Grant Agreement Number: 768953

Project acronym:
ICT4CART

Project full title:
ICT Infrastructure for Connected and Automated Road Transport

D7.2: Adaptation of the reference architecture at the test sites

Due delivery date: 29 February 2020

Actual delivery date: 3 March 2020

Organization name of lead participant for this deliverable: ASFINAG

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential , only for members of the consortium (including the GSA)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 768953

Document Control Sheet

Deliverable number:	D7.2
Deliverable responsible:	ASFINAG
Work package:	WP7: Test Sites Integration and Data Collection
Editor:	Friedrich Vogl (ASFINAG)

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Anna Adaktylos	ASFINAG	anna.adaktylos@asfinag.at
Gottfried Allmer	ASFINAG	gottfried.allmer@asfinag.at
Danilo Amendola	CRF	danilo.amendola@crf.it
Ilaria De Biasi	BRE	ilaria.debiasi@autobrennero.it
Edoardo Bonetto	LINKS	edoardo.bonetto@linksfoundation.com
Daniele Brevi	LINKS	daniele.brevi@linksfoundation.com
Michael Buchholz	UULM	michael.buchholz@uni-ulm.de
Silvia Capato	SWARCO	silvia.capato@swarco.com
Guillemette Massot	AIRBUS	guillemette.massot@airbus.com
Alessandro Pedron	BRE	alessandro.pedron@autobrennero.it
Anastasia Petrou	BMW	Anastasia.Petrou@bmw.de
Steffen Schulz	NOKIA	Steffen.schulz@nokia.com
Jan Strohbeck	UULM	jan.strohbeck@uni-ulm.de
Friedrich Vogl	ASFINAG	friedrich.vogl@asfinag.at

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	2019-08-01	Template version	F. Vogl (ASFINAG)
V0.2	2019-11-29	German TS draft version	J. Strohbeck (UULM)
V0.3	2020-01-13	Italian TS draft version	D. Amendola (CRF)
V0.3	2020-01-15	Austrian TS draft version	F. Vogl (ASFINAG)
V0.4	2020-01-24	Merged draft version	F. Vogl (ASFINAG)
V0.5	2020-01-27	Revised version with inputs from BMW and UULM	F. Vogl (ASFINAG)
V0.6	2020-02-03	Revised version with inputs from CRF and discussions at the Plenary	F. Vogl (ASFINAG)
V0.7	2020-02-10	Revised draft version with inputs from NOKIA	F. Vogl (ASFINAG)
V0.8	2020-02-11	Revised version with inputs from AIRBUS, BMW, CRF, LINKS and SWM	F. Vogl (ASFINAG)
V0.9	2020-02-14	Version ready for peer review	F. Vogl (ASFINAG)
V1.0	2020-02-27	Final version with processed review comments from UULM and IBM-IE	F. Vogl (ASFINAG)

Abstract
The purpose of this document is to outline the actual architectures adapted from the reference architecture (see ICT4CART public deliverable D3.1). Based on the specifics and capabilities of the corresponding test sites the reference architecture has been tailored to the needs and requirements of the use cases and scenarios (i.e. use case embodiments) to be demonstrated.

Legal Disclaimer

The document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

Abbreviations and Acronyms

Acronym	Definition
AMQP	Advanced Message Queuing Protocol
AV	Automated vehicle
BI	Basic Interface
CABS	Cooperative awareness basic service
CAM	Common awareness message
CAV	Cooperative automated vehicle
C-ITS	Cooperative intelligent transport systems
CPM	Collective perception message
CPS	Collective perception service
DENBS	Decentralised environmental notification basic service
DENM	Decentralised environmental notification message
EC	European Commission
EPM	Environment perception model
ETSI	European Telecommunications Standards Institute
GA	Grant Agreement
GLOSA	Green light optimal speed advisory
GNSS	Global Navigation Satellite Systems
HAD	Highly automated driving
HD	High definition
ICT	Information and communication technology
IP	Internet Protocol
ISAD	Infrastructure support for automated driving
ITS-G5	p-WLAN, Wi-Fi standard for car communication
IVIM	Infrastructure to vehicle information message
LiDAR	Light detection and ranging
LTE/5G	Cellular communication
MAPEM	MAP extended message
MEC	Multi-access edge computing
MobiVoc	Open mobility vocabulary
NTRIP	Networked Transport of RTCM via Internet Protocol
OBU	On-board unit
OEM	Original equipment manufacturer
PKI	Public key infrastructure
PO	Project officer
POI	Points of interest
QoS	Quality of Service
RAN	Radio access network
RLT	Road and lane topology
RSU	Road side unit
RTCM	Radio Technical Commission for Maritime Services
RTK	Real time kinematic
RTSP	Real time streaming protocol
SAE	Society of Automotive Engineers
SCN	Scenario
SP	Service provider
SPATEM	Signal phase and timing extended message

Acronym	Definition
TCC	Traffic control centre
TLA	Traffic Light Assistance
TTG	Time-to-green
V2I	Vehicle to infrastructure
V2V	Vehicle to vehicle
V-ITS-S	Vehicle ITS Station
VRU	Vulnerable Road User
WP	Work Package

Table of Contents

List of Figures

Executive Summary

The aim of the ICT4CART project is to design, implement and test a versatile ICT infrastructure in real-life conditions, which will enable the transition towards higher levels of automation. It focuses on four high-value use cases: Smart Parking & IoT services, dynamic adaptation of vehicle automation level based on infrastructure information, intersection crossing (urban) & lane merging (highway), and Cross-border Interoperability. ICT4CART use cases have been carefully selected based on specific criteria, which are: i) alignment with EU policies and relevant forums and initiatives, ii) significant impact on connected automation, iii) the ability to generalise on the results (applicable in other scenarios and environments), and iv) interest to the consortium members and relevance to their industrial roadmaps. Moreover, these use cases are serving one of the main targets of the project, which is to show that the proposed and implemented ICT infrastructure architecture is flexible, adaptable and can serve the needs of various automated driving use cases (safety critical, comfort, etc.) with different requirements, across test sites with different capabilities. The ICT4CART use cases are either global or local, are either associated with network slices or not, are either using Edge Clouds/Computing or not, are using different radio technologies and can be used everywhere (roaming aspect). They also consider mechanisms for cyber-security, authentication, integrity and privacy. For this purpose, four test sites are involved in ICT4CART, namely in Austria, in Germany, in Italy and, finally, a cross-border site at the border between Austria and Italy.

The main objective of WP7 is to integrate and test the solutions developed within ICT4CART in real-life conditions at the project test sites. This will be performed through the ICT4CART use cases and the corresponding traffic situations called “scenarios”, which have been defined in WP2. WP7 covers the integration of the modules that will be delivered by WP4, WP5 and WP6, and the data collection from all the test sites to be delivered to WP8 for the evaluation and impact assessment. The findings of WP2 include the specification of use cases, the analysis of market’s needs and system requirements. The ICT4CART Reference Architecture and key aspects of Flexible Networks, IT Environment and Cyber-Security & Data Privacy are part of WP3. Based on these findings, this document (D7.2) outlines the concrete ICT architectures to be implemented at the different test sites. These architectures are adaptations of the high-level reference architecture (see D3.1 [1]). The aim is to cover the different ICT4CART use cases (see D2.1 [2]) which will be demonstrated in the corresponding test site while staying interoperable with the other test sites.

First, the Introduction in Section 1 describes the aims of ICT4CART, i.e. the design and deployment of the ICT4CART technologies on the test sites covering all use cases. Section 2 summarises the ICT4CART Reference Architecture as developed in WP3 (see D3.1 [1]). After a brief description of the Architecture Adaptation Approach followed in Section 3, the following Sections 4 to 7 describe the ICT architectures that will be implemented in the test sites in Austria, Germany, Italy and the Cross-border test site. Finally, in Section 8, the interoperability of the demonstrated use cases and scenarios between the test sites is described on selected examples.

1 Introduction

1.1 Aim of the Project

Connected and automated vehicles, especially with SAE levels L3 & L4, are a focal point of ITS research. To enable and accelerate the deployment in our everyday life, ICT is a prerequisite. This is exactly the area ICT4CART is working on.

ICT4CART aims to address the gaps to deployment bringing together key players from automotive, telecom and IT industries, to shape the ICT landscape for Connected and Automated Road Transport, and to boost the EU competitiveness and innovation in this area.

The main goal of ICT4CART is to design, implement and test in real-life conditions a versatile ICT infrastructure that will enable the transition towards higher levels of automation (up to L4) addressing existing gaps and working with specific key ICT elements, namely hybrid connectivity, data management, cyber-security, data privacy and accurate localisation. ICT4CART builds on high-value use cases (urban and highway), which will be demonstrated and validated in real-life conditions at the test sites in Austria, Germany and Italy. Significant effort will be put also on cross-border interoperability, setting up a separate test site at the Italian-Austrian border.

1.2 Purpose of the document

The purpose of this document is to outline the concrete ICT architectures to be implemented at the different test sites. These architectures are adaptations of the high-level reference architecture (see D3.1 [1]). The aim is to cover the different ICT4CART use cases (see D2.1 [2]) which will be demonstrated in the corresponding test site while staying interoperable with the other test sites.

The deliverables *"D3.2 Flexible Networks Specification and Architecture"* [3], *"D3.3 IT Environment Specifications and Architecture"* [4] and *"D3.4 Cyber-Security and data privacy Specifications and Architecture"* [5] are major inputs to this document.

1.3 Targeted audience

This deliverable is addressed to any interested reader (i.e., PU dissemination level) who wishes to be informed about the adaptation of the reference architecture (as defined in D3.1 [1]) to the test sites and the use cases and scenarios defined in D2.1 [2].

2 ICT4CART Reference Architecture

The main goal of the ICT4CART project, as per the description of work, is to develop an innovative and generic ICT architecture that will enable the transition towards higher levels of automation (L3 to L4). Although the target architecture will be deployed in limited pilot sites, it is aimed to provide a reference architecture for pan-European deployment.

The ICT4CART ICT architecture is aimed to operate seamlessly with different communication technologies, i.e., ad-hoc networks (ETSI ITS-G5) and cellular networks (LTE/5G), referred to as hybrid communication. Low-latency services will be supported through multi-access edge computing (MEC) in cellular networks or similar functionality in ad-hoc networks. The ICT architecture will enable high-value use cases for automated driving, such as smart parking, intersection crossing in urban environments, lane merging in highway scenarios, and cross-border interoperability. A high-level view of the ICT architecture is provided in deliverable D3.1 [1].

The ICT architecture covers the following three aspects (sub-architectures), which are detailed in own documents:

- Telecommunication, which is the subject of deliverable D3.2 [3],
- IT environment, which is the subject of deliverable D3.3 [4]
- Privacy and cyber-security, which is the subject of deliverable D3.4 [5].

This chapter aims to provide a summary of the overall ICT4CART ICT architecture. The purpose is to provide context information for the IT environment specified in this document. For further details about the ICT architecture, please refer to deliverable D3.1 [1].

2.1 High-level architecture

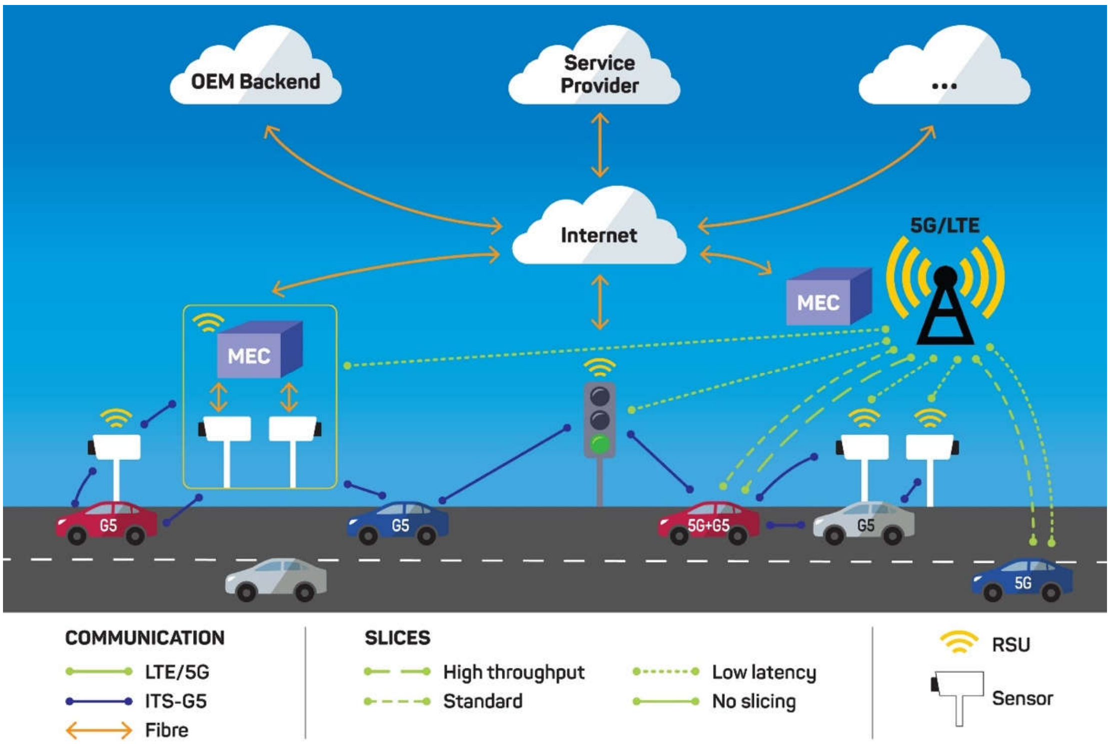

Figure 1 - ICT4CART High-Level Overview from D3.1 [1]

Figure 1 illustrates the ICT4CART overall ICT architecture. It shows the basic components involved in the ICT4CART system and their interactions. The main components are the vehicles, infrastructure (traffic sensors and processing units) and IT services (such as an OEM backend or other service providers). The basic communication technologies that are used are LTE/5G (cellular) and ITS-G5 (ad-hoc). When using 5G, slicing may be used to provide the quality of service (QoS) required for the kind of information to be transported, which is represented by the dashed lines in the figure. There can be slices, e.g., for low-latency communication (short dashes in the figure) or high-throughput communication (lines with longer dashes in the figure). As slicing is a 5G feature, it is not available when using LTE or ITS-G5. For further details on the communication, see Section 2.3.

Hybrid connectivity, i.e., using ITS-G5 and LTE/5G in parallel, is also depicted in the figure, as the infrastructure may provide information via both communication channels. Vehicles may retrieve/receive information using both communication pathways, either from the same source or from different sources. The vehicles in Figure 1 are either not connected, connected with ITS-G5 (G5), with LTE/5G (5G), or with both (5G+G5). A vehicle-to-vehicle (V2V) connection is possible via ITS-G5.

The road is equipped with roadside units (RSUs), connected sensors, and connected traffic signs (e.g., traffic lights). LTE/5G base stations receive and transmit data via the cellular network (green lines). ITS-G5 RSUs receive and transmit data via ITS-G5 (blue lines). Sensors and traffic lights are connected either via fibre cables (orange lines), cellular network, or via ITS-G5.

Figure 1 also shows the concept of MEC servers. MEC servers are located at the edge level of the network close to a base station of a cellular network, providing computation closer to end devices (in the ICT4CART use cases: vehicles), thereby avoiding time-consuming transmission of data via the Internet. This concept decreases latency, especially for mission-critical data, when compared to using a cloud server anywhere in the network.

Similar functionality to MEC servers can be provided by the processing capabilities of road infrastructure (e.g., sensors) in combination with RSUs. This is shown in the left part of the figure. For the sake of simplicity, these processing units are also denoted as MEC here. An RSU is an ITS-G5 communication unit on the infrastructure side. Such MEC servers in combination with RSUs can run ICT4CART applications or services in close proximity to the vehicle with low delays (relatively to cloud services). Information from the OEM Backend, service providers, and other cloud services ("…" cloud in Figure 1) can be received through the Internet.

2.2 Functional view

The ICT4CART architecture consists of a collection of functional blocks. The functional view, provided in Figure 2, organises the functional blocks into groups according to their common purpose: supporting services, sensors and actuators, applications, core services, hybrid wireless network, cooperative automated vehicle (CAV), and security & privacy. The individual functional components are described in detail in Section 3 of Deliverable 3.1 [1]. Data flows are not depicted in this diagram but will be shown in the next section.

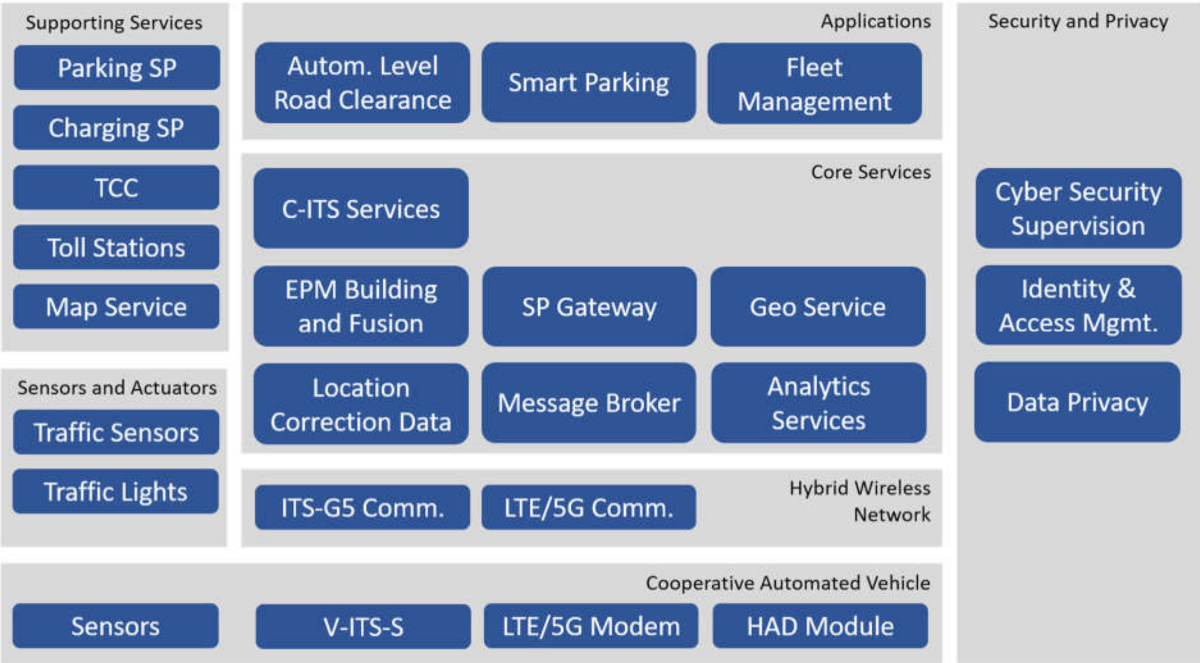

Figure 2 - ICT4CART Functional Architecture

2.3 Data/IT-Environment View

A high-level component viewpoint of the ICT4CART IT environment architecture is shown in Figure 3. As can be seen, the IT environment on infrastructure side is distributed over two types of platforms: cloud and MEC. Services requiring low latency (≤ 50 milliseconds) or with limited geospatial extent should be deployed on MEC servers, others should be deployed on the cloud. Vehicles should communicate with MEC services directly since MEC services and applications require low latency. However, they may communicate with cloud services using off-board access, which centralises access to these services depending on context. Please note that the vehicle is not considered as part of the IT environment. Rather, it is considered as a client. More details on the data flows and data types can be found in the deliverables D3.3 [4] and D3.1 [1].

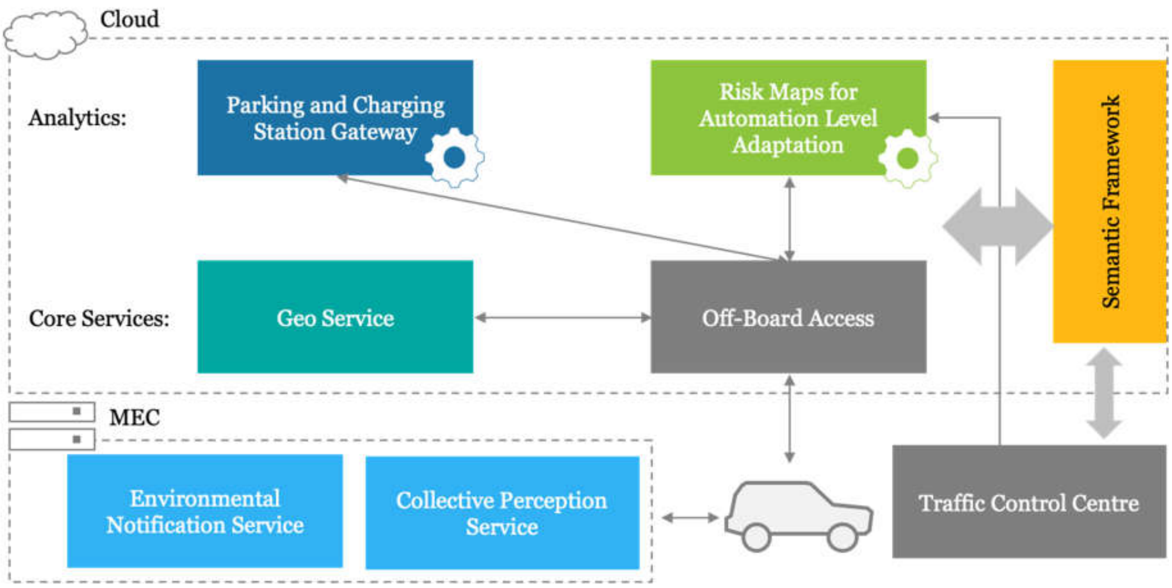

Figure 3 - ICT4CART Functional Architecture

2.4 Communication view

Deliverable 3.1 [1] also presents a communication view of the architecture. In essence, communication partners are viewed as ITS stations, and communication is performed using ITS messages via any transmission channel (hybrid communication), while only ITS-G5 and LTE/5G are used in this project. Further details on the hybrid communication can be found in Section 5 of deliverable 3.1 [1] and in deliverable 3.2 [3].

2.5 Cyber-Security & Privacy View

In deliverable D3.1 [1], multiple technologies for cyber-security and data privacy have been presented, such as the cyber security supervision service, the identity and access management service, and the data privacy mechanism based on group signatures with selective linkability. In this document, the integration of cyber-security and data privacy into the IT environment is not covered; for details on this please refer to Section 6 of deliverable D3.1 [1] and the deliverable D3.4 [5].

3 Architecture Adaptation Approach

The ICT4CART reference architecture recapitulated in Section 2 is adapted for each test site. Each test site architecture will take into account the specifics and capabilities of the corresponding test site and it will be tailored to the needs and requirements of the respective use cases and scenarios to be demonstrated. The common reference architecture of WP3 will guarantee the interoperability of the developed traffic and communication system innovations for all ICT4CART test sites. In most cases, some modules of the reference architecture will not be necessary and will therefore not be set into function, which is depicted by a greyed-out box in the respective architecture diagram. In addition, a detailed functional view diagram including the interactions between the functions is provided for each scenario.

4 Austrian Test Site Architecture

This chapter outlines the architecture of the Austrian test site and is split into subsections for the two scenarios that will be demonstrated there. A detailed description of the use cases and scenarios (i.e. use case embodiments) can be found in the deliverable D2.1 [2].

For each scenario, the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view are presented based on the detailed descriptions in D3.1 to D3.4 [1,3-5].

4.1 Scenario 2.1: Dynamic clearance, adaptation and handover of vehicle automation level at special conditions in Graz, Austria

In the following, the adaptions of the general architecture views on the Scenario 2.1 *"Dynamic clearance, adaptation and handover of vehicle automation level at special conditions in Graz, Austria"* are given for the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view.

4.1.1 Functional View

Figure 4 shows the function blocks used for this scenario in the Austrian test site. Unused modules are greyed out.

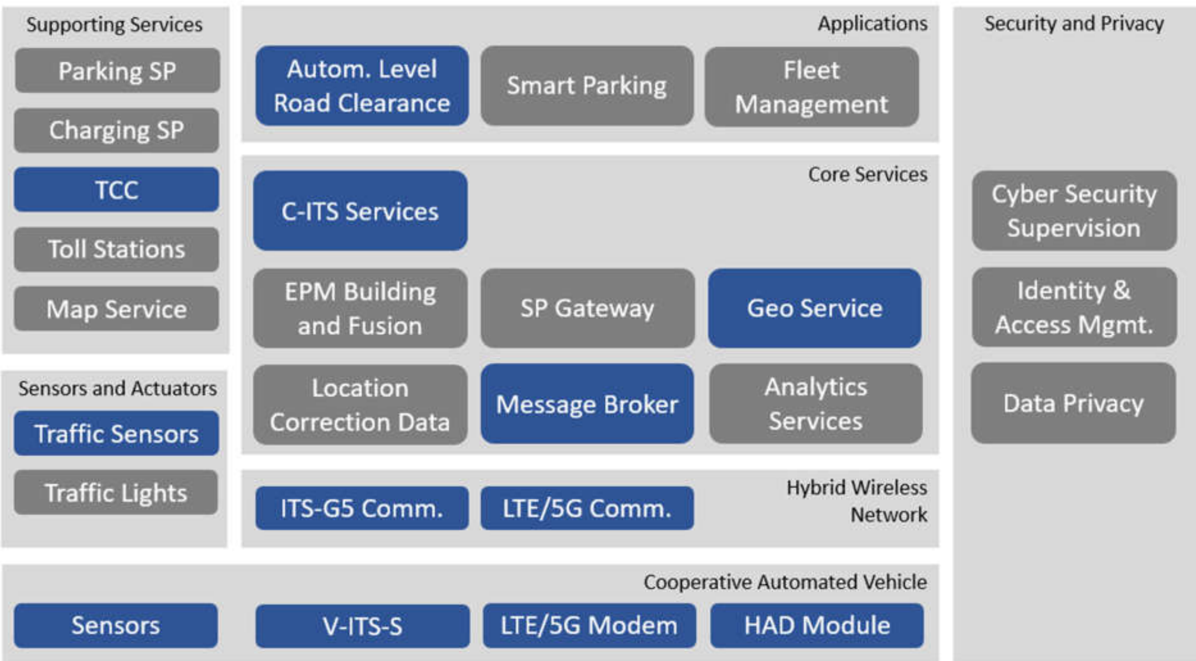

Figure 4 - Functional view - SCN 2.1 - Overview

From the **Supporting Services** group, only the Traffic Control Centre (**TCC**) is used which will provide information to the **C-ITS Services** and the **Automation Level Road Clearance** application.

From the **Sensors and Actuators** group, **Traffic Sensors** will provide the TCC with information.

From the **Applications** group, the **Automation Level Road Clearance** application utilises static and dynamic information to determine and prescribe a clearance for a road section and a specific automation level. A human operator can override the actual clearance, if required, before it is distributed. ASFINAG has recently analysed its entire road network with reference to the ISAD classification scheme [20] which determines how strongly a given road section can offer support for automated driving.

From the **Core Services** group, the following functions are in use for the Austrian test site:

- **C-ITS Services** generate IVI messages with their automated vehicle container to transmit the SAE level clearance and DEN messages to transmit information about accidents or wrong way drivers. More information about the C-ITS messages used can be found in the Table at the end of Section 4.1.2.
- The **Geo Service** will be used by the CAV to get information about the appropriate Message Broker for its current position respectively for its planned route.
- The **Message Broker** will be used to provide CAVs with messages of interest based on geographical location. There will be one Message Broker for Austria, deployed on a MEC infrastructure. The CAVs will subscribe to map tiles based on their location and/or planned route to receive relevant C-ITS messages.

The **Hybrid Wireless Network** will consist of **ITS-G5** roadside units located on the ASFINAG road infrastructure, and of **LTE/5G** communication technology provided by Magenta.

The **Cooperative Automated Vehicle (CAV)** will use an on-board unit (OBU) with both LTE/5G and ITS-G5 connectivity to establish continuous communication channel with the infrastructure. With that, it will receive SAE level clearance messages, get GNSS correction data for its current position, and subscribe to map tiles based on its location and/or planned route. Based on the received information, the CAV shall inform the driver about the availability of SAE level 2/3 functions and/or warn to take over the steering wheel due to changes in the traffic/weather/other conditions earlier than without the infrastructure's messages. This will improve the driving experience and comfort. The CAV may be equipped with other measurement techniques and safety equipment to collect relevant data and grant road safety. However, this equipment and these techniques are not related or connected to the ICT4CART infrastructure and, thus, omitted in this description.

In Figure 5 the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

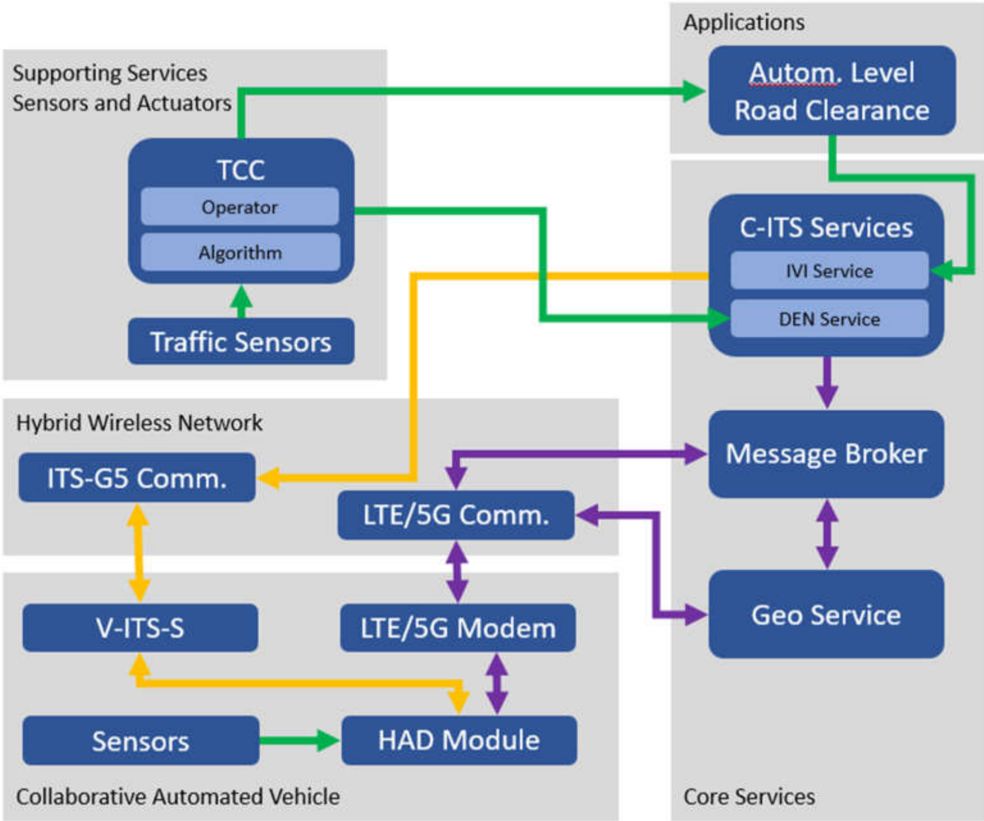

Figure 5 - Functional View - SCN 2.1 - Details

4.1.2 Data / IT Environment View

In this scenario, the following data flows of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 6):

1. Sensors submit data to the TCC about the current traffic situation, e.g., positions, speeds and directions of road users detected by sensors.
2. Information about special traffic situations (e.g. accidents or traffic jams) and general automation level recommendations is provided to a Central ITS Station for the dissemination by Roadside ITS Stations using ITS-G5, and to a Message Broker for subscribers using LTE/5G.
3. C-ITS messages are distributed to RSUs using a selection algorithm that considers both the positions of the RSUs and the relevance areas of the messages to be disseminated. The Message Broker can be seen as an RSU covering the whole dissemination area of the C-ITS system.
4. Vehicles equipped with ITS-G5 communication modules receive IVI and DEN messages directly from RSUs along the roadside.
5. Vehicles equipped with LTE/5G communication modules and AMQP clients can subscribe for the same messages on the Message Broker deployed on the MEC server. Filtering is possible by message type and geographic location.
6. Vehicles equipped with ITS-G5 send own messages like CAM or DENM that can be received by other vehicles and RSUs.

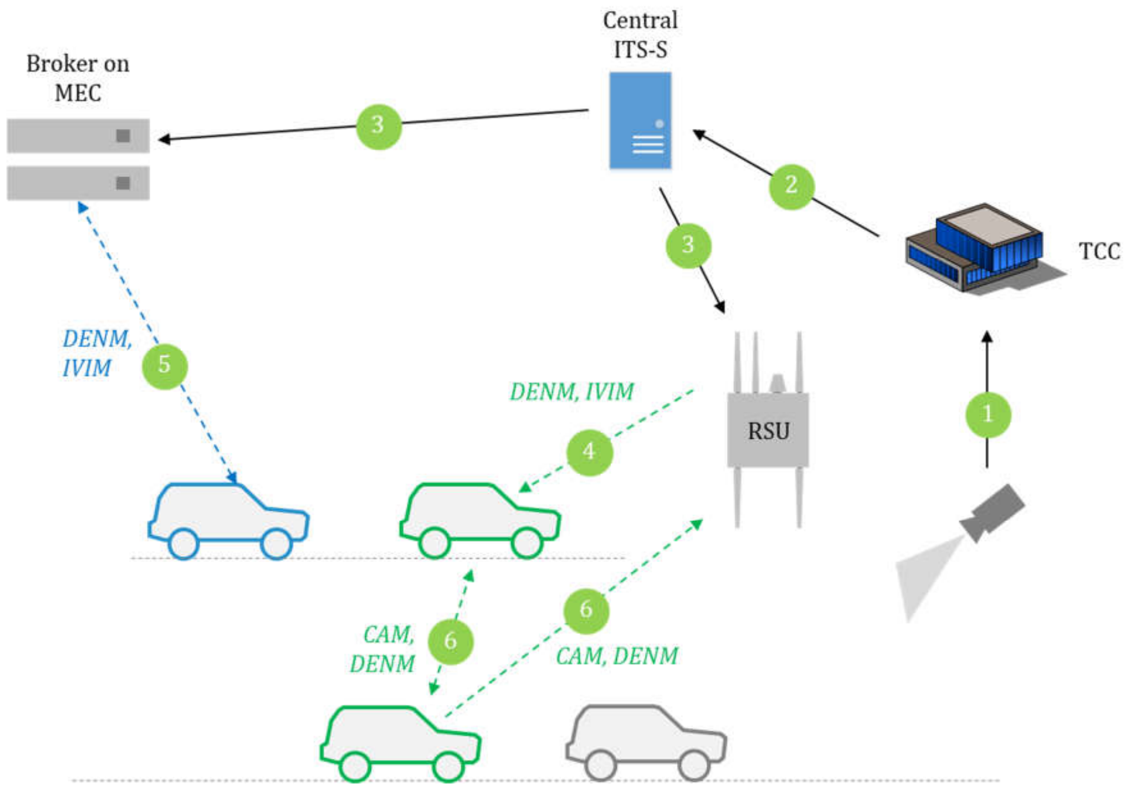

Figure 6 - Data / IT Environment View of the Austrian Test Site

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Situations and events (e.g., accident, road closure, etc.)	DENM as specified by ETSI EN 302 637-3 V1.3.1 [15]
	In-vehicle information (e.g., speed limits, SAE level recommendation)	IVIM as will be specified by ISO/TS 19321:2020 [12]
	Correction data for GNSS-based localisation	ETSI TS 103 301 [7]
Consumed by the IT Environment	Data received from vehicles either directly or indirectly through RSUs	CAM as specified by ETSI EN 302 637-2 V1.4.1 [11]

4.1.3 Communication View

In the Austrian test site, hybrid communication is used extensively. The infrastructure provides information (encoded in C-ITS messages) to the vehicles via two communication channels: ITS-G5 (ad-hoc network) and LTE/5G (cellular network). Figure 7 shows the possible communication paths.

For the cellular communication link to the vehicles, the information will be published onto an AMQP message broker deployed on a MEC server. Vehicles will be able to subscribe for specific messages in relevant geographic areas.

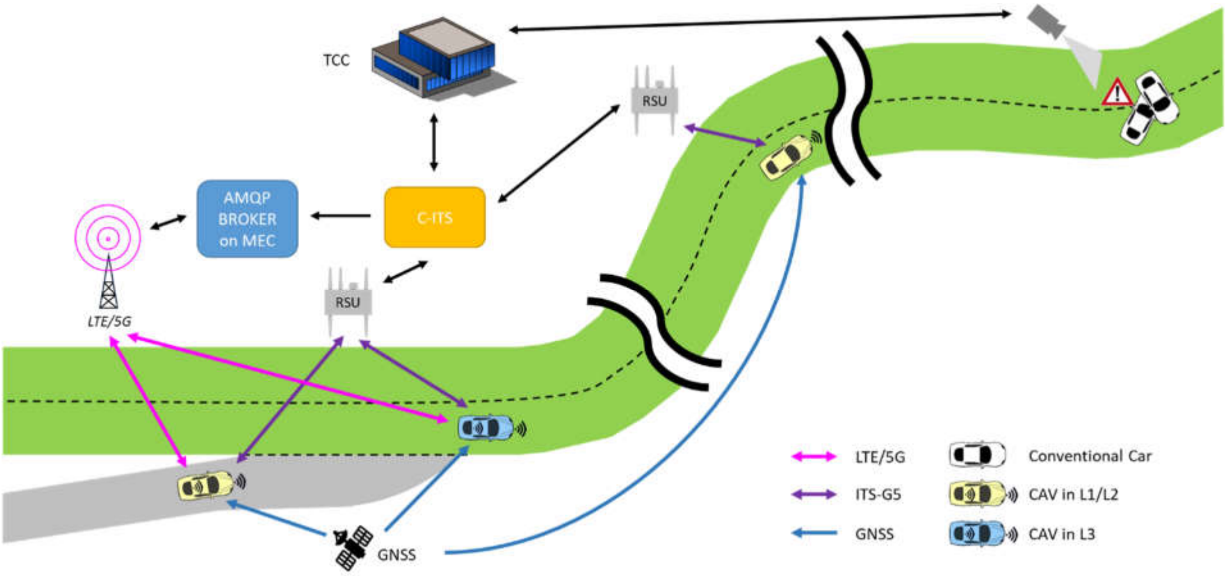

Figure 7 - Communication View of the Austrian Test Site

4.1.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

4.2 Scenario 3.4: Precise positioning in urban and highway location

This scenario demonstrates the dissemination of GNSS correction data via LTE/5G for high precision positioning of the vehicle in different areas (urban, highway). The use of the corrected position for automated driving functions is a prerequisite for other scenarios, like SCN3.1a in Ulm or SCN3.1b in Verona.

4.2.1 Functional View

Figure 8 shows the functional blocks used for this scenario in the Austrian test site. Unused modules are greyed out.

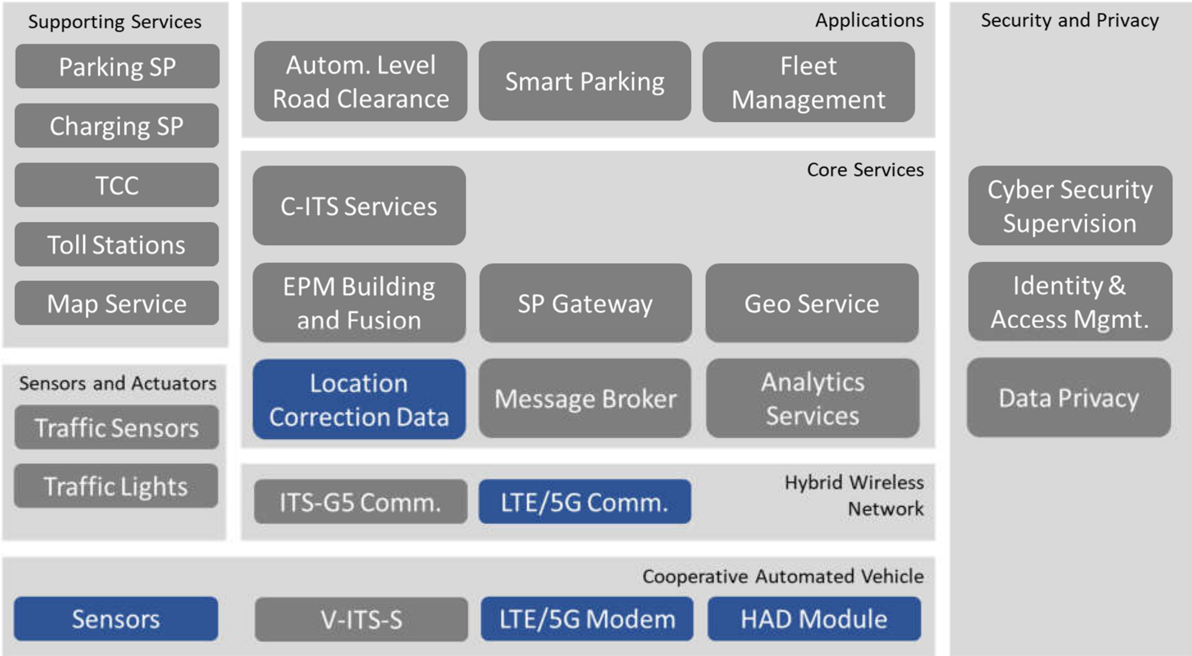

Figure 8 - Functional view - SCN3.4 Austrian test site - Overview

Location Correction Data:
This function is provided by the precise localisation service based on Real-Time-Kinematic (RTK) technique, which enhances the precision of the GNSS by using carrier phase measurements and correction data of RTK reference stations.

LTE/5G Communication:
The LTE/5G communication is used to transmit the location correction data.

LTE/5G Modem:
The LTE/5G modem in the vehicle receives the location correction data from the MEC server.

HAD Module:
The HAD Module uses the correction data to improve the received GNSS position.

Sensors:
The GNSS receiver provides the position data in the vehicle.

In Figure 9, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

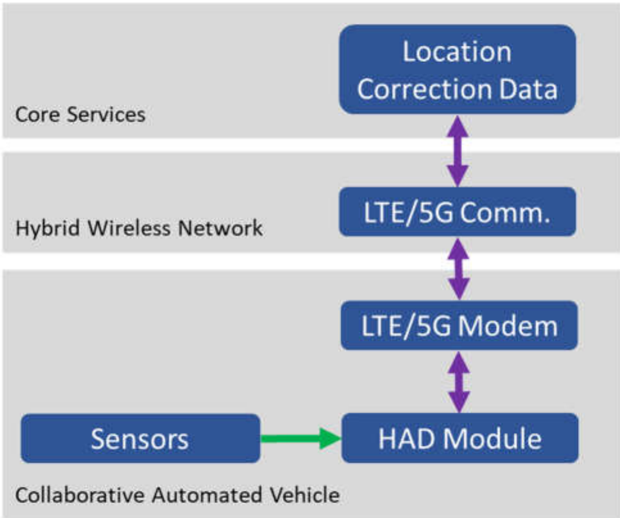

Figure 9 - Functional View - SCN3.4 Austrian test site - Details

4.2.2 Data / IT Environment View

The MEC server uses correction data from an external service provider (e.g., Satellite Positioning Service - SAPOS) and behaves as a proxy server between the client and the external service provider. The advantage of this approach is that the MEC server can provide a unique localisation service to the clients, independently of the individual external service provider in the different countries. Furthermore, the MEC server can use one set of correction data for a cluster of clients, e.g., all clients located in one LTE/5G radio cell (see Figure 10).

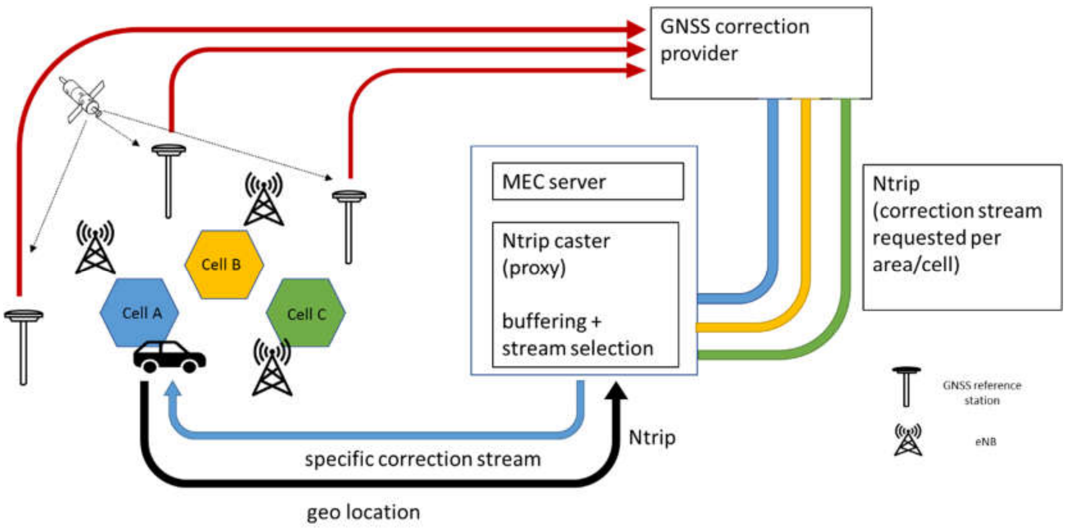

Figure 10 - Austrian Test Site Approach for Precise Localisation

The following table lists the relevant standards for the data that will be transmitted in this scenario:

	Data Type	Relevant Standards
Provided by the IT Environment	Correction data stream for RTK based localisation service	RTCM Standard 10403: "Differential GNSS (Global Navigation Satellite Systems) Services" [16]
Consumed by the IT Environment	Correction data stream from the GNSS reference stations	RTCM Standard 10403: "Differential GNSS (Global Navigation Satellite Systems) Services" [16]

4.2.3 Communication View

In this scenario, the transport mechanism of data over IP is used from the communication networks. The GNSS correction data are sent by the NTRIP protocol from the MEC server via LTE/5G to the modem installed in the vehicle.

4.2.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

5 German Test Site Architecture

This chapter outlines the architecture of the German test site. The description is structured by the three scenarios planned for the German test site. The following subsections illustrate the implementation of the architecture for the respective scenarios *"SCN 1.1 Smart Parking and IoT Services in City of Ulm, Germany"*, *"SCN 3.1a Virtual Mirror to 'see' surrounding traffic in urban environments in City of Ulm, Germany"*, and *"SCN 3.4 Precise Positioning in urban and highway location"* (see D2.1 [2] for a detailed description of the use cases and scenarios). For each scenario, the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view are presented based on the detailed descriptions in D3.1 to D3.4 [1,3-5].

5.1 Scenario 1.1: Smart Parking and IoT Services in City of Ulm, Germany

In the following, the adaptions of the general architecture views on the Scenario 1.1 *"Smart Parking and IoT Services in City of Ulm, Germany"* are given for the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view.

5.1.1 Functional View

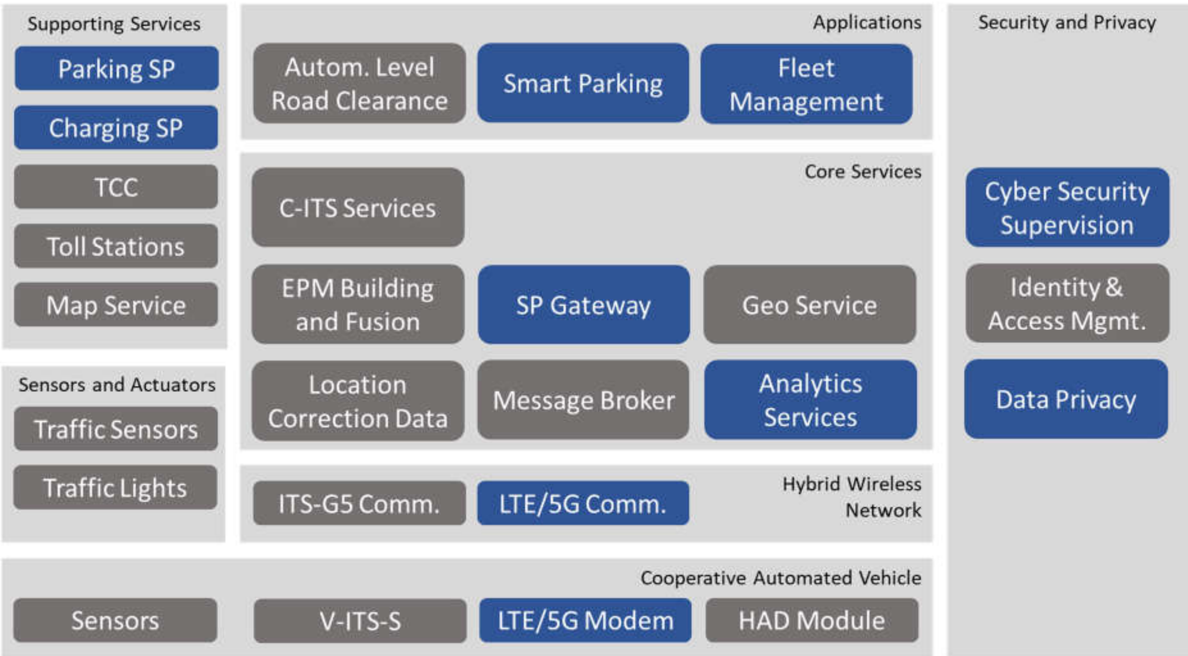

Figure 11 - Functional View - SNC1.1 - Overview

In Figure 11, the functional blocks relevant to this scenario are highlighted in blue. They have the following meanings:

Parking SP: Information about parking spots and parking garages are available in real time through an API provided by the City of Ulm.

Charging SP: Information about charging stations will be available in real time through an API provided by the City of Ulm.

SP Gateway: Parking and charging data from different providers go through the gateway and are prepared for processing.

Analytics service: This service analyses the data and produces predictions for the availability of parking and/or charging facilities.

Smart Parking: A smart parking application runs in the BMW cloud. Input data for the application are parking spot and garages availability as well as parking predictions. The application communicates with the vehicle to send driving instructions and a route to a parking facility. For demonstration purposes, parking data and predictions are shown via a web interface.

Fleet Management: A fleet management application runs in the BMW cloud. The application matches existing vehicles with incoming ride-hailing requests and communicates with the vehicle to send instructions and routes to various locations. For demonstration purposes, an emulator simulates vehicle movements and request for ride-hailing. Results are shown via a web interface.

LTE/5G communication: Communication between the vehicle and the BMW Cloud is established via LTE/5G to receive and send various information, like vehicle position and instructions. This component refers to the communication infrastructure.

LTE/5G Modem: Communication between the vehicle and the BMW Cloud is established via the LTE/5G modem in the vehicle to receive and send various information, like vehicle position and instructions. This component is a hardware component and is located in the vehicle.

Cyber security Supervision: The **Fleet Management** application sends information about vehicles and requests to a supervision centre, where threats or abnormal data are detected.

Data Privacy: This service will be demonstrated only on simulated data using a Fleet Simulator (not the Fleet Management Application in the BMW cloud). The **Cyber Security Supervision** service will receive pseudonymised data from the Fleet Simulator and send them to the Data Privacy service in order to link a set of anonymously authenticated signatures, determining which signatures originate from the same source.

In Figure 12, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

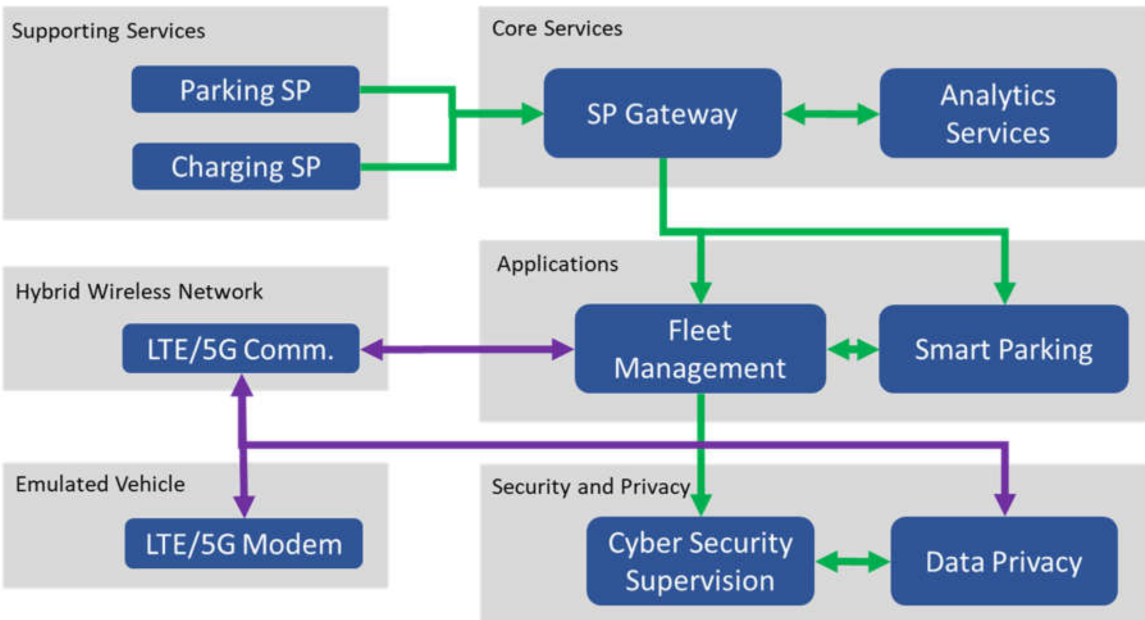

Figure 12 - Functional View - SCN1.1 - Details

5.1.2 Data / IT Environment View

Figure 13 shows the main data exchanged and IT components used within this scenario.

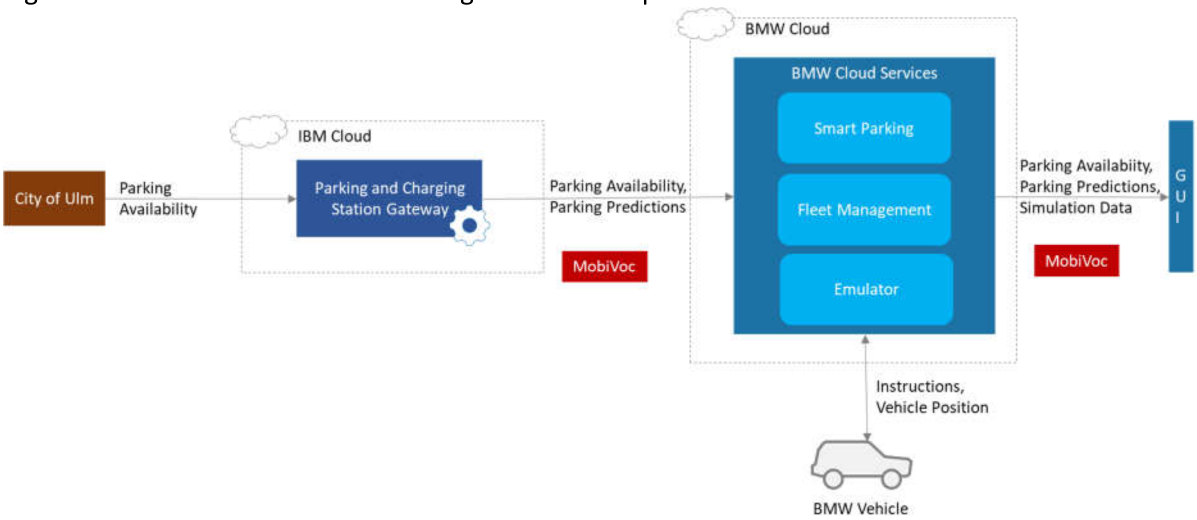

Figure 13 - Data/IT Environment View – German test site – SNC1.1

The Service Provider Gateway (Parking and Charging Station Gateway) retrieves parking data provided by the City of Ulm periodically. The SP Gateway transforms all retrieved data, if necessary, to the Open Mobility Vocabulary (MobiVoc) format and provides the harmonised data to BMW Cloud Services. In addition to the harmonisation of data, predictions for future parking space availability are derived and made available through an API. Predictions will be used by the fleet management component to intelligently and proactively relocate participating fleet vehicles.

5.1.3 Communication View

Figure 14 describes the communication paths between the various components in the “Smart Parking and IoT Services” use case.

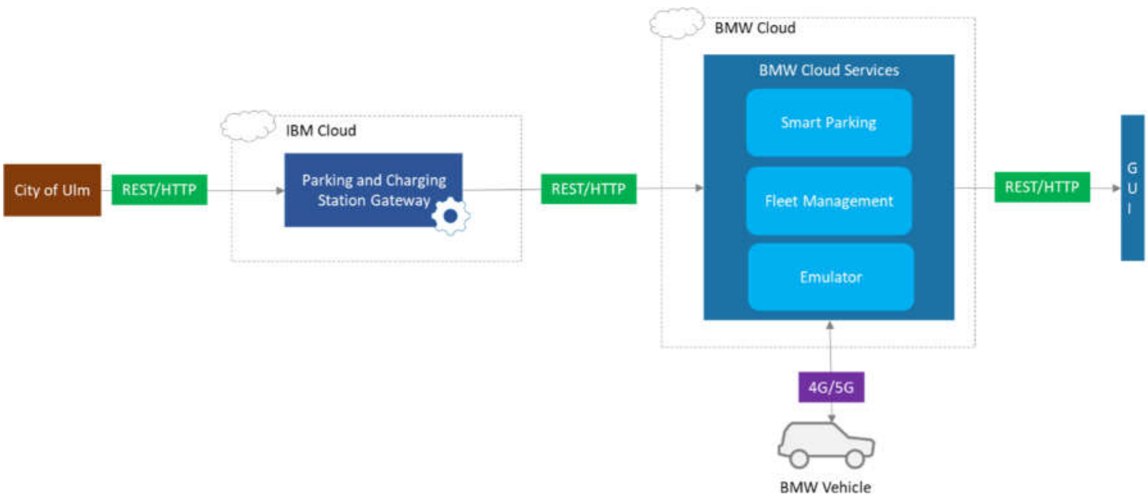

Figure 14 - Communication View – German test site – SNC1.1

The “Parking and Charging Station Gateway” component gathers all data via a REST interface provided by the data provider, in this case by City of Ulm. The same component offers, also via a REST interface, processed parking data and parking predictions for consumption. The BMW cloud components use the data to schedule their fleet and pass them on to a web interface used for demonstration purposes. Instructions and other information are sent to the vehicle using a 4G/5G communication channel.

5.1.4 Cyber-Security & Privacy View

Figure 15Figure 14 shows the cyber-security and privacy view of the adapted architecture for the "Smart Parking and IoT Services" use case.

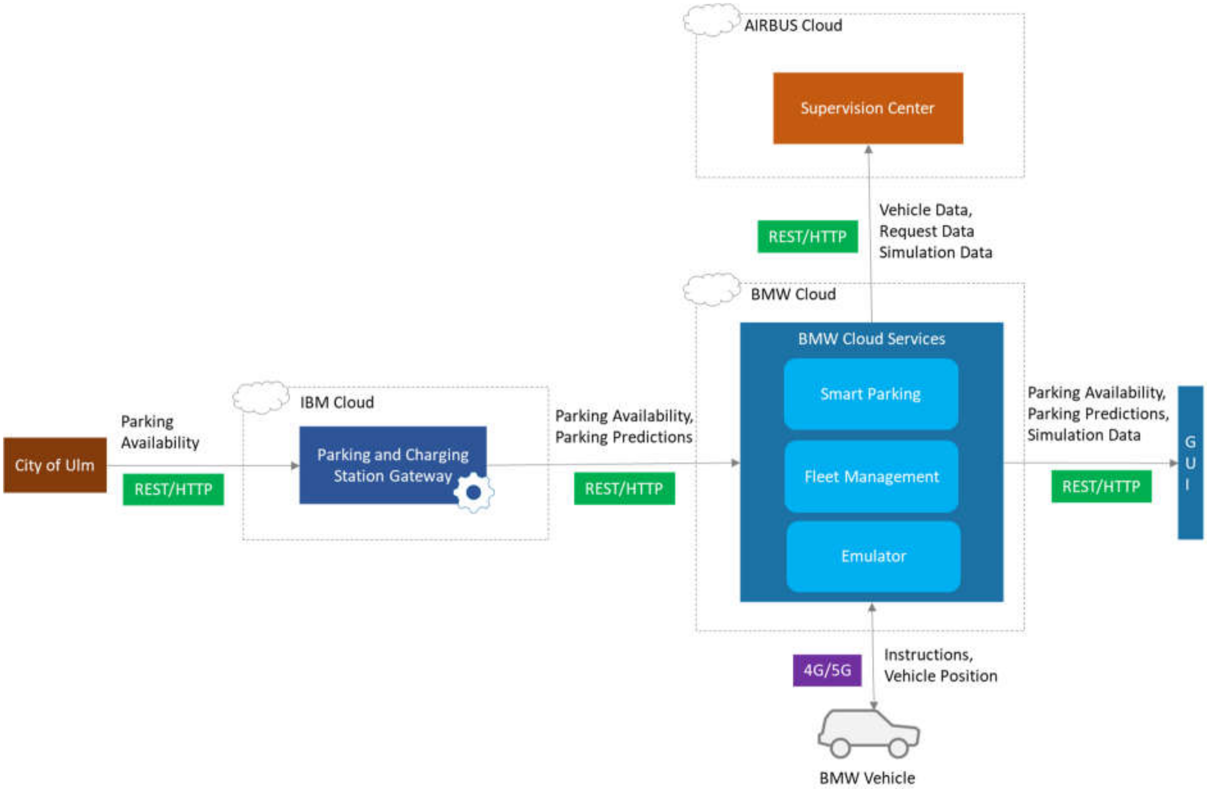

Figure 15 - Cyber-Security & Privacy View – German test site – SNC1.1

In the "Smart Parking and IoT Services" use case, there will be a connection of the BMW Emulator application with the Supervision Centre. The Emulator will send vehicle and request information during simulations to the Supervision Centre. The Supervision Centre will then use this information to detect abnormal states and possible threats.

However, as it is not possible to use the Data Privacy service with the BMW Emulator, it has been decided to use a Fleet Simulator provided by Airbus to demonstrate the capabilities of Data Privacy service. Simulated ITS Stations will get linkability credentials by sending requests to the Linkability Manager, which is the main component of the Data Privacy service. The supervision service will receive anonymously authenticated data and will be able, thanks to the Data Privacy service, to link and correlate those, determining which signatures originate from the same source. A next step will be to integrate the Data Privacy service with the Identity and Access Management. So, the Data Privacy service will rely on the Identity and Access Management service to check the authentication of an ITS station before providing it linkability credentials.

5.2 Scenario 3.1a: Virtual Mirror to "see" surrounding traffic in urban environments in City of Ulm, Germany

In the following, the adaptions of the general architecture views on the Scenario 3.1a *"Virtual Mirror to 'see' surrounding traffic in urban environments in City of Ulm, Germany"* are given for the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view.

5.2.1 Functional View

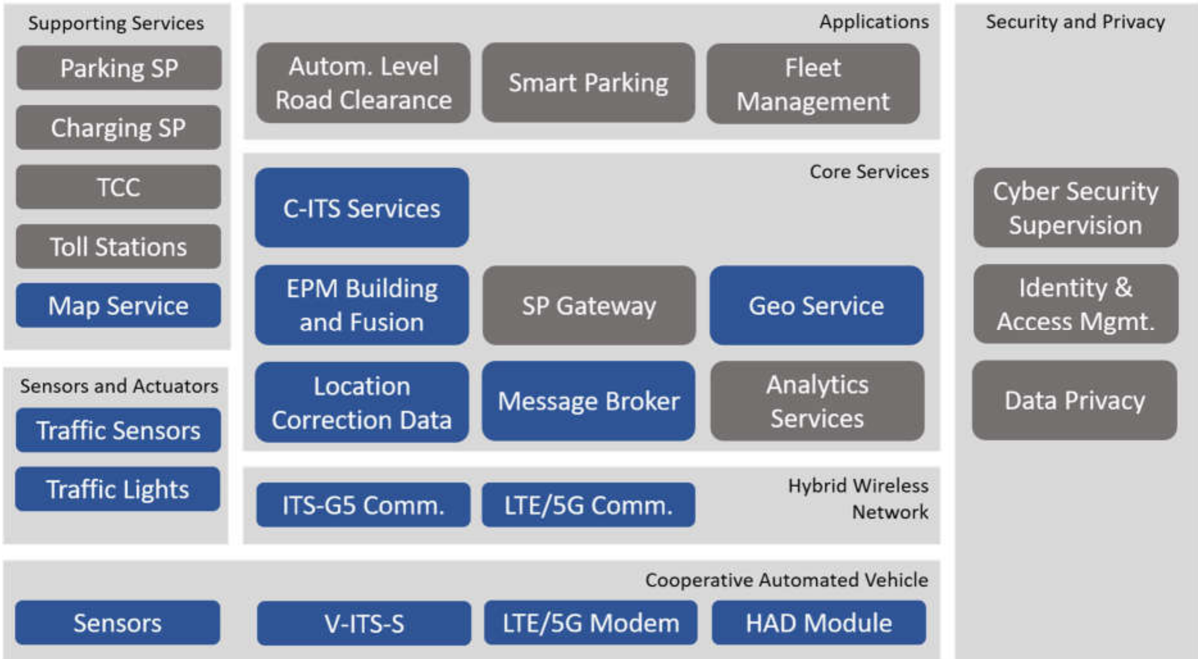

Figure 16 - Functional view - SCN 3.1a - Overview

In Figure 16, the functional blocks relevant to this scenario are highlighted in blue. They have the following meanings:

Map Service: The RSUs at the intersections will provide a local map of the intersection via MAP/MAPEM messages. For all other purposes (e.g. in the HAD module of the vehicle), static maps will be used.

Traffic sensors: The equipped intersection without traffic lights uses sensors such as cameras, stereo cameras and LiDAR sensors in order to perceive the environment and detect objects.

Traffic lights: The intersection with traffic lights will be equipped with an RSU which can send the traffic light state to nearby vehicles via ITS-G5 and LTE/5G.

C-ITS-Services: The CAV and infrastructure will communicate primarily via C-ITS services and C-ITS messages. The main effort will be concentrated on providing a service for EPMs, based on the CPS.

EPM Building and Fusion: An environment model for the traffic participants will be calculated on a MEC server based on data (detections) received from the infrastructure. Additionally, the EPM will be predicted to allow compensation for delays and anticipate the behaviour of the road users. This EPM and its predictions will be transmitted via ITS messages to the automated vehicles in the vicinity of the intersection.

Message broker: In order to send the EPM and other messages to vehicles in the vicinity of the intersection, a message broker will be used. Vehicles will be able to register at the broker, subscribe for specific services and then be sent the relevant messages as soon as they are available.

Geo service: A geo service will be implemented in order to aid the vehicles in discovering MEC servers and services. The geo service will send only information about MEC servers that can provide services relevant to the area that the vehicle is currently in.

ITS-G5 Communication, LTE/5G communication: All information from RSUs and MEC server will be communicated in a hybrid manner, i.e. using both ITS-G5 and LTE/5G.

Sensors: In-vehicle sensors of the AV include LiDAR, Radar and cameras, which are the basis to compute the vehicle's own internal EPM for general automated driving purposes.

V-ITS-S: With the V-ITS-S, the vehicle is enabled to send messages (e.g. CAM) and receive messages from the infrastructure or other vehicles, e.g. CPM, SPAT(EM), MAP(EM), DENM via ITS-G5.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can also be sent and received via LTE/5G.

HAD Module: The HAD module will be adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (merging into or crossing the intersection) safely and efficiently.

In Figure 17, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

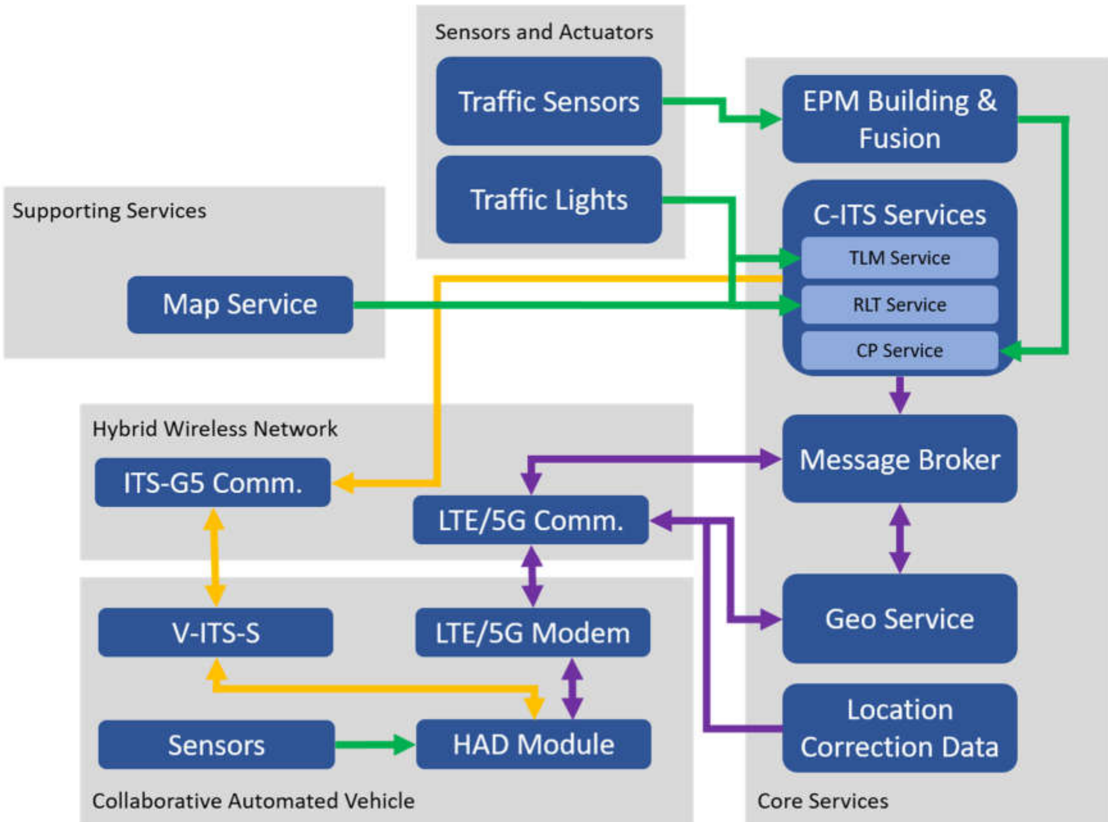

Figure 17 - Functional View - SCN3.1a - Details

5.2.2 Data / IT Environment View

In this scenario, only the data flows 1 to 4 of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 18):

1. Sensors submit data to a road-side unit (RSU) about the current “driving environment”, e.g., positions, speeds and directions of road users detected by sensors.
2. Vehicles equipped with communication modules receive data directly from an RSU or a MEC server, e.g., collective perception message (CPM), signal phase and timing extended message (SPATEM), map extended message (MAPEM).
3. Multiple RSUs and road sensors push their data to a multi-access edge computing (MEC) server in their vicinity.
4. A vehicle receives collective perception messages from a MEC server in its vicinity.

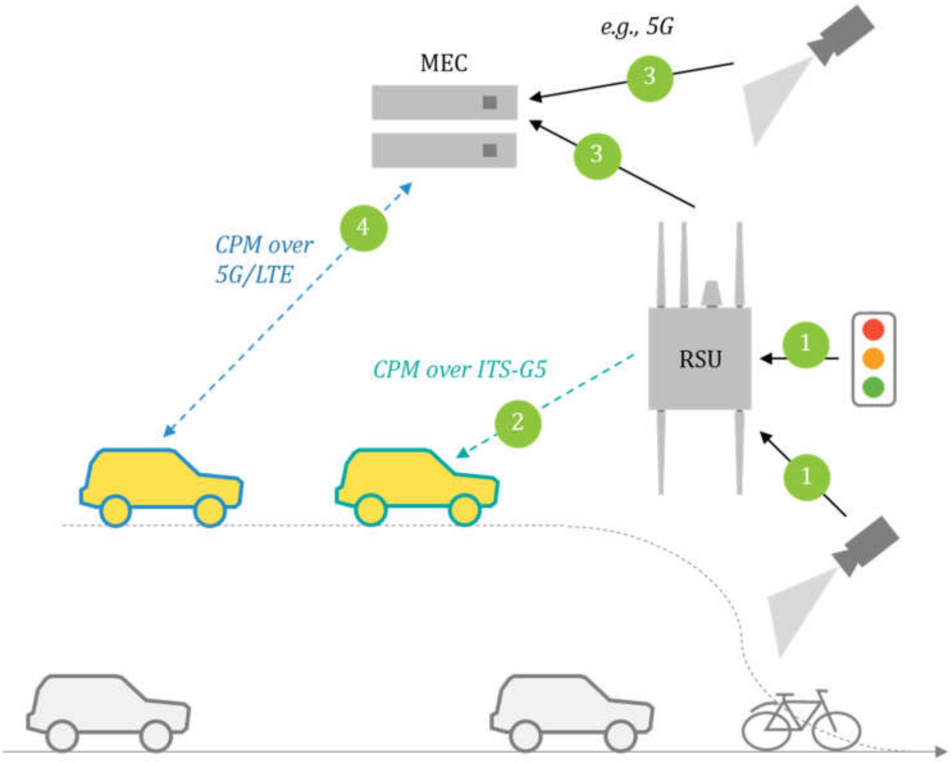

Figure 18 - Common Data Flows across ICT4CART Use Cases from D3.3 [4]

The following table lists the relevant standards for the data that will be transmitted in this scenario:

	Data Type	Relevant Standards
Provided by the IT Environment	Environment perception models (EPMs) and their predictions for use by the automated driving (AD) vehicles	CPM as will be specified in ETSI TS 103 324 [6] For the prediction of the EPM, no standard exists. Either a new message format is used for prediction or the CPM will be extended to cover the predictions additionally.
	Intersection map and topology	MAPEM as specified by ETSI TS 103 301 [7]
	Traffic light data	SPATEM as specified by ETSI TS 103 301 [7]
Consumed by the IT Environment	Data required to build EPMs, from RSUs and road signs and sensors	Proprietary sensor object format

5.2.3 Communication View

In this scenario, hybrid communication is used extensively. The infrastructure provides information (encoded in ITS messages) to the CAVs via two communication channels: ITS-G5 (ad-hoc network) and LTE/5G (cellular network). Figure 19 shows the possible communication paths for an example message (SPATEM).

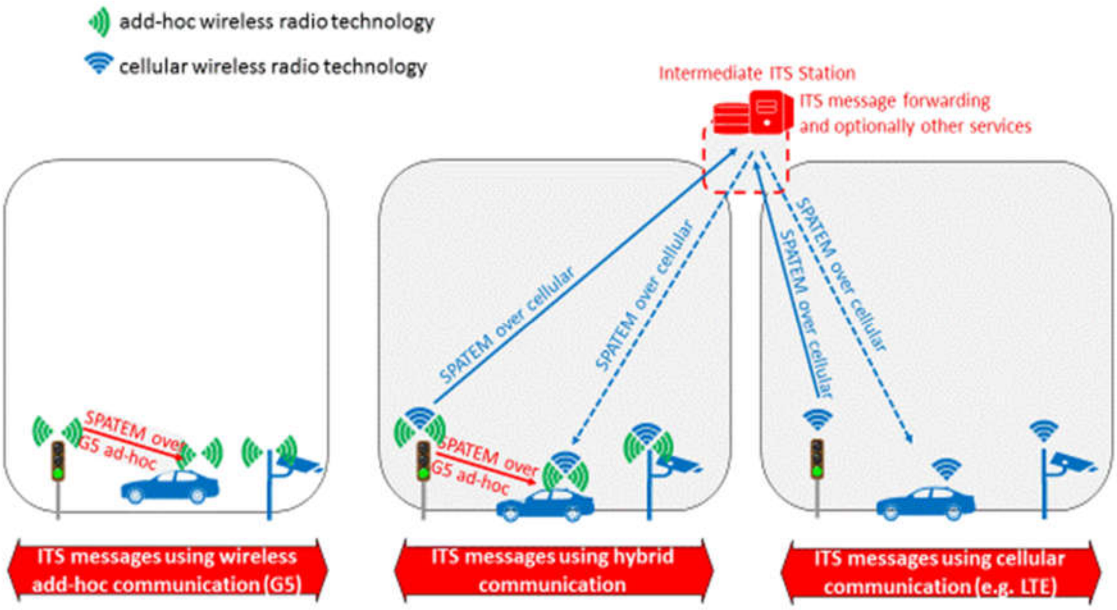

Figure 19 - Common Data Flows across ICT4CART Use Cases

5.2.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

5.3 Scenario 3.4: Precise positioning in urban and highway location

This scenario demonstrates the correction of GNSS data for high precision positioning of the vehicle in different areas (urban, suburban). The use of the corrected position for automated driving functions is a prerequisite for other scenarios, like SCN3.1a.

In the following, the adaptions of the general architecture views on the Scenario 3.4 *"Precise Positioning in urban and highway location"* are given for the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view.

5.3.1 Functional View

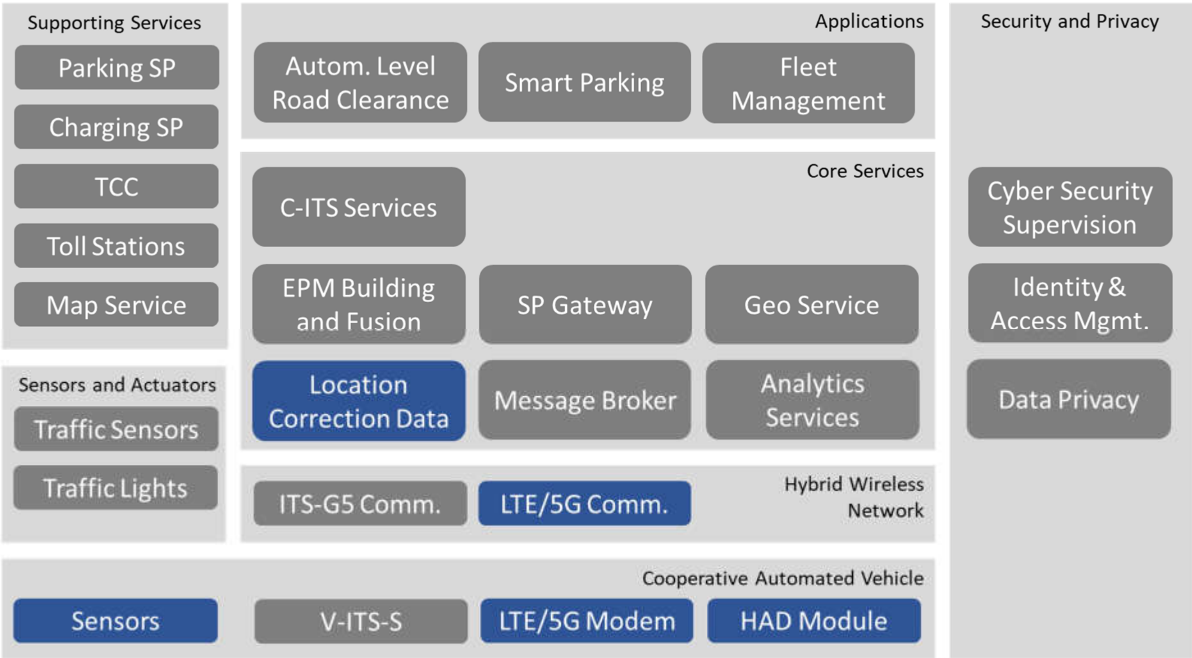

Figure 20 - Functional view - SCN3.4 German test site - Overview

In Figure 20, the functional blocks relevant to this scenario are highlighted in blue. They have the following meanings:

Location Correction Data:
This function is provided by the precise localisation service based on Real-Time-Kinematic (RTK) technique, which enhances the precision of the GNSS by using carrier phase measurements and correction data of RTK reference stations.

LTE/5G Communication:
The LTE/5G communication is used to transmit the location correction data.

LTE/5G Modem:
The LTE/5G modem in the vehicle receives the location correction data from the MEC server.

HAD Module:
The HAD Module uses the correction data to improve the received GNSS position.

Sensors:
The GNSS receiver provides the position data in the vehicle.

In Figure 21, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

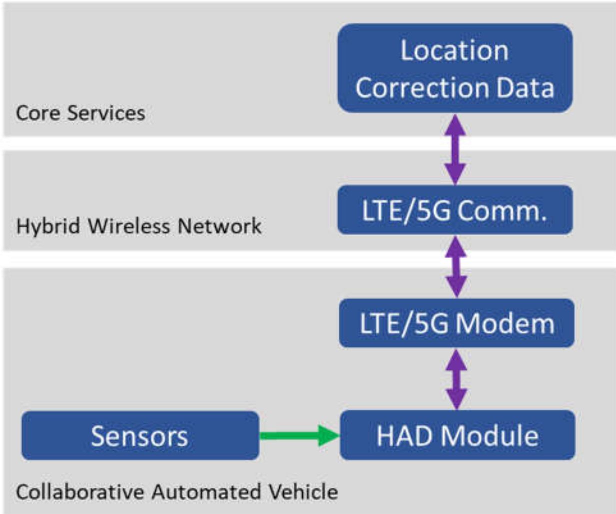

Figure 21 - Functional View - SCN3.4 German test site – Details

5.3.2 Data / IT Environment View

On the German test site, the correction data are provided by a dedicated RTK reference station, provisioned by a LTE/5G radio base station, to the MEC server and sent out to the vehicle (Figure 22).

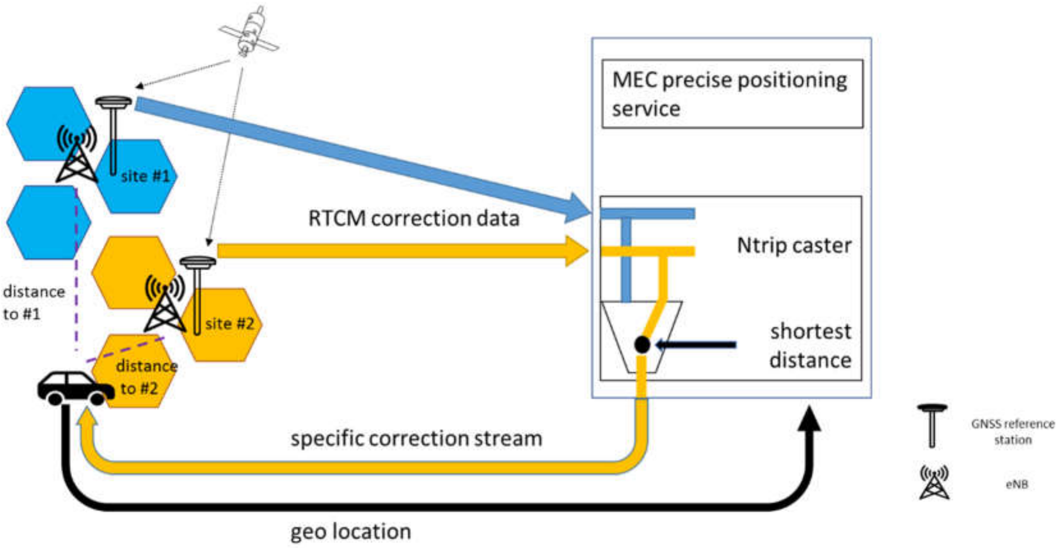

Figure 22 - German Test Site Approach for Precise Localisation

The MEC server selects the nearest RTK reference station in order to provide the appropriate correction data to the client.

The following table lists the relevant standards for the data that will be transmitted in this scenario:

	Data Type	Relevant Standards
Provided by the IT Environment	Correction data stream for RTK based localisation service	RTCM Standard 10403: "Differential GNSS (Global Navigation Satellite Systems) Services" [16]
Consumed by the IT Environment	Correction data stream from the GNSS reference stations	RTCM Standard 10403: "Differential GNSS (Global Navigation Satellite Systems) Services" [16]

5.3.3 Communication View

In this scenario, the transport mechanism of data over IP is used from the communication networks. The GNSS correction data are sent by the NTRIP protocol from the MEC server via LTE/5G to the modem installed in the vehicle.

5.3.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

6 Italian Test Site Architecture

The architecture for the Italian test site scenarios is illustrated on the following pages; each section is dedicated to a specific scenario. For each scenario, it is provided: (i) a Functional View with specific description for the components implemented into the scenario; (ii) a Data / IT Environment View in which data flow are illustrated; and (iii) a Communication View which details the communication aspects and illustrate how the components communicate each other.

6.1 Scenario 1.2: Smart Parking and IoT management in City of Verona, Italy

This scenario focuses on a CAV searching for a parking space in an outdoor parking area. The ICT4CART infrastructure is in charge of sending the required information about the available spot to the vehicle, specifying the location. This information is based on the processing of sensors data (i.e. detection cameras) using extended/under standardisation ETSI messages.

Thanks to this information, the CAV is able to perform the necessary driving actions and drive directly to the available space.

The ICT4CART infrastructure exploits Vehicle-to-Infrastructure (V2I) communication using the 4G/LTE cellular network.

6.1.1 Functional View

An overview of the functional view is provided in Figure 23 and each component implemented in the scenario is detailed in the following.

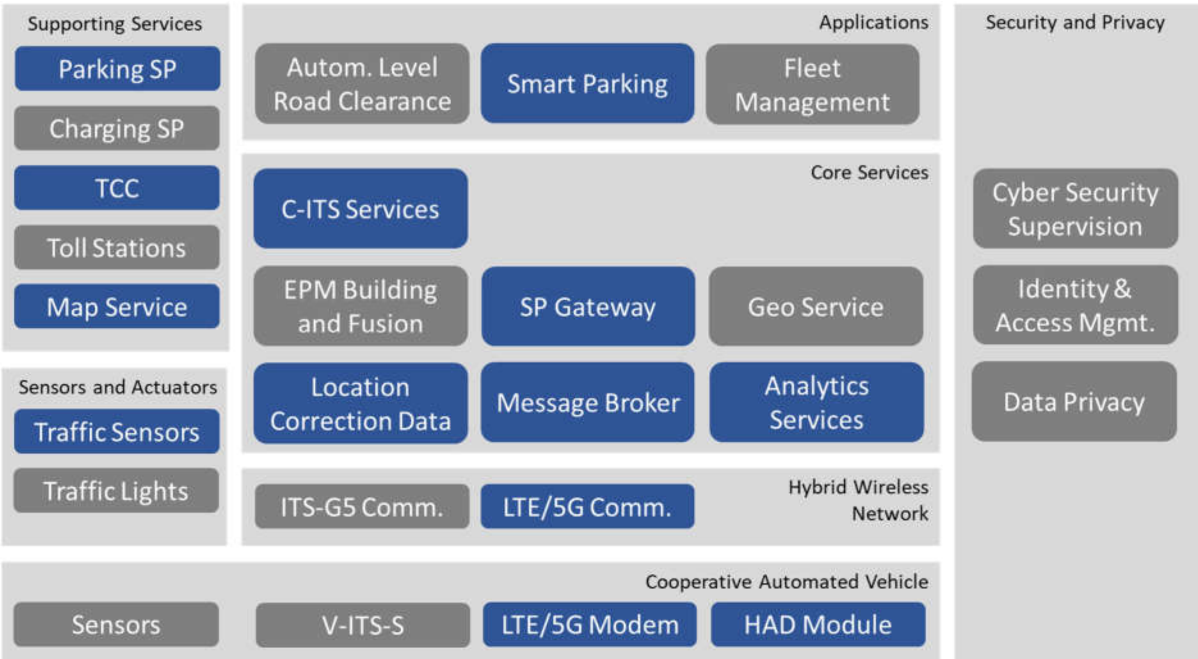

Figure 23 - Functional view – SCN 1.2 - Overview

Parking SP & Traffic sensors: The parking area in Verona is equipped with a camera with intelligent video analytics, able to detect the status (free/busy) of the parking lots in a certain defined parking area. The data coming from this camera is sent to the TCC of the City of Verona.

TCC: The Traffic Control Centre of City of Verona will gather the data coming from the detection camera and provide the information about the parking availability through the Internet in a standard format.

Map Service: A local map of the parking will be provided by the City of Verona.

SP Gateway: The SP Gateway will collect the data from the City of Verona and provide a single downstream interface to the communication infrastructure, providing parking space availability of the parking area monitored.

Analytics services: Analytics Services will refine data coming from the TCC by using algorithms before sending them to the SWARCO Cloud. The SP Gateway could use Analytics Services to make predictions of service availability for the near future. In particular, if the data is publicly available, the service can make a forecast of the number of available parking spaces in the monitored areas.

Smart Parking: The Smart Parking application replies to requests from CAVs to find a suitable parking space. Based on a requested location and a search radius, an available parking space is selected and the precise location is communicated.

C-ITS-Services: The CAV and infrastructure will communicate primarily via C-ITS services and C-ITS-messages. The main effort will be concentrated on providing parking information, generating messages based on the ETSI Point of Interest (POI) Message and/or MAP(EM) messages.

Message broker: In order to send the information about parking availability to the vehicles, a message broker will be used. Vehicles will be able to register at the broker, subscribe for specific services and receive the relevant messages as soon as they are available.

Location Correction Data: The Location Correction Data function will provide correction data for GNSS data by using physical reference stations or network-based ones. This function will allow precise positioning of the CAV.

LTE/5G communication: All information from the C-ITS-S and message broker will be communicated using LTE/5G.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can be received by the vehicle.

HAD Module: The HAD module will be adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (parking the vehicle in the available space) safely and efficiently.

In Figure 24, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

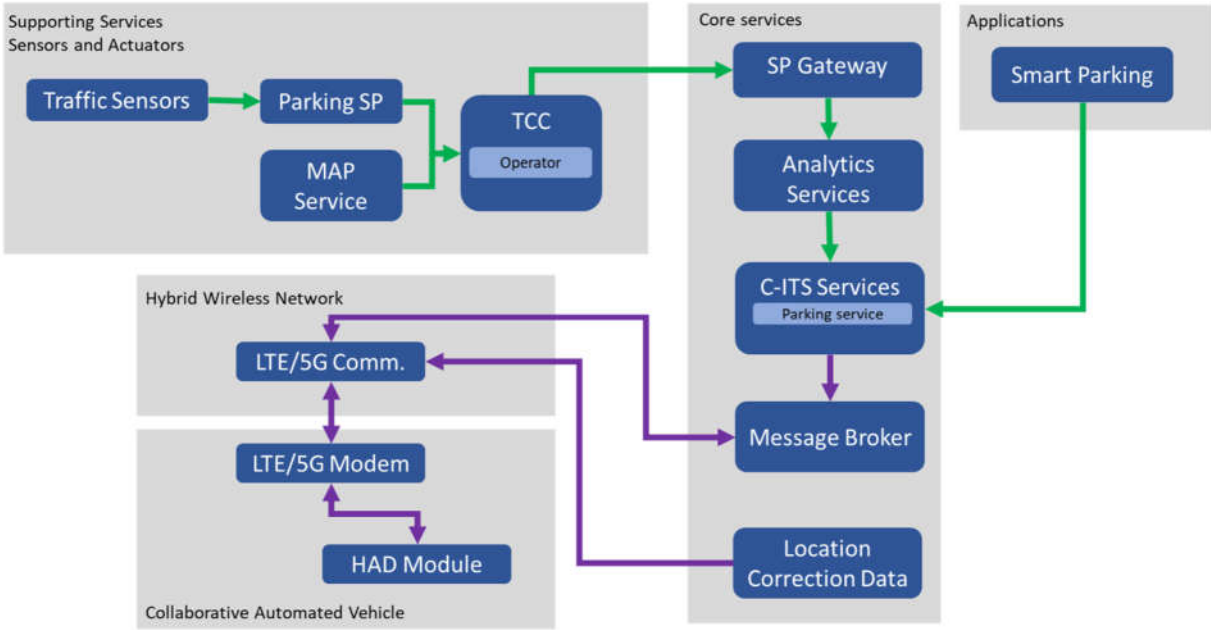

Figure 24 - Functional view - SCN 1.2 - Details

6.1.2 Data / IT Environment View

In this scenario, the following data flows of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 25):

1. Sensors submit data to the TCC about the current parking places availability.
2. The TCC makes the data available (in DATEX II format) to the Cloud (e.g. Service Provider Gateway and private automotive could) for analysis and for the generation of C-ITS messages.
3. C-ITS messages are sent to a Message Broker, to be distributed to the relevant dissemination area.
4. Vehicles equipped with LTE/5G communication modules and AMQP clients can subscribe for the same messages on the Message Broker. Filtering will be done by message type and geographic location. The vehicles receive standard messages with information about the exact location of free parking spots and with a forecast for the whole day.

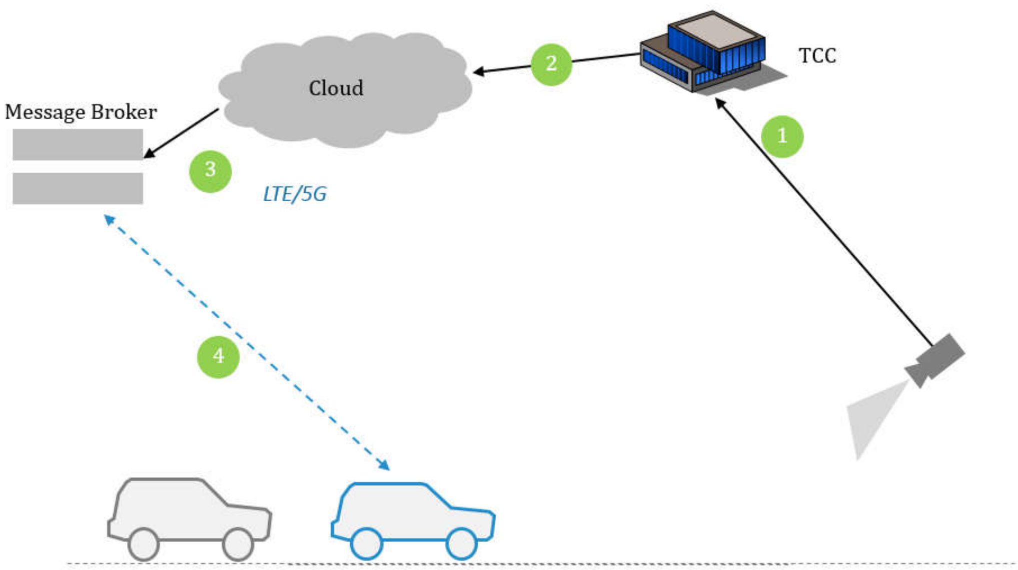

Figure 25 - Data / IT Environment View of the Smart Parking use case (City of Verona)

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Real-time parking spot availability	DATEX II [8], Open Mobility Vocabulary (MobiVoc) [9]
	Parking availability data	Based on EVCSM as specified in ETSI TS 101 556-1 [18]
Consumed by the IT Environment	Data received from parking service provider	Proprietary format

6.1.3 Communication View

In this scenario, only LTE/5G communication is used. The infrastructure provides information (encoded in ITS messages) to the CAVs via one communication channel: LTE/5G (cellular network).

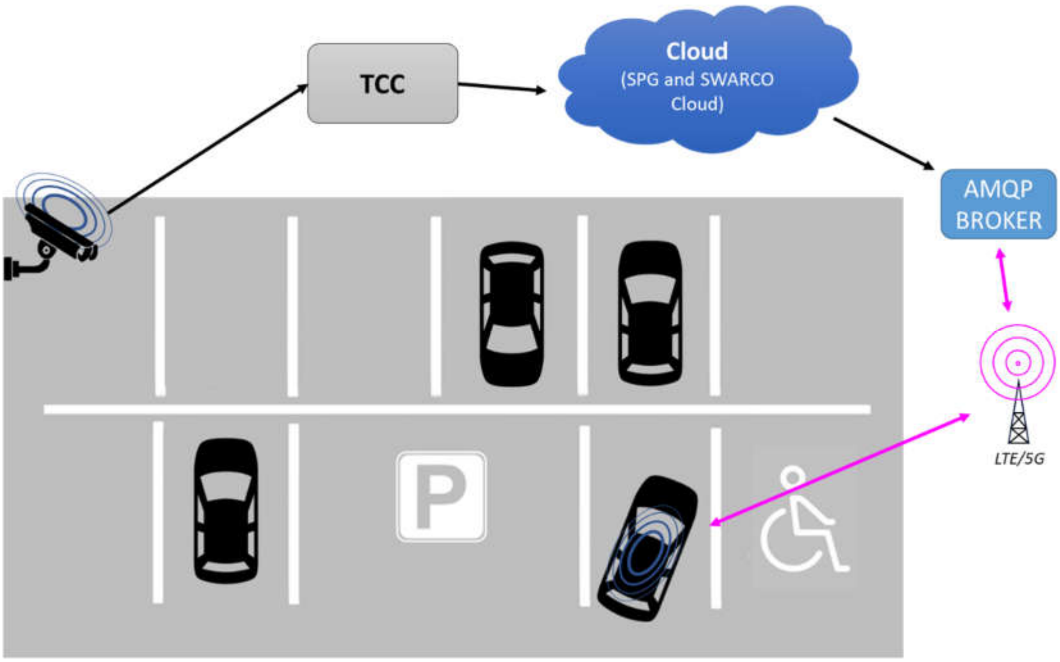

Figure 26 - Communication View of the Smart Parking use case (City of Verona)

6.1.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

6.2 Scenario 2.2: Dynamic adaptation of vehicle automation level on Trento, Italy

This scenario focuses on the exit ramp and on the approach of the vehicle to the toll station. The ICT4CART infrastructure is in charge of detecting all the involved vehicles and predicting their dynamics while they are leaving the motorway.

The ICT4CART infrastructure provides an EPM containing the information of all detected vehicles based on the processing of sensors data (i.e., cameras) using standard ETSI C-ITS messages. Furthermore, the ICT4CART infrastructure provides information about the topology of the exit ramp and of the toll station and toll-related information (e.g., the available toll lanes and their occupancy, availability of an AD reserved lane).

Thanks to this information, the CAV can refine its driving action, adapting its velocity on the exit ramp, selecting the less congested toll station lane, and possibly downscaling the automation level (or even disengage automation). Another possible application is the guidance of an autonomous vehicle toward a particular toll lane reserved to self-driving vehicles.

The ICT4CART infrastructure also exploits the EPM to implement active road safety applications that aims to alert vehicles of possible dangers such as wrong way driving, traffic conditions or collision risk.

6.2.1 Functional View

An overview of the functional view is provided in Figure 27 and each component implemented in the scenario is detailed in the following.

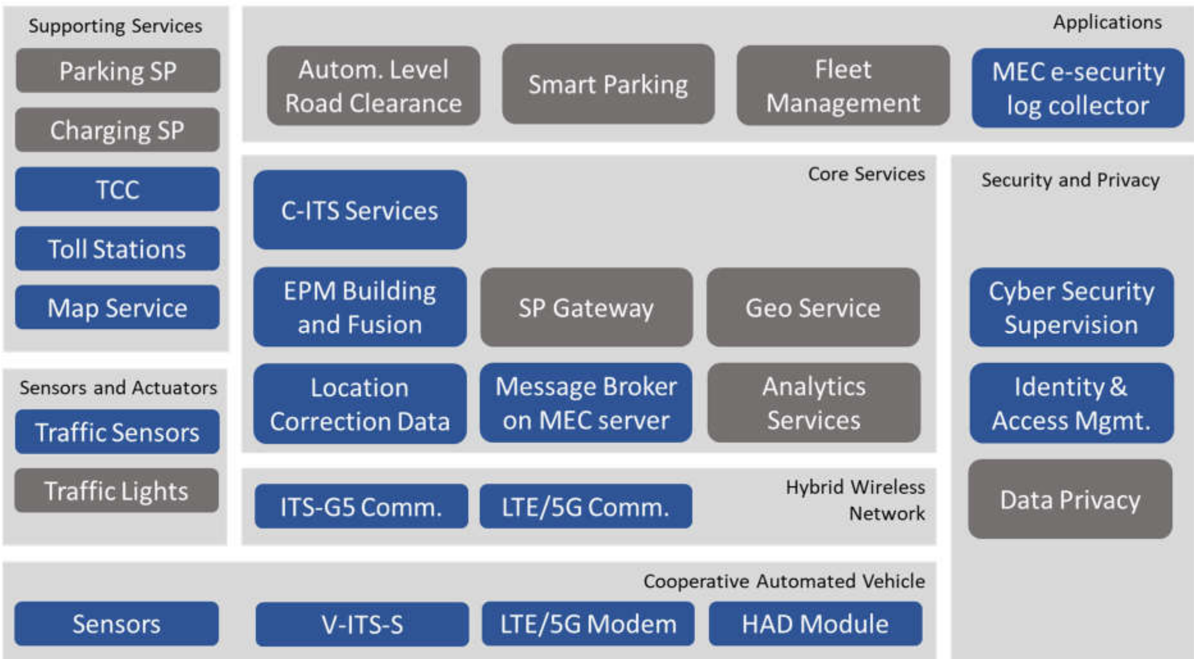

Figure 27 - Functional view - SCN 2.2 - Overview

TCC: The Traffic Control Centre manages the highway, monitors its status and validates the generation of security relevant C-ITS messages.

Toll Station: A software, interfaced with the RSU near the tolling station, simulates the toll lane status (exit toll lane open/closed/reserved for free flow service).

Map Service: The topology of the exit ramp and of the tolling station is provided to vehicles through MAPEM messages; the messages are based on digital map information of the exit ramp and the tolling station site.

Traffic sensors: Cameras are used to sense the environment in order to detect vehicles that are on the exit ramp and approach the tolling station.

C-ITS-Services: Decentralised Environmental Notification Basic Service (DENBS), Collective Perception Service (CPS), Cooperative Awareness Basic Service (CABS), Road and Lane Topology (RLT) service.

EPM Building and Fusion: An EPM is built based on the information gathered by the roadside sensors. The information of the EPM is provided to all connected actors through the CPS.

Message Broker on MEC server: A publish/subscribe approach is used to disseminate C-ITS messages via the LTE/5G communication link using a custom Message Broker that runs on the MEC server. C-ITS services publish the C-ITS messages on the Message Broker, and the vehicles can subscribe to specific topics in order to receive messages of interest in the MEC server's relevant geographical area.

Location Correction Data: To allow precise positioning of the CAV, the Location Correction Data function provides correction data for GNSS data by using network-based reference stations.

ITS-G5 Communication, LTE/5G communication: ITS-G5 and LTE/5G communication are used to provide a hybrid communication approach to disseminate C-ITS messages.

Sensor: In-vehicle sensors of the AV include, Radar, GNSS receiver (including RTK, if necessary) and cameras, which are the basis to compute the vehicle's own internal EPM for general automated driving purposes.

V-ITS-S: With the V-ITS-S, the vehicle is enabled to send messages (e.g. CAM, DENM) and receive ITS messages from the infrastructure or other vehicles (e.g. CPM, SPAT(EM), MAP(EM), DENM etc.) via ITS-G5 interface.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can also be sent and received via LTE/5G.

HAD Module: The HAD module is adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (merging into or crossing the intersection) safely and efficiently. In this scenario, the vehicle approaching the tool station receives messages from the infrastructure and adapts the speed and/or automation level (e.g. downscale or deactivate the automation level).

Identity and Access Management: The Identity and Access Management service provides authentication and authorisation for ITS-S which need to access ITS communications and services.

Cyber Security Supervision: The supervision centre receives logs from vehicle mainly coming from C-ITS messages authentication service.

MEC e-security log collector: This application receives the logs about cyber-security events from the CAV and it forwards them to the Cyber Security Supervision centre.

In Figure 28, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

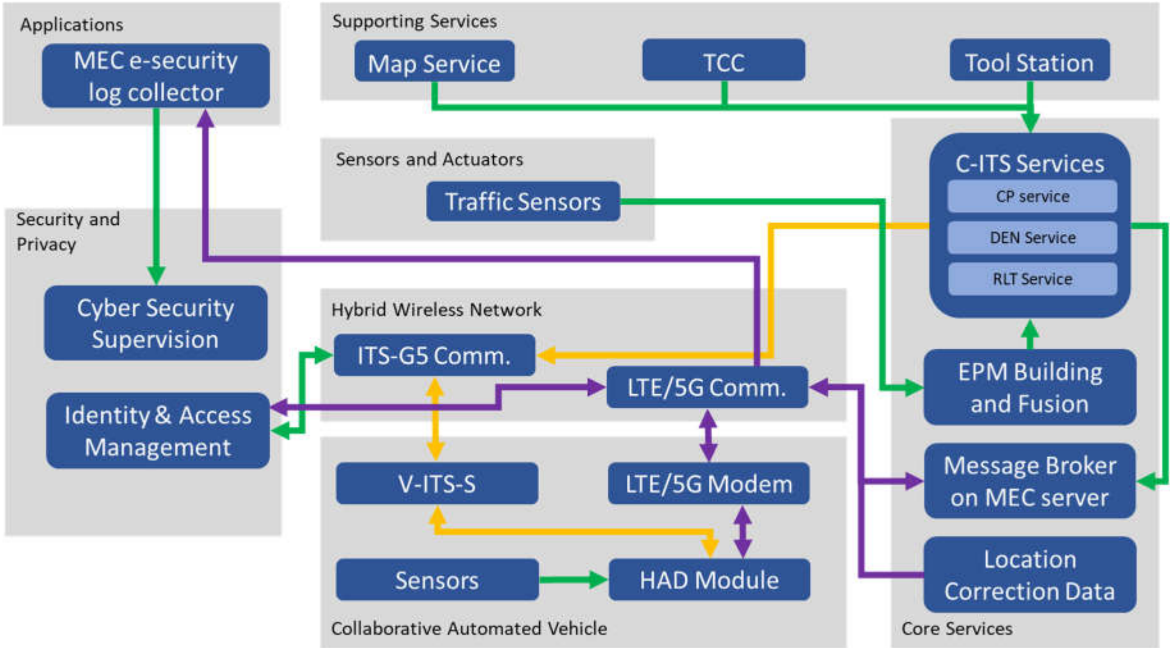

Figure 28 - Functional view - SCN 2.2 - Details

6.2.2 Data / IT Environment View

In this scenario, only the data flows 1 to 5 of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 29):

1. Cameras located at the toll station send the gathered raw data to the RSU, which processes the images to detect vehicles, and connected vehicles broadcast CAM messages that are collected by the RSU.
2. RSU broadcasts on the ITS-G5 communication channel the relevant C-ITS messages.
3. The RSU provides to the C-ITS services running on the MEC server the relevant collected information retrieved from the video processing (e.g., positions, speeds and directions of vehicles) and by the processing of received CAM.
4. C-ITS services running on the MEC server send C-ITS messages via the LTE/5G communication channel.
5. TCC sends information about security relevant events to the DENBS and the "Tolling station service" sends simulated information related to the dynamic status of the tolling station to the RLT service.

The C-ITS services (i.e., DENBS, CPS, RLT) can run either on the RSU or on the MEC server. An objective of this scenario is to test different possibilities and to understand which the best solution is.

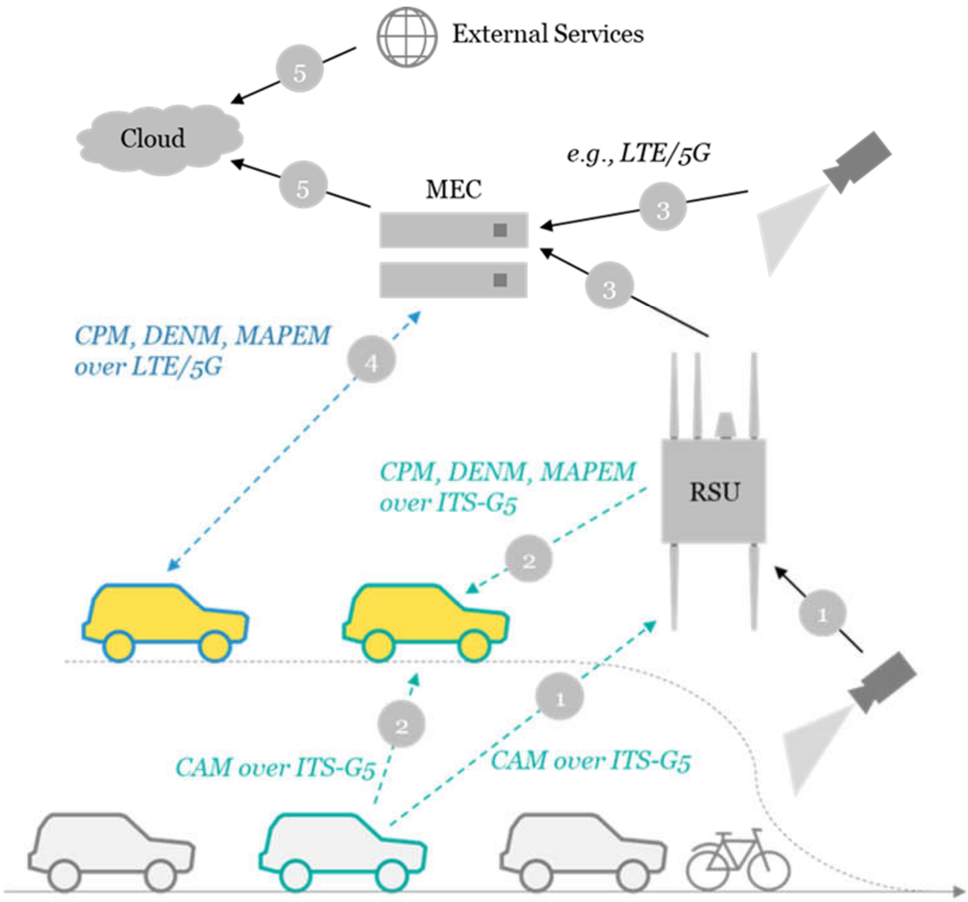

Figure 29 - Common Data Flows across ICT4CART Use Cases from D3.3 [4]

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Environment perception models (EPMs)	EPMs are sent using Collective Perception Messages (CPM) as specified in ETSI TS 103 324 [6] No specific standards are present for building the EPMs.
	Road Lane and Topology data	MAPEM as specified by ETSI TS 103 301 [7]
	Decentralised Environmental Notification data	DENM as specified by ETSI EN 302 637-3 v1.2.1 [19] (optionally some tests with v1.3.0 [14])
	Cooperative Awareness information	CAM as specified by ETSI EN 302 637-2 v1.4.0 [10]
Consumed by the IT Environment	Camera data used for building EPMs	Video flows based on H.264 or other standard video codec and Real Time Streaming Protocol (RTSP)
	Tolling station service data	Proprietary format
	Data from traffic sensors	Proprietary format

6.2.3 Communication View

The C-ITS messages DENM, MAPEM and CPM are sent on the ETSI ITS-G5 communication link and also on the LTE/5G communication link to implement the hybrid communication approach.

The following C-ITS services are included in the communication view of this scenario that is illustrated in Figure 30:

- The CPS creates an EPM based on the information extracted from the cameras' data and on the information processed from the CAM of the connected vehicles, and it broadcasts a CPM containing this information;
- The DENBS broadcasts a DENM of hazardous events defined exploiting information received from the TCC and/or from the RSU;
- The RLT service broadcasts MAPEM.

A custom Message Broker, that is based on a publish/subscribe approach, is implemented to provide C-ITS messages on the LTE/G5 communication link. The Message Broker is executed on the MEC server. C-ITS services (running either on the MEC server or on the RSU) publish the generated messages and the vehicles can register to the topics of interest for receiving via LTE/5G the relevant messages as soon as they are available.

The RSU is in charge of broadcasting C-ITS messages on the ITS-G5 link. The RSU subscribes to the relevant topics to retrieve the C-ITS messages generated by C-ITS services running on the MEC server and to broadcast them on the ITS-G5 link.

The Wind Tre backbone guarantees static connection to the MEC server to external services.

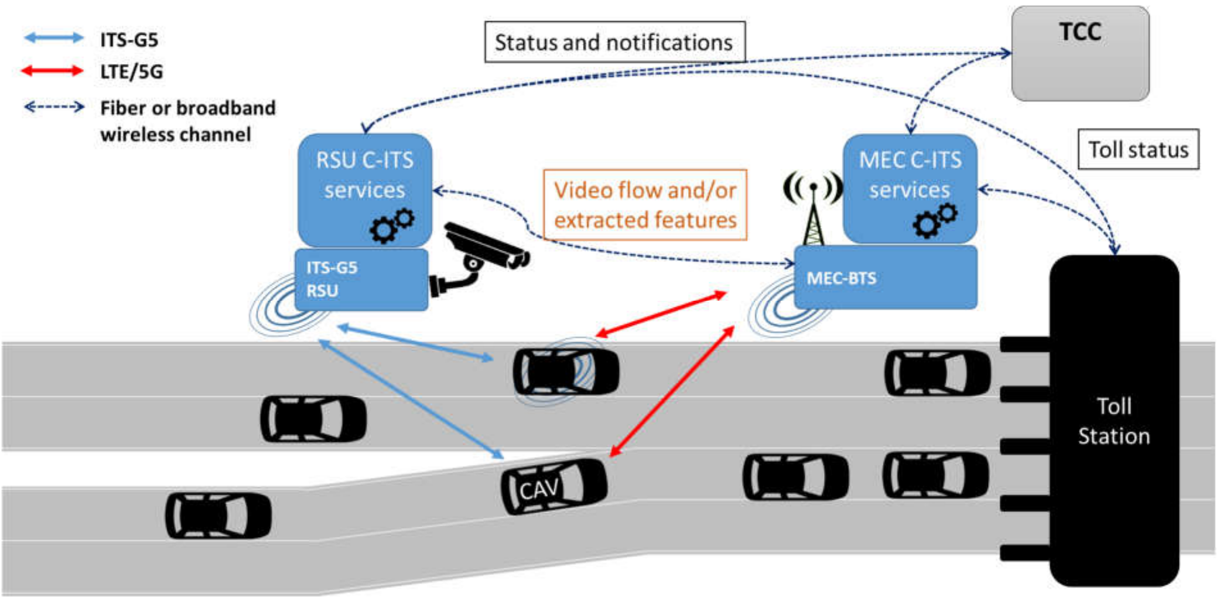

Figure 30 - Communication view of SCN2.2

6.2.4 Cyber-Security & Privacy View

The authentication of C-ITS messages will be performed using the PKI provided by the ICT4CART infrastructure and considering the relevant ETSI standards.

In real conditions, the supervision centre will be implemented by receiving logs from the vehicle OBU. A lab session will be organised during which the supervision centre capabilities will be demonstrated.

To do so, the vehicle OBU will send logs mainly related to C-ITS message authentication. Logs will be partially simulated in order to mimic cyber-attacks and to illustrate their detection by the supervision centre. The simulations will concern the transmission of C-ITS messages with wrong security information, such an incorrect signature or certificate.

6.3 Scenario 2.3: Dynamic adaptation of vehicle automation level in Verona, Italy

This scenario focuses on the dynamic adaptation of vehicle automation and speed in an urban scenario. The location to implement the scenario in the City of Verona is the crossroad between Via Venti Settembre/Vicolo Madonnina and Via Cantarane.

The ICT4CART infrastructure monitors the crosswalk, which is located on Via Venti Settembre before the urban intersection, and it is in charge of detecting vulnerable road users (VRU). This crosswalk is of particular interest because the vehicles approaching have low visibility of the crosswalk. In this specific scenario, the infrastructure has to communicate with the vehicle so that it can adapt its behaviour to avoid danger and possible collision with other vehicles and VRUs (e.g. pedestrian and bicycle). The infrastructure must provide virtual mirror information. Based on this information, the vehicle can optimise longitudinal control, adapt the automation level (i.e. downscale the automation level) and avoid dangerous situations.

6.3.1 Functional View

An overview for the functional view is provided in Figure 31 and each component implemented in the scenario is detailed in the following.

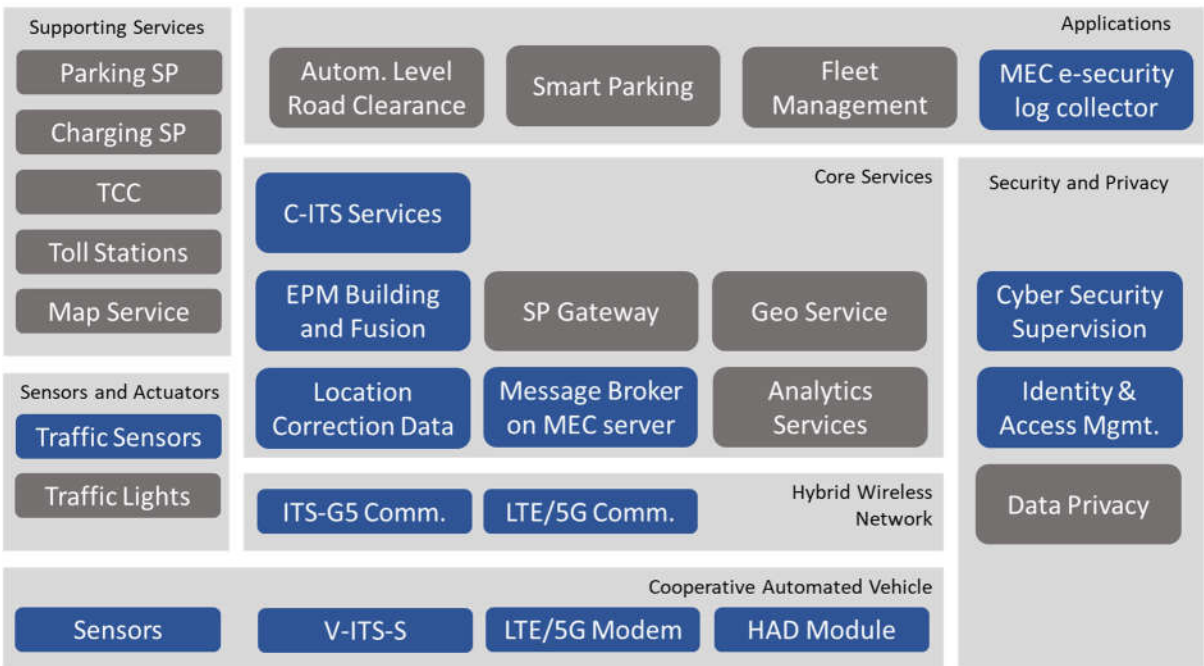

Figure 31 - Functional view - SCN2.3 - Overview

C-ITS-Services: Decentralised Environmental Notification Basic Service (DENBS), Collective Perception Service (CPS), Cooperative Awareness Basic Service (CABS).

Traffic sensors: Camera and LiDAR are used to sense the environment of the intersection in order to detect all road actors in the surrounding.

EPM Building and Fusion: An EPM is built based on the information gathered by the roadside sensors.

The information of the EPM will be provided to all connected actors through the Collective Perception Service.

Message broker on MEC server: A publish/subscribe approach is used to disseminate C-ITS messages via the LTE/5G communication link using a custom Message Broker that runs on the MEC server. C-ITS services publish the C-ITS messages on the Message Broker, and the vehicles can subscribe to specific topics in order to receive messages of interest in the MEC server's relevant geographical area.

Location Correction Data: To allow precise positioning of the CAV, the Location Correction Data function provides correction data for GNSS data by using network-based reference stations.

ITS-G5 Communication, LTE/5G communication: ITS-G5 and LTE/5G communication are used to provide a hybrid communication approach to disseminate C-ITS messages.

LTE/5G communication: The information from the C-ITS-S and message broker can be communicated using LTE/5G.

Sensors: In-vehicle sensors of the AV include Radar and cameras, which are the basis to compute the vehicle's own internal EPM for general automated driving purposes.

V-ITS-S: With the V-ITS-S, the vehicle is enabled to send messages (e.g. CAM) and receive messages from the infrastructure or other vehicles, e.g. CPM, SPAT(EM), MAP(EM), DENM via ITS-G5.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can also be sent and received via LTE/5G.

HAD Module: The HAD module will be adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (merging into or crossing the intersection) safely and efficiently. The CAV, considering the information contained into the CPM, DENM, and GLOSA messages, can revise its AD level and/or speed.

Identity and Access Management: The Identity and Access Management service will provide authentication and authorisation for ITS-S which need to access ITS communications and services.

Cyber Security Supervision: The supervision centre will receive logs from participating vehicles mainly coming from C-ITS messages authentication.

MEC e-security log collector: This application receives the logs about cyber-security events from the CAV and it forwards them to the Cyber Security Supervision centre.

In Figure 32, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

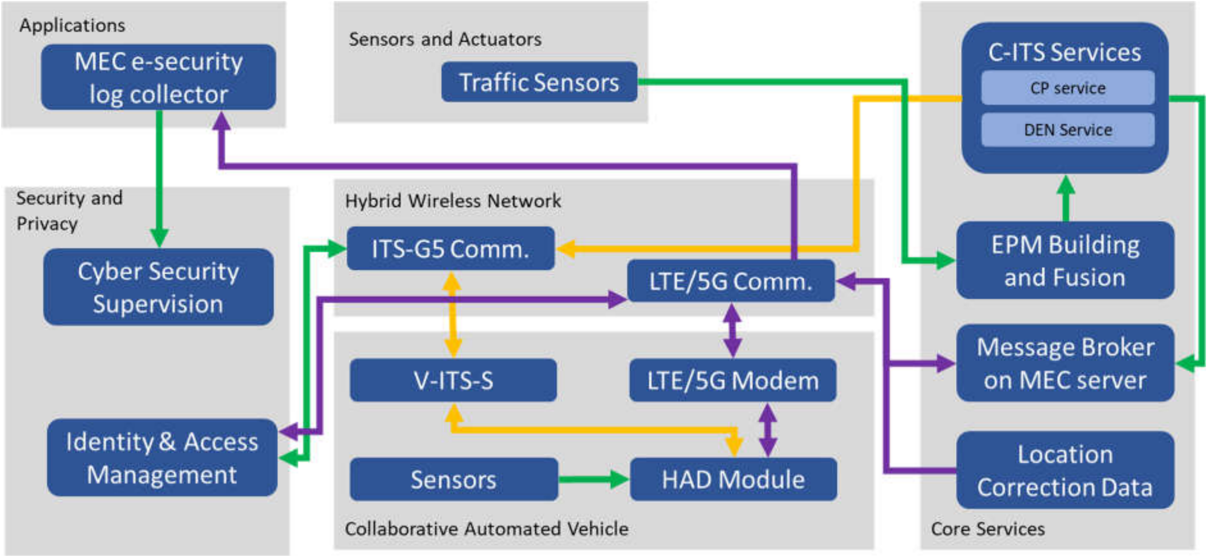

Figure 32 - Functional view - SCN2.3 – Details

6.3.2 Data / IT Environment View

In this scenario, only the data flows 1 to 4 of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 33):

1. Camera and LiDAR located at the intersection send the gathered raw data to the RSU, which processes them to detect the road actors present, and connected vehicles broadcast CAM messages that are collected by the RSU.
2. RSU broadcasts on the ITS-G5 communication channel the relevant C-ITS messages.
3. The RSU provides to the C-ITS services running on the MEC server the relevant collected information retrieved from the video processing (e.g., positions, speeds and directions of vehicles) and by the processing of received CAM.
4. C-ITS services running on the MEC server send C-ITS messages via the LTE/5G communication channel.

The C-ITS services (i.e., DENBS, CPS) can run either on the RSU or on the MEC server. An objective of this scenario is to test different possibilities and to understand which the best solution is.

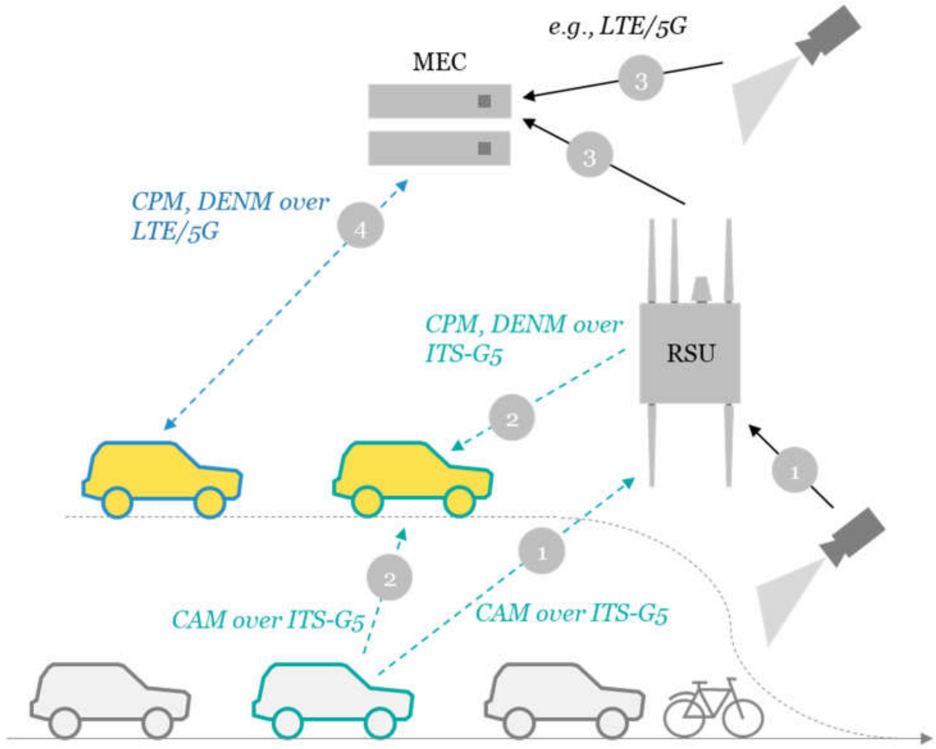

Figure 33 - Common Data Flows across ICT4CART Use Cases from D3.3 [4]

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Environment perception models (EPMs)	EPMs are sent using Collective Perception Messages (CPM) as specified in ETSI TS 103 324 [6] No specific standards are present for building the EPMs.
	Decentralised Environmental Notification data	DENM as specified by ETSI EN 302 637-3 v1.3.0 [14]
	Cooperative Awareness information	CAM as specified by ETSI EN 302 637-2 v1.4.0 [10]
Consumed by the IT Environment	Camera and LiDAR data used for building EPMs	Camera: Video flows based on H.264 or other standard video codec and Real Time Streaming Protocol (RTSP) LiDAR: point cloud data

6.3.3 Communication View

In this scenario, the ITS-G5 communication channel and the LTE/5G communication channel, via the Message Broker on the MEC server, are used. The vehicle approaches the urban intersection. In the proximity of the intersection, there are other vehicles and VRUs that are crossing the crosswalk.

The RSU uses the information from infrastructure sensors, C-ITS messages and visual cameras to identify a possible hazard. As the risk is identified, the infrastructure builds an EPM using the resources of the MEC server, and consequently sends a message to the vehicles in the area through the ITS-G5 channel.

This service will be based on the broadcasting of a CPM. This is a message that complements the CAM. It provides the position and dynamics information of all the road users that the broadcasting ITS station is aware of. The environmental model can be processed either on a RSU that is located close to the intersection, or on a MEC server.

The C-ITS messages DENM and CPM are sent on the ETSI ITS-G5 communication link and also on the LTE/5G communication link to implement the hybrid communication approach.

A custom Message Broker, that is based on a publish/subscribe approach, is implemented to provide C-ITS messages on the LTE/G5 communication link. The Message Broker is executed on the MEC server. C-ITS services (running either on the MEC server or on the RSU) publish the generated messages and the vehicles can register to the topics of interest for receiving via LTE/5G the relevant messages as soon as they are available.

The RSU is in charge of broadcasting C-ITS messages on the ITS-G5 link. The RSU subscribes to the relevant topics to retrieve the C-ITS messages generated by C-ITS services running on the MEC server and to broadcast them on the ITS-G5 link.

The connected vehicle that receive a CPM and/or DENM could use the information received to adapt its automation level and/or its speed. This could help to prevent risk for the VRUs that are crossing the road.

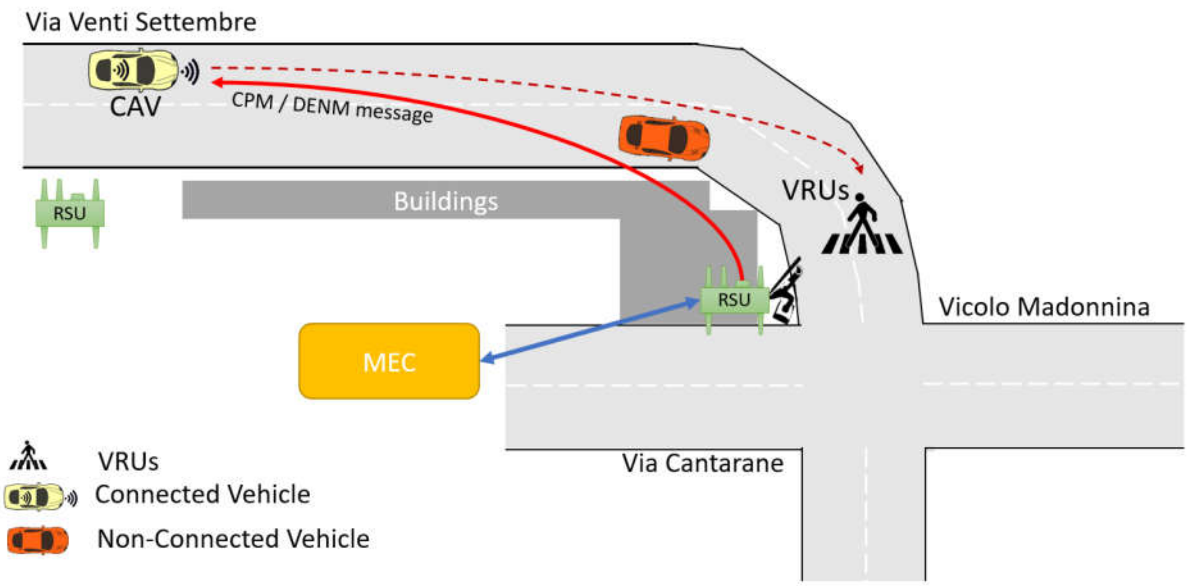

Figure 34 - Communication View - - SCN2.3 Dynamic adaptation of vehicle automation level in Verona

6.3.4 Cyber-Security & Privacy View

The authentication of C-ITS messages will be performed using the PKI provided by the ICT4CART infrastructure and considering the relevant ETSI standards.

In real conditions, the supervision centre will be implemented by receiving logs from the vehicle OBU. A lab session will be organised during which the supervision centre capabilities will be demonstrated. To do so, the vehicle OBU will send logs mainly related to C-ITS message authentication. Logs will be partially simulated in order to mimic cyber-attacks and to illustrate their detection by the supervision centre. The simulations will concern the transmission of C-ITS messages with wrong security information, such an incorrect signature or certificate.

6.4 Scenario 3.1b: Virtual mirror to "see" surrounding traffic in city of Verona, Italy

This scenario concerns an urban intersection in the city of Verona. The main objective of this scenario is to demonstrate that a CAV can benefit from the information about the surrounding environment that the ICT4CART infrastructure can provide.

The ICT4CART infrastructure monitors the intersection to identify road actors (e.g., vehicles, bicycles, pedestrians) using information from sensors (e.g., visual cameras, LiDARs) and from already connected users (i.e., analysing the CAMs sent by vehicles).

The gathered information is used to build an EPM of the intersection that provides details about the position of the identified road users and their dynamics. The EPM is then provided using the standard C-ITS message CPM that is being standardised by ETSI in the Technical Specification 103 324. The CAV can then exploit the received information to refine the driving action.

The ICT4CART infrastructure can also exploit the information present in the EPM to implement active road safety applications that can alert vehicles of possible dangers, such as collision risk, using DENM.

6.4.1 Functional View

An overview for the functional view is provided in Figure 35 and each component implemented in the scenario is detailed in the following.

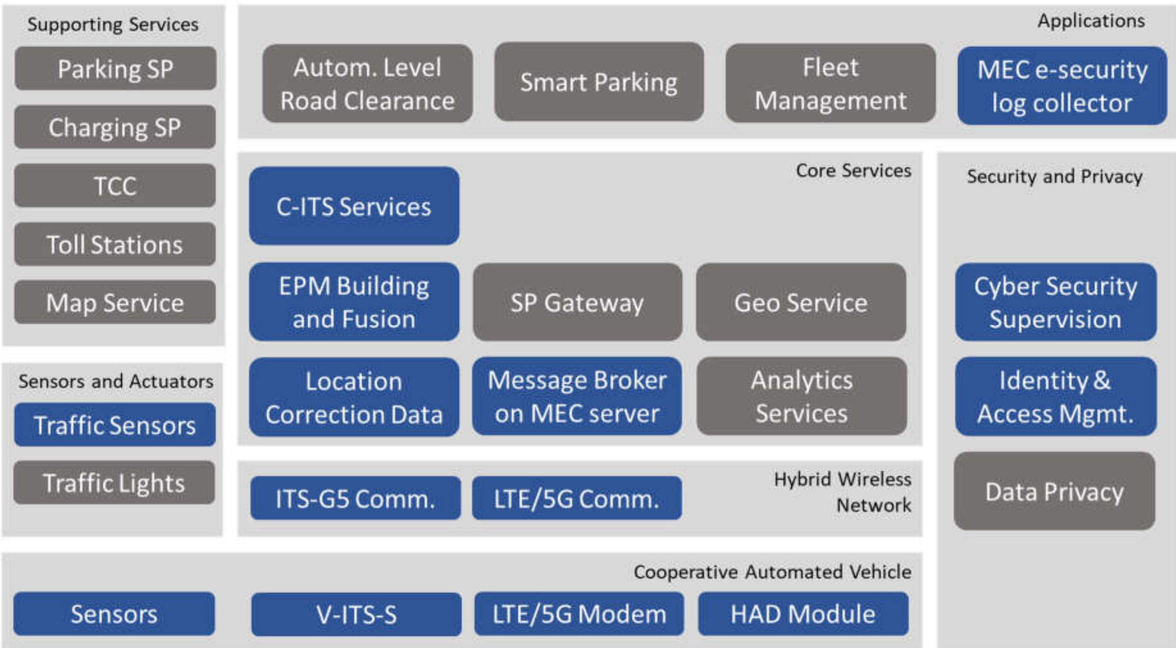

Figure 35 - Functional view - SCN 3.1b - Overview

Traffic sensors: Camera and LiDAR are used to sense the environment of the intersection in order to detect all road actors in the surrounding.

C-ITS-Services: Decentralised Environmental Notification Basic Service (DENBS), Collective Perception Service (CPS), Cooperative Awareness Basic Service (CABS).

EPM Building and Fusion: An EPM is built based on the information gathered by the roadside sensors. The information of the EPM will be provided to all connected actors through the CPS.

Message broker on MEC server: A publish/subscribe approach is used to disseminate C-ITS messages via the LTE/5G communication link using a custom Message Broker that runs on the MEC server. C-ITS services publish the C-ITS messages on the Message Broker, and the vehicles can subscribe to specific topics in order to receive messages of interest in the MEC server's relevant geographical area.

Location Correction Data: To allow precise positioning of the CAV, the Location Correction Data function provides correction data for GNSS data by using network-based reference stations.

ITS-G5 Communication, LTE/5G communication: ITS-G5 and LTE/5G communication are used to provide a hybrid communication approach to disseminate C-ITS messages.

LTE/5G communication: The information from the C-ITS-S and message broker can be communicated using LTE/5G.

Sensors: In-vehicle sensors of the AV include Radar and cameras, which are the basis to compute the vehicle's own internal EPM for general automated driving purposes.

V-ITS-S: With the V-ITS-S, the vehicle is enabled to send messages (e.g. CAM) and receive messages from the infrastructure or other vehicles, e.g. CPM, SPAT(EM), MAP(EM), DENM via ITS-G5.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can also be sent and received via LTE/5G.

HAD Module: The HAD module will be adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (merging into or crossing the intersection) safely and efficiently. The CAV, considering the information contained in the CPM, DENM and GLOSA messages, can revise its AD level and/or speed.

Identity and Access Management: The Identity and Access Management service will provide authentication and authorisation for ITS-S which need to access ITS communications and services.

Cyber Security Supervision: The supervision centre will receive logs from participating vehicles mainly coming from C-ITS messages authentication.

MEC e-security log collector: This application receives the logs about cyber-security events from the CAV and it forwards them to the Cyber Security Supervision centre.

In Figure 36, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

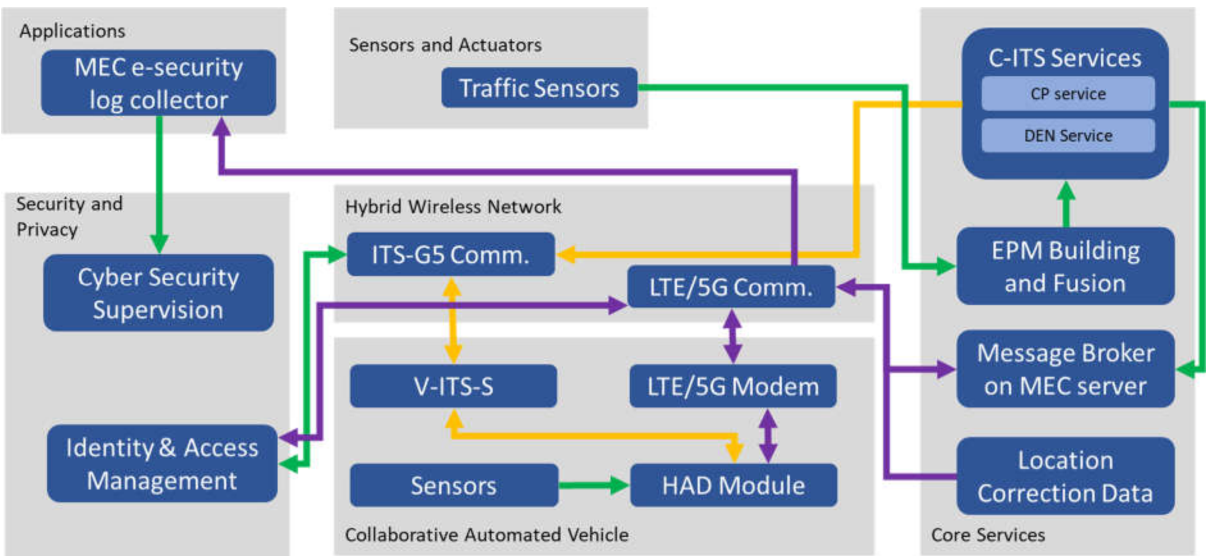

Figure 36 - Functional view - SCN 3.1b - Details

6.4.2 Data / IT Environment View

In this scenario, only the data flows 1 to 4 of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 37):

1. Camera and LiDAR located at the intersection send the gathered raw data to the RSU, which processes them to detect the road actors present, and connected vehicles broadcast CAM messages that are collected by the RSU.
2. RSU broadcasts on the ITS-G5 communication channel the relevant C-ITS messages.
3. The RSU provides to the C-ITS services running on the MEC server the relevant collected information retrieved from the video processing (e.g., positions, speeds and directions of vehicles) and by the processing of received CAM.
4. C-ITS services running on the MEC server send C-ITS messages via the LTE/5G communication channel.

The C-ITS services (i.e., DENBS, CPS) can run either on the RSU or on the MEC server. An objective of this scenario is to test different possibilities and to understand which the best solution is.

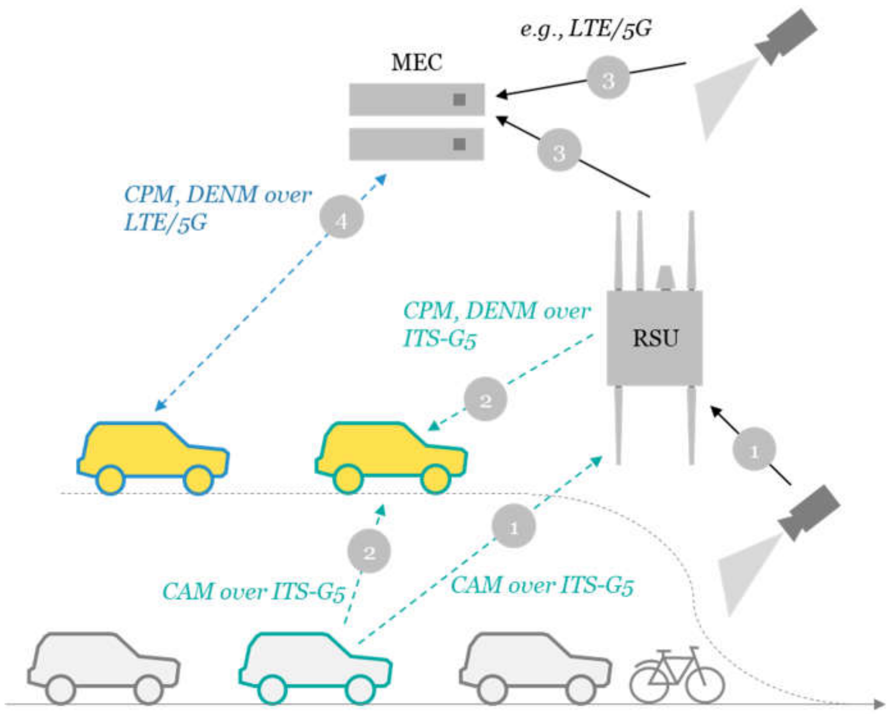

Figure 37 - Common Data Flows across ICT4CART Use Cases from D3.3 [4]

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Environment perception models (EPMs)	EPMs are sent using Collective Perception Messages (CPM) as specified in ETSI TS 103 324 [6] No specific standards are present for building the EPMs.
	Decentralised Environmental Notification data	DENM as specified by ETSI EN 302 637-3 v1.3.0 [14]
	Cooperative Awareness information	CAM as specified by ETSI EN 302 637-2 v1.4.0 [10]
Consumed by the IT Environment	Camera and LiDAR data used for building EPMs	Camera: Video flows based on H.264 or other standard video codec and Real Time Streaming Protocol (RTSP) LiDAR: point cloud data

6.4.3 Communication View

The C-ITS messages DENM and CPM are sent on the ETSI ITS-G5 communication link and also on the LTE/5G communication link to implement the hybrid communication approach.

The following C-ITS services are included in the communication view of this scenario:

- The CPS creates an EPM based on the information elaborated from the cameras' data and on the information extracted from the CAM of the connected vehicles and it broadcasts a CPM containing this information;
- The DENBS broadcasts a DENM of hazardous events defined exploiting information received from the RSU.

LINKS will implement a custom Message Broker that is based on a publish/subscribe approach that can provide C-ITS messages on the LTE/G5 communication link. The Message Broker is executed on the MEC server. C-ITS services (either running on the MEC server or on the RSU) publish the generated messages and the vehicles can register to the topics of interest for receiving via LTE/5G the relevant messages as soon as they are available.

The RSU is in charge of broadcasting C-ITS messages on the ITS-G5 link. The RSU subscribes to the relevant topics to retrieve the C-ITS messages generated by C-ITS services running on the MEC server and to broadcast them on the ITS-G5 link.

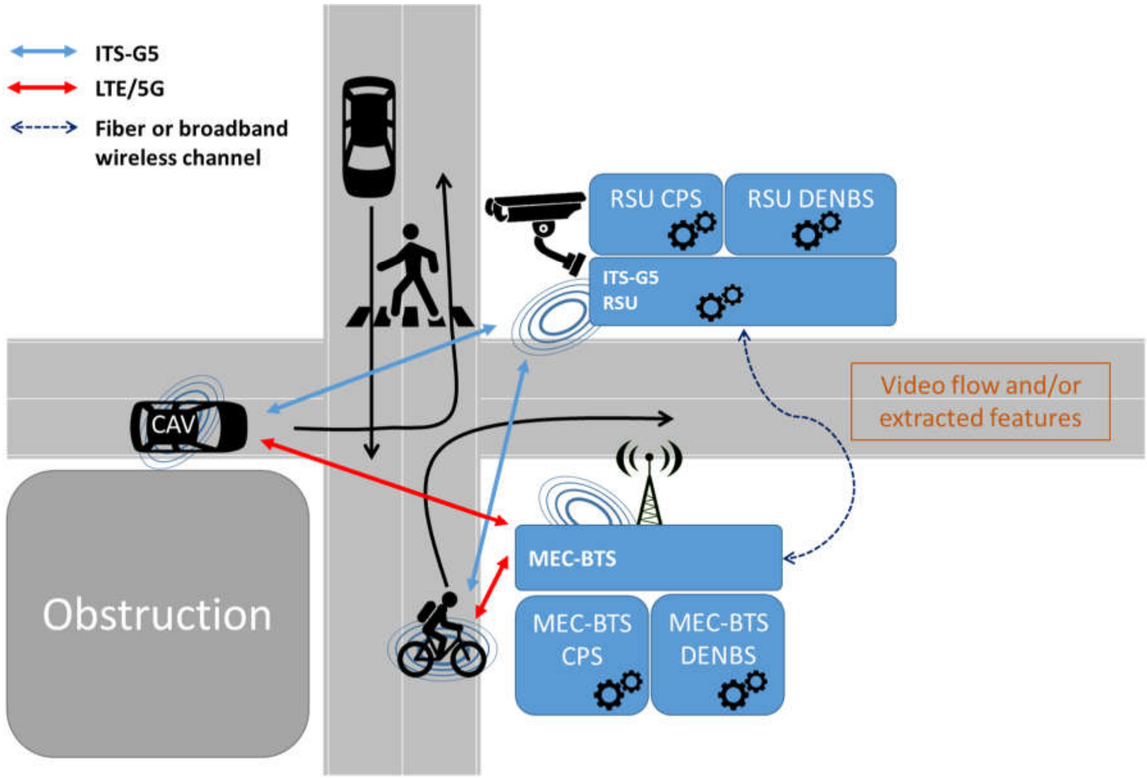

Figure 38 - Communication View - SCN3.1b Virtual mirror to "see" surrounding traffic in city of Verona, Italy

6.4.4 Cyber-Security & Privacy View

The authentication of C-ITS messages will be performed using the PKI provided by the ICT4CART infrastructure and considering the relevant ETSI standards.

In real conditions, the supervision centre will be implemented by receiving logs from the vehicle OBU. A lab session will be organised during which the supervision centre capabilities will be demonstrated. To do so, the vehicle OBU will send logs mainly related to C-ITS message authentication. Logs will be partially simulated in order to mimic cyber-attacks and to illustrate their detection by the supervision centre. The simulations will concern the transmission of C-ITS messages with wrong security information, such an incorrect signature or certificate.

6.5 Scenario 3.2: GLOSA (Green Light Optimized Speed Advisory) in City of Verona, Italy

This scenario focuses on an urban intersection in city of Verona monitored by the ICT4CART infrastructure. When a CAV is approaching the intersection, based on the vehicle position, the ICT4CART infrastructure sends information regarding the time to the next green phase and on the optimal speed to maintain to reach it. The CAV can rely on the information received to reach it at the beginning of the next green phase and refine its driving action accordingly. The ICT4CART infrastructure securely communicates with the vehicle using the 4G/LTE mobile network.

6.5.1 Functional View

An overview for the functional view is provided in Figure 39 and each component implemented in the scenario is detailed in the following.

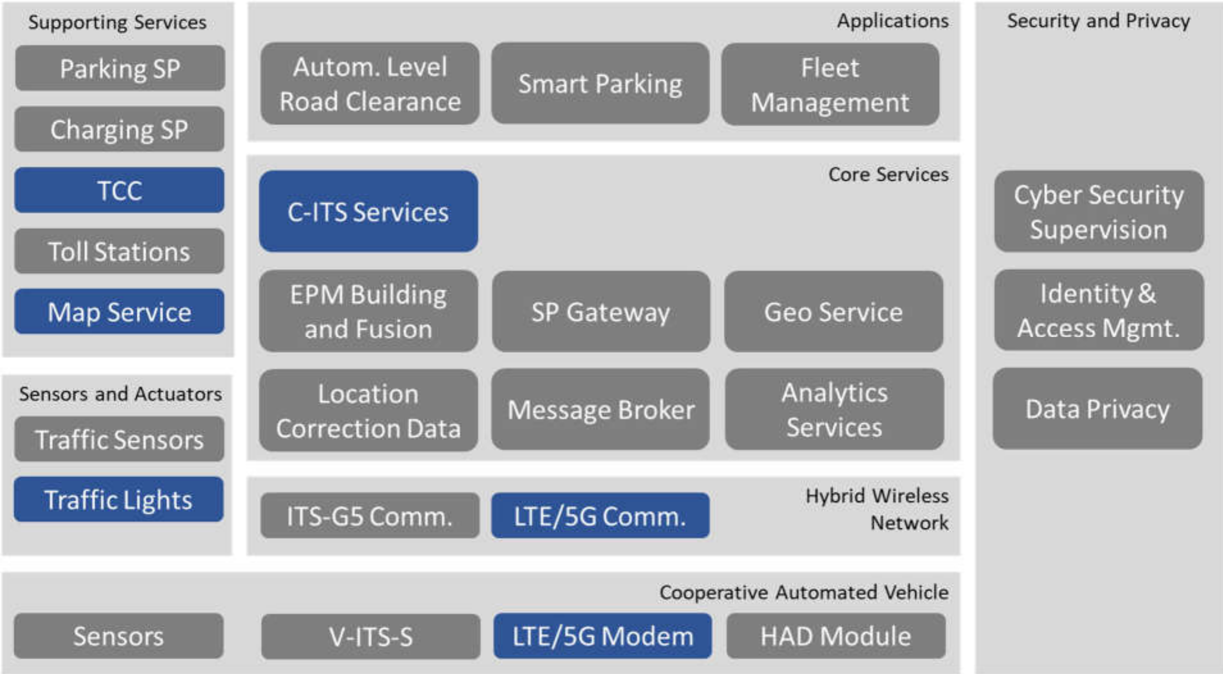

Figure 39 - Functional view - SCN 3.2 - Overview

Traffic lights: The connected traffic lights will send the traffic light status via wired connection to the TCC of the City of Verona.

TCC: The Traffic Control Centre of the City of Verona will provide the traffic light information to the C-ITS services.

Map Service: A local map of the intersection will be provided via MAPEM messages. For all other purposes (e.g. in the HAD module of the vehicle), static maps will be used.

C-ITS Services: The CAV and infrastructure will communicate primarily via C-ITS services and C-ITS-messages. The C-ITS-S will generate SPATEM messages, based on the ETSI standard, containing the real-time information of the traffic light signal phase and timing of the intersection. SPATEM and MAPEM messages will then be sent to the Traffic Light Assistance (TLA) Application on the MEC server, which will calculate, based on the position of the vehicle, the optimal speed for approaching the intersection at the next green phase (Green Light Optimized Speed Advice – GLOSA) and the time-to-green countdown (TTG). The TLA service will be finally provided to the vehicles.

LTE/5G communication: All information from the C-ITS-S and message broker will be communicated using LTE/5G.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can be received by the vehicle.

In Figure 40, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

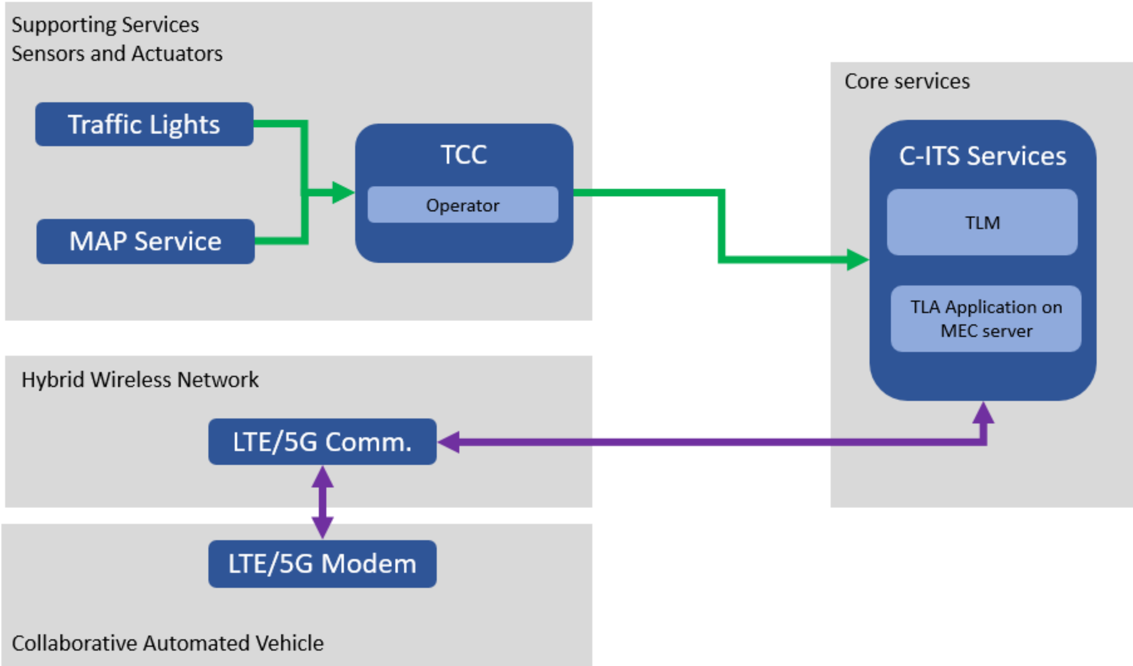

Figure 40 - Functional view - SCN 3.2 - Details

6.5.2 Data / IT Environment View

In this scenario, the following data flows of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 41Figure 18):

1. The connected traffic lights will submit data to the TCC about the traffic light status.
2. This information is provided to a Central ITS Station for the generation of C-ITS messages.
3. C-ITS messages (SPATEM/MAPEM) are sent to an application on a MEC server.
4. Vehicles equipped with LTE/5G communication modules will receive information about the optimal speed for approaching the intersection at the next green phase and the time-to-green countdown.

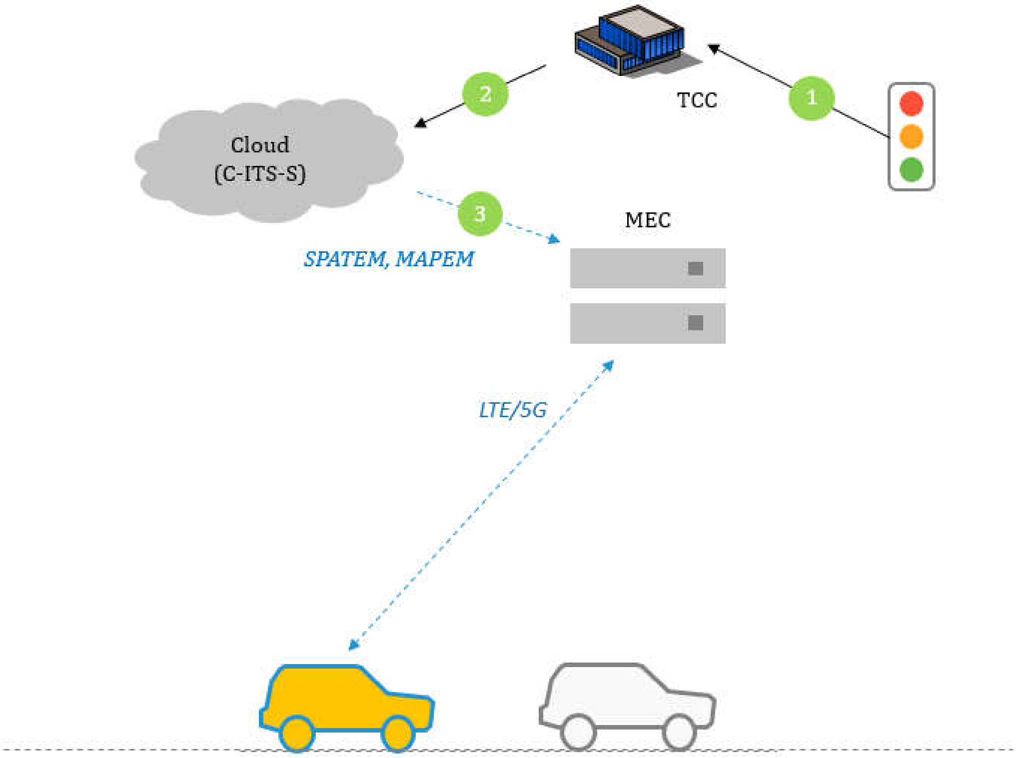

Figure 41 - Data / IT Environment View of the GLOSA use case (City of Verona)

The following table lists the relevant standards for the data that will be transmitted in this scenario:

	Data Type	Relevant Standards
Provided by the IT Environment	Intersection map and topology	MAPEM as specified by ETSI TS 103 301 [7]
	Traffic light data	SPATEM as specified by ETSI TS 103 301 [7]
Consumed by the IT Environment	Data received from the traffic lights	Proprietary format

6.5.3 Communication View

In this scenario, only LTE/5G communication is used. The infrastructure provides information (encoded in ITS messages) to the CAVs via one communication channel: LTE/5G (cellular network).

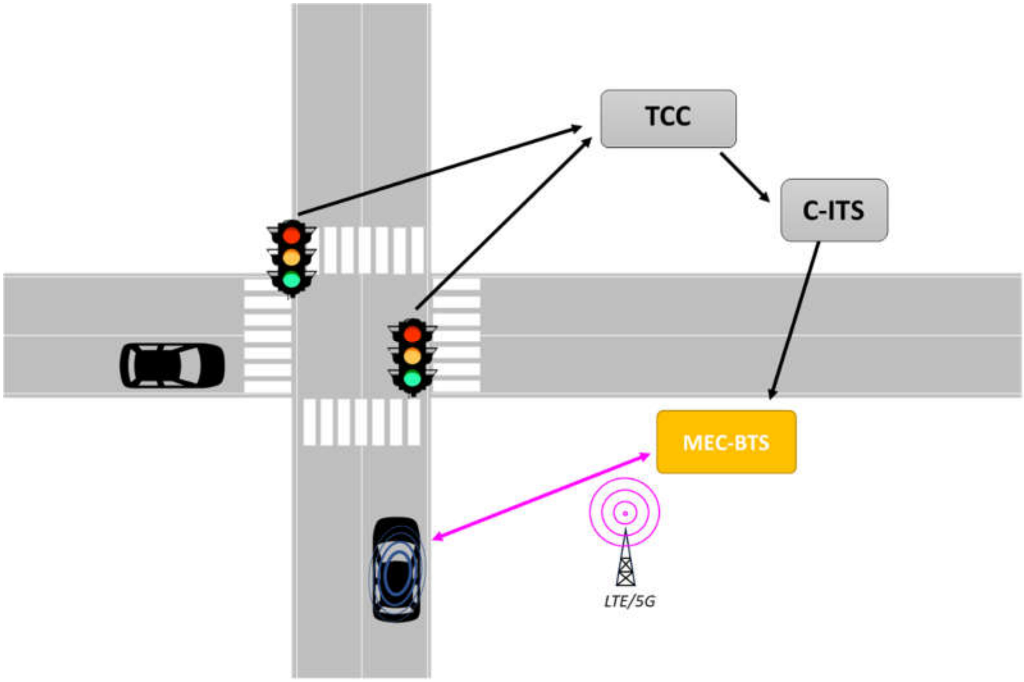

Figure 42 - Communication View of the GLOSA use case (City of Verona)

6.5.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

6.6 Scenario 3.3: Lane merging in Autostrada del Brennero, Italy

This scenario focuses on the CAV exiting from a gas station and merging into the highway lane. The objective of this scenario is to demonstrate that the ICT4CART infrastructure can ease the lane merging of the CAV with information that cannot be retrieved by the CAV itself using its on-board sensors.

The ICT4CART infrastructure identifies the incoming vehicles monitoring the highway lanes with cameras and collecting the information from CAMs sent by the connected vehicles. The information about the incoming vehicles and their dynamics is organised in an EPM and the ICT4CART infrastructure provides this information using the CPM that is in course of standardisation by ETSI in the Technical Specification 103 324. The CAV on the entrance ramp can adjust its driving action based on the information contained in the CPM.

The ICT4CART infrastructure also provides active road safety applications that can alert the CAV of collision risk using DENM based on the information present in the EPM.

6.6.1 Functional View

An overview for the functional view is provided in Figure 43 and each component implemented in the scenario is detailed in the following.

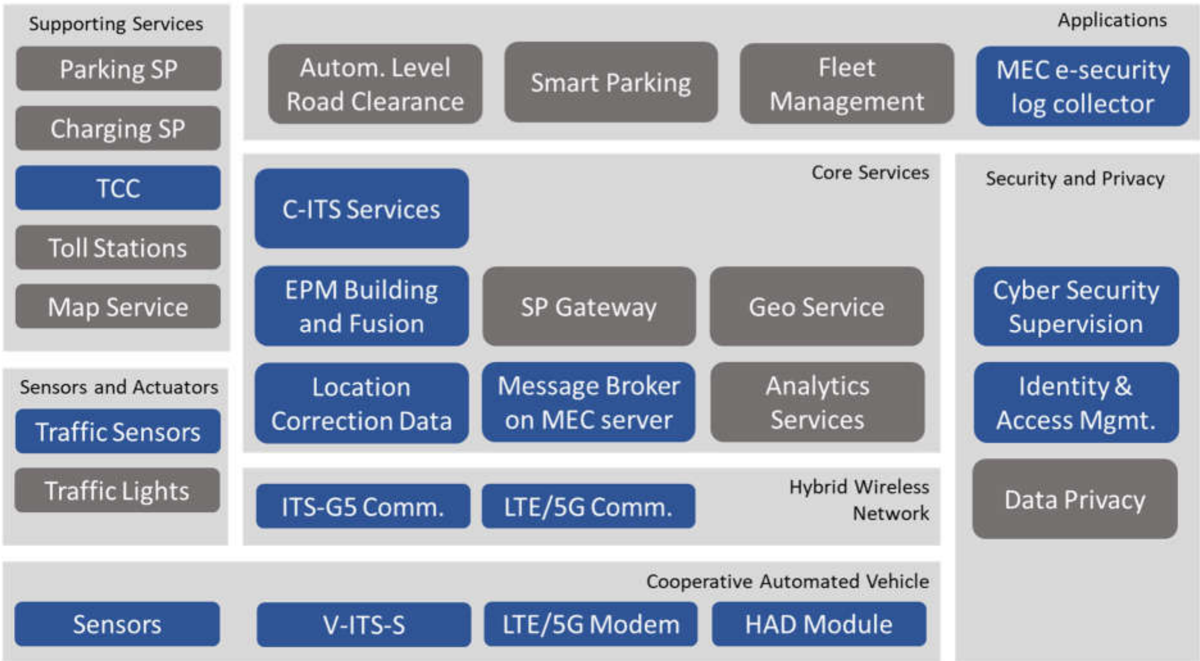

Figure 43 - Functional view - SCN 3.3 - Overview

TCC: The Traffic Control Centre manages the highway, monitors its status and validates the generation of security relevant C-ITS messages.

Traffic sensors: A camera is used to sense the environment of the highway lanes in order to detect the incoming vehicles.

C-ITS-Services: Decentralised Environmental Notification Basic Service (DENBS), Collective Perception Service (CPS), Cooperative Awareness Basic Service (CABS).

EPM Building and Fusion: An EPM is built based on the information gathered by the road-side sensors. The information of the EPM will be provided to all connected actors through the CPS.

Message broker on MEC server: A publish/subscribe approach is used to disseminate C-ITS messages via the LTE/5G communication link using a custom Message Broker that runs on the MEC server. C-ITS services publish the C-ITS messages on the Message Broker, and the vehicles can subscribe to specific topics in order to receive messages of interest in the MEC server's relevant geographical area.

Location Correction Data: To allow precise positioning of the CAV, the Location Correction Data function provides correction data for GNSS data by using either physical reference stations or network-based ones.

ITS-G5 Communication, LTE/5G communication: ITS-G5 and LTE/5G communication are used to provide a hybrid communication approach to disseminate C-ITS messages.

LTE/5G communication: The information from the C-ITS-S and message broker can be communicated using LTE/5G.

Sensors: In-vehicle sensors of the AV include Radar and cameras, which are the basis to compute the vehicle's own internal EPM for general automated driving purposes.

V-ITS-S: With the V-ITS-S, the vehicle is enabled to send messages (e.g. CAM) and receive messages from the infrastructure or other vehicles, e.g. CPM, SPAT(EM), MAP(EM), DENM via ITS-G5.

LTE/5G Modem: Via the LTE/5G modem in the vehicle, the ITS messages can also be sent and received via LTE/5G.

HAD Module: The HAD module will be adapted to additionally use the information provided by the infrastructure, in order to fulfil the use case (merging into the motorway lane) safely and efficiently. The CAV, considering the information contained in the CPM and DENM messages, can revise its AD level and/or speed.

Identity and Access Management: The Identity and Access Management service will provide authentication and authorisation for ITS-S which need to access ITS communications and services.

Cyber Security Supervision: The supervision centre will receive logs from participating vehicles mainly coming from C-ITS messages authentication.

MEC e-security log collector: This application receives the logs about cyber-security events from the CAV and it forwards them to the Cyber Security Supervision centre.

In Figure 44, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

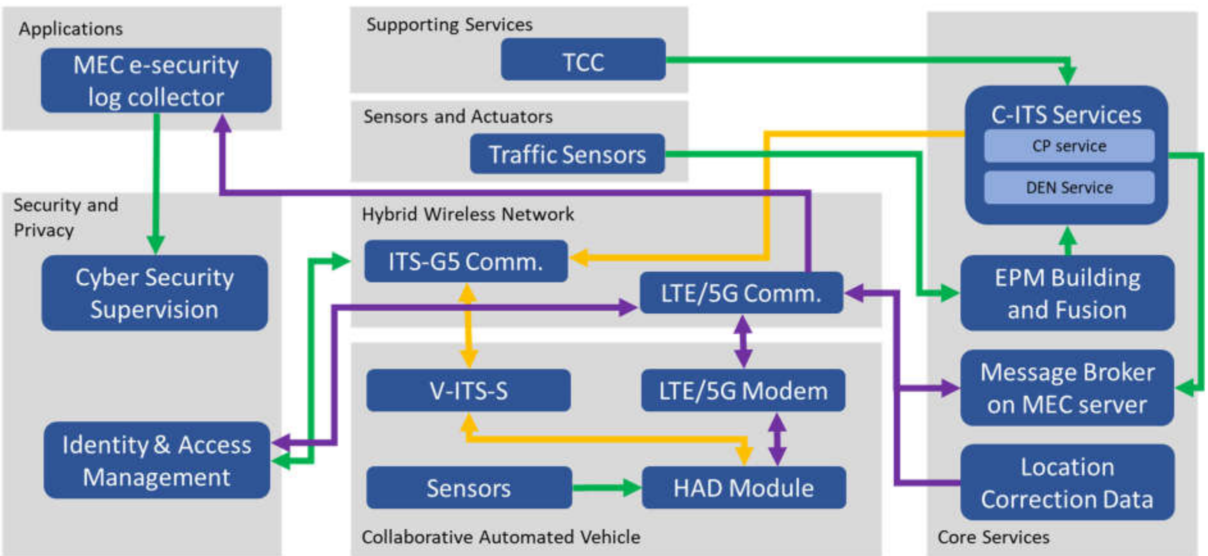

Figure 44 - Functional view - SCN 3.3 - Details

6.6.2 Data / IT Environment View

In this scenario, only the data flows 1 to 5 of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 45):

1. Cameras located close to the lane merging area send the gathered raw data to the RSU, which processes the images to detect the road actors present, and connected vehicles broadcast CAM messages that are collected by the RSU.
2. RSU broadcasts on the ITS-G5 communication channel the relevant C-ITS messages.
3. The RSU provides to the C-ITS services running on the MEC server the relevant collected information retrieved from the video processing (e.g., positions, speeds and directions of

vehicles) and by the processing of received CAM.
4. C-ITS services running on the MEC server send C-ITS messages via the LTE/5G communication channel.
5. TCC sends information about security relevant events to the DENBS.

The C-ITS services (i.e., DENBS, CPS) can run either on the RSU or on the MEC server. An objective of this scenario is to test different possibilities and to understand which the best solution is.

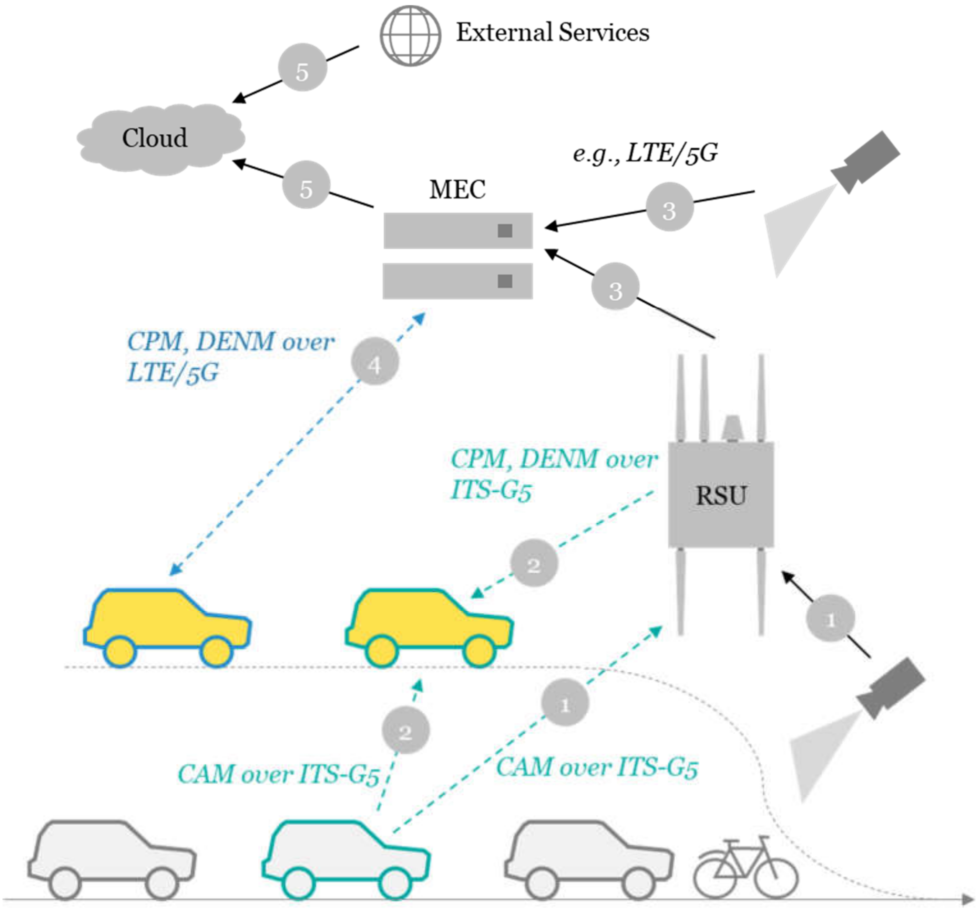

Figure 45 - Common Data Flows across ICT4CART Use Cases from D3.3 [4]

The following table lists the relevant standards for the data that will be transmitted in this scenario:

	Data Type	Relevant Standards
Provided by the IT Environment	Environment perception models (EPMs)	EPMs are sent using Collective Perception Messages (CPM) as specified in ETSI TS 103 324 [6] No specific standards are present for building the EPMs.
	Decentralised Environmental Notification data	DENM as specified by ETSI EN 302 637-3 v1.3.0 [14]
	Cooperative Awareness information	CAM as specified by ETSI EN 302 637-2 v1.4.0 [10]
Consumed by the IT Environment	Cameras data used for building EPMs	Video flows based on H.264 or other standard video codec and Real Time Streaming Protocol (RTSP)

6.6.3 Communication View

The C-ITS messages DENM and CPM are sent on the ETSI ITS-G5 communication link and also on the LTE/5G communication link to implement the hybrid communication approach.

The following C-ITS services are included in the communication view of this scenario:

- The CPS creates an EPM based on the information processed from the cameras' data and on the information extracted from the CAM of the connected vehicles and it broadcasts a CPM containing this information;
- The DENBS broadcasts a DENM of hazardous events defined exploiting information received from the TCC and/or from the RSU.

A custom Message Broker, that is based on a publish/subscribe approach, is implemented to provide C-ITS messages on the LTE/G5 communication link. The Message Broker is executed on the MEC server. C-ITS services (either running on the MEC server or on the RSU) publish the generated messages and the vehicles can register to the topics of interest for receiving via LTE/5G the relevant messages as soon as they are available.

The RSU is in charge to broadcast C-ITS messages on the ITS-G5 link. The RSU subscribes to the relevant topics to retrieve the C-ITS messages generated by C-ITS services running on the MEC server and to broadcast them on the ITS-G5 link.

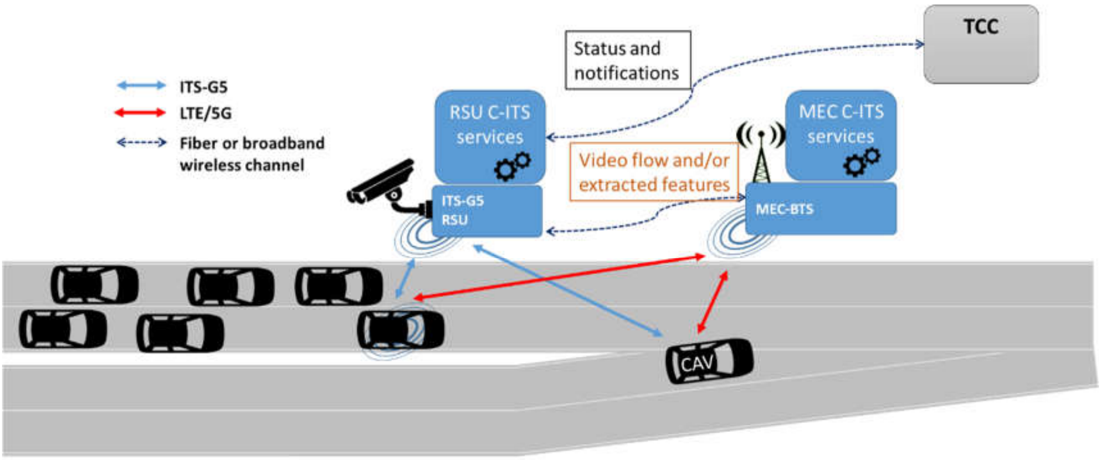

Figure 46 - Communication View - SCN3.1b Virtual mirror to "see" surrounding traffic in city of Verona, Italy

6.6.4 Cyber-Security & Privacy View

The authentication of C-ITS messages will be performed using the PKI provided by the ICT4CART infrastructure and considering the relevant ETSI standards.

In real conditions, the supervision centre will be implemented by receiving logs from the vehicle OBU. A lab session will be organised during which the supervision centre capabilities will be demonstrated. To do so, the vehicle OBU will send logs mainly related to C-ITS message authentication. Logs will be partially simulated in order to mimic cyber-attacks and to illustrate their detection by the supervision centre. The simulations will concern the transmission of C-ITS messages with wrong security information, such an incorrect signature or certificate.

7 Cross-border Test Site Architecture

This chapter outlines the architecture of the Cross-border test site and is split into subsections for the two scenarios that will be demonstrated. A detailed description of the use cases and scenarios can be found in the deliverable D2.1 [2].

For each scenario, the functional view, the data/IT environment view, the communication view, as well as the cyber-security & privacy view, are presented based on the detailed descriptions in D3.1 to D3.4 [1,3-5].

7.1 Scenario 4.1: Cross border interoperability between Italy-Austria (dynamic adaptation of vehicle automation level) at Brenner border

The Cross-border scenario is designed in partnership between the Austrian and Italian Test Sites, both the infrastructure of the Austrian motorway and Italian motorway are involved in the scenario. The location for this scenario is the Brenner border between Austria and Italy. As described in the Deliverable D2.1 [2], the solution in this scenario is based on the hybrid communication exploiting the communication channel of ETSI ITS-G5 and the communication channel through LTE/5G.

To guarantee an extensive interoperability in this use case, a cross-project team was involved in the alignment with the C-ROADS Italy project [21]. This is due to the tremendous effort to implement an interoperable Message Broker between the European countries. C-ROADS accepted to provide the Message Broker instance for the Italian side, which will be deployed in the Cloud. Then, ICT4CART should concentrate on the demonstration of interoperability between the countries with hybrid communication channels. Both ETSI ITS-G5 and LTE/5G will be used to provide a seamless and continuous communication to the vehicles which are crossing the border.

The definition of the scenario will be further refined during the second phase of the project.

7.1.1 Functional View

Figure 47 shows the function blocks used for this scenario in the Cross-border test site. Unused modules are greyed out.

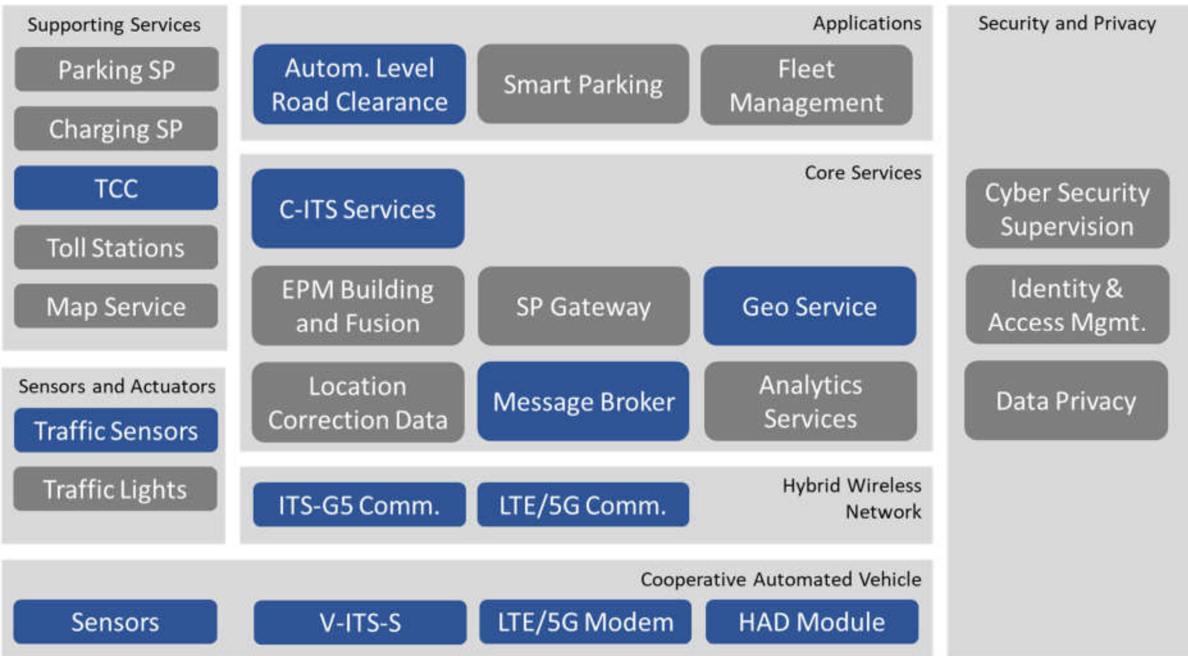

Figure 47 - Functional view - SCN 4.1 - Overview

From the **Supporting Services** group, only the **TCC** is used which will provide information to the **C-ITS Services** and the **Automation Level Road Clearance** application.

From the **Sensors and Actuators** group, **Traffic Sensors** will provide the TCC with information. This applies to both countries.

From the **Applications** group, the **Automation Level Road Clearance** application utilises static and dynamic information to determine and prescribe a clearance for a road section and a specific automation level. A human operator can override the actual clearance, if required, before it is distributed. ASFINAG has recently analysed its entire road network with reference to the ISAD classification scheme [20] which determines how strongly a given road section can offer support for automated driving.

From the **Core Services** group, the following functions are in use for the Cross-border test site:

- **C-ITS Services** generate IVI messages with their automated vehicle container to transmit the SAE level clearance and DEN messages to transmit information about accidents or wrong way drivers.
- The **Geo Service** will be used by the CAV to get information about the appropriate Message Broker for its current position respectively for its planned route.
- The **Message Broker** will be used to provide CAVs with messages of interest based on geographical location. There will be one Message Broker for Austria, deployed on a MEC infrastructure and one Message Broker for Italy provided by C-ROADS Italy. The CAVs will subscribe to map tiles based on their location and/or planned route to receive relevant C-ITS messages.

The **Hybrid Wireless Network** will consist of **ITS-G5** roadside units located on the ASFINAG road infrastructure and of **LTE/5G** communication technology provided by Magenta.

The **CAV** will use an on-board LTE/5G and ITS-G5 unit to establish a continuous communication channel with the infrastructure. With that, it will receive SAE level clearance messages, get GNSS correction data for its current position, and subscribe to map tiles based on its location and/or planned route. Based on the received information, the CAV shall inform the driver about the availability of SAE level 2/3 functions. Moreover, it warns the driver to take over the steering wheel due to changes in the traffic/weather/other conditions, earlier than without the infrastructure's messages to improve the driver experience and comfort. The CAV may be equipped with other measurement techniques and safety equipment to collect relevant data and grant road safety. However, these equipment and techniques are not related or connected to the ICT4CART infrastructure.

In Figure 48, the utilised functions from the overall reference architecture are shown with their interactions. Purple lines show paths for data that are sent or received via LTE/5G, while yellow lines show paths for data that are sent or received via ITS-G5. Note that this does not mean that these connections are wireless, it just represents the flow of the corresponding data. Green paths are for data that are agnostic of a particular communication channel.

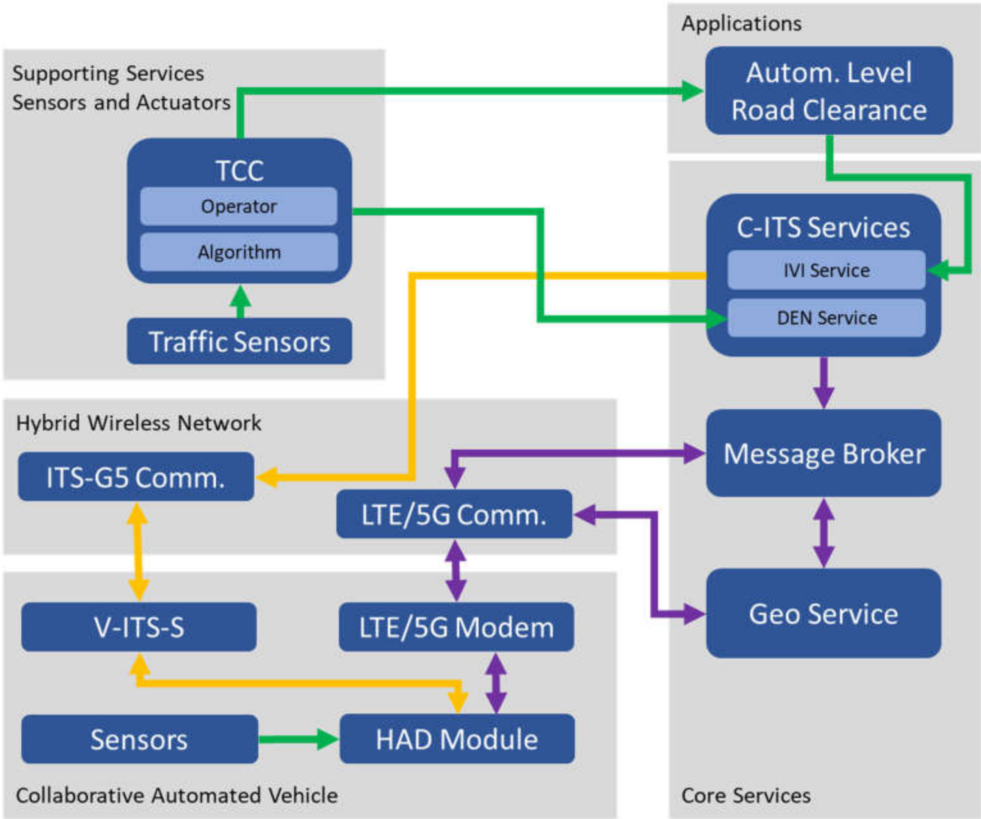

Figure 48 - Functional View - SCN 4.1 - Details

7.1.2 Data / IT Environment View

In this scenario, the following data flows of the overall data and IT environment architecture (cf. D3.3 [4]) are used (see also Figure 49):

1. Sensors submit data to the TCC about the current traffic situation, e.g., positions, speeds and directions of road users detected by sensors.
2. Information about special traffic situations (e.g. accidents or traffic jams) and general automation level recommendations is provided to a Central ITS Station for the dissemination by Roadside ITS Stations using ITS-G5 and to a Message Broker for subscribers using LTE/5G.
3. C-ITS messages are distributed to RSUs based on a selection algorithm considering both the positions of the RSUs and the relevance areas of the messages to be disseminated. The Message Broker can be seen as an RSU covering the whole dissemination area of the C-ITS system.
4. Vehicles equipped with ITS-G5 communication modules receive IVI and DEN messages directly from RSUs along the roadside.
5. Vehicles equipped with LTE/5G communication modules and AMQP clients can subscribe for the same messages on the Message Broker. Filtering will be able by message type and geographic location.
6. Vehicles equipped with ITS-G5 send own messages like CAM or DENM that can be received by other vehicles and RSUs.
7. The C-ROADS Italy Message Broker will subscribe for C-ITS messages from the Austrian Message Broker to disseminate them to vehicles connected to the Italian Broker only.

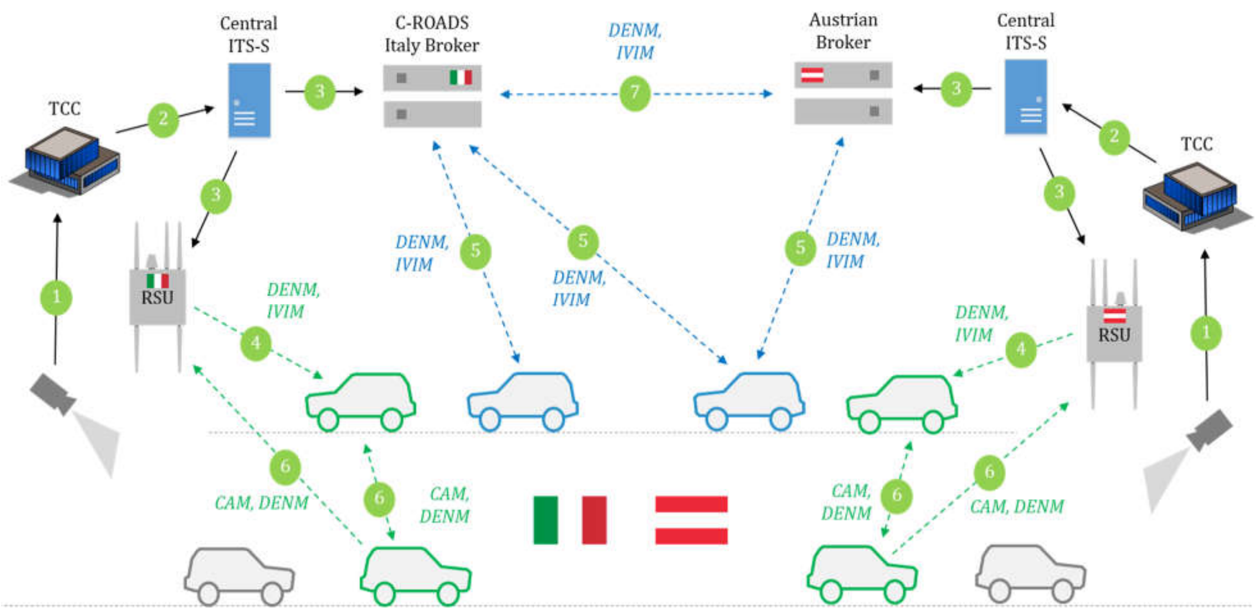

Figure 49 - Data / IT Environment View of the Cross-border Test Site

The following table lists the relevant standards for the data that will be transmitted in this scenario:

Data Type		Relevant Standards
Provided by the IT Environment	Situations and events (e.g., accident, road closure, etc.)	DENM as specified by ETSI EN 302 637-3 V1.3.1 [15]
	In-vehicle information (e.g., speed limits, SAE level recommendation)	IVIM as will be specified by ISO/TS 19321:2020 [12]
	Correction data for GNSS-based localisation	ETSI TS 103 301 [7]
	IP based Basic Interface (BI) between C-ITS actors	Specification for interoperability of backend hybrid C-ITS communication by WG2 Technical Aspects / TF 4 Hybrid Communication of the C-ROADS platform V1.5 [17]
Consumed by the IT Environment	Data received from vehicles either directly or indirectly through RSUs	CAM as specified by ETSI EN 302 637-2 V1.4.1 [11]
	IP based Basic Interface (BI) between C-ITS actors	Specification for interoperability of backend hybrid C-ITS communication by WG2 Technical Aspects / TF 4 Hybrid Communication of the C-ROADS platform V1.5 [17]

7.1.3 Communication View

In the Cross-border test site, hybrid communication is used extensively. The infrastructure provides information (encoded in C-ITS messages) to the vehicles via two communication channels: ITS-G5 (ad-hoc network) and LTE/5G (cellular network). Figure 50 shows the possible communication paths.

For the cellular communication link to the vehicles, the information will be published onto an AMQP message broker deployed on a MEC server. Vehicles will be able to subscribe for specific messages in relevant geographic areas.

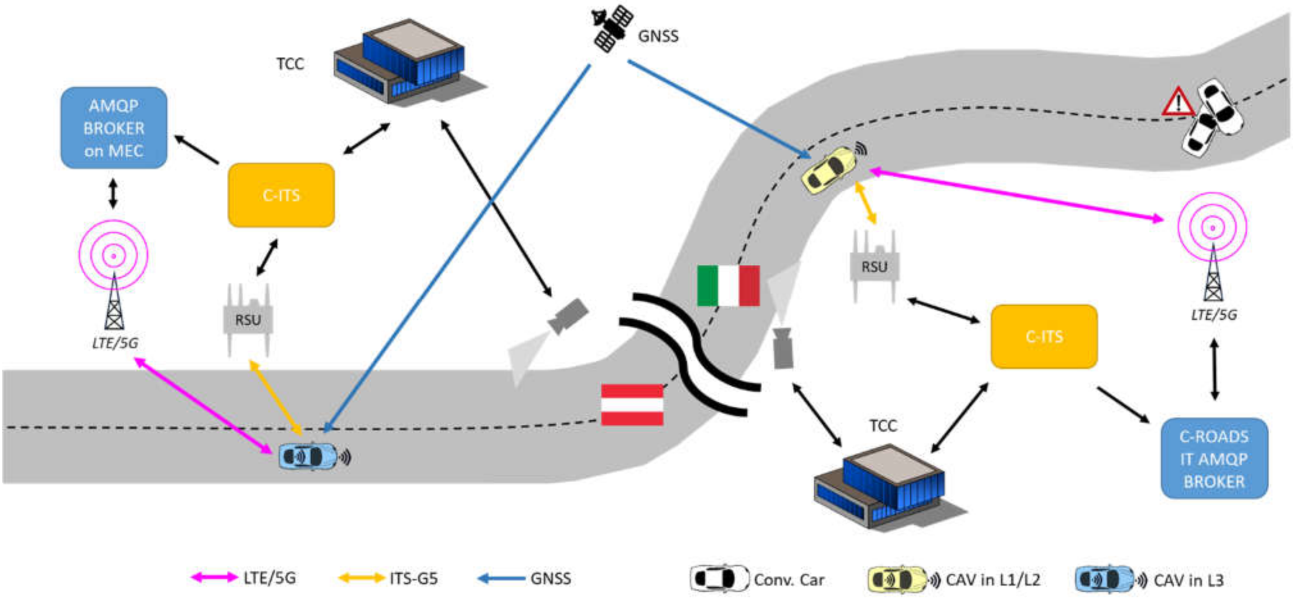

Figure 50 - Communication View of the Cross-border Test Site

7.1.4 Cyber-Security & Privacy View

In this scenario, the Cyber-Security and Privacy components are purely conceptual and will not be implemented.

7.2 Scenario 3.4: Precise positioning in urban and highway location

For the precise positioning scenario to be demonstrated in the Cross-border test site at the Brenner border between Austria and Italy, the same architecture as described in Section 4.2 will be used.

8 Interoperability

By adapting the ICT4CART Reference Architecture to the specific needs of the Test Sites, the resulting individual architectures remain interoperable, which is outlined below based on one example per use case.

8.1 Analytics Services

Example of interoperability in UC1 "Smart Parking and IoT Services" in Ulm and Verona.

As described in D5.1 and in Figure 51, the IT-Environment, and in consequence also the analytics framework, is designed so that it operates the same way both in Ulm and Verona, even though the implementation of UC1 has various differences in the two involved test sites.

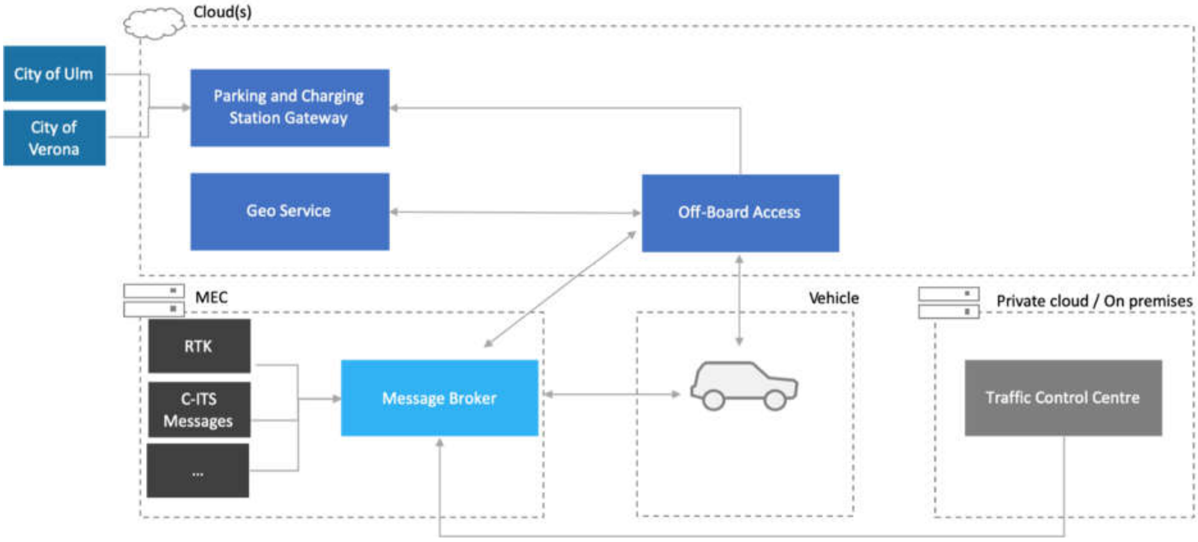

Figure 51 - ICT4CART IT Environment and Data Exchange Services Component View

The Similarities and differences for UC1 in the involved test sites are:

- Both cities provide parking data to the "Parking and Charging Station Gateway".
- The gateway processes data that are then available for consumption from OEM clouds.
- In Ulm both parking availability and parking prediction data will be consumed from the OEM cloud.
- In Verona only parking availability will be consumed from the OEM cloud.
- In both test sites the OEM cloud takes care of communication with the vehicle in a secure and safe way (via the "off-board access" component).

8.2 Ad-hoc Communication

Example of interoperability in UC2 "Dynamic adaptation of vehicle automation level based on infrastructure" in Graz and Trento.

Short range ITS-G5 is used in all test sites of the project. The technology is either already part of the existing test site infrastructure or it will be implemented within the framework of the project. Its implementation follows the existing European standards and profiles, guaranteeing technology interoperability in all pilots.

For example, in UC2, the roadside units of the ICT4CART infrastructure will broadcast standard ETSI messages (DENM, IVIM and CPM), with information about traffic situations and the driving environment, using ITS-G5 in the Austrian (Graz) and Italian (Trento and Verona) test sites. All the vehicles equipped with ITS-G5 communication modules will be able to receive these messages directly from the RSUs along the roadside. Thanks to this information, the CAV will refine its driving action, adapting the automation level (e.g. downscaling or even disengaging automation).

In addition, the utilisation of a combination of this ad-hoc network with cellular communication will ensure the achievement of the required levels of redundancy, reliability, and network availability, necessary to realise cross-border interoperability.

8.3 Precise Positioning

Example of interoperability in UC3 “Intersection crossing (urban) & lane merging (highway) – “virtual mirror” in Germany, Austria and Italy.

The Precise Positioning solution is using physical RTK in Ulm and network based RTK with different correction sources in Austria and Italy. The interoperability is reached by distributing the correction information on a common way via the MEC server.

8.4 Hybrid C-ITS using an AMQP Message Broker

Example of interoperability in UC4 “Cross border interoperability between Italy-Austria (dynamic adaptation of vehicle automation level) at Brenner border.

The implemented Message Brokers for the exchange of messages between the road infrastructures and the vehicles follow the recommendations of the C-ROADS Platform. The message broker used in Italy is provided by C-ROADS Italy [21] and will use the Basic Interface (BI) as described in the Specification for interoperability of backend hybrid C-ITS communication [17] to retrieve C-ITS messages from Austria. The same BI will be used by the AMQP clients implemented in the test vehicles to subscribe to C-ITS message from both message brokers.

9 References

[1] "ICT4CART Reference Architecture", ICT4CART deliverable D3.1. May 2019.

[2] "Specification of Use Cases", ICT4CART deliverable D2.1. February 2019.

[3] "Flexible Networks Specifications and Architecture", ICT4CART deliverable D3.2. August 2019.

[4] "IT Environment Specifications and Architecture", ICT4CART deliverable D3.3. August 2019.

[5] "Cyber-security and data privacy Specifications and Architecture", ICT4CART deliverable D3.4. August 2019.

[6] ETSI TS 103 324 (under development): "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Specification of the Collective Perception Service".

[7] ETSI TS 103 301 V1.3.1 (2020-02): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

[8] DATEX II Specification, https://datex2.eu/support/downloads

[9] Open Mobility Vocabulary (MobiVoc), https://www.mobivoc.org

[10] ETSI EN 302 637-2 V1.4.0 (2018-08): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[11] ETSI EN 302 637-2 V1.4.1 (2019-04): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[12] ISO/TS 19321:2020 (under development): "Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures" [12]

[13] ETSI EN 302 637-3 V1.2.2 (2014-11): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service"

[14] ETSI EN 302 637-3 V1.3.0 (2018-08): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service"

[15] ETSI EN 302 637-3 V1.3.1 (2019-04): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service"

[16] RTCM 10403.3 (2016-10): "Differential GNSS (Global Navigation Satellite Systems) Services"

[17] "Specification for interoperability of backend hybrid C-ITS communication", (2019-07), C-ROADS platform specification V1.5, WG2/TF4 Technical Aspects/Hybrid Communication

[18] ETSI TS 101 556-1 V1.1.1 (2012-07): "Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Electric Vehicle Charging Spot Notification Specification"

[19] ETSI EN 302 637-3 V1.2.1 (2014-09): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service"

[20] Erhart, J., Harrer, M., Rührup, S., Seebacher, S., Wimmer, Y. (to appear). "Infrastructure support for automated driving: Further enhancements on the ISAD classes in Austria." Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

[21] C-ROADS Italy Project, https://www.c-roads.eu/pilots/core-members/italy/Partner/project/show/c-roads-italy.html