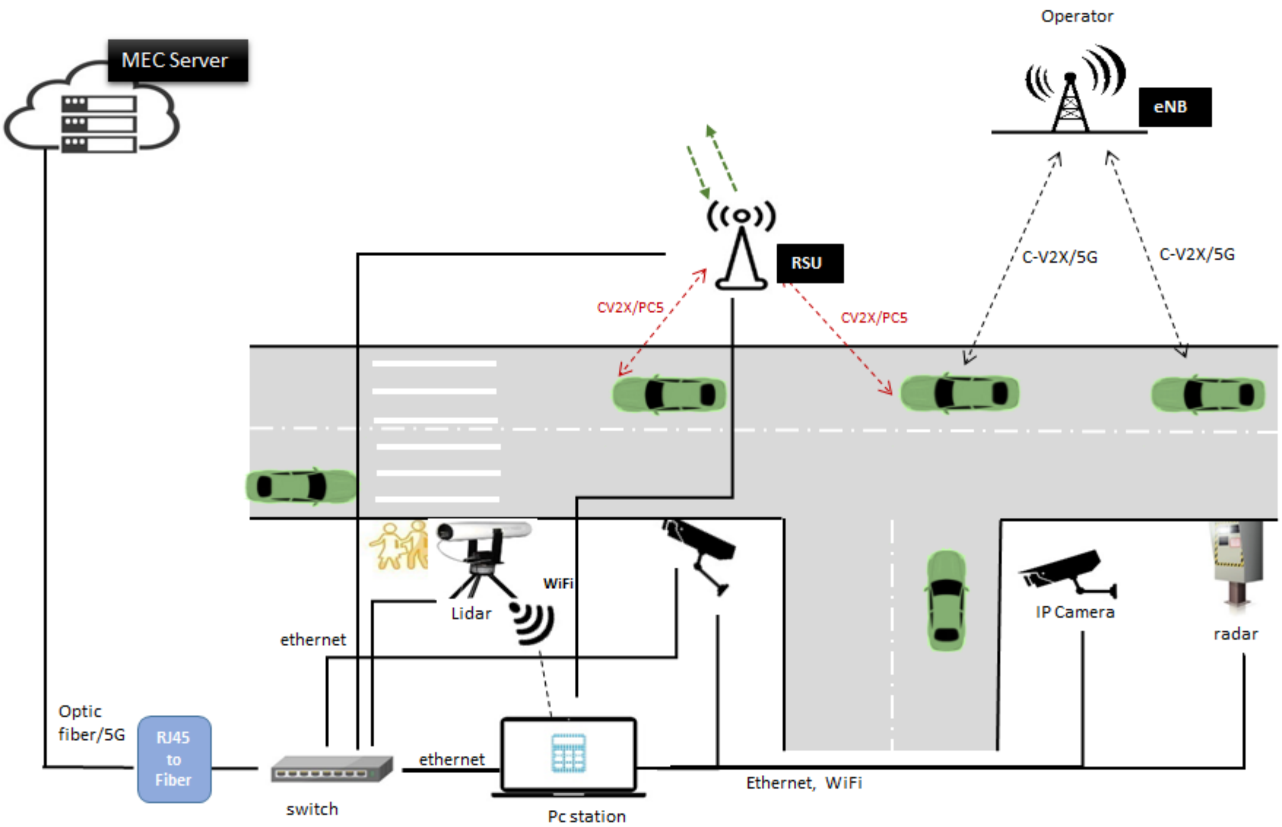


Figure 48 Physical infrastructure at French trial site

During the 5G-MOBIX project, the sensors, and cameras systems will be transferred to UTAC/CERAM site to carry out tests there.

In addition, cameras, lidars at the site. They will be connected through Wi-Fi or Ethernet connection to the MEC server. This latter is responsible of the fusion of different data coming from cameras, sensors, lidars, etc.

Roadside Perception infrastructure

The Roadside Perception is the capability to enhance the vehicles' local perception by roadside sensor information. Particularly, while a vehicle builds a certain level of perception based on its embedded sensors, the roadside perception is to enhance the vehicle's perception with the information obtained from the roadside sensors.

Different types of sensors are installed at the roadside, such as

- Optical camera,
- Thermic (I/R) camera,
- Lidar,
- LEDDAR (Light-Emitting Diode Detection And Ranging, focused light is used, Time-of-Flight to derive distance, mechanical type of sensor, flash and detect the environment, up to 50 m in theory less in practice). LEDDARS are typical cheaper than Lidars, and Object detection performance is better than radars. LEDDARS is not necessarily better in terms of classification performance.

The goal behind these sensors is

- Provide the sensor raw data to a central server, that can be digital images, cloud points or digital descriptions of objects, size, speed.
- Detect, localise, and classify road objects such stationary vehicles, work zone elements, this information to be broadcasted to vehicles in the area and transmitted to the MEC.

MEC infrastructure

The MEC server is interacting with all the RSUs and road infrastructure equipment installed along the testing area. Its main goal is to ensure that:

- RSUs and infrastructures are provided with the good configuration parameters to work properly
- Infrastructures must periodically report their status (through logs for example) and send their data (video from camera, photos, traffic light status, etc.) to the RSU server.
- The RSU server is responsible to store and maintain data received from RSUs and infrastructures. It has also to provide other servers (such as Teleoperation center, Dispatcher and OEM server) with the needed data.

Cross-border aspects

- Different ways to support interoperability at information exchange level
- Support of user story in inter-PLMN networks
- Support of edge server with hand-over between edge servers

7.1.2. Roadside & cloud infrastructure for NL US12 (Cooperative Collision Avoidance)

Description

The user story Cooperative Collision Avoidance (CoCA) is a safety-critical service where information is exchanged between ego-vehicle and alter-vehicles and between ego-vehicle and infrastructure (and vice versa) for collision avoidance. Connected and Automated Vehicles (CAV) and intelligent infrastructure solutions together are capable to provide technical and communications support for CoCA. 5G technologies provide the required low latency communications environment that is a prerequisite for any safety-critical ITS system or service

The CoCA service is to be deployed at a merging point of the A270 Motorway - N270 Highway between Eindhoven and Helmond (NL). CoCA targets to solve a challenging traffic situation on the motorway/highway environment. The Vehicle A ('ego vehicle', a foreign registered vehicle driving on the Dutch motorway/highway network) will make itself 'visible' and known to other traffic participants and to the infrastructure for Edge Computing through C-ITS messaging via 5G networks, and Cellular V2X (C-V2X) communication i.e. either LTE-based or 5G NR-based V2X. The Vehicle B ('alter vehicle', a Dutch registered vehicle) will submit similar information of its presence, speed and direction of movement to 'ego vehicle' and infrastructure as described above. Hence the 'Edge Cloud' infrastructure facilities can perform calculations and offload from the vehicles to the infrastructure and then return the suggested manoeuvring messages.

At the merging point of A270-N270 roads, the most critical path for cooperative automated driving is joining from a smaller road to the Motorway traffic flow via the left turn over the direct traffic flow that has a right-of-way for driving in highly automated mode through the merging point. The 'ego vehicle' that is approaching the merging point from a smaller road must be able to clear itself safely across the motorway/highway lanes to join the main traffic flow. When deemed necessary, the 'ego vehicle' need to safely stop autonomously before crossing the motorway/highway and start driving only when its calculated trajectory path is safe and clear for autonomous manoeuvring. For this purpose, the 'ego vehicle' must be able to utilise both its own desired trajectory and timing data and information from the roadside sensors as well.

The edge CCAM server is used to collect and distribute information from vehicles like awareness message (CAM) and Manoeuvre Coordination Messages (MCS). All information is collected by the edge CCAM server and forwarded in real-time to all relevant vehicles in the area around the merging point.

High-level architecture of the roadside and cloud infrastructure

The high-level architecture of the CCAM infrastructure for the CoCA service is shown in Figure 49.

The functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, the information exchange is shown in yellow. The architecture does not cover the cross-border aspects.

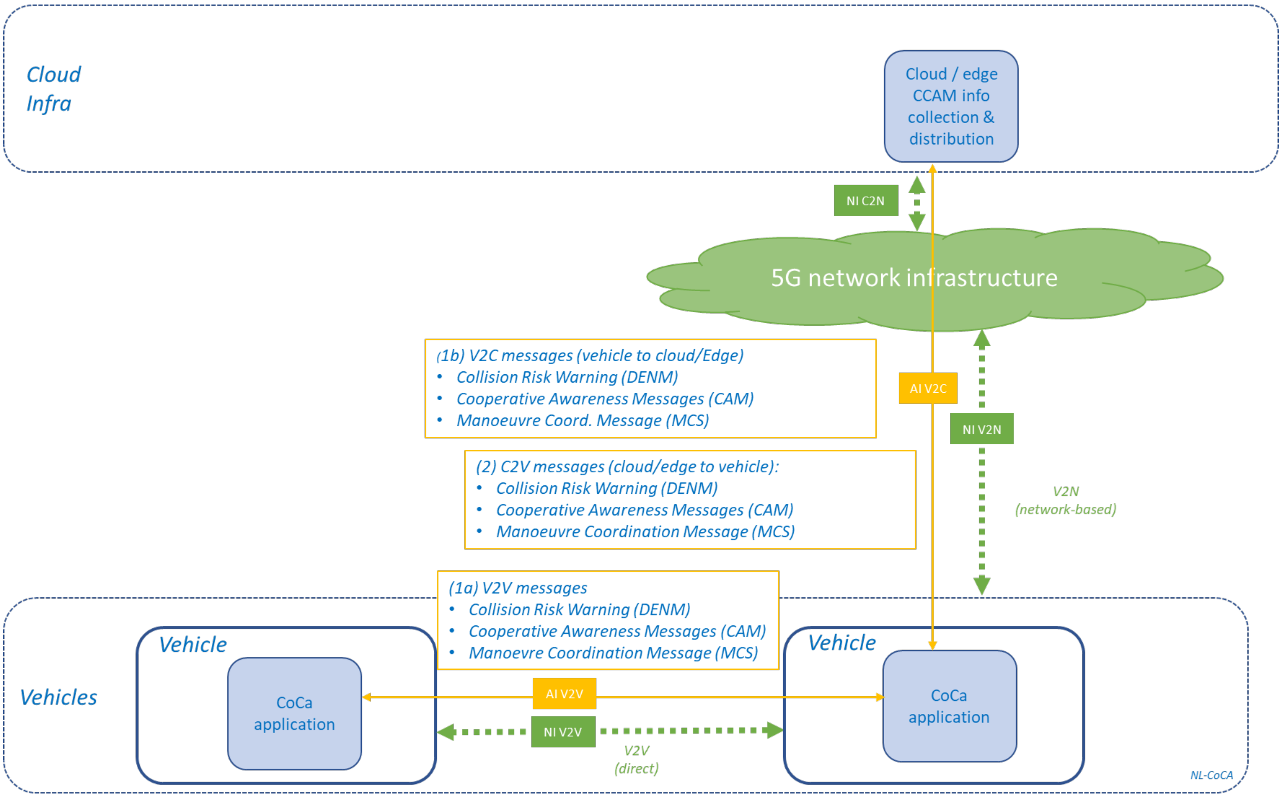


Figure 49 CCAM architecture of NL US12 (Cooperative Collision Avoidance)

Sequence diagram

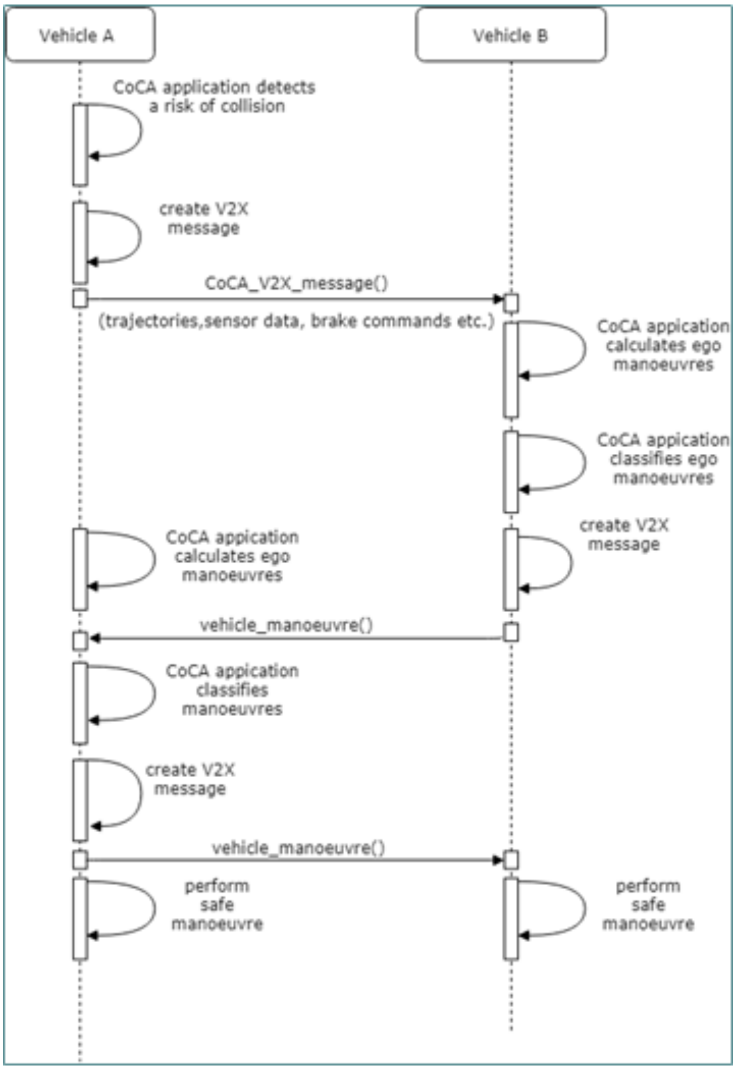


Figure 50 Sequence diagram of NL US12 (Cooperative Collision Avoidance)

Detailed specifications

Message sets: the user story CoCA makes use of different standardized ITS message sets:

1) Cooperative Awareness Messages (CAM) from vehicle to vehicle as defined in ETSI EN 302 637-2: these messages contain information on vehicle characteristics (size, special vehicle), position, speed and direction.
2) Manoeuvre Coordination Messages (MCS) from vehicle to vehicle. ETSI TS 103 561 is work in progress, another specification needs to be used on MCS. For CoCA the vehicles exchange information to support tactical manoeuvre planning (i.e. 5-10 seconds). The CoCA V2X messages are:
    a. Planned Trajectory (PT): Current path the Ego Vehicle is following (5-10 s ahead) and PTs of Other Vehicles and the Ego Vehicle are collision-free.

b. Desired Trajectory (DT): this is the desired trajectory of the Ego Vehicle and superior to the PT. In case the DT of the Ego Vehicle collides with a PT of one Other Vehicle (OV) and can't be followed without collision, cooperative manoeuvring is required via a 'Coordination request' and a Coordination Response (Reject, Accept)

The coordination sequence consists of the following steps:

- Detect coordination need:
  - PTs are constantly broadcasted
  - Other Vehicle (OV) detects the need to cooperate
- Communicate coordination need:
  - Send additional DT
  - DT collides with one PT of Other Vehicle
- Evaluate:
  - Other Vehicle receives Ego Vehicle's DT that will collide with its own PT
  - Other Vehicle evaluates whether to accept the cooperation request
- Rejection of DT:
  - Other Vehicle may reject DT by ignoring DT
  - Ego Vehicle has to calculate another DT
- Accept DT:
  - Oher Vehicle adapts its own PT so that PT will become collision-free
  - Use of Right-of-Way rules
- EV Action:
  - When DT becomes collision-free -> adapted as new PT
- OV Action:
  - Other Vehicle maintains its planned manoeuvre until Ego Vehicle finished its manoeuvre
  - Other Vehicle must adopt its planned manoeuvre equivalent to elapsed time

The messages are exchanged either via:

- Direct V2V communication (without 5G network infrastructure) between vehicles with direct communication units.
- Network-based communication: each vehicle is connected to a central CCAM server to send CAM and MCS messages from the ego-vehicle and receive information from alter-vehicles or roadside systems. The same concept for geo-messaging server as described for the NL US3 on Collective Perception of Environment will be used (see section 7.3.3). Note: the use of MCS is subject to availability of detailed message contents, packet size, frequency, reliability and latency technical specifications.

The distribution of messages is supported via an Edge CCAM server (connected to 5G network of mobile operator). The distribution of messages is based on filters like geographical area.

Cross-border aspects

- Different AV vehicles: interoperability at information exchange level
- Support of user story in inter-PLMN networks
- Support of edge server with hand-over between edge servers within PLMN

7.1.3. Roadside & cloud infrastructure for CN US15 (Cloud-assisted advanced driving)

Description

The scenario automated driving with coordinated overtaking and collision avoidance of this user story CN US15 tries to enable the vehicle to assess the probability of an accident better and coordinate the exchange of information in addition to safety information, sensor data, braking and acceleration command lists, horizontal and vertical control in the application of road traffic flow through V2X communication.

The autonomous vehicle is equipped with advanced onboard sensors, controllers, actuators and other devices. It integrates modern communication and network technology to realize intelligent information exchange and sharing between the vehicle and X (vehicle, road, human, cloud, etc.) and has functioned such as complex environment perception, intelligent decision-making, and collaborative control. In our China site, the roadside unit, remote control centre and cloud server will monitor and control the autonomous vehicles in real time, to realize the various testes of Internet-connected applications of vehicles safely and efficiently.

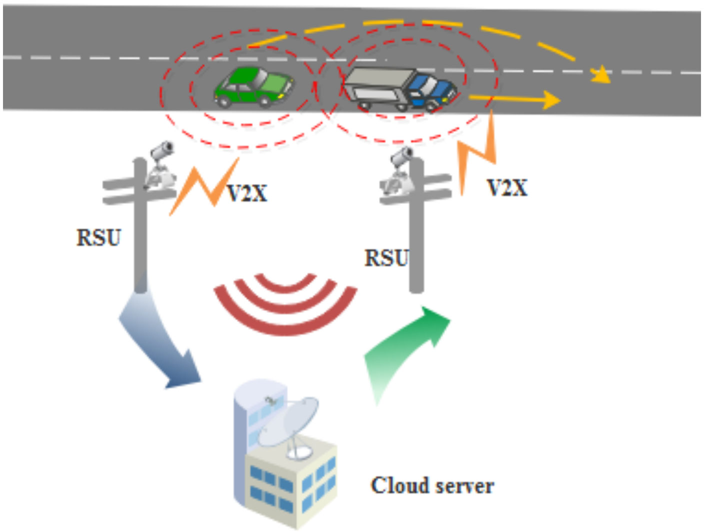


Figure 51 High-level illustration of CN US15 (Cloud-assisted advanced driving)

High-level architecture of the roadside & cloud infrastructure

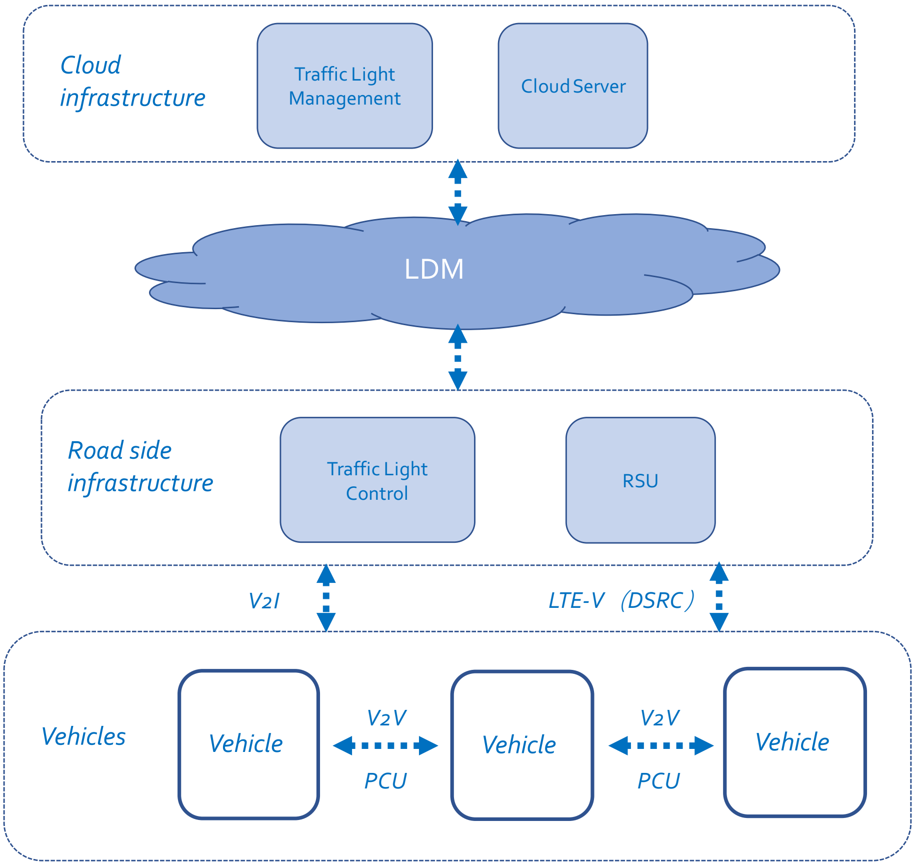


Figure 52 High-level architecture of the CN US15 (Cloud-assisted advanced driving)

Sequence diagram

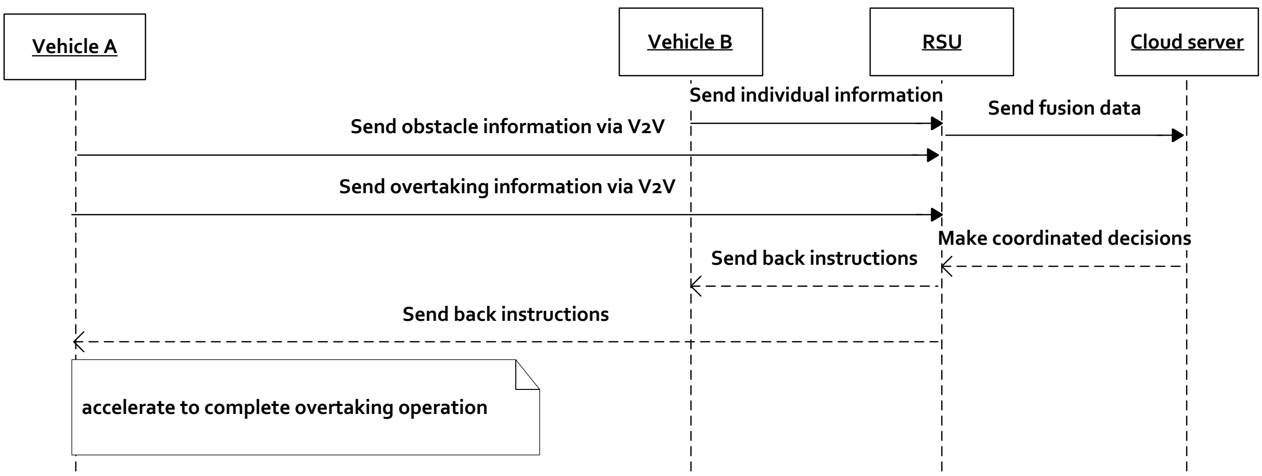


Figure 53 Sequence diagram of the CN US15 (Cloud-assisted advanced driving)

Detailed specifications

In Coordinated overtaking and collision avoidance scenario, Vehicle A and Vehicle B are both running in a straight line along the right lane. Vehicle B is traveling at a constant speed in front of Vehicle A, and both vehicles keep a small distance. In the beginning, the remote-control centre issues the overtaking order to vehicle A through the RSU. After receiving the order, Vehicle A sends the overtaking information to Vehicle B through V2V communication and receive the real-time information from Vehicle B via V2V, which includes the position, speed and heading angle of the vehicle. Thus, Vehicle A makes an automatic decision according to the information of Vehicle B.

Cross-border aspects

Collaborative vehicle driving can effectively reduce the complexity of road traffic control and management, reduce environmental pollution and ensure road traffic safety at the same time. The present user story is feasible to test in the 5G-MOBIX cross-border corridors (ES-PT), so it is tested at a local site first.

7.2. Category 2: Platooning

In this section the roadside and cloud infrastructure are described for the following User stories:

1. GR-TR US4 (Platooning with "see what I see" functionality in cross-border settings)
2. DE US7 (Platooning)
3. CN US16 (Road Safety and Traffic Efficiency)

7.2.1. Roadside & cloud infrastructure for DE US7 (Platooning)

Description

The user story "SAE L-4 Platooning" at the German trial site is designed to show case the role of augmented digital infrastructure in addressing the challenges of SAE L-4 vehicle platoons in mixed traffic, with the presence of legacy vehicles. 5G network plays an important role in providing low latency, high bandwidth, and flexible communication infrastructure for autonomous vehicles, road infrastructure including various sensors and edge computing, and data transport to data centre. The digital infrastructure also includes CCAM, ITS, and data analytic services, which provide extended perception to vehicles, coordinate and control road infrastructures, among others. Due to delay and bandwidth constraints these services are deployed on distributed roadside edge computing (eRSU) platform and centrally orchestrated by the global service management components in data centre.

This section describes the roadside and data centre infrastructure components involved in SAE L-4 Platooning user story. The digital infrastructure will support the platooning user story by:

- Enriching the perception of CCAM by feeding in the data from roadside sensors including traffic analysis, road-condition, object detection, traffic light, and intelligent street lights etc.,
- Utilizing 5G's access agnostic, virtualized control plane hosted close to the roadside to meet the URLLC requirements of safety-related vehicle-roadside sensor interactions.
- Orchestrating the 5G services near the edge and complementing those with AI approaches to assist lane-keeping / leaving, speed adaptation, and turning decisions of CCAM vehicles.

High-level architecture of the CCAM infrastructure

This user story demonstrates platooning operations of SAE L-4 AVs in mixed traffic, i.e., with the presence of traditional vehicles. We do not only rely on the AV's capabilities but also on the roadside infrastructure. This result in a three-level solution architecture i.e., vehicle level, edge level, and cloud level shown in Figure 54.

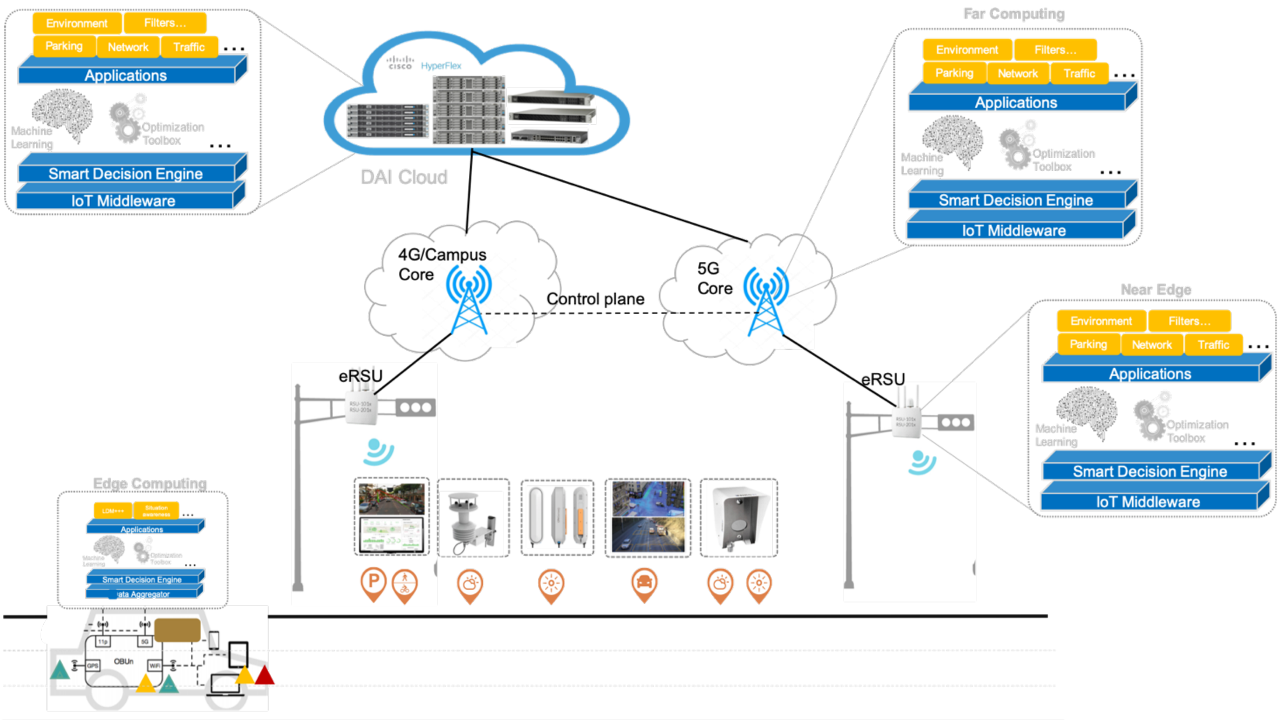


Figure 54 Three-level solution of German trial site

At the vehicle level, the AV is typically equipped with a combination of sensors, actuators, sophisticated algorithms, and powerful processors to execute CCAM applications. There are hundreds of such sensors and actuators which are situated in various parts of the vehicle. All these sensors feed data to the local CCAM applications, for example a Local Dynamic Map (LDM), allowing the vehicle to perceive its environment. The AV also has short range and broad band wireless interfaces enabling data exchange with other AVs, edge and cloud components.

Edge level is the intermediate level, which corresponds to an extended roadside unit (eRSU), that hosts the additional computing hardware and communication interfaces to support CCAM applications. It does not only allow the Vehicle to Infrastructure / Vehicle (V2X) communication but also serves as a MEC host for local services and decision toolbox. Edge level (i.e., eRSU) creates an upstream communication - towards the central data centre/cloud and downstream communication - towards the sensors and vehicles. The eRSU on the downstream interfaces with various on-road deployed sensors over Wi-Fi and vehicles over DSRC (802.11p) links. At this level, an IoT middleware is deployed to enable the data collection from environment (via on-road deployed sensors: traffic analysis, road-condition, object detection, traffic light, and intelligent street lights, etc.) and from vehicles. We also implement and deploy an Edge Dynamic Map (EDM) service, which creates the map/patterns based on the information collected from neighbouring sensors and vehicles provided information. These map/patterns/pieces of information are continuously or on demand fed to the LDM for more informed decision making of vehicles. EDM service is also accessible to mobile users through eRSU wireless and 4G interfaces, enabling traditional vehicle and other road users to be integrated in the autonomous driving infrastructure.

Cloud level hosts the backend of all the on-road deployed sensors, communication network core, network operation controllers, service orchestrator, computation infrastructure, optimization and machine learning toolboxes. Cooperative ITS services are hosted here and provide crucial support for fully automated vehicles in absence of human involvements. These services create patterns for the EDM service based on the sensory data collected from vehicles and all on-road sensors.

The following subsections detail on the specification of the infrastructure components for the support of SAE L4 platooning user story, which is described in D2.1. We will focus on the augmented components in the sophisticated "overtaking operation" during platooning.

Sequence diagram

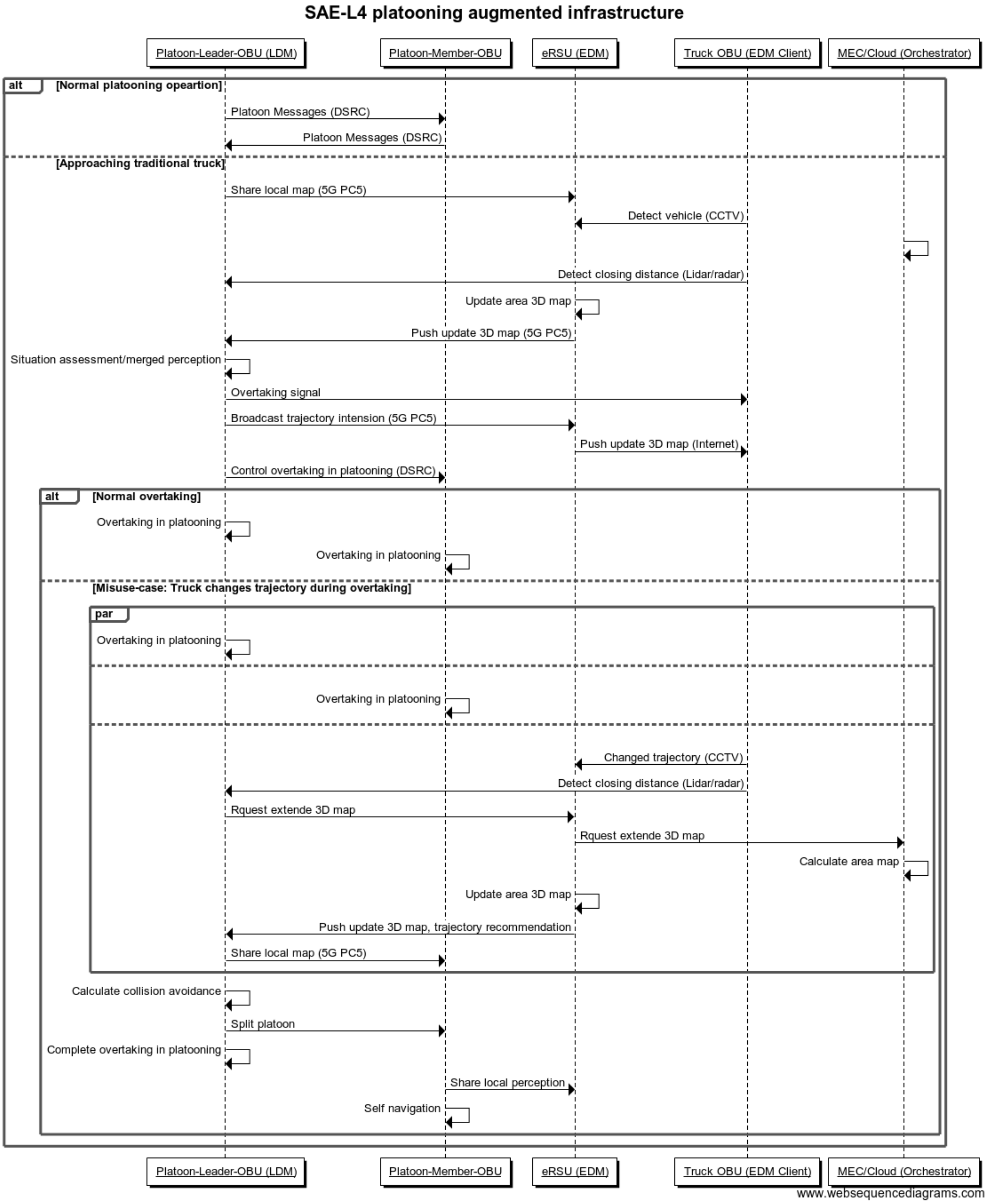


Figure 55 Sequence Diagram for DE US7 SAE-L4 platooning in the German trial site

Detailed specifications for CCAM infrastructure

The platooning operations can be divided into intra platooning group and CCAM infrastructure operations. A detailed architecture of the system components and connectivity is depicted in Figure 56. We now detail the specification of the infrastructure components involved in the user story.

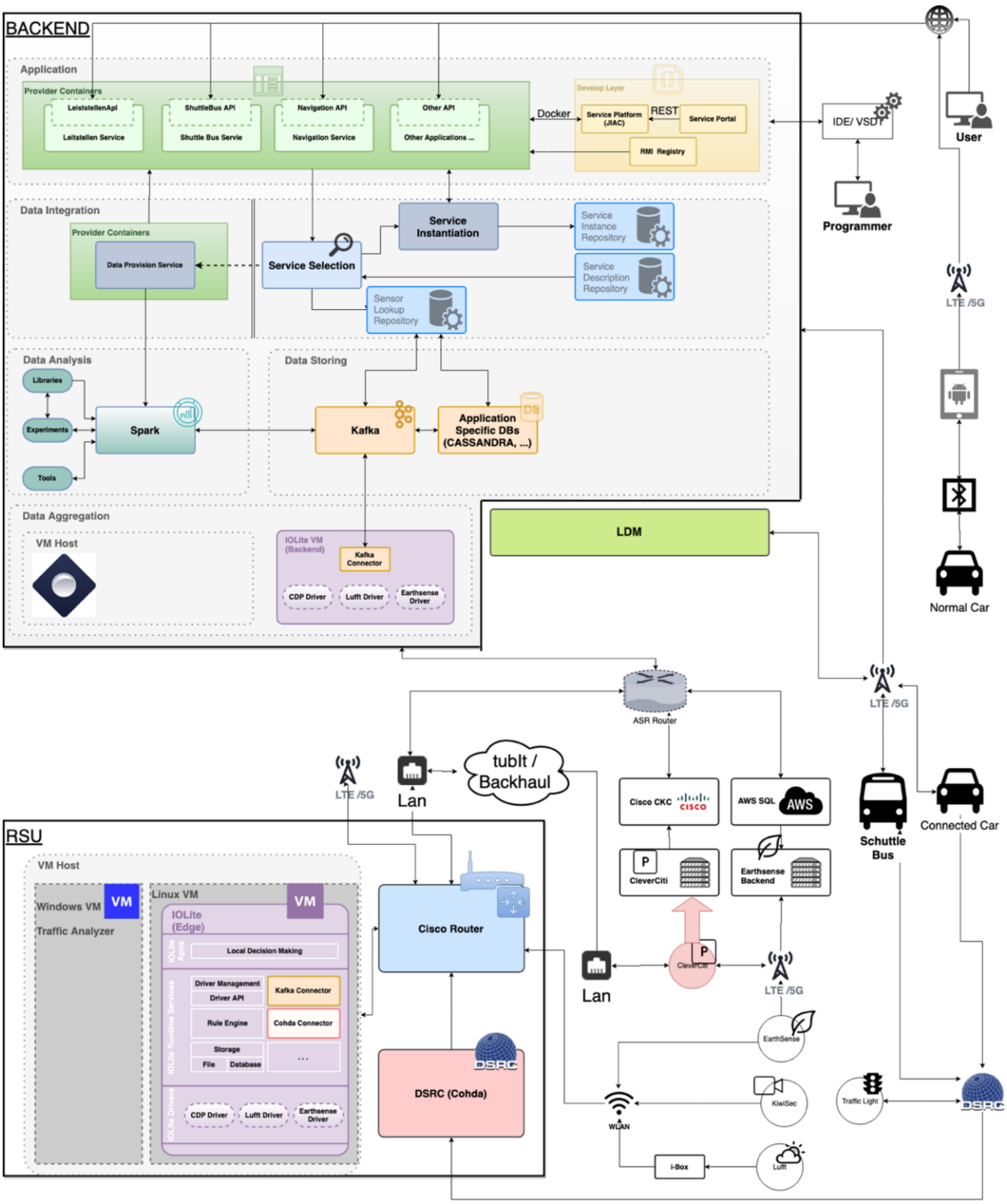


Figure 56 End-to-end Infrastructure components and network interfaces for platooning user story implementation.

V2X interfaces specification

During platooning, the AVs rely on V2I and V2V communication to exchange perception and control information. The LDM component in the AV constantly updates its environment perception and shares this information with the EDM instances hosted on the eRSUs using available Wi-Fi, LTE D2D and 5G PC5 sidelink interfaces. This allows additional information for the EDM and GDM to construct a virtual map of a broader area. The global map is also shared with all vehicles in the area through EDM applications. Based on the environment perceptions, the AVs coordinate their driving decision through DSRC interfaces. The vehicle interfaces are specified following:

- V2V: interfaces include both short-range low delay communication for autonomous driving operations and high bandwidth communication for CCAM application and vehicle perception.
  - The short-range interface is based on DSRC (802.11p) wireless technology. On DSRC interface cooperative driving and traffic control application protocols and messages are implemented:
    - Decentralised Environmental Notification Messages (DENM), Cooperative Awareness Messages (CAM) or Basic Safety Message (BSM).
    - Other roadside infrastructure related messages are also transmitted over DSRC interface: Signal Phase and Timing Message (SPAT), In Vehicle Information Message (IVI), and Service Request Message (SRM).
  - More capable interfaces are used by CCAM application protocols and messages, which are described in more details next.
- V2I (eRSU): communication for CCAM applications relies on high bandwidth technologies with higher delay in contrast to the short-range communication technology. These interfaces are based on C-V2X (LTE-V2X), 3GPP PC5 (5G-V2X) and Wi-Fi technologies. These interfaces are required for application specific and management protocols, e.g., media transfer, the ITS V2X reference architecture protocols[30], and other IP-based protocols.

eRSU interfaces specification

CCAM infrastructure operations involve the real-time update of the GDM and EDM maps, their interactions with other ITS and road management applications, and the management of network and edge computing resources for those applications. CCAM applications have a global instance deployed in data center and other location specific instances deployed on-demand on eRSUs. EDM instances on eRSUs are constantly fed with data from nearby road sensors through Wi-Fi and wired interfaces. EDM instances synchronize the analysed sensor information with their global instance using application specific protocols through 4G/5G upstream and wired interfaces (where available).

- eRSU-2-eRSU: communication is based on very high bandwidth and low latency mmWave and direct Wi-Fi connection. These links serve as reliable transport and back-haul network for roadside

[30] "ETSI TS 103 097 v1.2.1 (2015-06)-intelligent transport systems (its); security; security header and certificate formats,"

infrastructure. The interfaces between eRSUs are used by the SDN data and control plane, which provide virtualized network for distributed MEC platform hosted on the eRSUs.

- eRSU-2-MEC/Cloud: communication is mainly provided by 4G/5G broadband interface. The use of MNO MEC infrastructure in core network for CCAM applications allows their low delay communication from eRSU. Autonomous vehicles with broadband access can make use of this interface for the CCAM services.

Cloud infrastructure interfaces specification

The network slice management and orchestration service are deployed in the central cloud platform, which coordinates difference network functions deployed on eRSUs and AVs. Mobility and applications aware network management protocols are developed to meet e2e QoS requirements of CCAM applications.

- eRSU (MEC)-2-Cloud: to meet the high availability and QoS requirements of CCAM scenarios, MEC infrastructure with central and distributed mobile edge hosts is the main platform for microservice based CCAM application. Mobile edge CCMA services are the web services composed by the REST based protocol[31].
- Multi-Cloud: platforms with large computing and network capacity host various backend components of CCAM services, e.g., data analytics, data fusion, data bases, service implementations, among others. Depending on application scenario and service providers, CCAM services can be deploy on different cloud, near and far edge platforms. This raises the challenges for service composition and interactions. The solutions for such a highly flexible deployment can based on network virtualization technologies, e.g., SD-WAN, tunnelling, and hybrid cloud management and orchestration.

[31] "Mobile Edge Computing (MEC); General principles for Mobile Edge Service APIs," https://www.etsi.org/deliver/etsi_gs/MEC/001_099/009/01.01.01_60/gs_MEC009v010101p.pdf

RSU specification

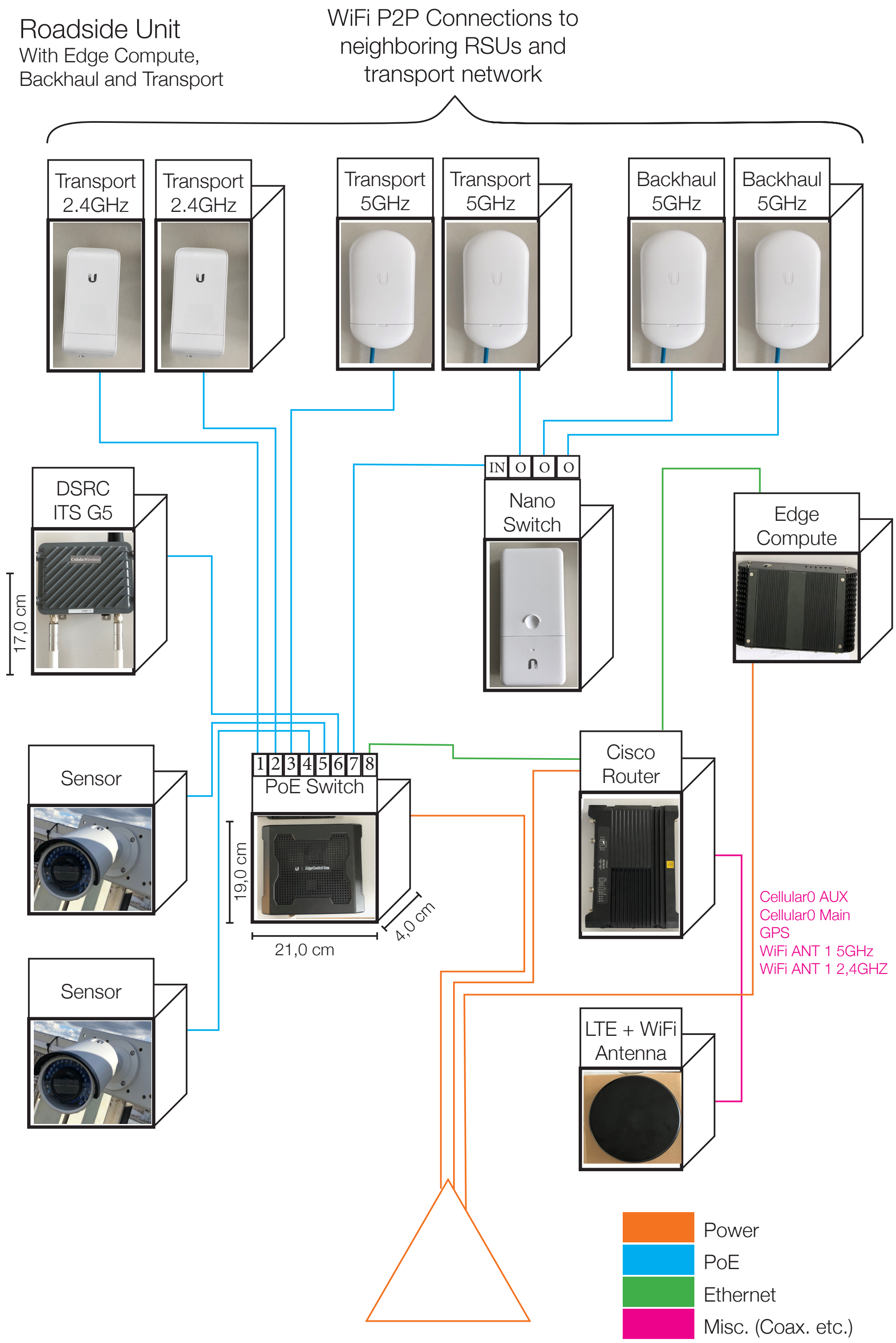


Figure 57 Extended Roadside Unit at the German Trial site, including Edge Compute resources

The extended roadside unit (eRSU) contains communication infrastructure and compute resources. For the access network, the roadside unit provides either ITS G5 or DSRC and an additional Wi-Fi interface. The transport network is created by two interfaces: LTE and a redundant P2P wireless link. In some cases, neighbouring eRSUs are connected through another P2P wireless link. The eRSU in Figure 57 is connected to the transport network and two neighbouring roadside units. To provide edge computing resources, a machine is connected to the router in the roadside unit. Depending on the deployment, roadside sensors are connected through either wired or wireless connections. As the transport network is created by wireless links, only a 230V power supply is required to provide power to the devices (230V, Power-over-Ethernet (PoE), PoE+). One of the deployed eRSUs is shown in Figure 59.

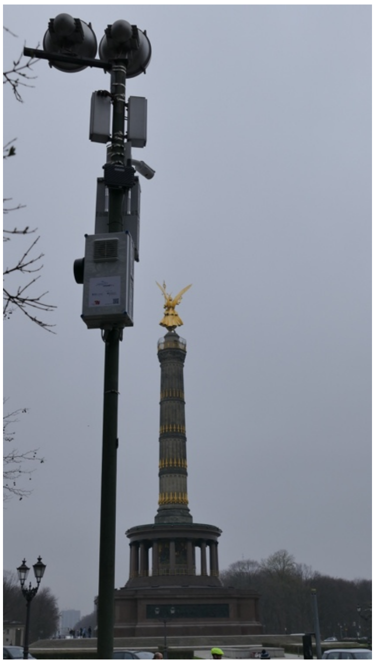


Figure 58 Deployment of an eRSU in the German Trial site

Cross-border aspects

During platooning operations, handover between eRSUs must be supported. This results in changing eRSU providers and network providers for eRSU upstream communication. Such mobility situation involves cross MNOs and border handover, the global MANO orchestrates handover process by preparing handover context and trigger handover process. During the handover, mobility management messages are communicated to the involving eRSUs.

7.2.2. Roadside & cloud infrastructure for CN US16 (Road Safety and Traffic Efficiency)

This user story is about Vehicles Platooning with at least 2 automated cars.

Description

In this case, we will upgrade the intersection safety information system, which consists of road radar, traffic signals, and LDM servers and RSUs. Based on them, our purpose is to detect pedestrians and avoid accidents. The Figure 59 shows that autonomous driving vehicles in a fleet communicate with each other through LTE-V, and provides the basic planning for the rear vehicle through V2V communication (including chasing, continuous running, acceleration, deceleration, obstacle avoidance, overall acceleration, and deceleration, etc.).

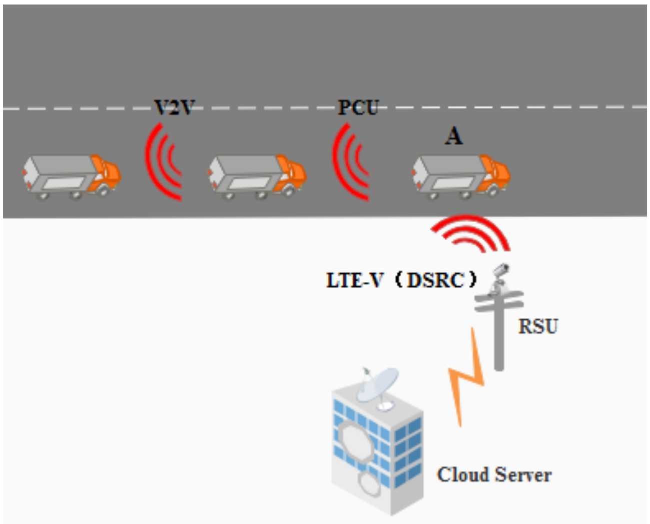


Figure 59 High-level illustration of CN US16 (scenario 2: Vehicles Platooning)

High-level architecture of the roadside & cloud infrastructure

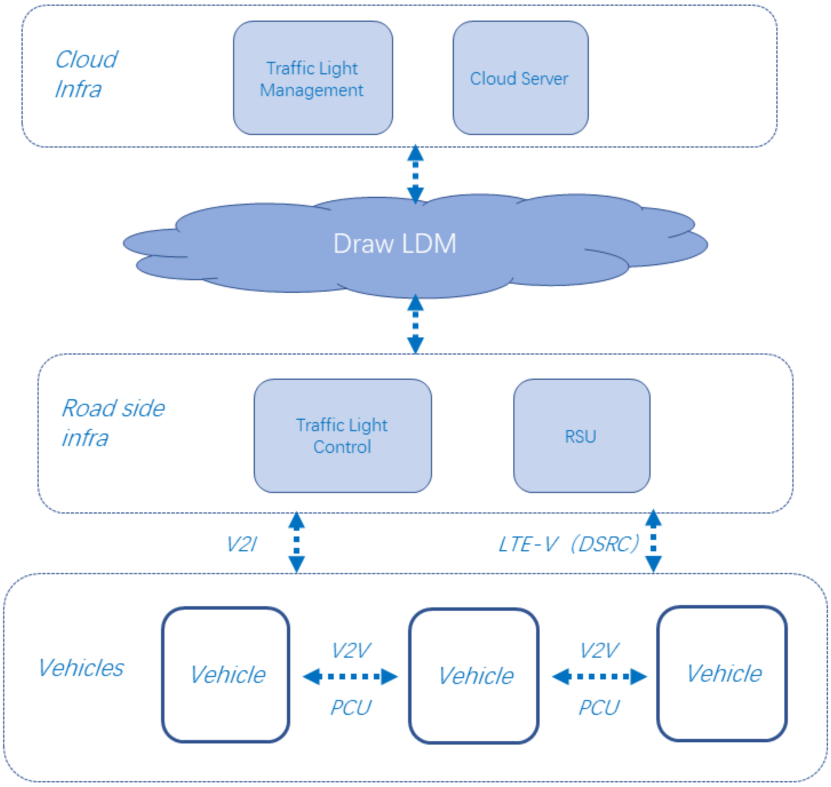


Figure 60 High-level architecture of CN US16 (scenario 2: Vehicles Platooning)

Sequence diagram

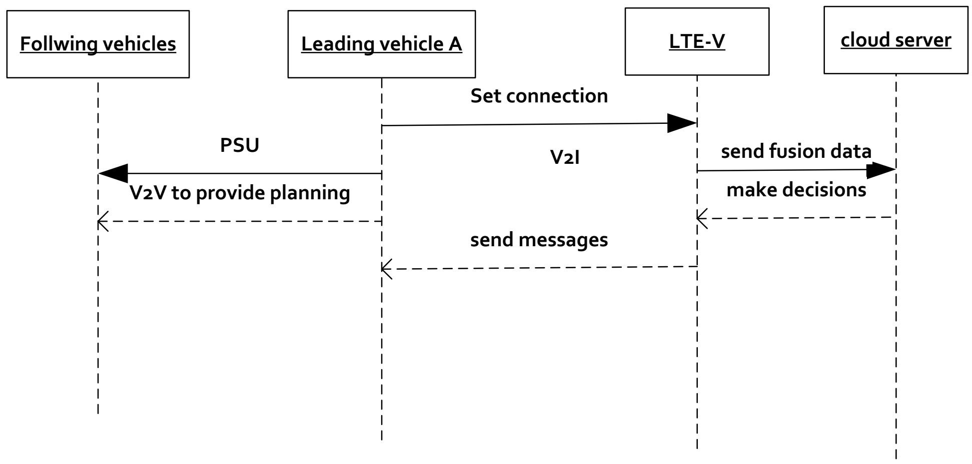


Figure 61 Sequence diagram of CN US16 (scenario 2: Vehicles Platooning)

Detailed specifications

In the Vehicles Platooning, autonomous driving vehicles in a fleet communicate with each other through LTE-V2X at the start. Among them, the leading vehicle (Vehicle A) includes the platoon control unit (PCU), which coordinates the vehicles in the fleet to ensure a certain safe distance and to drive in a platoon. The leading vehicle communicates with the control center through V2I to obtain the test scheme and the global path planning. Then it provides the basic planning for the rear vehicle through V2V communication (including chasing, continuous running, acceleration, deceleration, obstacle avoidance, overall acceleration, and deceleration, etc.). The following vehicle also has a certain perception and planning decision-making ability.

Cross-border aspects

The present user story hopes to avoid the potential risks of human-vehicle conflicts which are common situations in cross-border corridors. Our cloud center has very high performances, such as HD Map, path planning and real-time decision making.

7.3. Category 3: Extended Sensors

In this section the roadside and cloud infrastructure are described for the following User stories:

1. GR-TR US5 (Extended sensors for assisted border-crossing)
2. EDM-enabled extended sensors with surround view generation (DE US7)
3. Extended sensors with redundant Edge processing (FI US8)
4. Extended sensors with CPM messages (NL US14)

7.3.1. Roadside & cloud infrastructure for DE US7 (EDM-enabled extended sensors with surround view generation)

Description

The objective of this user story is to share local dynamic map (LDM) data and raw sensor data for real-time prediction and planning tasks made possible by 5G technology. More precisely, the user story deals with a situation when the perception obtained by the on-board sensors is not enough and needs to be enhanced by sensor data from other traffic participants. Furthermore, a 360° surround view for passengers is to be created using sensor data from the vehicle, roadside infrastructure, and surrounding vehicles.

The user story scenario contains several connected vehicles equipped with sensors as well as roadside infrastructure comprising sensors and edge computing infrastructure (near edge – eRSU and far edge – 5G mobile access edge). The vehicles and the eRSU using their respective sensor data build their individual situational awareness, identifying objects, lane markings or the road condition to support their prediction and planning functions. However, each individual vehicle's sensors as well as roadside sensors are limited in the perception, i.e., the sensors view could be obstructed by objects, limited by weather conditions, or not covering a specific area. To mitigate the lack of environment information, vehicles share extracts (regions of interest) from their LDMs and/or sensor raw data and the eRSU shares its Edged Dynamic Map (EDM).

High-level architecture of the CCAM infrastructure

The high-level architecture of the CCAM infrastructure for the user story "Cooperative perception with HD maps and surround view" is shown in Figure 62. In the architecture, details of the functional blocks for the user story are presented.

The autonomous vehicles are equipped with onboard sensors, especially Lidar, radar, and camera sensors, which provide data for its local environment perception. Additional data from road infrastructure, e.g., eRSU and road sensors is transferred to the AV's OBU through various network interfaces. The middleware layer adapts different network interfaces, data transport protocols and formats to create a unified access to raw sensor data. Data aggregation layer with specific handler modules for each type of data retrieves raw data through the middleware and transforms them to be used by cooperative perception application components. Specifically, the object detection and localization components create a local dynamic map (LDM) through fusion of HD-map, sensor data, and ROI extraction. A surround view is generated as the result and presented to SAE-L4 driver on the onboard HMI device. Via 5G-D2D and other network interfaces, the LDM of the AV is also shared with the road infrastructure (eRSU), which will generate an edge dynamic map (EDM) together with the local perception of surrounding AVs. The EDM is in turn shared with all AVs, which reinforces and extends their local perceptions. Based on the perceived environment surround view, autonomous diving application plans and control AV's actuators allowing it to adapt its trajectory and speed to the driving environment.

Augmented infrastructure in German trial site is based on a distributed multi cloud and edge computing platform. The central cloud is connected with the distributed MEC components on eRSU by virtual network slices on backhaul and 5G networks. These networks transfer the data and control plane of the management and orchestration of the distributed cloud infrastructure. Central MANO components for virtualization infrastructure and CCAM services are hosted in the central cloud platform, which coordinates the end-to-end system supporting the user story.

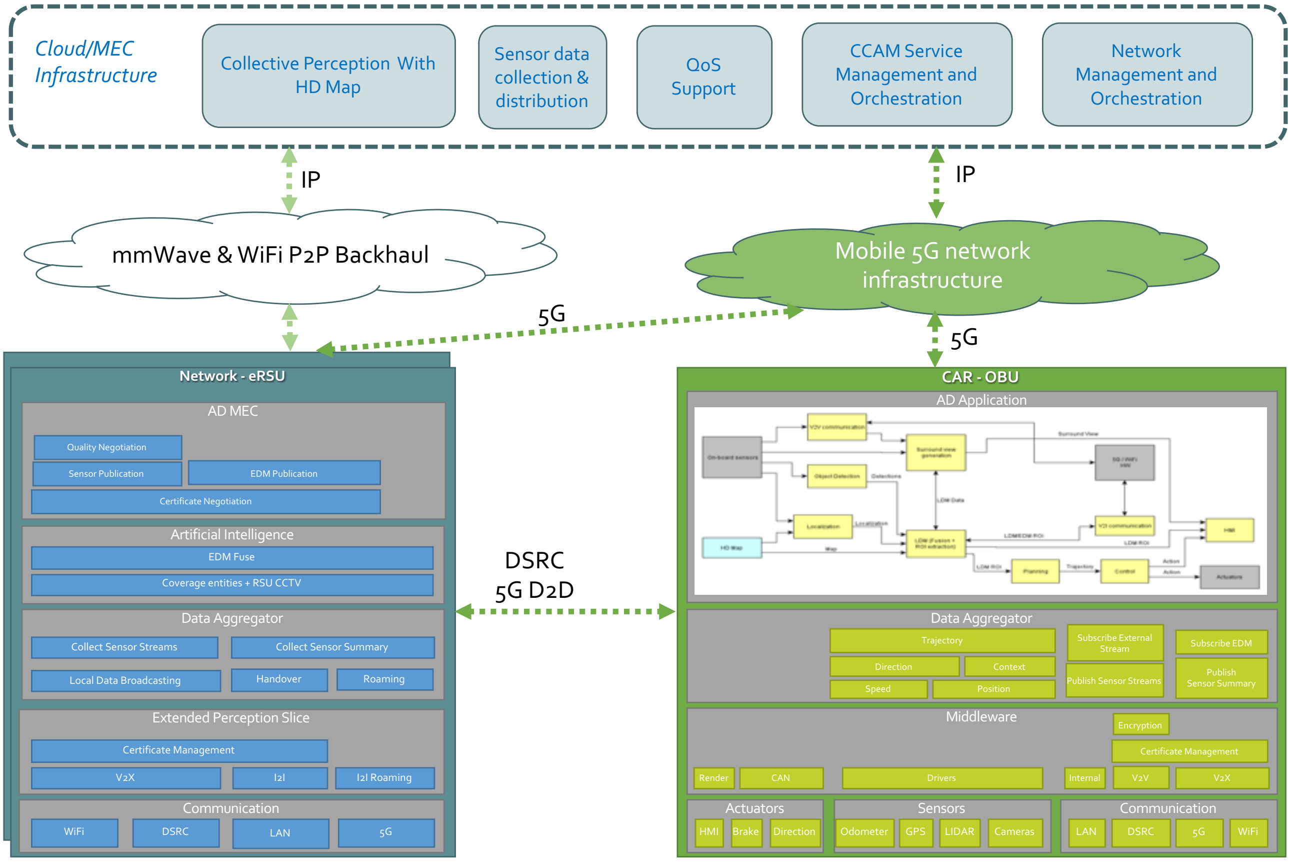


Figure 62 CCAM architecture for Cooperative perception with HD maps and surround view user story.

Sequence diagram

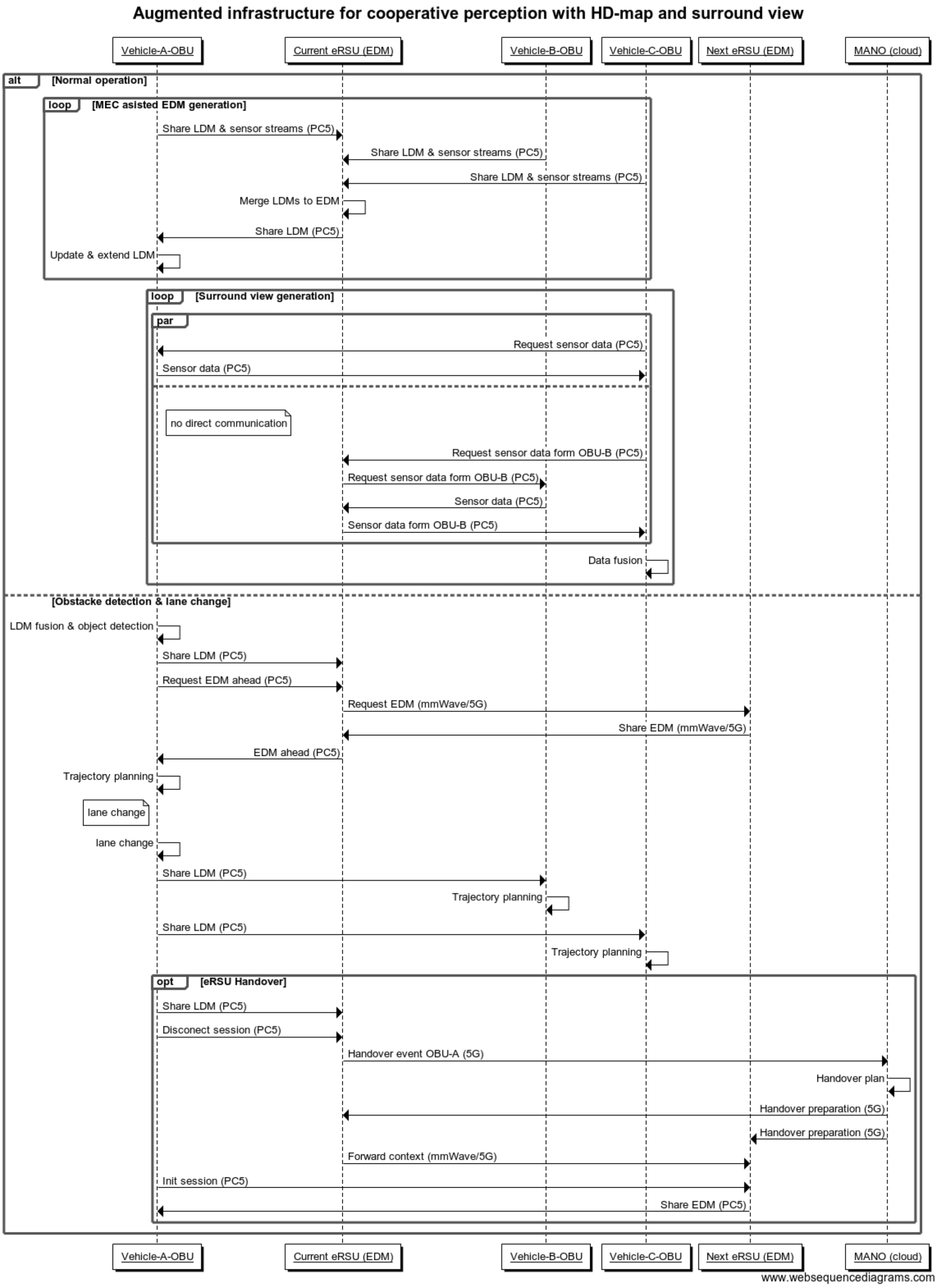


Figure 63 Augmented infrastructure for "cooperative perception with HD-map and surround view" user story

Detailed specifications

V2X interfaces specification

The main V2X interfaces for cooperative perception operations are 5G PC5 sidelink or Wi-Fi, which enable large bandwidth for the transmission of visual sensor data among vehicles and eRSU. However, these interfaces come with higher delay, in contrast to the short-range communication technology. These interfaces are required for application specific and management protocols, e.g., media transfer, the ITS V2X reference architecture protocols [1], and other IP based protocols.

eRSU interfaces specification

CCAM infrastructure operations in cooperative perception user story involve the real-time update of the GDM, EDM maps, their interactions with other ITS and road management applications, and the management of network and edge computing resources for those applications. Global CCAM application instances is deployed in data center manage and coordinate decentralized EDM instances using application specific protocols through 4G/5G interfaces, e.g., during handover.

- eRSU-2-eRSU: communication is based on very high bandwidth and low latency mmWave and direct Wi-Fi connection. These links serve as reliable transport and back-haul network for roadside infrastructure. The interfaces between eRSUs are used for the context transfer during handover and roaming.
- eRSU-2-MEC/Cloud: communication is mainly provided by 4G/5G broadband interface. The use of MNO MEC infrastructure in core network for CCAM applications allows their low delay communication from eRSU. Autonomous vehicles with broadband access can make use of this interface for the CCAM services. For mobility event involving cross MNOs and border, the global MANO orchestrates handover process by preparing handover context and trigger handover process. During the handover, mobility management messages are communicated to the involving eRSUs.

Cloud infrastructure specification

The network slice management and orchestration service are deployed in central cloud platform, which coordinates difference network functions deployed on eRSUs and AVs. Mobility and applications aware network management protocols are developed to meet e2e QoS requirements of CCAM applications.

- eRSU (MEC)-2-Cloud: to meet the high availability and QoS requirements of CCAM scenarios, MEC infrastructure with central and distributed mobile edge hosts is the main platform for microservice based CCAM application. Mobile edge CCMA services are the web services composed by the REST based protocol[32].

[32] "Mobile Edge Computing (MEC); General principles for Mobile Edge Service APIs," https://www.etsi.org/deliver/etsi_gs/MEC/001_099/009/01.01.01_60/gs_MEC009v010101p.pdf

- Multi-Cloud: platforms with large computing and network capacity host various backend components of CCAM services, e.g., data analytic, data fusion, data bases, service implementations, among others. Depending on application scenario and service providers, CCAM services can be deploy on different cloud, near and far edge platforms. This raises the challenges for service composition and interactions. The solutions for such highly flexible deployment can based on network virtualization technologies, e.g. SD-WAN, tunnelling, and hybrid cloud management and orchestration.

Cross-border aspects

During platooning operations, handover between eRSUs must be supported. This results in changing eRSU providers and network providers for eRSU upstream communication. Such mobility situation involves cross MNOs and border handover, the global MANO orchestrates handover process by preparing handover context and trigger handover process. During the handover, mobility management messages are communicated to the involving eRSUs, as shown in Figure 56.

7.3.2. Roadside & cloud infrastructure for FI US8 (Extended sensors with redundant Edge processing)

Description

In this user story, the video-based cooperative perception for automated vehicles, we evaluate the reliability and performance of networking and edge computing services in x-border scenarios. We will evaluate the functionalities and performance (e.g. processing delay, migration overhead) of an automated vehicle using edge computing for cooperative perception, including auto discovery of edge nodes, adaptive task allocation, and seamless service migration.

High-level architecture of the CCAM infrastructure

The high-level architecture of the CCAM infrastructure for the FI video-based cooperative perception user story is shown in Figure 64 below. The cooperative perception is developed by processing video streams received from L4 vehicles and roadside cameras. The processing of the cooperative perception is done on a MEC platform. Furthermore, the handover of computations from one MEC to another occurs when the vehicle roams between PLMNs (this multi-PLMN/MEC aspect is not depicted in the figure for simplicity), or when any MEC gets overloaded. Otherwise, the common convention is used to represent in blue the functional elements in the physical layers, while the network / communication elements are shown in green, and the end-to-end information exchange for video-based cooperative perception is shown in yellow.

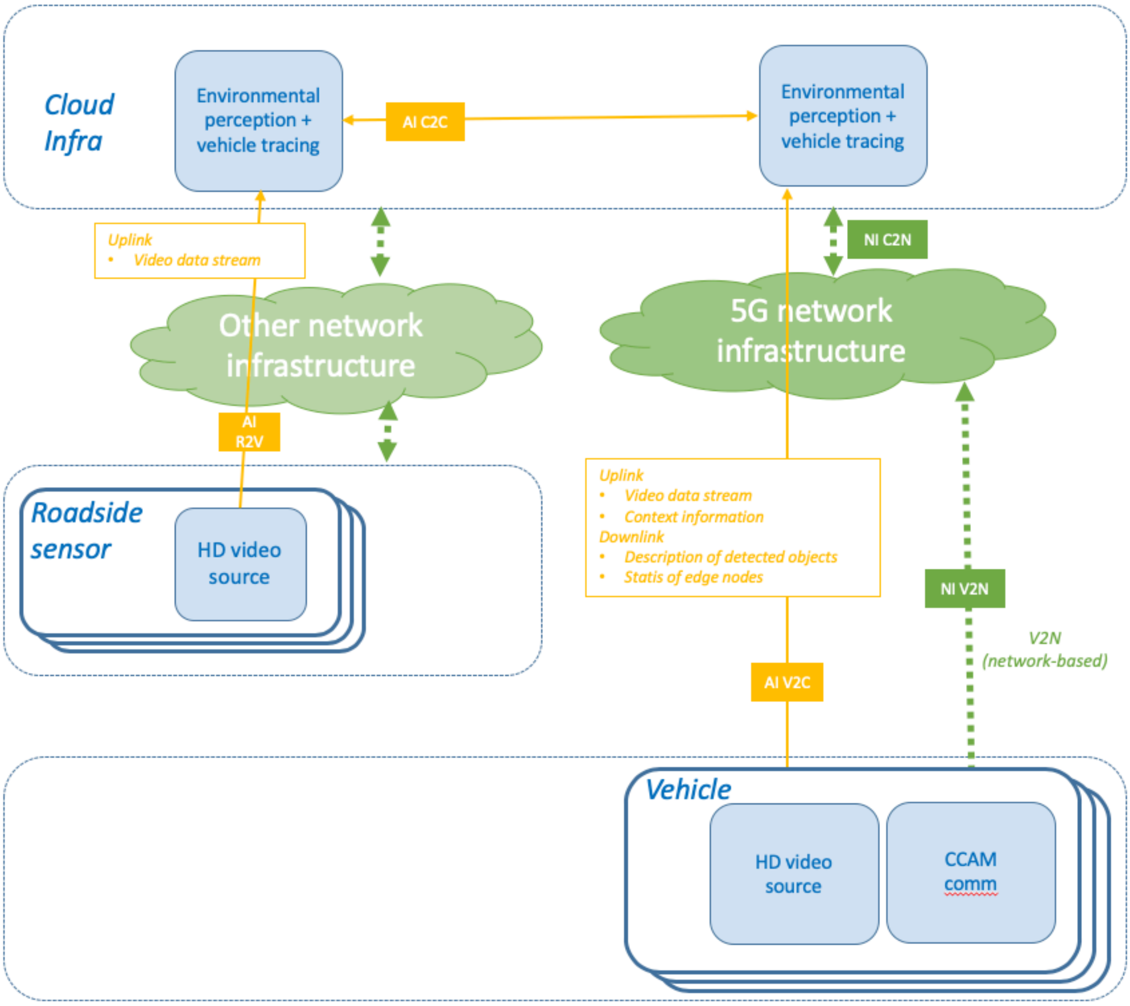
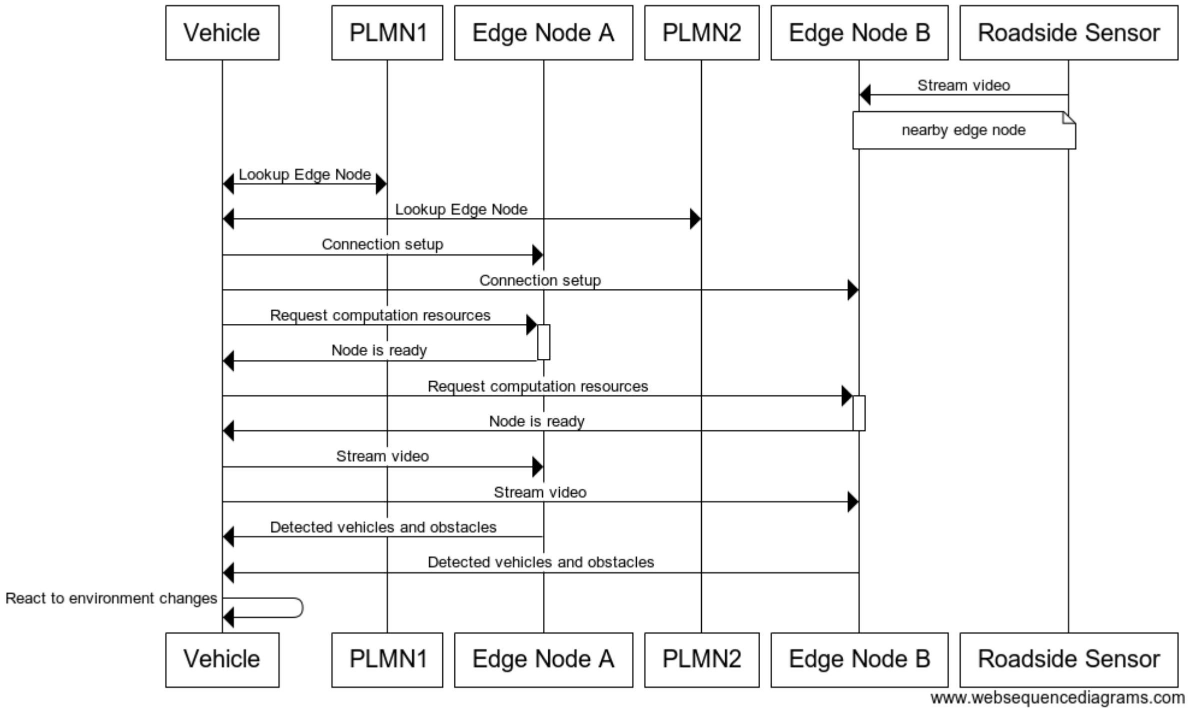


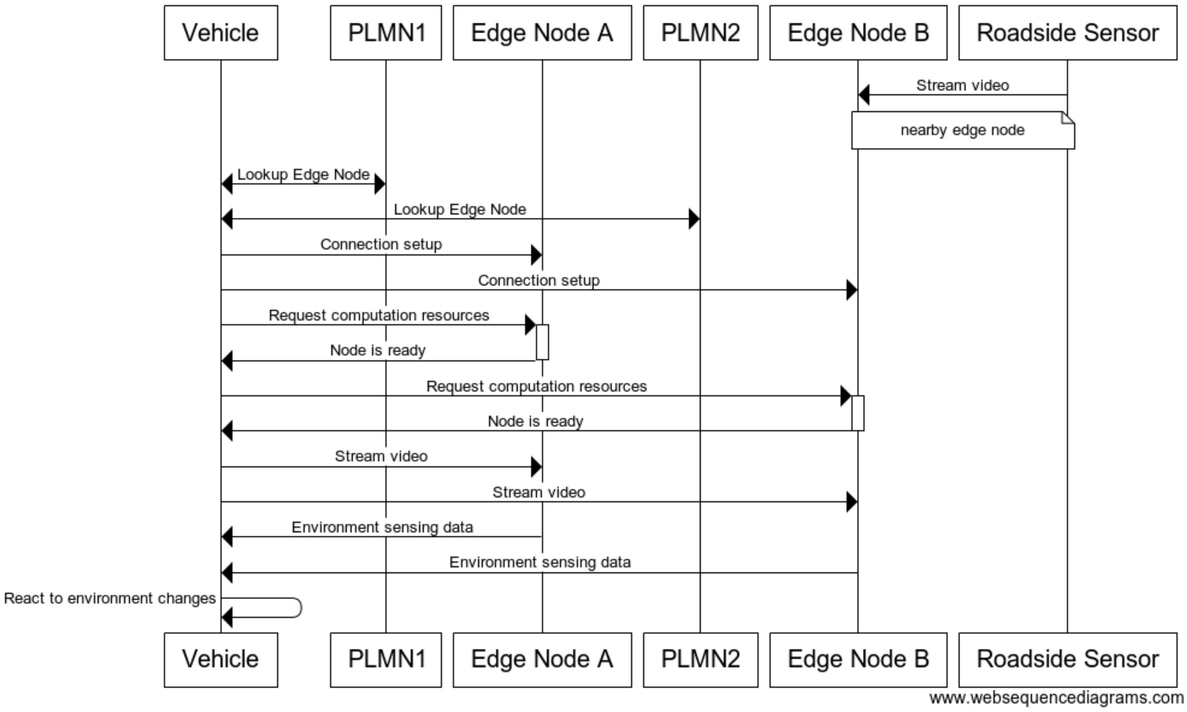
Figure 64 CCAM architecture for support of video-based cooperative perception user story

Sequence diagram

The sequence diagram for the video-based cooperative perception user story emphasizing the interactions between different elements in the previously described CCAM architecture is shown in Figure 2 below.



Scenario 1 MEC cooperative perception



Scenario2 MEC dynamic migration

Figure 65 Cooperative perceptions sequence diagrams

Detailed specifications

The video-based cooperative perception user story involves the transfer of the following between the vehicle, roadside sensors and the edge nodes:

1) Uplink data (from vehicles):
    a. Video: HD video with 1080p resolution and 30 frames per second (FPS)
    b. Context information: Data structure including at least identity of the vehicle, pose (longitude, latitude, orientation), moving speed, and profiles of processing tasks (latency constraints, computing/communication workload description) in case of computation offloading.
2) Uplink data (from roadside sensors):
    a. Video: jpeg compressed image buffers
    b. Context information: Data structure including at least identity of the roadside sensor, pose (longitude, latitude, orientation).
3) Downlink data (from edge nodes to vehicles):
    a. Description of detected objects (e.g. object type, location, moving speed, size) and the confidence.
    b. Safety related alerts if applicable
    c. Status of edge node (e.g. available computing capacity, coverage, provided service list)

Roadside sensors are connected to their nearby MEC nodes beforehand and are streaming live videos all the time. So, the connection setup process for roadside sensors is neglected in the diagrams. Vehicles may run into/outside a MEC's territory at any time. Whenever a vehicle enters a new PLMN, it uses DNS to lookup the IP address of the nearby edge node and connects to it afterwards. A vehicle may use multiple PLMNs/MECs at the same time. If so, it separates its video source into several pieces, frame by frame. Each edge node handles a bunch of frames and responds to the client independently. For example, the video is captured at 30 fps, then 15 of the frames are streamed to edge node A while the other 15 frames are streamed to edge node B. The vehicle can utilize the responses (E.g., location of the obstacles in front of it) from all of the connected edge nodes to make decision, E.g., it should stop because an obstacle is on its path. When an edge node fails (server down or out of range), the vehicle can still rely on other edge nodes to make decision, although with a little decrease in confidence. To reuse previous results, a vehicle can require an edge node to migrate its context to another edge node. For example, a CNN model trained for a specific vehicle can be migrated all the way as it goes.

The cooperative perception is performed on the edge node side. A single edge node receives video streams of multiple vehicles and roadside sensors (not shown in the diagrams), resulting in a good understanding of its surrounding environments. It generates a map and update the location of vehicles and the obstacles (human, animals, stones, etc.) continuously. For example, a crash accident can be detected by processing the data received from roadside sensors and on-vehicle sensors. Then the accident event will be broadcasted quickly to all of the edge node's connected vehicles.

The Finland (Espoo) pre-deployment trial site is located within the Otaniemi area of Aalto University. The actual roads targeted for the 5G-MOBIX trials includes the interconnected Maarintie and Otakaari roads with a total length of about 1.2 km. The deployed roadside sensor station to be leveraged in the cooperative perception user story is located on Maarintie road (see Figure 66) and mounted at a height of 6m from the ground. The roadside sensor station includes a video camera. The RGB sensor used inside vehicles is Garmin dashcam 55. It captures 1080p videos at 30 FPS.

Figure 66 Location of the roadside sensor (shown inset) within the Espoo Otaniemi trial site (the primary road targeted for the trials is shown blue colour)

The Espoo pre-deployment trial site also makes use of the cloud infrastructure from the Aalto Data Centre (see Figure xx) to run the different cloud-based 4G/5G network functions and 5G-MOBIX CCAM functions or services. The Aalto Data Centre physically is located by one of the test roads (Otakaari) in the Espoo trial site. The operator of the data centre (Aalto IT Services) provides a number of features or services that are accessible to 5G-MOBIX, these include (but are not limited to):

- L1 SM fiber connections in Otaniemi campus area
- 1G L2 connections in Otaniemi campus area
- VMware virtual servers
- Data center server services for partners or projects opting to deploy own servers
- Public IP addresses
- Cloud services from Amazon Web Services (AWS) and Microsoft Azure, including express route from our Aalto network to Azure Cloud
- Stringent security including firewalling etc.

Figure 67 Some of the server infrastructure deployed at Aalto Data Centre

Cross-border aspects

- The user story considers video-based cooperative perception whereby the vehicle roams between different PLMNs and while simultaneously handing over computation (for cooperative perception) from one edge node to another.

7.3.3. Roadside & cloud infrastructure for NL US14 (Extended sensors with CPM messages)

Description

The objective of the user story Collective Perception of Environment (CPE) is to enhance the environmental perception of vehicles by enabling the real-time data exchange between vehicles and roadside systems. AD vehicles with SAE level 4 capability require predictive information of environment sufficiently ahead in time. AD vehicles are equipped with on-board sensors, however, with limited range to detect objects and obstacles. CPE extends this range by providing perception of areas not visible to the ego-vehicle due to curves, corners or obstacles in the roads. AD vehicles equipped with 5G technology could share raw sensor data from cameras, LIDAR, etc. or share pre-processed data such as dynamic objects and planned trajectories as the Collective Perception Message (CPM). Additionally, other driving condition data such as weather situation and traffic information can be shared via central CCAM servers.

High-level architecture of the CCAM infrastructure

The high-level architecture of the CCAM infrastructure for the user story CPE is shown in Figure 68.

The functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, the information exchange is shown in yellow. The architecture does not cover the cross-order aspects.

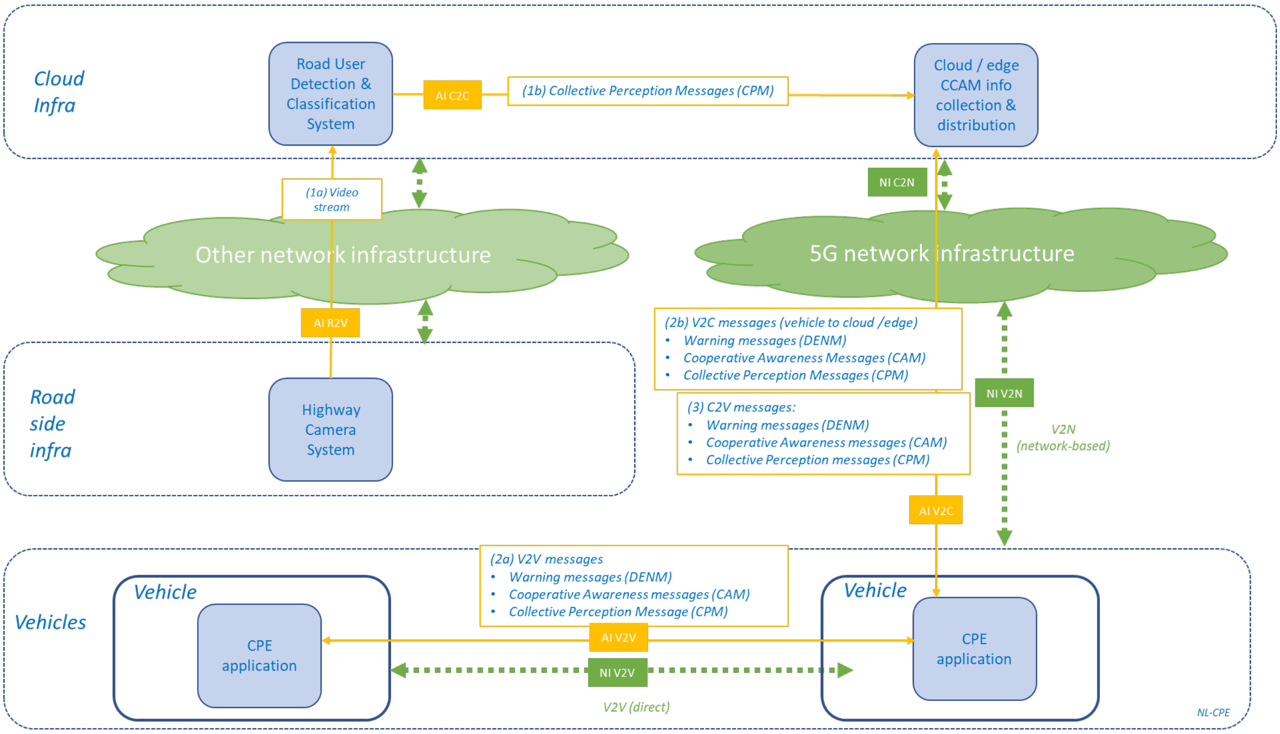


Figure 68 CCAM architecture for support of NL US14 (Collective Perception)

Sequence diagram

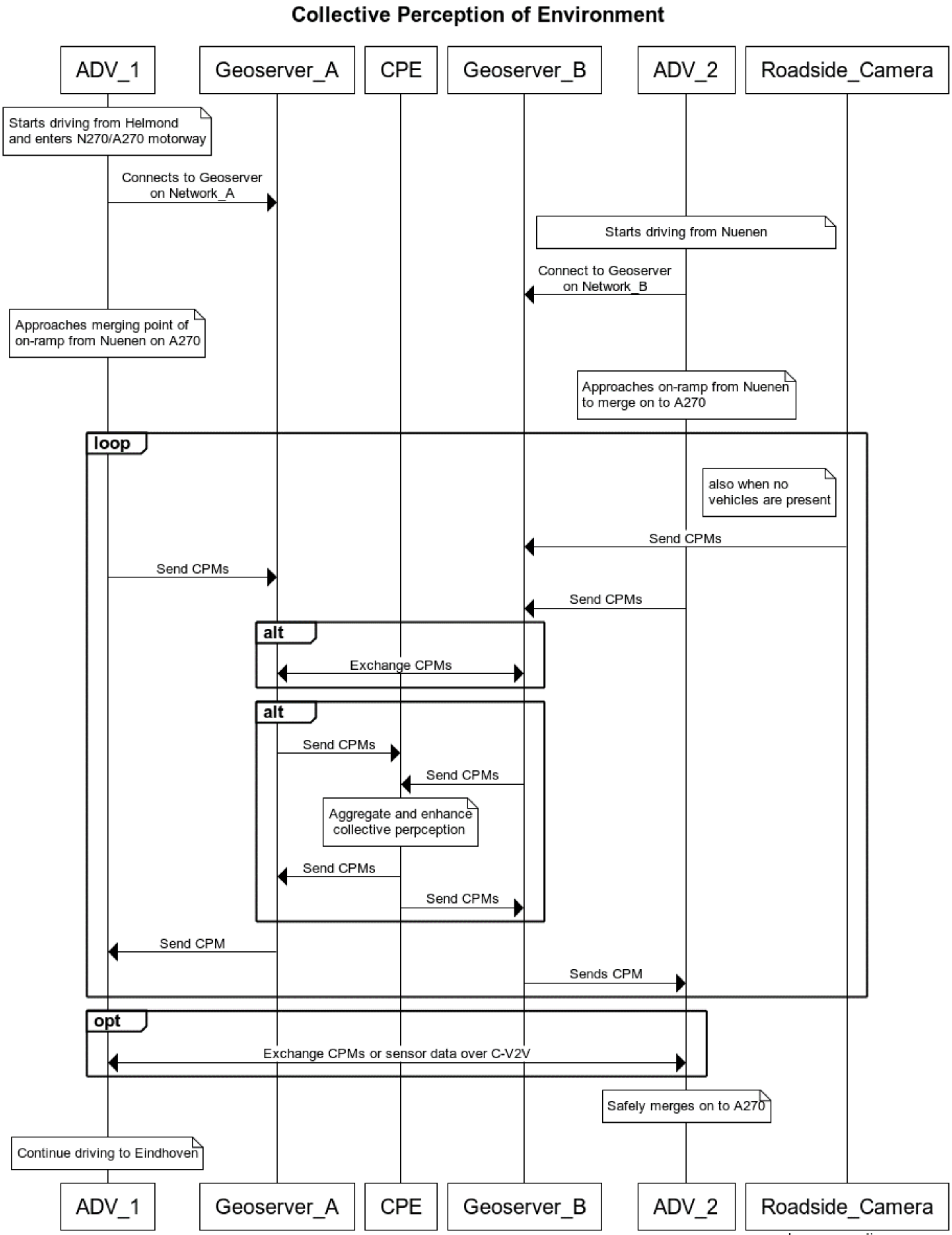


Figure 69 Sequence diagram of NL US14 (Collective Perception)

Detailed specifications

Message sets: the user story CPE makes use of different standardized ITS message sets:

1) Cooperative Awareness Messages (CAM) from vehicle-to-vehicle as defined in ETSI EN 302 637: these messages contain information on vehicle characteristics (size, special vehicle), position, speed and direction.
2) Collective Perception Message as currently standardized in draft ETSI TR 103 562, possibly with extensions if required.
3) Radio Technical Commission for Maritime Services (RTCM), for accurate positioning of the vehicles. The standard for Networked Transport of RTCM via Internet Protocol (Ntrip) [RTCM 10410.0] describes an application-level protocol that supports streaming of Global Navigation Satellite System (GNSS) data over the Internet.

The messages can be exchanged either via:

- Network-based communication: each vehicle (ADV_1 and ADV_2 in Figure 69) is connected to a central CCAM server (geo-messaging server in network A or B) to send CAM and CPM messages from the vehicles and receive information from other-vehicles or roadside systems. The network-based distribution of messages is based on geographical area of relevance and is based on the MQTT-based messaging protocol developed in the project CONCORDA. The distribution of messages to vehicles is supported via:
    c. Central CCAM server (connected via Internet)
    d. Edge CCAM server (connected to 5G network of operator A and B): the edge geo-messaging servers in network A and B are also interconnected.
- Direct communication (i.e. without 5G network infrastructure) between vehicles. State of the art solution will be used, based on availability, either ITS G5 or 5G sidelink based.

Cameras will be used to obtain detailed information on all vehicles in the merging area on the high-way. Multiple cameras cover the merging area, and object detection software is providing detailed information on all vehicles at an update rate of 10 Hz. The information will be distributed to the vehicles and/or CPE service based on CPM messages, exchanged via the geo-messaging server.

Cross-border aspects

- Different AV vehicles: interoperability at information exchange level
- Support of user story in inter-PLMN networks
- Support of edge server with hand-over between edge servers within PLMN

7.3.4. Roadside & cloud infrastructure for CN US16 (Road safety and traffic efficiency services)

Description

In this user story, we will upgrade the intersection safety information system, which consists of road radar, traffic signals, and LDM servers and RSUs. Based on them, our purpose is to detect pedestrians and avoid accidents. The other figure shows that autonomous driving vehicle fleer communicates with each other through LTE-V2X and provides the basic planning for the rear vehicle through V2V communication (including chasing, continuous running, acceleration, deceleration, obstacle avoidance, overall acceleration, and deceleration, etc.).

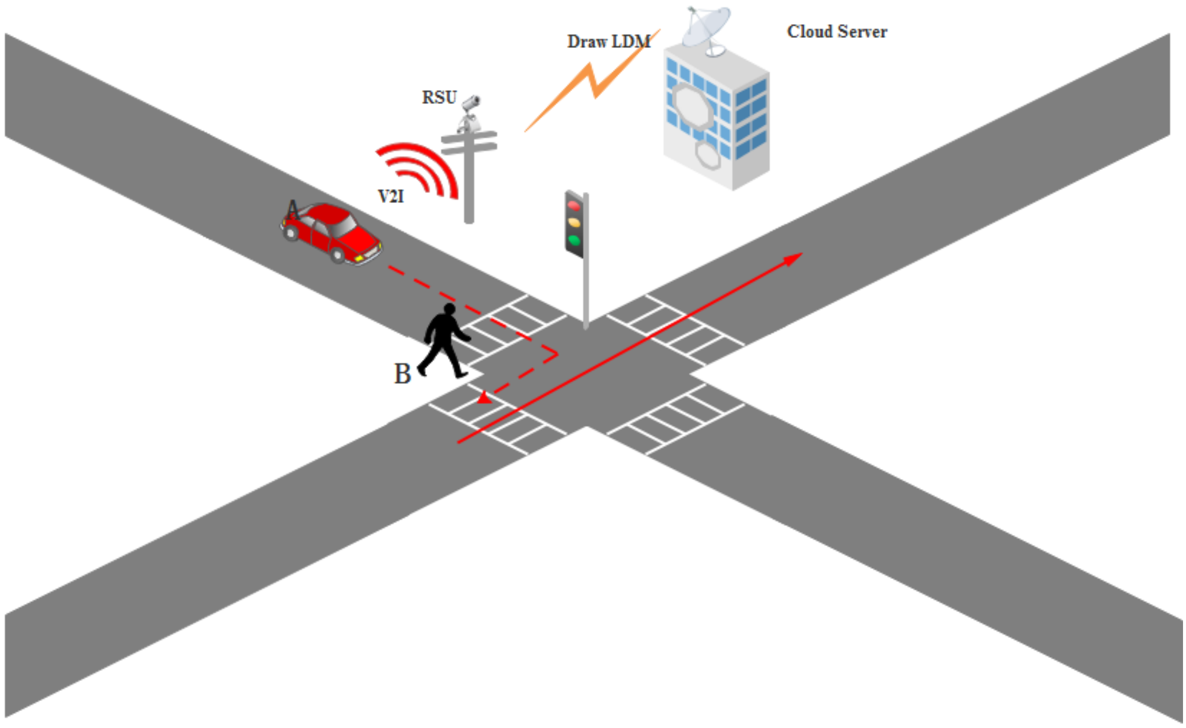


Figure 70 High-level illustration of CN US16 (scenario 1: Travel through intersection)

High-level architecture of the roadside & cloud infrastructure

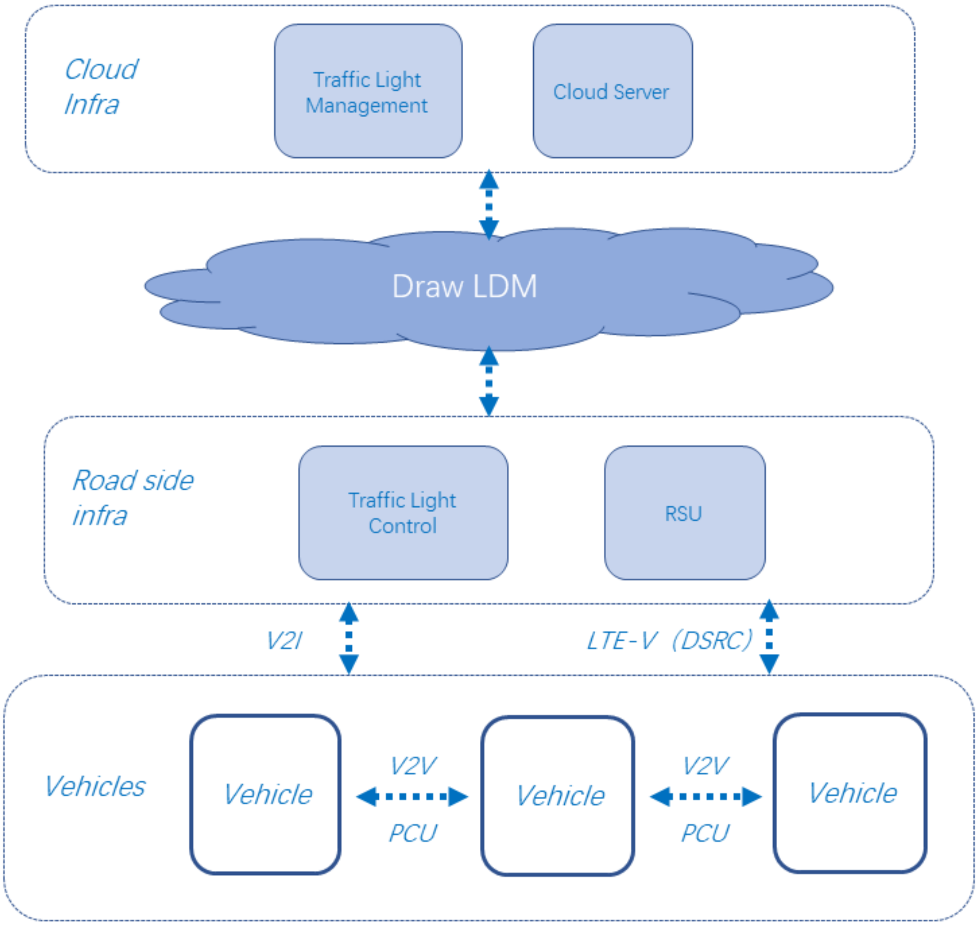


Figure 71 High-level architecture of CN US16 (scenario 1: Travel through intersection)

Sequence diagram

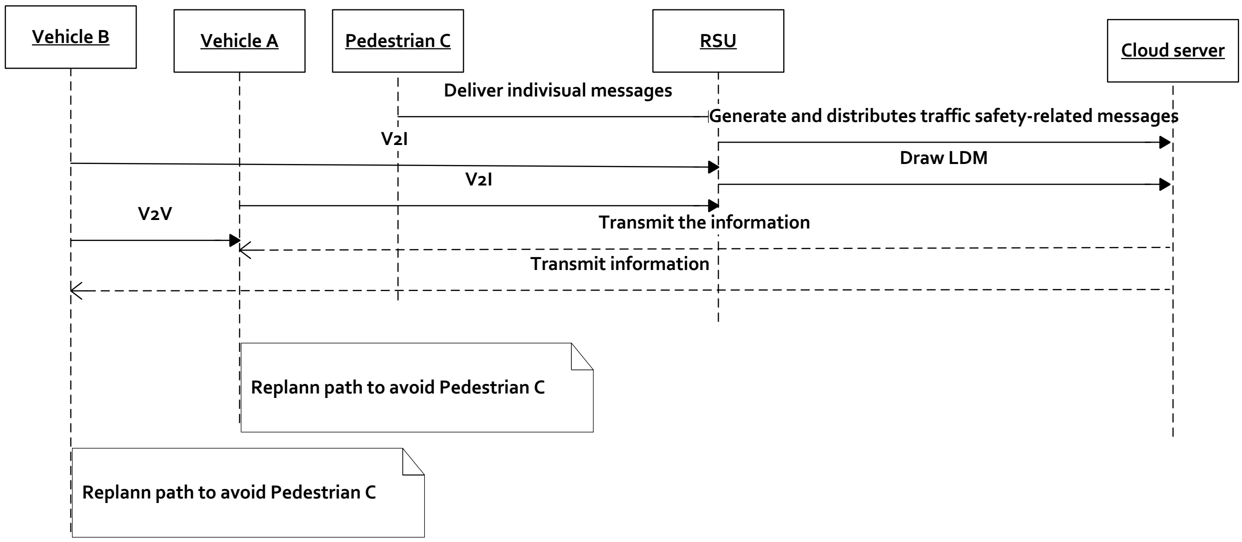


Figure 72 Sequence diagram of CN US16 (scenario 1: Travel through the intersection)

Detailed specifications

In the scenario Travel through the intersection, an autonomous Vehicle A passes through the intersection, and the control center remotely controls an autonomous test vehicle (Vehicle B) and monitors a mobile pedestrian C. Vehicle A notifies the control center when it arrives at the intersection. Vehicle B and Pedestrian C also reach the adjacent intersection. As shown in the Figure, Vehicle A aims to turn right at the intersection. Vehicle B goes straight through the intersection, at the same time Pedestrian C crosses the road. During the test, Vehicle A notifies the RSU and obtains the information of traffic lights and Pedestrian C through LDM and obtains the information of Vehicle B through V2V communication. In this way, Vehicle A can avoid a collision with Vehicle B and Pedestrian C.

Cross-border aspects

The present user story hopes to avoid the potential risks of human-vehicle conflicts which are common situations in cross-border corridors. Our cloud center has very high performances, such as HD Map, path planning and real-time decision making, which may be the most different from other sites. We also have two MNO partners, so we will compare their devices in the same case and try to find which one is more suitable for ours.

7.4. Category 4: Remote Driving

The following user stories are related to Remote Driving:

1. ES-PT US3 (Automated shuttle remote driving across borders)

2. FI US9 (Remote Driving)
3. NL US13 (Remote Driving)
4. CN US19 (Remote driving with data ownership focus)
5. KR US18 (Remote Driving)

7.4.1. Roadside & cloud infrastructure for FI US9 (Remote Driving)

Description

In this remote driving user story, the remote human operators would utilise live data feeds from vehicular sensors (LIDAR, radar, camera, etc.) to formulate and send back commands for controlling the vehicle in a reliable manner over a V2N connection between an L4 vehicle and a remote driving application used by the remote human operator. The V2N connection transfers the sensor data feed (high-resolution perception data) from the vehicle to the remote human operator (in the uplink direction). The sensor data provides the human operator a "driver's view" for that vehicle and allows the human operator to send appropriate command messages (e.g. command trajectories) back to the L4 vehicle (in the downlink direction). The reliability and effectiveness of the decisions and commands from a remote human operator of an L4 vehicle is contingent on the quality and timeliness of the data received from the vehicle's sensor feeds. The safe operation also requires prompt delivery of the commands to the vehicle. Therefore, any significant constraints or disruptions in the data transfer would not be tolerable in a remote driving scenario.

High-level architecture of the CCAM infrastructure

The high-level architecture of the CCAM infrastructure for the FI remote driving user story is shown in Figure 73. As the user story does not involve the use of roadside infrastructure, they are not shown in the architecture diagram for simplicity. Otherwise, the common convention is used to represent in blue the functional elements in the physical layers, while the network / communication elements are shown in green, and the end-to-end information exchange for remote driving is shown in yellow.

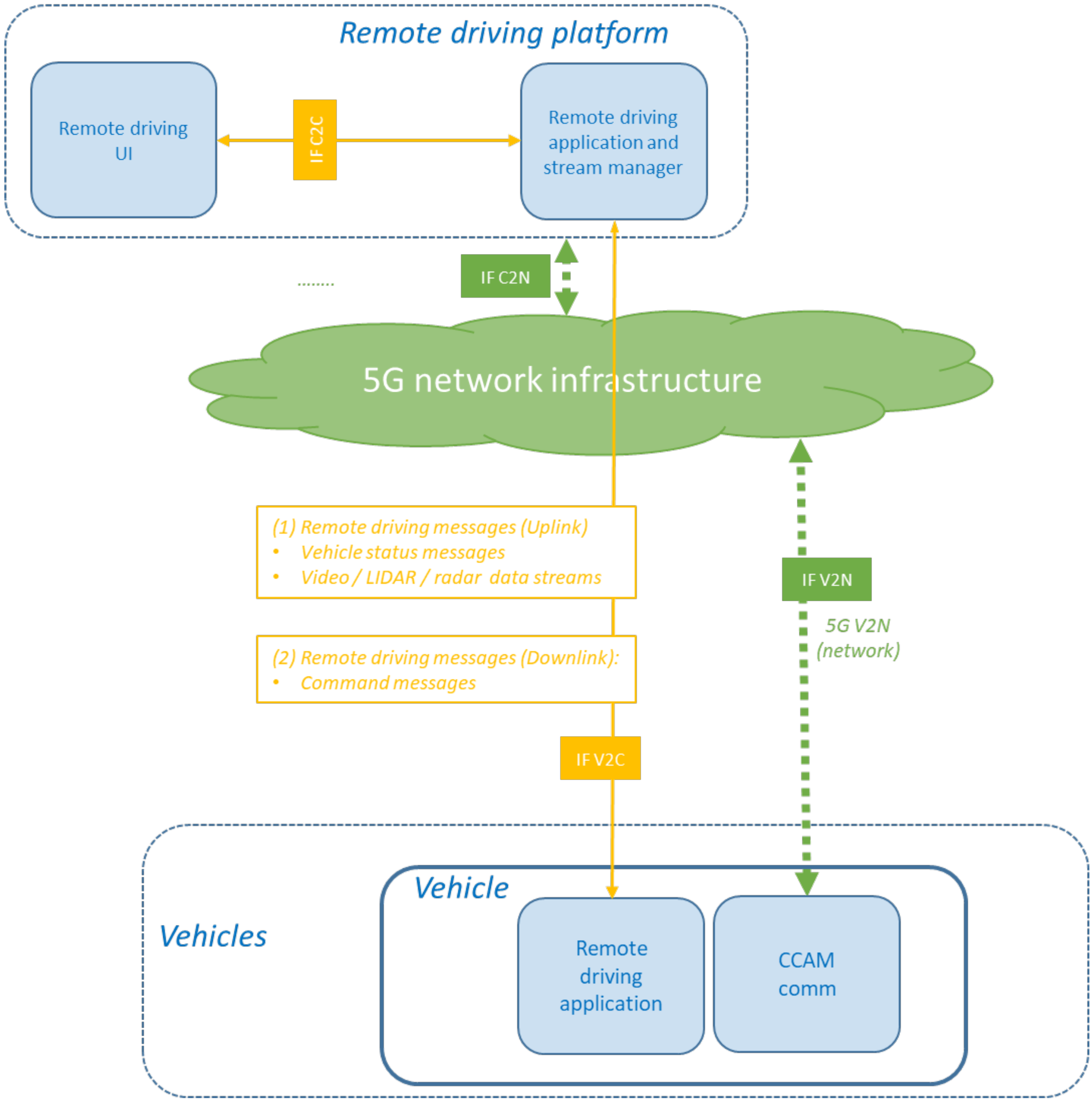


Figure 73 CCAM architecture for support of FI US9 (Remote Driving)

Sequence diagram

The sequence diagram for the remote diagram user story emphasizing the interactions between different elements in the previously described CCAM architecture is shown in Figure 74 below.

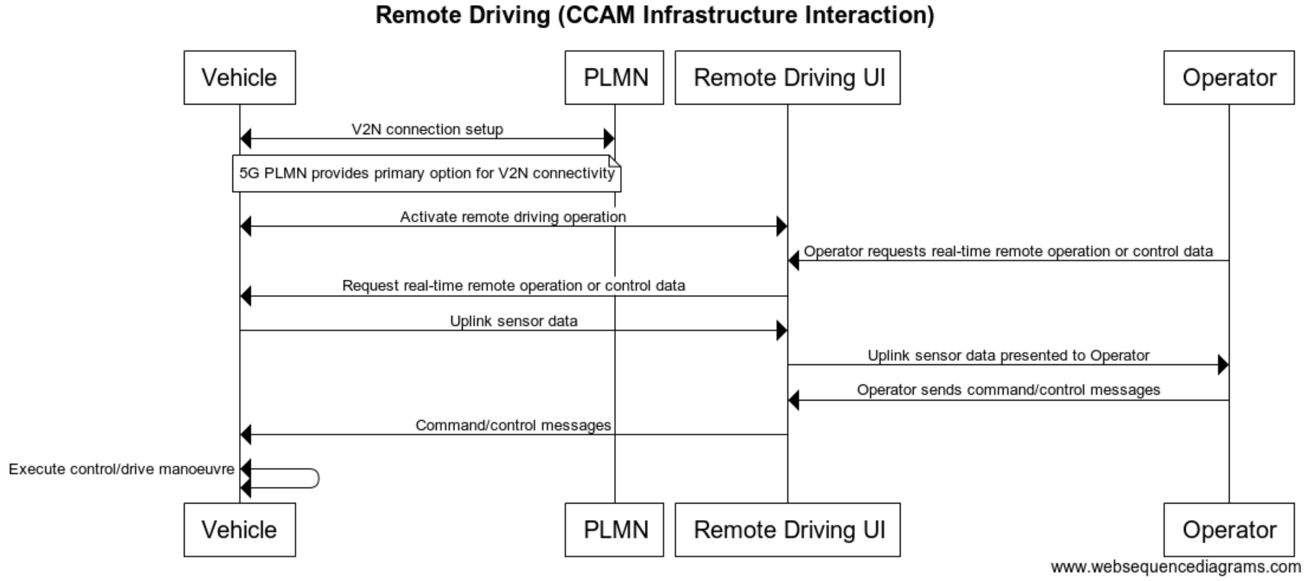


Figure 74 Sequence diagram of FI US9 (Remote Driving)

Detailed specifications

<u>Uplink and downlink data format</u>

The remote driving user story involves the transfer of messages or data between the vehicle and the remote operations centre. The data transfer is inside VPN (Virtual Private Network) tunnel using messaging middle ware from ROS (Robot Operating System) providing serialization, transport, and discovery functions for the data, data producers and consumers. The data and messaging middleware provides also metadata about the messages e.g. min, max range of the sensor or field of view as well as integral information about the data itself, such as time stamps. The main data types are described below:

1) Uplink messages or data (from the vehicle):
    a. Raw sensor data:
        i. Video: jpeg compressed image buffers
        ii. Video: MPEG Transport Stream (MPEG-TS). Video delivery is done using DASH (Dynamic Adaptive Streaming over HTTP)
        iii. Radar: range data as float lists of ranges and distances
        iv. LIDAR: list of range data described above
    b. Vehicle status messages: Data structure including at least pose (longitude, latitude, orientation), motion state (velocity, acceleration, steering angle), internal state (executing trajectory, avoiding obstacle, stopped, …), energy level and various temperatures (outside, CPUs, cabin, etc.)
2) Downlink Vehicle control messages
    a. Remote driving command messages:
        i. State control command (paused, manual control, remote control, autonomous, etc.)

ii. Trajectory to be executed: list of waypoints (pose, velocity)
iii. Command to start executing the trajectory
iv. Direct driving command: Desired motion status (velocity and steering angle) sent in fixed frequent interval

Remote driving application

The sensors in the vehicle are data sources or services that publish their data to the subscribers inside the VPN. Remote driving application then subscribe the sensor feeds from the vehicle and provides the command data sources for the vehicle to subscribe. Thus, the data channels between the vehicle and remote operations centre are established. The subscription is established or ended on demand and only the data subscribed for it is sent. This limits the network load from excess amount of unused high bandwidth sensor data.

The remote driving application visualises and decompresses the sensor feeds for the remote operator. The data can be merged e.g. colouring of the LIDAR based 3D point cloud based on the camera information, and perspectives for the data can be altered for better situational awareness. The application also provides the means for the operator to instruct the new trajectories and in case of verified low latency connection, to do direct teleoperation of the vehicle, as visualized in Figure 75 below.

Figure 75 Remote driving with direct teleoperation

Video archiving and playback platform

The remote operator may have the possibility to view video footage taken from the L4 vehicle prior to a remote driving request. For instance, video footage taken 5-10s or 50m before the remote driving was trigger would allow the remote operator to have further understanding of the triggering events. To that end, the LEVIS (Live strEaming VehIcle System) platform will also be leveraged in this user story to obtain HD video streams (with location tags) from the vehicle. Video camera(s) and LEVIS-Client application on the vehicle offers the users (subscribers of the video stream) with different features, including Live Streaming, Local Recording and Uploading Recorded Streams. The different streams could be accessed through LEVIS web platform by third-parties software and subscribed users. In the case of remote driving user story, the subscriber would include the remote operator.

The overall LEVIS architecture is depicted below in Figure 76. The LEVIS web platform offers a secure platform that enables only authenticated users to access the different streams for watching and enables streams' owners to manage their streams. Furthermore, LEVIS offer social interactions functionality that enables users (subscribed to same video stream) to share contents among themselves, as well as, have live chatting and commenting on a stream being viewed simultaneously by multiple users. In remote driving context, this could be useful if multiple human operators are involved in same or different remote operations centres.

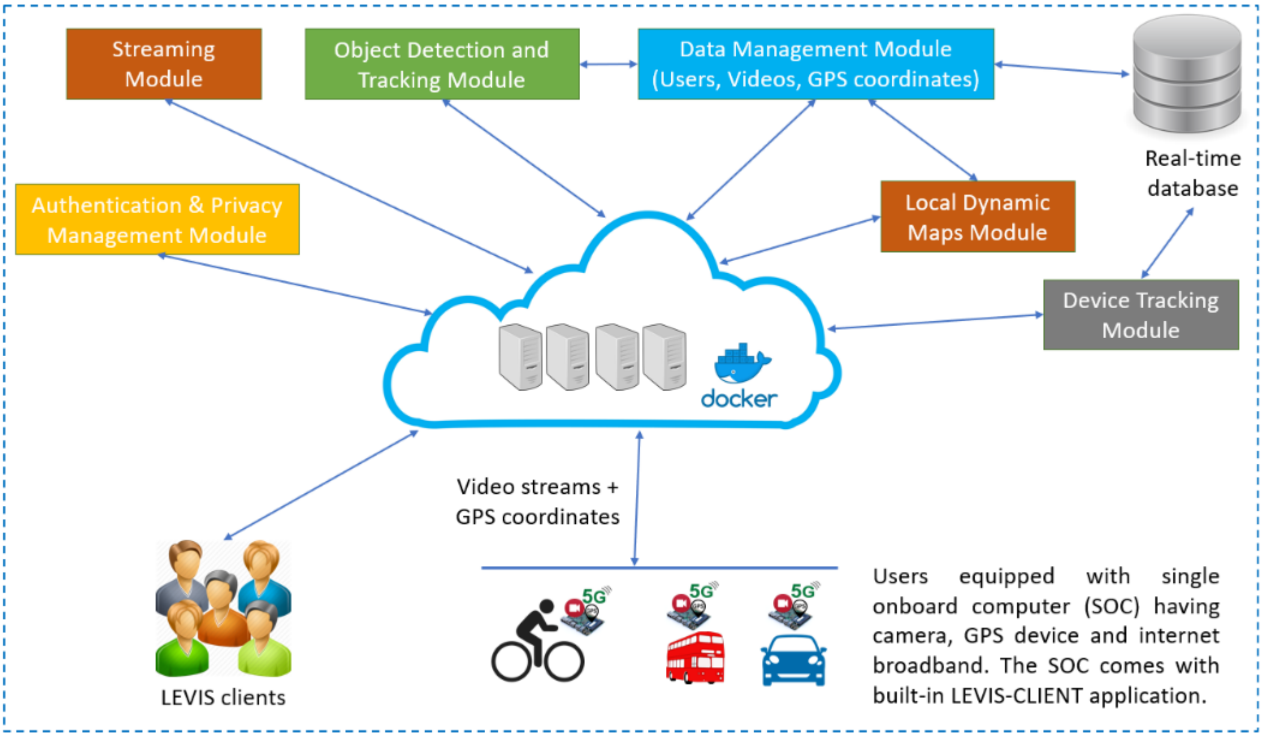


Figure 76 Architecture of the LEVIS platform

Cross-border aspects

- The user story considers remote driving when vehicle roams between different PLMNs

7.4.2. Roadside & cloud infrastructure for NL US13 (Remote Driving)

Description

In a situation where the AD vehicle is unable to manoeuvre further (due to a failure or unexpected driving condition), a remote human operator takes over control of the vehicle and drives it to a point where AD can be resumed. As an example, this can be in situations like border control, construction zones and inclement weather. To tele-operate a vehicle, the vehicle with multiple onboard sensors should stream this information (synchronised and with low latency) to the human operator and at the same time the human operator needs a low latency connection for the control task of manoeuvring the vehicle in real time.

High-level architecture of the CCAM infrastructure

The high-level architecture of the CCAM infrastructure for the tele-operation and tele-monitoring service is shown in Figure 77. No roadside systems are used in this user story

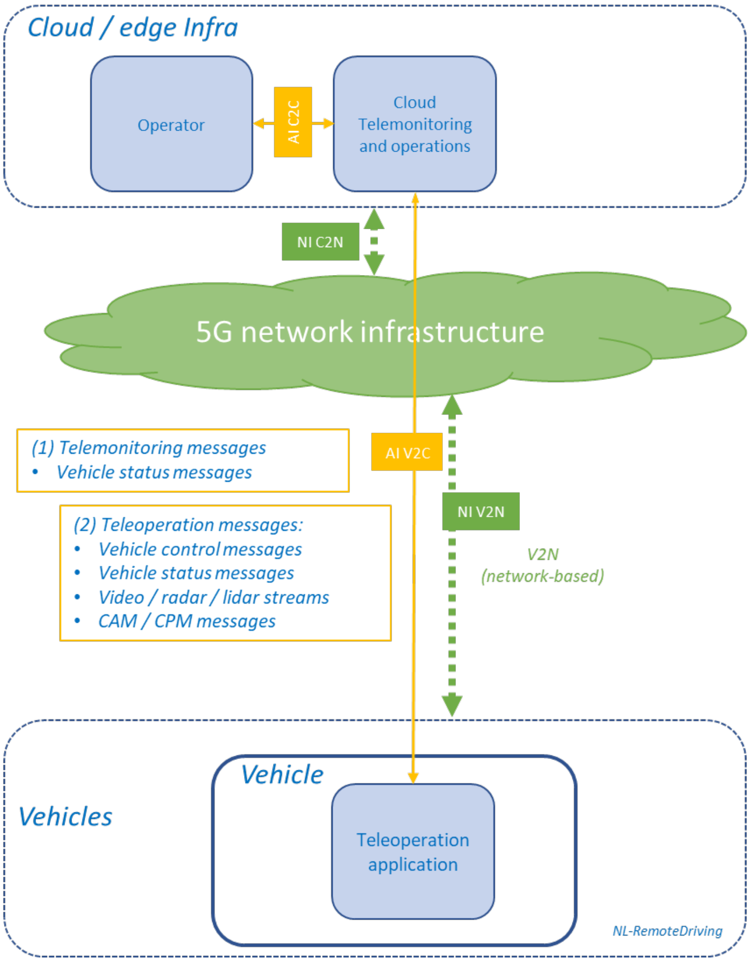


Figure 77 CCAM architecture for support of NL US13 (Remote Driving)

The functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, the information exchange is shown in yellow. The architecture does not cover the cross-border aspects.

Sequence diagram

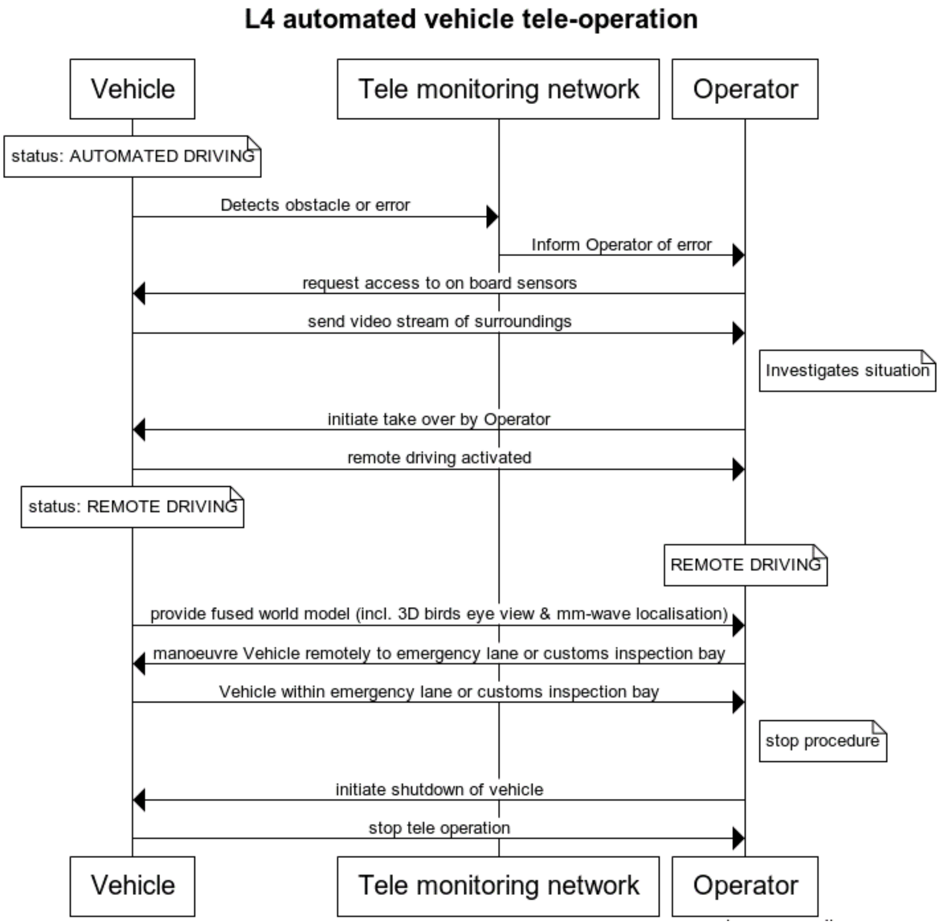


Figure 78 Sequence diagram of NL US13 (Remote Driving)

Detailed specifications

The user story makes use of different message sets:

1) Tele monitoring messages: vehicle status messages such drive status.
2) Teleoperation messages:
    a. Sensor data: video, lidar (& possible radar)
    b. Vehicle status messages, such as pose (position) & twist (speed)
    c. Vehicle control messages, such as trajectory

The message will be exchanged via network-based communication. Thus, the vehicle will be connected to a central tele-operation server to send status messages and request for tele-operation. The server will also be used during tele-operation to exchange information to control the vehicle.

The distribution of messages is supported via:

1) Central CCAM server (connected via Internet)
2) Edge CCAM server (connected to 5G network of operator X)

Cross-border aspects

The implementation of this user story brings valuable results including:

- Support of user story in inter-PLMN networks
- Support of user story with edge server and hand-over between edge servers

7.4.3. Roadside & cloud infrastructure for CN US19 (Remote driving with data ownership focus

Description

This user story tries to enable the vehicle to assess the probability of an accident better and coordinate the exchange of information in addition to safety information, sensor data, braking and acceleration command lists, horizontal and vertical control in the application of road traffic flow throughV2X communication.

The autonomous vehicle is equipped with advanced onboard sensors, controllers, actuators and other devices. It integrates modern communication and network technology to realize intelligent information exchange and sharing between the vehicle and X (vehicle, road, human, cloud, etc.) and has functioned such as complex environment perception, intelligent decision-making, and collaborative control. In our China site, the roadside unit, remote control centre and cloud server will monitor and control the autonomous vehicles in real time, to realize the various testes of Internet-connected applications of vehicles safely and efficiently.

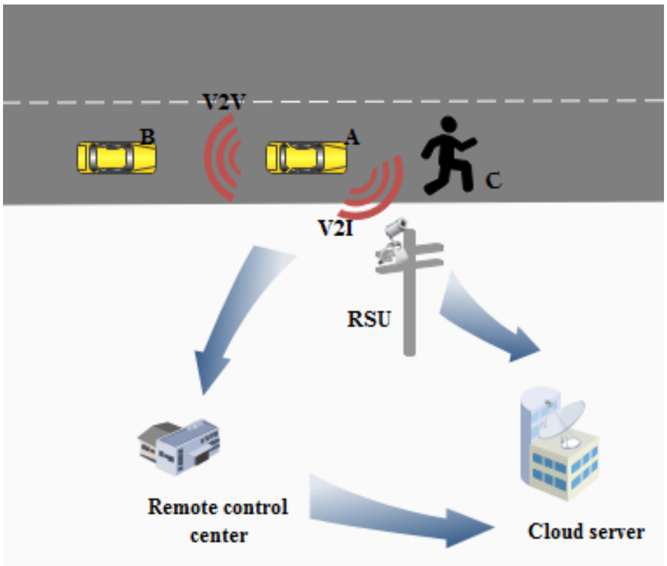


Figure 79 High-level illustration of user story CN US19 (Remote driving with data ownership focus)

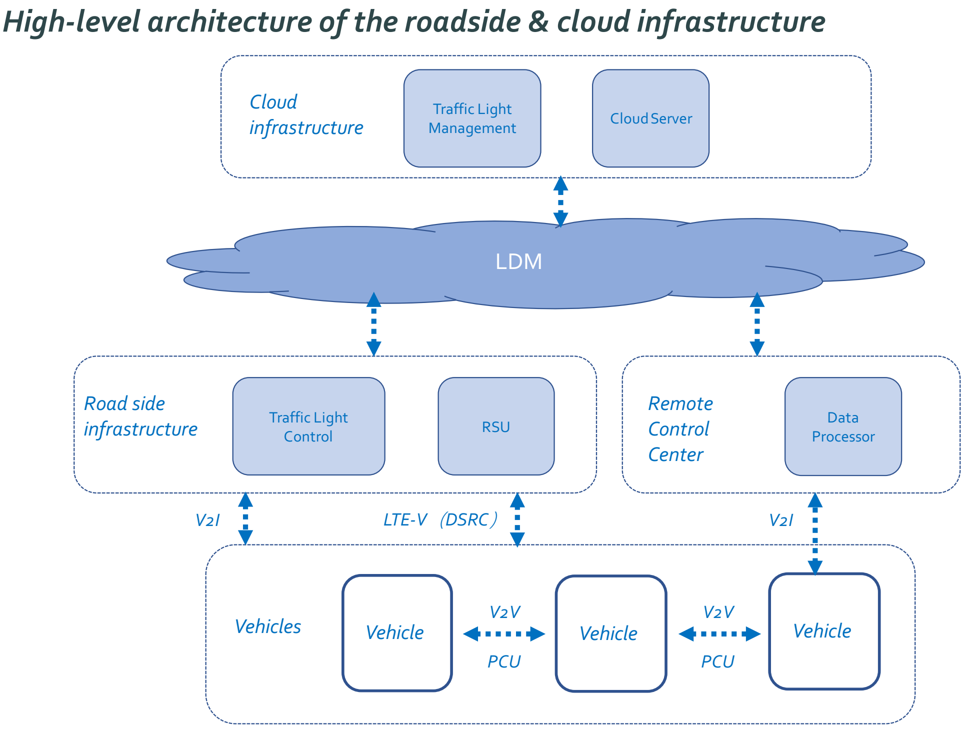


Figure 80 CCAM architecture of the user story CN US19 (Remote driving with data ownership focus)

Sequence diagram

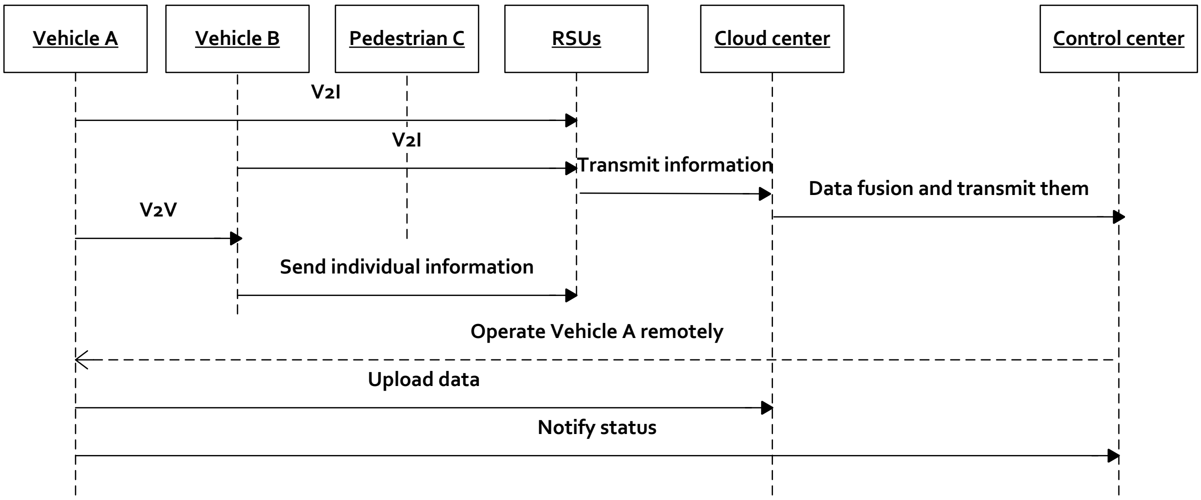


Figure 81 Sequence diagram of the user story CN US19 (Remote driving with data ownership focus)

Detailed specifications

In the Remote Manoeuvre scenario (Scenario 2), the control center first plans the scheme and then sends the global path information to Vehicle B through RSU. During the experiment, subject vehicle A communicates with RSU via V2I and with test vehicle B via V2V. After obtaining real-time information, local path planning will be carried out to complete the plan. After the test, Vehicle A notifies the control center and uploads various data to the cloud server.

Cross-border aspects

Our remote and cloud center has very high performances, such as HD Map, path planning and real-time decision making, which may be the most different from other sites. We also have two MNO partners, so we will compare their devices in the same case and try to find which one is more suitable for ours.

7.4.4. Roadside & cloud infrastructure for KR US18 (Remote Driving)

1.1.1.1.4. Description

Remote driving user story enables remote operator to access the right of control in case of automated vehicle in under malfunction or driver is in accident. The most important factors for realizing remote driving should comprise the following: Ensuring enough field of view and high definition of view for front camera, ultra-low latency to sharing live video stream between vehicle equipped cameras and remote site, and reliable connectivity to control remote driving vehicle in remote site. Consequently, remote driving vehicle needs to be shared not only driving information like speed, position, and videos (front, right and left side, and rear), but also vehicle status information like steering angle, gear position, throttle pedal position, and fuel consumption with remote operator. The driving and status information provided by the remote driving vehicle should be transmitted to the human operator at the remote site with ultra-low latency. To share high definition live video stream data with remote site in real-time, very high up-link data rate should be required and it will be realised by 5G network. At the same time, the control data to driving remote vehicle should be generated by human operator at the remote site and be streamed to the remote driving vehicle through down-link with low latency.

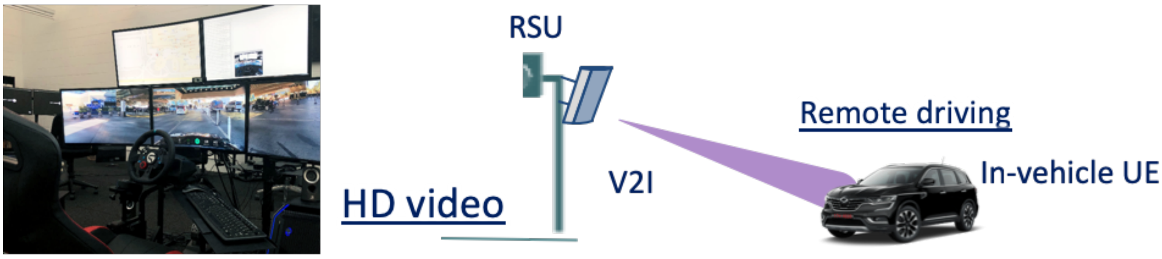


Figure 82 Remote driving user story from the South-Korea local test site

1.1.1.1.5. High-level architecture of the CCAM infrastructure

Figure 85 depicts a high-level architecture of the CCAM infrastructure that will be used for the remote driving service. The eMBB will be implemented to provide moving vehicles with a broadband mmWave-band V2I link that allows RDV to share raw sensor data and high definition video steam with remote site. In addition, the network slicing will be implemented to ensure mission critical data exchange with low latency up and down link access between RDV and remote site.

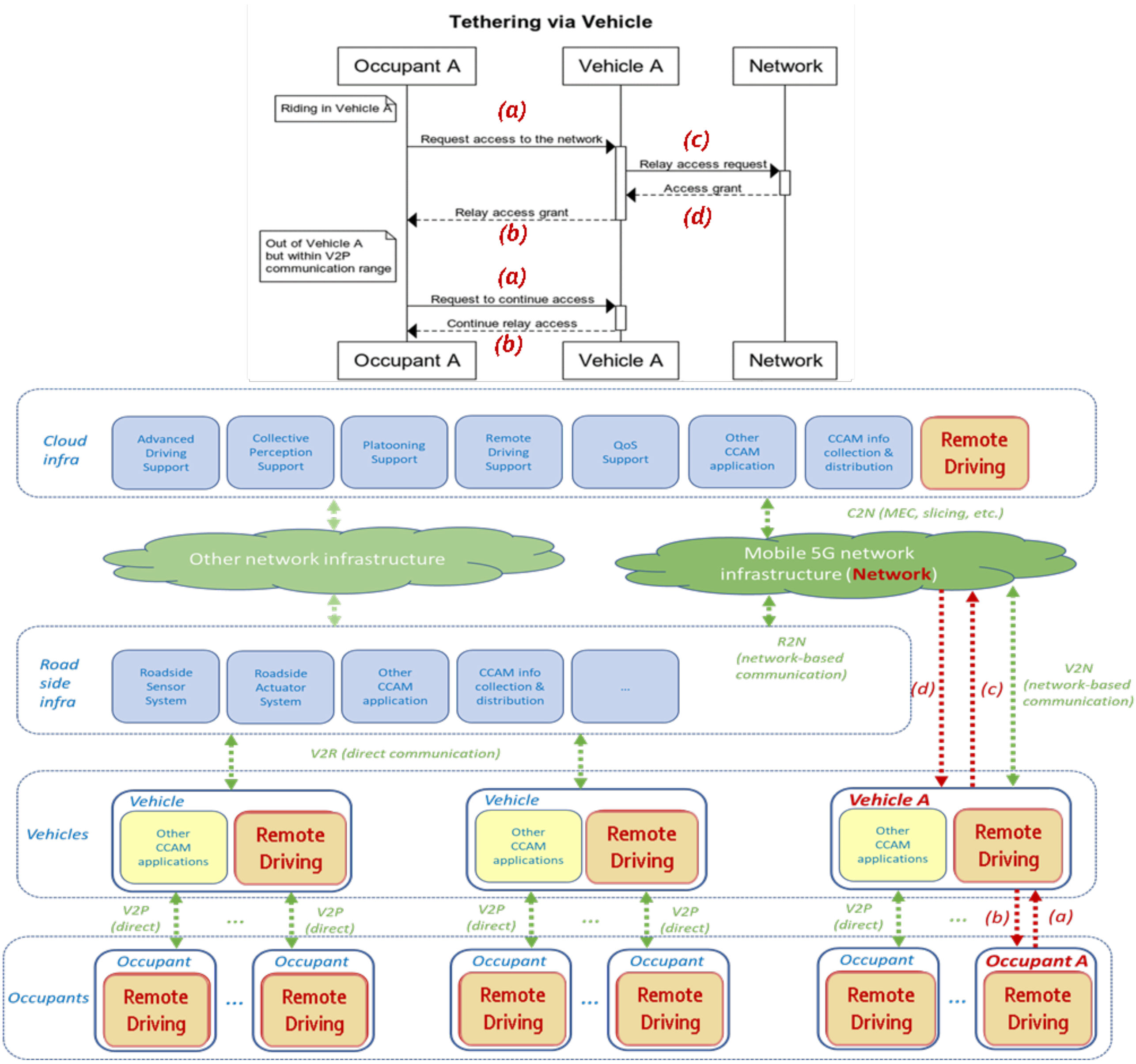


Figure 83 CCAM architecture for support of KR /UC2 (Remote Driving)

Detailed specification

The user story makes use of different message sets:

1) Status information messages: These messages are consisted of sensor data, live video stream, and vehicle status data. It will be are provided by the vehicle to human operator in the remote control center.
2) Remote driving control messages: These messages are consisted of steering wheel, throttle, and transmission control data. These data are used when the operator is going to intervene and take over the vehicle control.

The messages between AD vehicle and remote control center are exchanged via network-based communication.

Cross-border aspects

- The user story is similar to user stories in the ES-PT cross-border corridor, so it serves as a pre-test.
- Especially, the South-Korea trial site should be focused on the RDV system based on real-time high definition multi-video live streams (1 front, left and right side, and rear) to ensure the safety of the RDV.
- The user story is hard to test in real road situation because of possibility of the car accident or occurring traffic congestion during the test, therefore it is tested at a local site
- Test results and scenario will be shared with cross-border so that it will help to minimize trial and error of the ES-PT cross-border corridor.
- The present user story completes the set of user stories tested in cross-border corridors with:
  - A prototype system of mmWave-band 3GPP 5G NR V2I communications that introduce key enabling technologies capable of overcoming various technical challenges caused by using mmWave and supporting high mobility.
  - The user story will be tested at South-Korea test site, which offers urban type proving ground located in Yeonggwang area (300m x 300m).

7.5. Category 5: Vehicle Quality of Service Support

The following user stories are related to Vehicle QoS Support:

1. ES-PT US2 (Public transport with HD media services and video surveillance)
2. FR US11 (QoS adaption for Security Check in hybrid V2X environment)
3. KR US17 (Tethering via Vehicle using mmWave communication)

Note: the FI US8 (cooperative perception) supports QoS via two simultaneous PLMN connections to monitor QoS for edge services and steer traffic to the connection which meets QoS requirements. This user story category is broader than the category as described in 3GPP TS 22.186.

7.5.1. Roadside & cloud infrastructure for FR US11 (QoS adaption for Security Check in hybrid V2X environment)

Description

The present use case deals with a situation where a suspicious vehicle is detected by a police car on the road. The police car requests the Vehicle Identification Number (VIN) and other information (IP address) from vehicle A, and then notifies this information to the police centre. Upon reception of VIN, the police centre checks its VIN data base and obtains the vehicle related information (ex: owner). Furthermore, the police centre can perform real-time security control/tracking by requesting roadside sensor data from MEC1 as well as sensor and camera data from the vehicle.

Vehicle A starts to stream its camera video to the police centre according to the current link quality. Meanwhile, the vehicle is crossing the border, network and application handover procedures have to be executed. At the application level, security check will be continued by the police centre 2. At the network level, a change of access network is needed. Depending on the mounting positions of the eNodeB/gNodeBs and also the types of the networks, the user may experience different issues such as a coverage gap or a sudden degradation of communication quality. In order to ensure the continuous security check, the vehicle shall perform soft handover to the prioritized available network technology according to a priority-based network selection algorithm. MEC predictive QoS support could also be used to provide Handover time prediction and QoE optimization in order to maintain the service continuity.

Then, the vehicle will adjust its transmission parameters (data type, data size, transmission rate, etc) by taking into account the QoS change of the network link.

The vehicle tracking can be followed by manual security control by the police. To do so, the police instructs the vehicle to stop in a safe area by transmitting Manoeuvre Coordination Message (MCM).

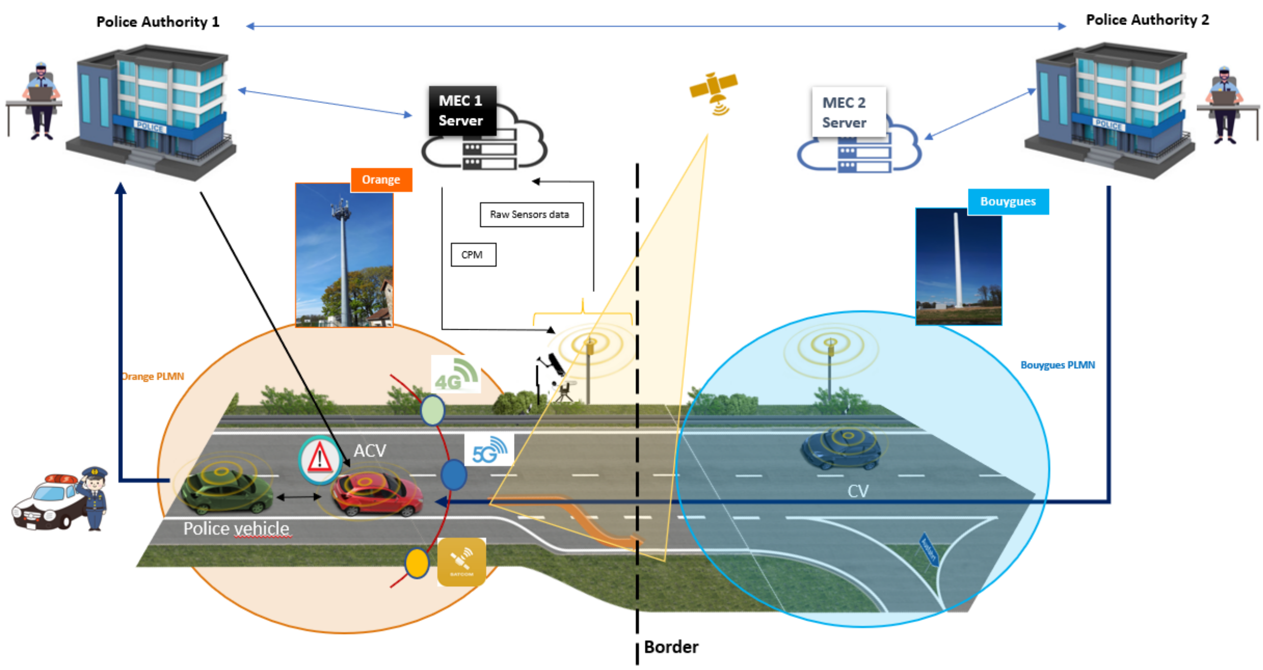


Figure 84: Remote Driving user story

High-level architecture of the CCAM infrastructure

Figure 85 depicts a high-level architecture of the CCAM infrastructure that will be used for the teleoperation service. As it already mentioned in the description of the user story, this latter does not require a road system to support the user story.

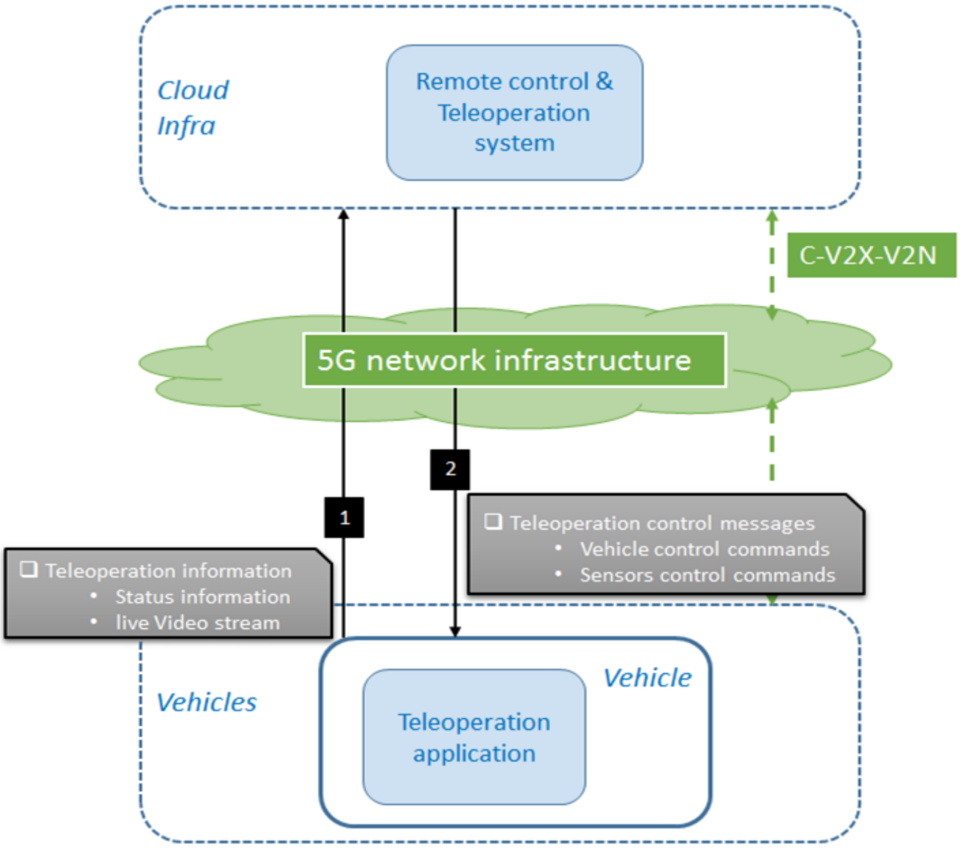


Figure 85:CCAM architecture for support of FR US11 (Remote Driving)

Detailed specification

The user story makes use of different message sets:

1) Telemonitoring information: this information is provided by the vehicle and transmitted towards the teleoperation centre. It helps the operator to monitor the AD vehicle system (sensors data, live video stream, etc).
2) Teleoperation control messages: These messages are used when the operator is going to intervene and take over the vehicle control.
    a. Sensors control messages: Raw sensor data: video, radar, lidar. Operator can control remotely the sensors and ask some control functions (changing camera angle, etc).
    b. Vehicle status messages
    c. Vehicle control messages: These messages allow the operator to control vehicle's parameters (steering, velocity, etc.) when it's being taken to the safe area.

The message is exchanged via network-based communication: the vehicle is connected to a central tele-operation server to send status messages and request for tele-operation. The server is also used during tele-operation to exchange information to control the vehicle.

The distribution of messages is supported via:

1) Central CCAM server (connected via Internet)
2) Edge CCAM server (connected to 5G network of operator X)

Cross-border aspects

- Support of user story in inter-PLMN networks

7.5.2. Roadside & cloud infrastructure for KR US17 (Tethering via Vehicle)

Description

Tethering via Vehicle user story enables in-vehicle UEs and pedestrian UEs to access the network with the help of a vehicle relay which is deployed at a vehicle. For in-vehicle UEs, through Tethering via Vehicle user story, it is possible to avoid high penetration loss occurring from the metallic vehicle surface, thereby achieving more reliable wireless connectivity as well as reduced UE power consumption. The in-vehicle UEs are also benefited from the minimized handover operations. Only the vehicle relays involve in the handover operations. For pedestrian UEs, Tethering via Vehicle user story enables more reliable connectivity, increased throughput and reduced UE power consumption since it reduces the communication range of the pedestrian UEs.

In a typical deployment, a vehicle relay can have the Internet connectivity to the network through a radio base station (BS) e.g. a macrocell base station, microcell base station, and BS-type roadside unit (RSU). Another UE such as UE-type RSU can also provide the Internet connectivity to the network. Tethering via Vehicle user story generally supports eMBB-type services such as web surfing, file transfer and video streaming. Hence, it intrinsically requires high data throughput up to several Gbps. To satisfy such very high throughput, large bandwidth is necessary which is quite difficult in lower frequency bands below 6 GHz. Therefore, mmWave frequency band should be employed to support such high throughput and to satisfy the Tethering via Vehicle user story.

High-level architecture of the roadside & cloud infrastructure

The high-level architecture of the CCAM infrastructure for the "Tethering via Vehicle" user story is illustrated in Figure 86. Functionalities related to "Tethering via Vehicle" user story can be realized by utilizing virtualized network infrastructure across cloud, roadside, vehicle, and occupants.

The functional elements in the physical layers are shown in blue, the network / communication elements are shown in green, the information exchange is shown in yellow. The architecture does not cover the cross-order aspects.

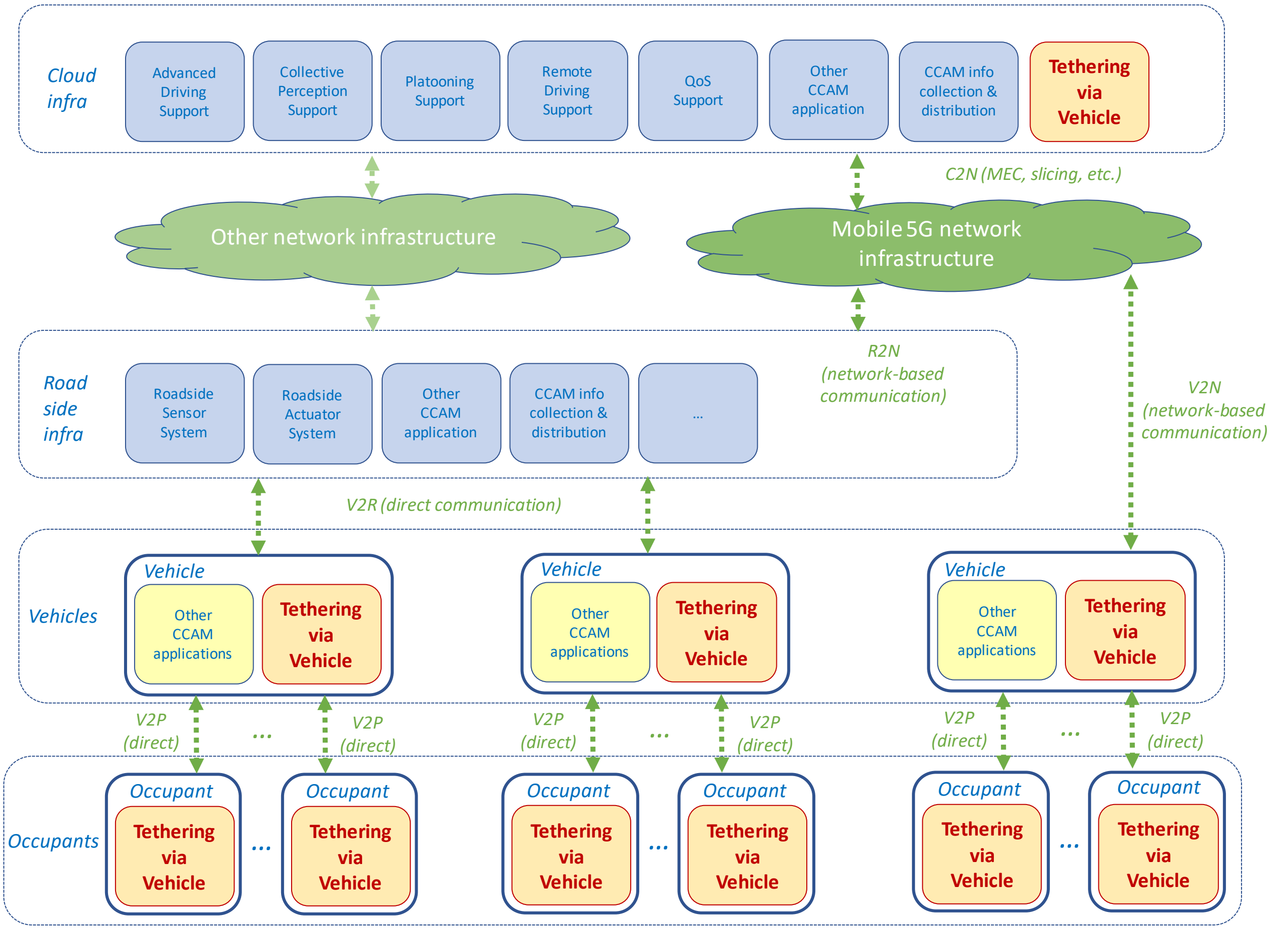


Figure 86 CCAM architecture for the "Tethering via Vehicle" user story.

Sequence diagram

The Figure 87 depicts the sequence diagram for the user story "Tethering via Vehicle" and how the block components and the interconnections are mapped into the architecture presented in Figure 86.

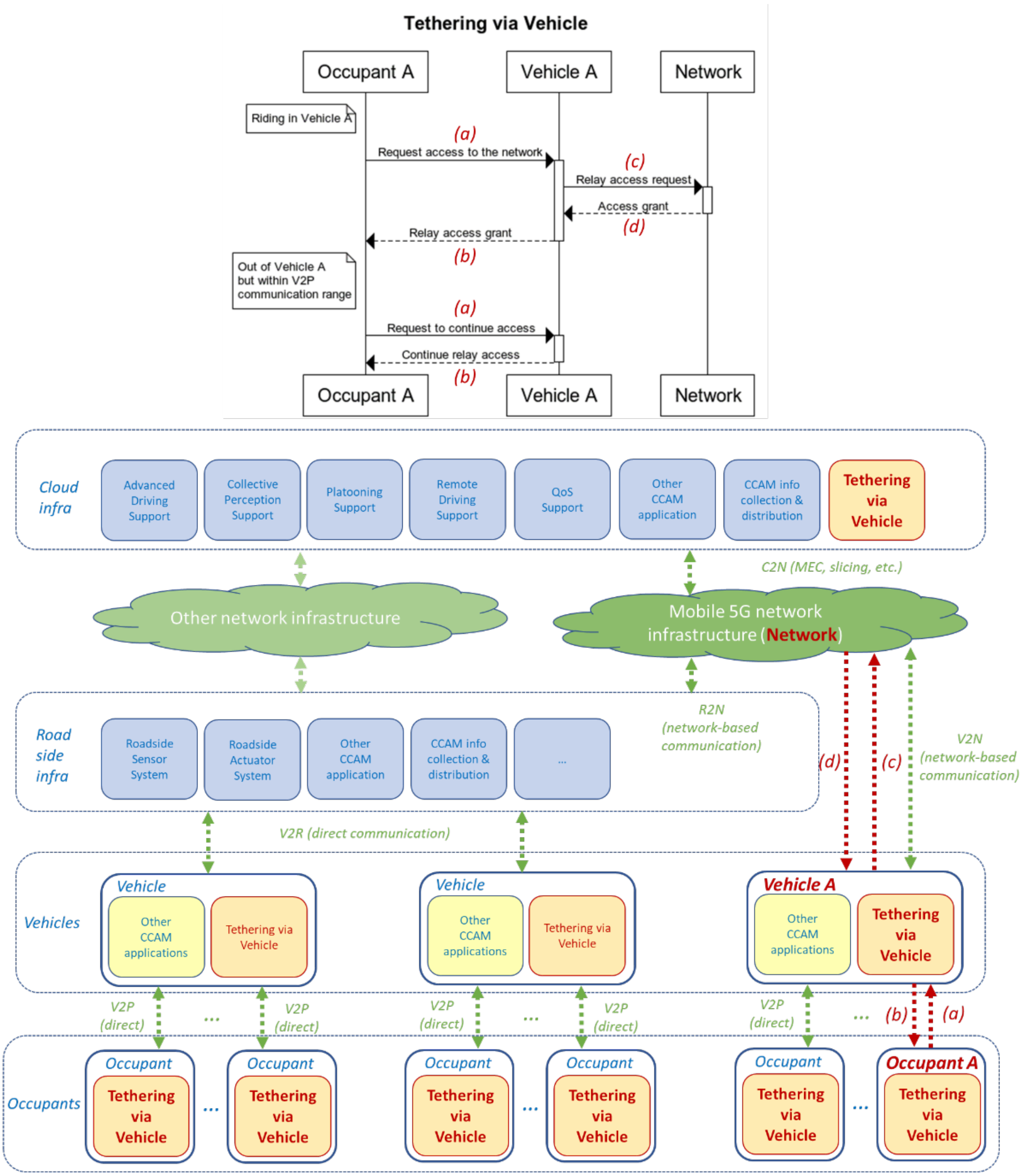


Figure 87 Sequence diagram of Tethering via Vehicle user story mapped into the architecture. Detailed specifications

RSUs and vehicles are connected based on the 3GPP 5G air interface (Uu) protocols. The RSUs include layer 1 (or physical layer) modem and mmWave array antennas in the KR user story, and they are normally deployed along roads. Digital units (DUs) are comprised of higher layer functionalities and are connected to the RSUs through optical cables. The DUs are connected to a 5G core network, which provides gateways to the Internet. Figure 88 illustrates the main components deployed in the user story.

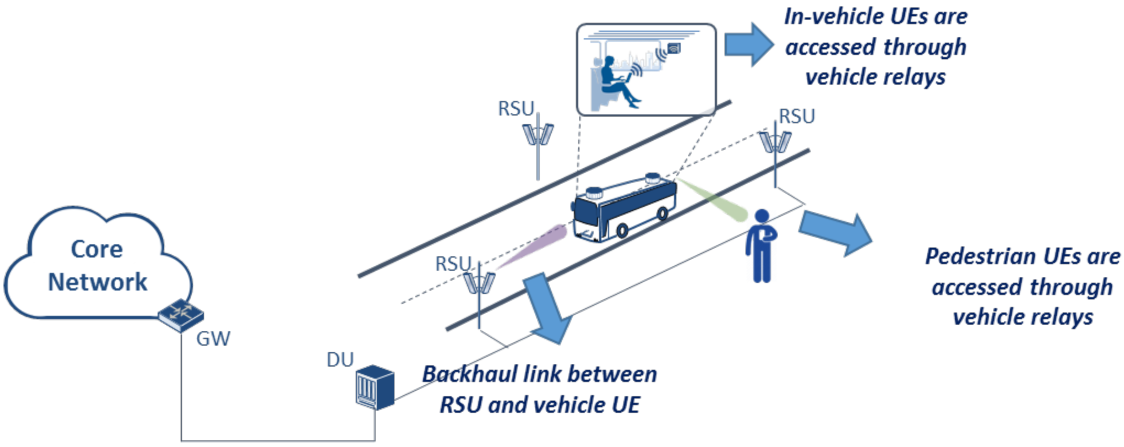


Figure 88 Example of Tethering via Vehicle user story

Meanwhile, the 3GPP 5G new radio specifications provide systematic layer 1 parameters for a variety of applications such as eMBB, URLLC and mMTC. The KR site trial system selects best applicable parameter sets for high data rate services based on mmWave. The table below details some physical layer characteristics and numerology features.

Parameter	$\mu = 2$	$\mu = 3$
Carrier frequency band (GHz)	22.1 – 22.7	
Max. number of component carriers (CCs) per gNB	6	
Max. number of CCs per UE	3	
Bandwidth per CC (MHz)	100	
Subcarrier spacing (kHz)	60	120
Number of PRBs (Physical Resource Blocks) 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 (CP) duration (µs)	1.17	0.57
OFDM symbol including CP (µs)	17.84	8.92

The Uu interfaces between a base station and UE consist of layered protocol structures for user plane and control plane as defined in 3GPP TS38.300. Overall, we find the similar protocol stack structure between

5G NR and 4G LTE except SDAP (Service Data Adaptation Protocol) introduced newly in the user plane for 5G, as shown in Figure 89.

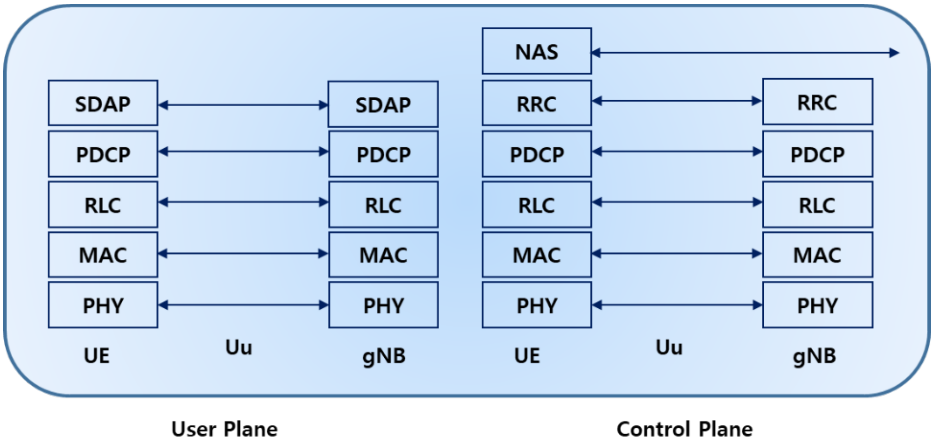


Figure 89 Protocol stack for 5G NR for User Plane (left) and Control Plane (right)

Cross-border aspects

- The user story is similar to the one in the ES-PT cross-border corridor (real time 4K video streaming and services for users), so it serves as a pre-test.
  - The user story is not convenient to test in the 5G-MOBIX cross-border corridors since it is planned to be tested using a prototype system operating at the local unlicensed band called FACS (Flexible Access Common Spectrum in South-Korea, 22~23.6GHz) allocated by the South-Korean government. For this reason, it will be tested at a local site.
- The present user story completes the set of user stories tested in cross-border corridors with:
  - a user story that targets broadband in-vehicle hotspot allowing onboard passengers to connect the Internet, which is a common situation in cross-border corridors and is not covered in the cross-border user stories.
  - A prototype system of mmWave-band 3GPP 5G NR V2I communications that introduce key enabling technologies capable of overcoming various technical challenges caused by using mmWave and supporting high mobility.

7.6. 5G QoS Performance Tool

An ad-hoc QoS tool (QoS OBU) will evaluate QoS performance provided by a 5G network where quality levels are based on network traffic monitoring by CCAM applications generating traffic. The proposed performance tool will generate CCAM traffic using 5G networks, according with the use case categories specified by 5G-MOBIX defined in D2.1. Using the hardware defined in D2.4, a set of KPIs defined in D2.5 will be measured. QoS OBU is flexible and versatile enough to evaluate other use case categories and/or trial sites and/or cross borders. For each user story, on-board KPIs will be collected and transmitted to a "5G QoS Performance Tool" (a centralized component of the platform). Besides these radio-probed KPIs, metrics will be enriched with KPIs obtained from the wired infrastructure side by using the API of the Nokia KPI Tool, responsible for providing core-network KPIs. Both information sources (5G radio modem and 5G core network) will be correlated based on KPIs timestamp information and following data fusion principles.

QoS OBU will be capable of generating CCAM traffic to deterministically replicate a user story or scenario multiple times via simulating a situation with the objective of obtaining 5G QoS results with a statistical significance.

To reduce the (predictable) impact on the 5G network performance (including 5G radio access), a 4G radio access network is used to transmit telematics data from the QoS OBU to the vehicles or as an alternative, indicators will be collected and transmitted only after the KPIs are collected.

To better clarify the infrastructure that will be used, Figure 90 shows a view with physical cross border road and vehicles, 5G networks and cloud infrastructure with the red boxes showing the 5G QoS tool elements. Moreover, other connections and dependencies are presented, such the Nokia KPI performance tool/API.

Figure 91 shows the same elements plotted on the reference architecture applied to the three user story scenarios on the ES-PT corridor.

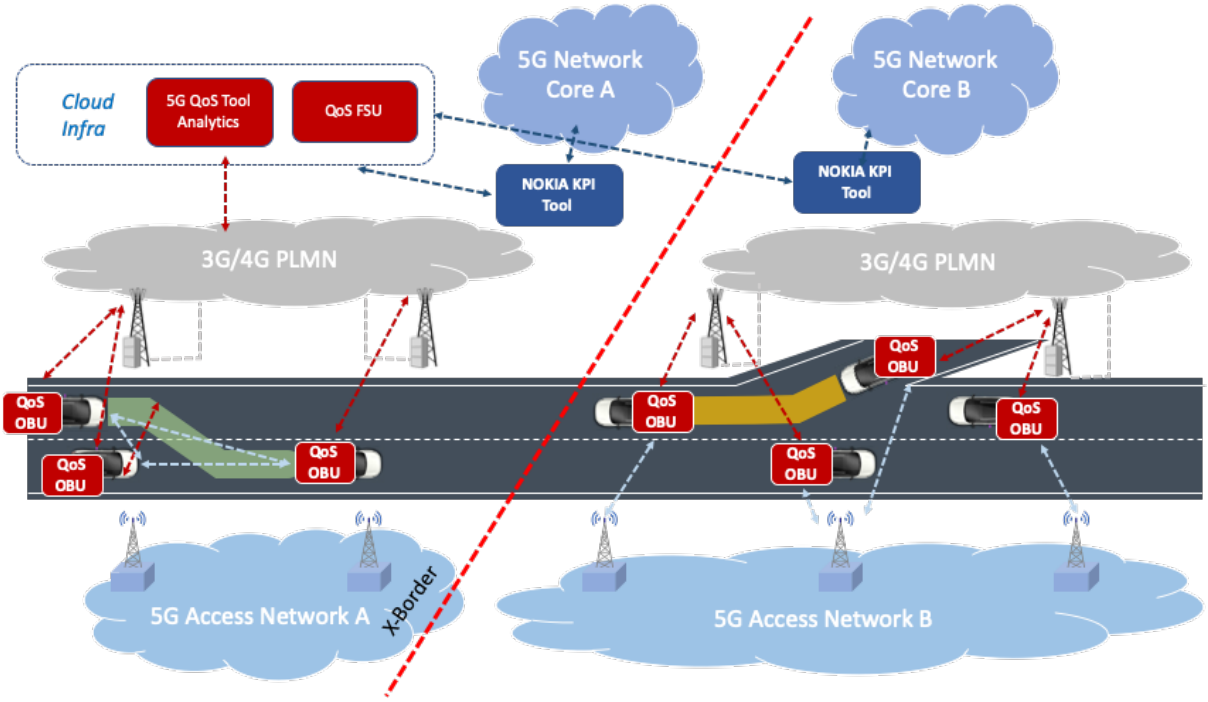


Figure 90 View on the use of 5G QoS Performance Tool in ES-PT Corridor

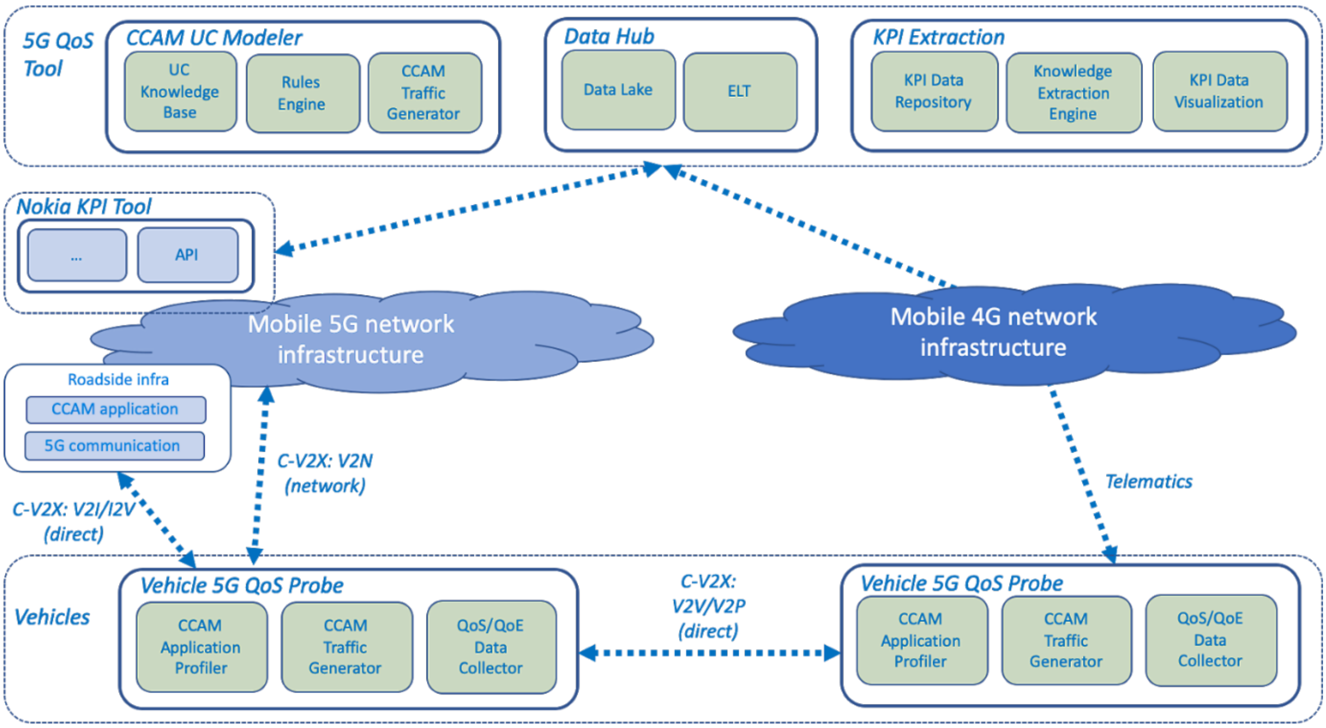


Figure 91 Architecture with central elements of 5G QoS tool and vehicle 5G QoS probes

Considering the infrastructure side, the 5G QoS tool will be supported by three main components:

1) CCAM User story (US) Modeler, responsible for modelling CCAM use case categories or user stories;

2) Data Hub, responsible for data management captured by the 5G QoS OBU;

3) KPI Extraction, responsible for knowledge extraction from the data previously obtained and for KPI generation to QoS/QoE assessment.

These components are described with details below.

1) CCAM US Modeler

The CCAM US modeler is responsible to model CCAM use case categories, and contains 3 components, the US Knowledge Base, a Rules Engine and the CCAM Traffic Generator.

The US Knowledge Base component is responsible for the CCAM US knowledge base maintenance and their use case categories. This knowledge base will contain US data, such as traffic models, traffic synthetic data, replay models (based on a spatial-temporal database) and US requirements.

The rules engines will contain a playbook of US scenarios that will provide a script for US replays.

The CCAM Traffic Generator is responsible for replicating CCAM US traffic mimicking real-world traffic models. The CCAM US modeler will use the definitions and requirements gathered from the Delivery D2.1., combined with field knowledge gathered during the trial sites tests.

2) Data Hub

The Data Hub will implement an Extract Load and Transform (ELT) pipeline that handles raw stream data stored in a Data Lake, generated by the 5G QoS OBU and the core-network (accessed using Nokia API/KPI tool).

The Data Lake receive QoS raw data coming from the 5G probes that are being transmitted by 4G networks to avoid any impact on 5G performance caused by QoS messaging overhead. The CCAM traffic from 5G interface is also stored to be processed by other modules. All the raw historical data will be stored, along with metadata and processed data needed for integrating several data sources.

In the ELT module, besides the ingestion of data produced by the several sources, it also responsible for performing basic transformations (e.g. normalization, fusion) on the data. Such transformations may be needed to accommodate the different grain that exists on data, and to prepare the calculation of KPIs in the next module.

3) KPI Extraction

Further processing will be supported by the KPI Extraction module. This module stores normalized data to support KPI generation and visualization.

The KPI data repository is a structured database that stores a clean and conform data for KPI calculation. Data stored will have, at least, a temporal and spatial dimension, necessary to compute spatial-temporal KPIs analysis. Further analysis will depend on the available KPI under consideration, defined in the deliverables D2.5 and updated in D5.1.

The KPI Knowledge Extraction Engine module can derive new KPIs based on the original ones. Thus, it is possible to retrieve new relevant relations between QoS parameters that are monitored and 5G performance indicators.

This module presents KPIs in a web based interactive dashboard. The users of the module can analyse and visualize relevant parameters, such as physical distance between vehicles and 5G radio base stations and related CCAM (radio) performance parameters.

On the vehicle side, the 5G QoS OBU will contain three main modules:

- The **CCAM Application Profiler** CCAM Application Profiler is responsible for CCAM data acquisition and for uploading the obtained data to the CCAM US Modeler for traffic modelling and playbook specification.
- The **CCAM Traffic Generator** replays previously obtained CCAM US traffic to simulate the CCAM US according to a previously observed data pattern.
- The **QoS/QoE Data Collector** collects performance indicators from the multiple and available layers to upload it to the KPI Extraction component at the 5G QoS Tool platform.