Grant Agreement Number: 768953

Project acronym: ICT4CART

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

D.2.1

Specification of Use Cases

Due delivery date: 28/02/2019

Actual delivery date: 15/03/2019

Organization name of lead participant for this deliverable: ICCS

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:	D.2.1
Deliverable responsible:	ICCS
Workpackage:	WP2
Editor:	ICCS

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Panagiotis Lytrivis	ICCS	panagiotis.lytrivis@iccs.gr
Vasilis Sourlas	ICCS	v.sourlas@iccs.gr
Visintainer Filippo	CRF	filippo.visintainer@crf.it
Amendola Danilo	CRF	danilo.amendola@crf.it
Test side leaders and SCN leaders.		

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
v0.1	24/01/2019	Template version	V. Sourlas (ICCS)
v0.2	22/02/2019	Document consolidation	V. Sourlas (ICCS)
v0.3	27/02/2019	UULM modifications	M. Buchholz (ICCS)
v0.4	28/02/2019	ASFINAG modifications	G. Allmer (ASFINAG)
v0.5	02/03/2019	First finalizing for general review	A. Adaktylos (ASFINAG)
v0.6	03/03/2019	Second finalizing for general review	G. Allmer (ASFINAG)
V0.7	05/03/2019	ATE review	M. Dirnwöber (ATE)
V0.8	13/03/2019	CRF review	D. Amendola (CRF)
V1.0	15/03/2019	Final version for submission	V. Sourlas (ICCS)

Abstract
This deliverable, entitled "Specification of Use Cases", is to set the scene, where the project will actively contribute. It begins with an analysis of the current status of the four test sites and goes from the defined use case instances (called "scenarios") to the definition of functional and non-functional requirements. The defined requirements will serve as input to the following project work such as specification and definition of its architecture, and subsequently to the development work.

Legal Disclaimer

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

Abbreviations and Acronyms

Acronym	Definition
AD	Automated Driving
API	Application Programming Interface
AV	Automated Vehicle
AVC	Automatic Vehicle Classification
AVI	Automatic Vehicle Identification
CAM	Cooperative Awareness Messages
CCTV	Closed Circuit Television
C-ITS	Cooperative Intelligent Transport Systems
COU	City of Ulm
CPM	Collective Perception Message
DENM	Decentralised Environmental Notification Message
ETSI	European Telecommunications Standards Initiative
FCD	Floating car data
GLOSA	Green Light Optimized Speed Advisory
GNSS	Global Navigation Satellite System
IAM	Identity and Access Management
ICT	Information and Communication Technology
ITS	Intelligent Transport System
LIDAR	Light detection and ranging
LoRaWAN	Long Range Wide Area Network
LTE	Long Term Evolution
MAP	Mobile Application Part
MAPEM	MAP (topology) Extended Message
MEC	Mobile Edge Computing
OBU	On Board Unit
PGI	Parking Guidance and Information (Verona)
RIS	Roadside ITS Station (both 802.11p and eG PP C-VCX)
RSU	Road Site Unit
RTCM	Radio Technical Commission for Maritime Services
RTK	Real Time Kinematics
SCN	Scenario
SPG	Service Provider Gateway
SPATEM	Signal Phase and Timing Extended Message
TLA	Traffic Light Assistance
TLC	Traffic Light Controller
TMC	Traffic Management Centre
TTG	Time To Green
UC	Use Case
V2I	Vehicle to Infrastructure
VDS	Video Detection System
VMS	Variable Message Sign
VRU	Vulnerable Road User

Table of Contents

Executive Summary

The purpose of this deliverable is to set the scene, where the project will actively contribute. It begins with an analysis of the current status of the four test sites (Austria, Germany, Italy, and cross border site), and goes from the defined use case instances (called "scenarios - **SCN**") to the definition of functional and non-functional requirements. The defined requirements will serve as an input to the following project work such as specification and definition of its architecture, and subsequently to the development work.

ICT4CART use cases were carefully selected based on specific criteria. These are: *i*) alignment with EU policy 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 and 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 can be global or local, can be associated with network slices or not, can use Edge Clouds/Computing or not, can use different radio technologies and can be used everywhere (roaming aspect). They also consider mechanisms for cyber-security, authentication, integrity and privacy. The following Use Cases (UCs) will be implemented to validate and demonstrate ICT4CART developments: **UC1**) Smart Parking & IoT services, **UC2**) Dynamic adaptation of vehicle automation level based on infrastructure information, **UC3**) Intersection crossing (urban) & lane merging (highway) – "virtual mirror", **UC4**) Cross Border Interoperability.

For each of the UCs, the project focuses on several representative traffic situations, called "scenarios" hereinafter, which demonstrate the influence of the project outcome to the most critical traffic conditions in matters of safety and performance. For each scenario, the realisation prerequisites, the required physical and digital equipment, are considered. Throughout that process, a comparison of the current technological level with the ICT4CART potential upgrades is inevitable.

Moreover, considering the story (the sequence of actions) for each one of the scenarios, a concise list of the functional requirements is completed. The way that the ICT4CART components should perform and interact with each other in order to provide the specific functionalities can then be defined. The outcome is a catalogue of non-functional requirements. In this document, the term non-functional requirements, is used to describe the requirements that ensure the correct operation of the ICT4CART components in the system, e.g., performance, operation conditions, scalability requirements etc. Ensuring that the scenario based catalogue of requirements is concise, a mapping can then be performed with the ICT4CART components of a high-level architecture in WP3.

1 Introduction

1.1 Aim of the project

Today, significant and rapid advances in both telecom and IT industries can be accredited to fast-growing disruptive technologies. Amongst these, the ETSI ITS-G5 technology appears to be quite mature. Moreover, the LTE/5G technology is evolving rapidly, while LTE-Vehicle (LTE-V) features low cost and rapid deployment since it can utilize existing LTE technology. In the light also of the above, several ICT challenges related to connectivity, data management, cyber-security and ICT infrastructure architectures still play a significant role and need to be addressed in order to enable road vehicle automation. Thus, it is of utmost importance for the vehicle automation to work on the direction of advancing the digital and ICT infrastructure, taking also into consideration the limitations in both resources and investments, in the physical transport infrastructure.

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 localization. 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

Instead of working with generic solutions with questionable impact, ICT4CART builds on four specific high-value use cases (from both urban and highway environments), aligned with the EU strategy and policy, which will be demonstrated and validated under real-life conditions at the project test sites in Austria, Germany, Italy and across borders (Italy-Austria). This document provides a description of the examined UCs and their instances (SCNs) to be deployed in each involved test site. Also, a first analysis of their functional and non-functional requirements is presented. Reassuring that the scenario based catalogue of requirements is concise, a mapping can then be performed with the ICT4CART components of a high-level architecture in WP3.

1.3 Intended readership

This deliverable is addressed to any interested reader (i.e., PU dissemination level), who wishes to be informed of the various Use Cases and their corresponding Scenarios that are going to be examined in the course of the ICT4CART project, and that will be the means for the project to accomplish its main goal to design and implement a versatile ICT architecture to enable the transition towards higher levels of automation (up to L4).

2 ICT4CART test sites

ICT4CART will perform various demonstration events in the four involved sites, where the corresponding Use Cases and Scenarios will be tested. Below a short presentation of each site is provided.

2.1 Austrian Test Site

The Austrian Test Site includes 20km of A2 motorway between “Laßnitzhöhe” and City of Graz (see Figure 1).

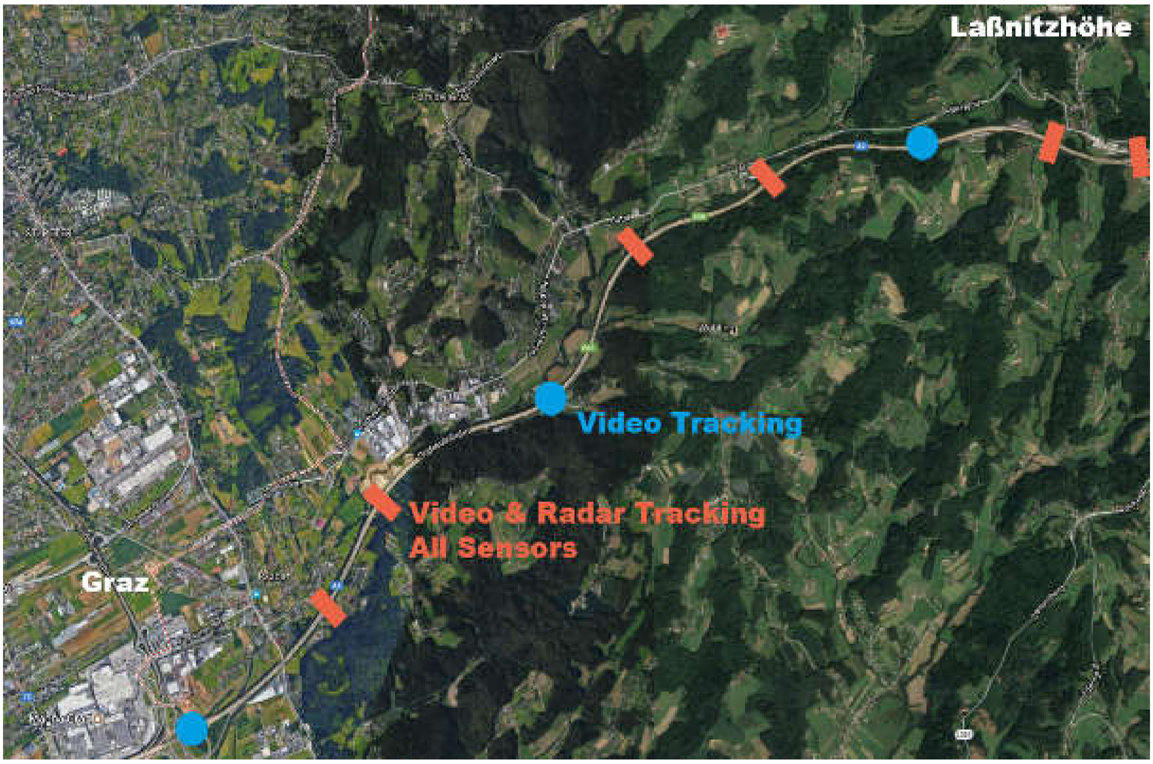


Figure 1: Map of the Austrian Test Site

The test site is equipped with C-ITS road-side units (VMS information, road works warnings, and other event information), video cameras (traffic management, single vehicle detection), single-vehicle counters, and environmental sensors. It enables testing of ITS-G5 short range communication, cellular communication, LTE-V and real time communication with the traffic control centre. The infrastructure is based on a fibre-optic network that provides IP-based network connectivity to gantries.

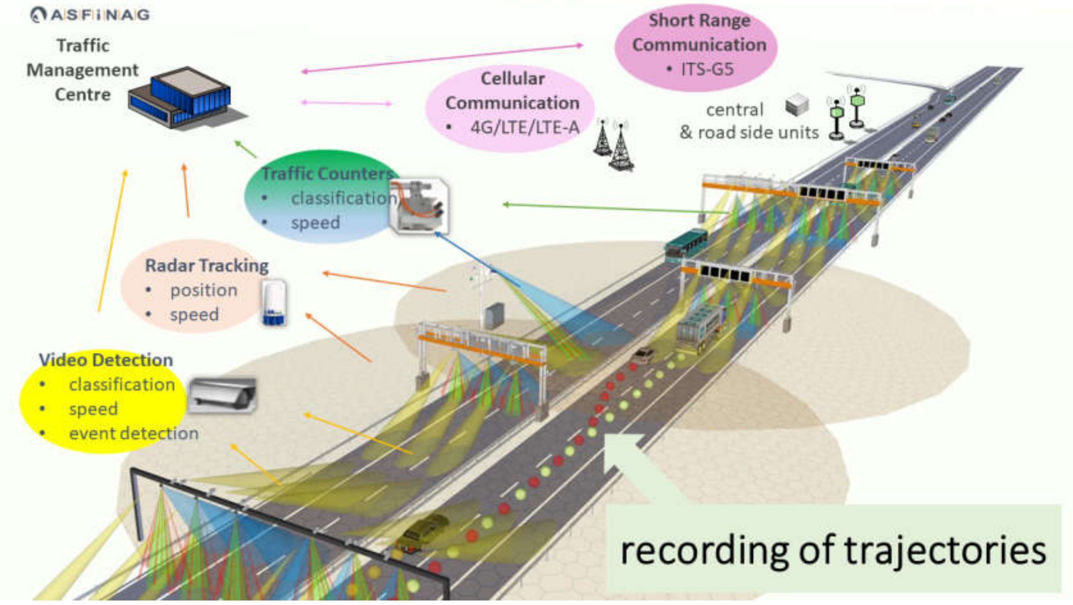


Figure 2: Austrian Test Site digital infrastructure

The intention is to provide the testing party with the complete precise trajectories of the tested vehicleand of all surrounding vehicles for each test run. The data can be played back via a 3-D simulation tool. This is achieved by segmenting the test track in the way depicted in Figure 3.

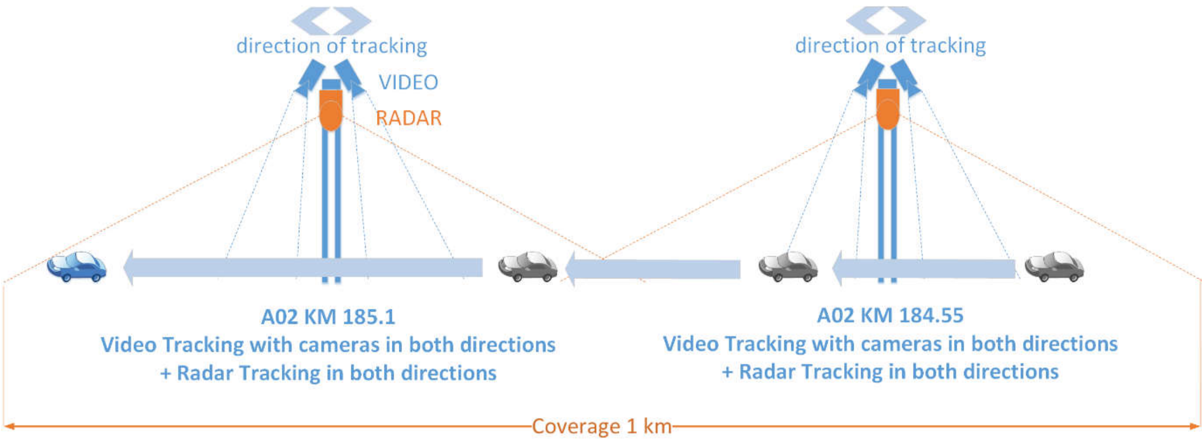


Figure 3: Austrian Test Site setup segment

The Austrian Test Site provides a test framework for the testing of the distributed IT environment and the flexible network architecture in ICT4CART. In the project, the Austrian Test Framework will be used with partner SWARCO for ITS-G5 and with partner T-Mobile for 4G/LTE.

Concerning the connectivity interfaces the following are valid for the Austrian s:

- For ITS-G5 testing, the interface is the C-ITS-Station, providing 802.11p specification ECo-AT Release 3.6. Industry has been testing against this specification from 2013 through 2016 in Phase 1 of the ECo-AT Living Lab. It is the newest available ITS-G5 standard. It provides a CAM and a DENM interface.
- For ITS-G5 V2V testing, the interface is in the vehicle.
- For 4G/LTE the interface is the cloud API, called "ASFINAG CONTENT DATEX II interface", providing DATEX II 2.3 in dedicated data channels, as documented on www.datex2.eu, DEPLOYMENTS, DII PROFILE DIRECTORY. It is the newest available DATEX II standard. It is in live operation providing ASFINAG's central traffic control centre with real time data for every

day traffic management. For data into the vehicle, it provides a RESTful API for IT clouds to connect to. The API is approved by the CEF DATEX II group of the European Commission and is published along with all the implementation details.

- For 4G/LTE FCD (Floating Car Data) from vehicle to infrastructure, the receiving infrastructure can make use of DATEX II 2.3, or of proprietary JSON formats.
- For 4G/LTE LTE-V testing, the interface is the 4G/LTE base station.

2.2 German Test Site

The German Test Site is located in the City of Ulm and its surrounding area. In Figure 4, an exemplary selection of possible roads for the testing are highlighted. The coverage of the 4G/LTE test network of NOKIA, including the corresponding 5 radio sites, is indicated as additional information.

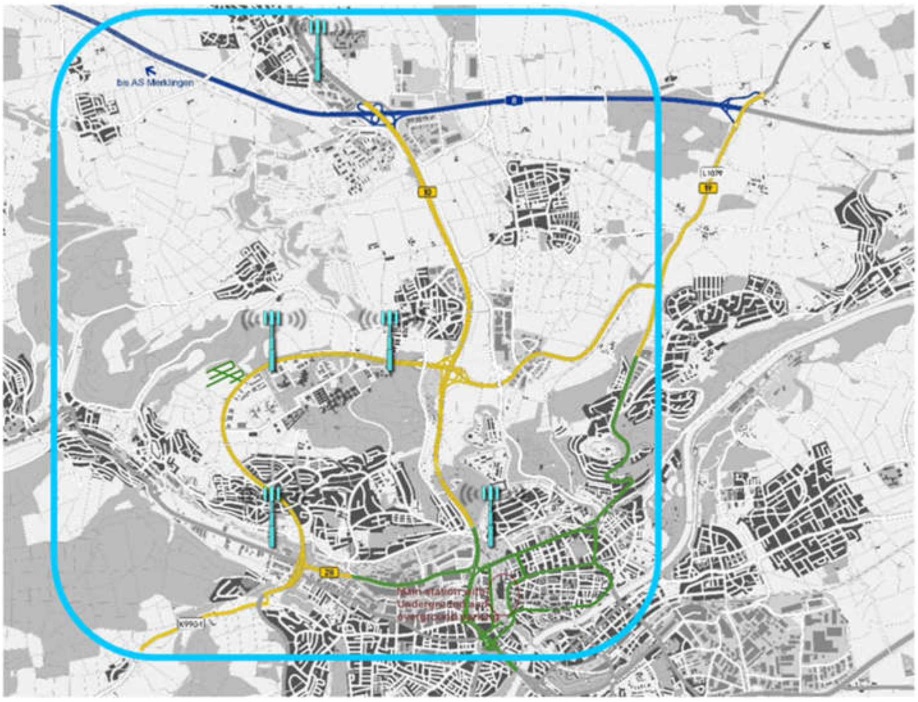


Figure 4: City of Ulm; blue: motorway (Autobahn A8), yellow: rural roads, green: intra-urban roads, light blue: radio sites and coverage

Several over ground and underground parking garages, as well as on-street parking in the inner city are included in the Ulm site. With respect to smart parking, ICT4CART will probably concentrate on an over ground parking garage near the main station.

NOKIA's test network is available from Autobahn A8 to inner city, covering many types of roads from motorway to small inner city side streets. The intersection for the intersection crossing use case is the crossing Loher Str. and Mähringerstr in Ulm-Lehr. Precise localization will be shown in the area of the NOKIA mobile test network.

The seamless integration of different communication technologies (ITS-G5 and 5G/LTE) in infrastructure will be also shown at one traffic light crossing (probably crossing Berliner Ring and Talstraße/Albert-Einstein-Allee).

The available equipment at the German Test Site is highlighted below:

- An LTE cellular test network with MEC server in the northern parts of Ulm operated by NOKIA;
- Two infrastructure sensor units operated by University of ULM, comprising:

  - two laser scanners on each sensor unit,
  - two stereo camera units on each sensor unit,
  - a common central data acquisition and data processing for both units, and
  - a communication unit for cellular networks, connected to the NOKIA mobile test network.

  The sensor units are located at a crossing in the suburb Ulm-Lehr, where the line of sight entering on a main road from a side road is highly limited by a residential house very close to the corner of the crossing (see Figure 5). These sensors were built up within the project MEC-View funded by the German Federal Government.
- Two fully automated (L4) research vehicles. Each vehicle is equipped with:
  - RTK-DGPS reference systems,
  - several sensors (LiDAR, RADAR, cameras, etc.) for environmental modelling,
  - CAN logging,
  - LTE communication already available,
  - ITS-G5 to be included within the course of the project.
- Parking guidance system for parking garages with open interfaces operated by the City of Ulm (COU).
- Access to charging station occupancy information operated by a daughter-company of the City of Ulm.

The COU also operates all traffic lights within the city borders, of which one will be equipped with communication means for traffic light status communication to connected vehicles by SWARCO during the project. For the development of (predictive) algorithms, also historical parking data is available.

Figure 5: The crossroad in the City of Ulm to be used in ICT4CART Use Cases, with the currently installed sensors and cameras

2.3 Italian Test Site

The Italian Test Site includes the City of Verona and the A22 motorway. Among the several cities, the A22 motorway runs across the city of Verona, where ICT4CART plans a C-ITS test site in urban environment.

For this reason, one of the main topics of the Italian Test Site will be on how to tackle connected and automated driving passing from motorway to an urban scenario and vice-versa. The service provision across motorway and city will be obtained through a harmonised infrastructure. It is important to note that the Municipality of Verona is already interfaced with the cloud server at the moment. Wind-Tre will provide the LTE cellular network with MEC server capabilities to be integrated into the Italian Test Site according to the ICT4CART infrastructure architecture. LINKS will provide the on-board units which are offering hybrid connectivity compliant to the ICT4CART architecture and will develop MEC servers dedicated to vehicle safety. Finally, CRF will provide two vehicle prototypes (one connected and automated, and one connected).

The test site will focus on the junction between the urban and motorway environment, in particular the entrance/exit ramps from the motorway main road near Trento and the entrance to the city of Verona. Gas stations along the motorway are also being considered within the A22 motorway use cases. In Verona, the test site will face smart parking, GLOSA services and the "Virtual Mirror" use cases.

A22 Motorway

The toll road A22 (Autostrada del Brennero), itself is in existence since 1974 and is operated by A22 - Autostrada del Brennero S.p.A company. It is a 314 km long Italian highway running from Brennero to Modena. A 9 km stretch along the motorway, south of Trento, is specifically equipped with C-ITS systems. The motorway has 2 lanes per direction, plus a so-called dynamic third lane, opened in case of extraordinary traffic conditions. Thanks to C-ROADS[1], the test site is equipped with 48 RSUs from Brennero to Modena and features C-ITS Day 1[2] services via ETSI ITS-G5.

Within ICT4CART, the test site will host two use cases: dynamic adaptation of vehicle automation level, which focuses mainly on the road stretches before and at the exits from the motorway (to toll or gas stations), and the lane merging, which focuses on the entrance to the main roads.

Dynamic adaptation of vehicle automation level on Trento motorway will focus on the motorway exit ramp to a toll station. The vehicle that is approaching the exit ramps is advised with a traffic jam warning, and it can then downscale automation level according to the traffic conditions. In addition, ICT4CART infrastructure could advise the connected vehicle on which toll lane to approach, considering both traffic information provided by the infrastructure and dynamic information relative to the toll stations. This information includes, for example, which ones are opened or which ones accept certain payment methods. Currently, A22 is verifying which data can be provided.

LINKS will provide the cameras (and possibly LIDAR) detection service and a MEC infrastructure with notification messages (DENM) over LTE and the RSU communication system over ETSI ITS-G5.

[1] https://www.c-roads.eu/platform.html

[2] https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

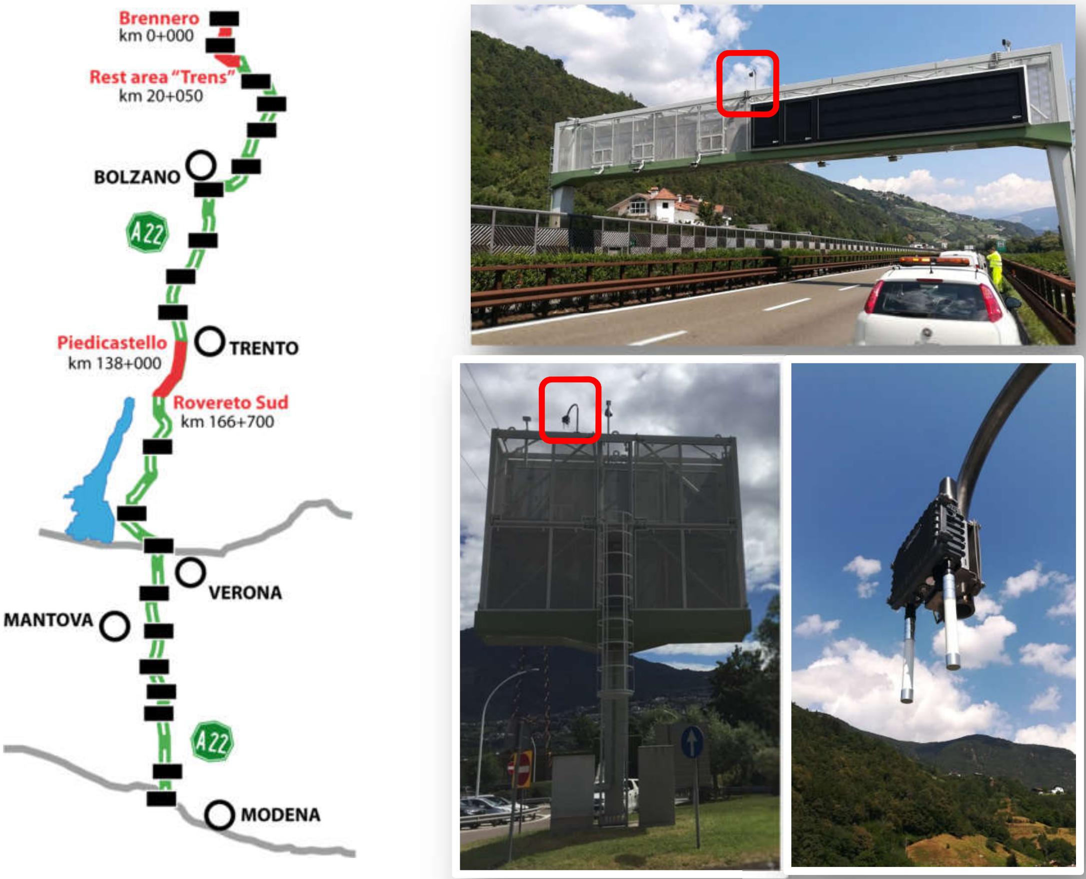


Figure 6: Map of the Italian Test Site, C-ITS infrastructure (RSU locations) and road view of A22 motorway

A22 hosts the hardware and facilitates the installation; it can provide power supply and data connection. Possible additions in ICT4CART that will be considered along the development of the use case are:

- Wrong-way driving application;
- Detection of occupied lanes at the toll or gas stations;
- MAP messages delivery with respect to the exit ramp or the toll station via V2X infrastructure;
- A connection to Verona or to a local MEC server for infrastructure based applications.

With regards to the maps of the exit ramps or the toll stations, A22 can provide digital mapping, since it hosts the place where the trial is made. From this input, local MAP messages could be generated by LINKS. Alternatively, CRF can make measurements via RTK to construct new maps.

Figure 7: Map and panoramic view of Trento Centro A22 exit to be used in ICT4CART

Lane merging in Autostrada del Brennero concerns the entrance ramp to the motorway main carriageway. LINKS camera (and possibly LIDAR) monitors incoming vehicles (collision threats), which is an add-on to C-ROADS infrastructure. A potential issue is the DENM messages from infrastructure that bear too little information to be effective for the automation. LINKS will use for this purpose the Collective Perception (CPM) ETSI message, which is a new message type in the process of standardization. LINKS will evaluate to present the results of the experimentation to the ETSI CPM working group, possibly giving feedback about the use of CPM messages.

With regard to the A22 test site, the following upgrades are to be done in the course of ICT4CART and the needs of the corresponding Use Case:

- Data connectivity along A22 and location;
- 4G video stream to Wind-Tre MEC server, and connection to A22 C-ITS-RSU. Field of view requirements for the camera detection;
- MEC on RSU directly, instead of Wind-Tre MEC (4G latencies issue);
- MAP messages for topology: precise geographic data may be available for toll stations.

The equipment available at the A22 motorway is:

- 5 roadside stations (RIS) for V2I communication;
- 48 roadside stations (RSU) from Brennero to Modena featuring C-ITS Day 1 services via 802.11p (C-ROADS infrastructure);
- Legacy road sensors and service centre;
- Full cellular network coverage in the C-ITS interested area.

In addition, CRF can support the test site with GNSS RTK precise position system, i.e.:

- Rover station that can be installed on vehicle prototypes;
- Portable base stations that can send RTK correction via radio modem (RTCM protocol) to the rover;
- In alternative to radio modem, IP connection between vehicle rover station and internet to retrieve RTK from local planning services.

City of Verona

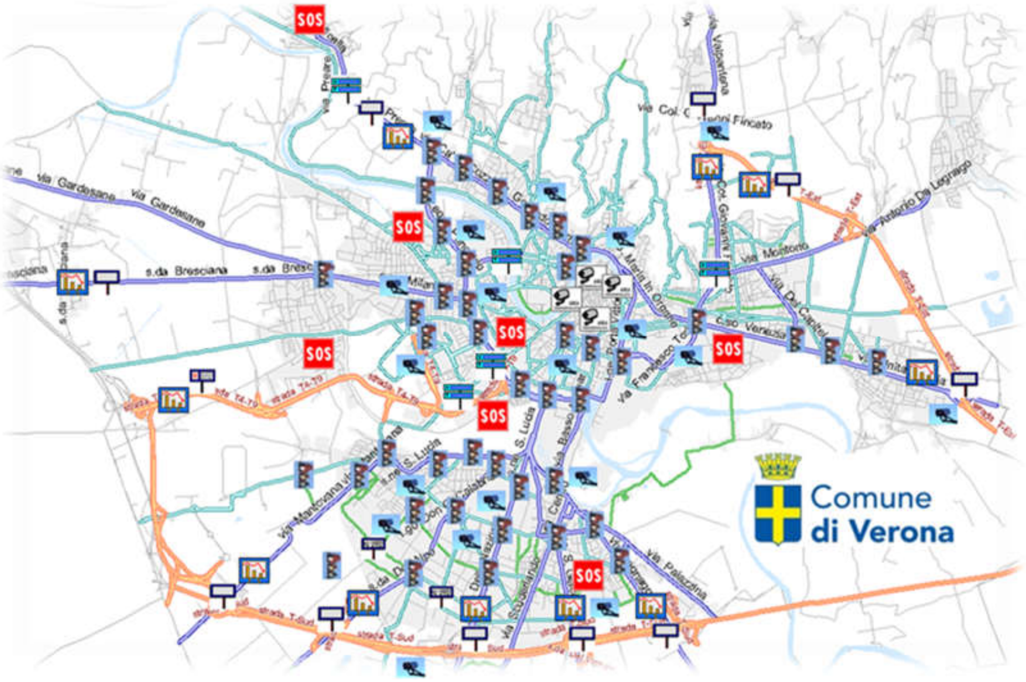


Figure 8: Map of the Italian Test Site – City of Verona and A22 motorway

Verona is a city in the Veneto region of northern Italy. The Verona use cases will mainly regard two scenarios: smart parking and urban crossing considering signalized intersections.

Concerning **smart parking,** currently 13 lots are monitored in order to inform the drivers about the availability of free slots. Experiments in ICT4CART will address surface parking, where management and ticketing system are present and the GNSS signal is available for vehicles. Currently, single places are not monitored. A possible add-on in ICT4CART can regard the integration of LoRa gateway to parking sensors. The gateway would gather sensors' availability input on the spaces and then output the data to the parking service that can inform the clients with the precise coordinates of the single parking slot. Most likely, the test site could be in Porta Nuova where an outdoor parking is located. Single place monitoring system can be implemented in this location. Porta Nuova is also close to the mapped traffic lights site that is in Via Città di Nimes. CRF will provide a vehicle OBU that connects to 4G/LTE cellular network to retrieve updated parking information. The focus will be on connectivity and precise positioning aspects, in order to move towards possible future in-vehicle application and to get accurate parking information from city infrastructure, potentially applicable to automated vehicles.

With respect to the state of the art, the Parking Availability Service could be handled by a MEC server by Wind-Tre. Thus, minimizing latency, SWARCO provides data and MEC is used as a communication gateway. The area of the parking lot has to be mapped and sharing map information is an open point.

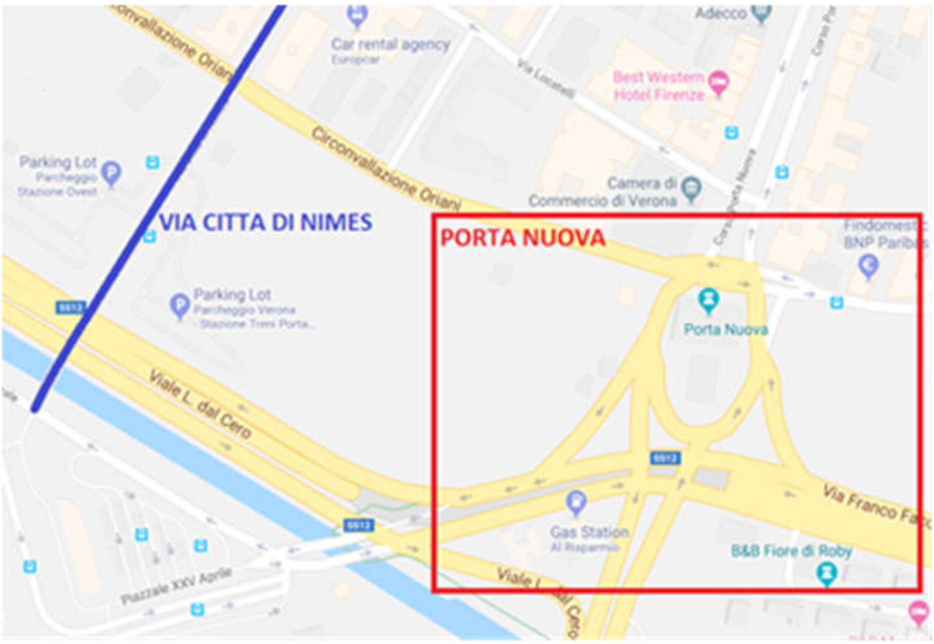


Figure 9: View of the Verona potential site

In the **GLOSA/intersection related** use cases (**Dynamic adaptation of AD level, Intersection Crossing, Virtual mirror**), the RSUs installed are currently placed within the central area of the city covering the main arteries entering the city. The pilot site is also equipped with state-of-the-art backend systems able to deliver dynamic traffic light information (GLOSA) for all signalised intersections operating in the city. The infrastructure will inform the vehicles with real-time speed advice to cross the intersection in front with a green light on. It also delivers all kinds of traffic data that could be used within specific advices, reducing incidents by warning drivers about queuing traffic in blind spots, or dangerous situations ahead. In ICT4CART, Verona will extend its current RSU infrastructure, integrating SWARCO GLOSA with Wind-Tre MEC server, and test new use-cases related to virtual mirror thanks to the cooperation with LINKS (providing OBUs and MEC applications) and CRF (providing vehicles). Possible additional infrastructure systems could come from LINKS (MEC RSU with vision and depth sensors at intersections) for the virtual mirror use case and possibly also a prototype of a connected bicycle.

In summary, the equipment currently available in the City of Verona (CDV) is:

- 142 connected traffic lights stations, of which 62 are centralised, with more than 600 sensors on the territory;
- RSU ITS-G5;
- AVI: Automatic Vehicle Identification - 13 electronically controlled ways to control goods access and bus paths. All the events are managed by operators and sent to info mobility channels (social networks, web, SMS, etc.);
- In the Control Room, special platforms for integration like the “City Supervisor” allow monitoring of more data sources and representing them on a map;
- PGI: Parking Guidance and Information – a parking identification system;
- AVC: Automatic Vehicle Classification - 13 traffic stations for 24h traffic data collection;
- VMS: 7 variable message panels in restricted access areas, 13 panels to access urban areas, 6 for internal road network, 52 electronic panels to parking directions;
- SOS: 13 SOS columns + 1 emergency lay-by in the new underpass “Galtarossa”;
- VDS: Video Detection System - 32 CCTVs on road network.

2.4 Cross-border Test Site (Austria-Italy)

This is not a totally new test site, but it originates form coupling parts of the Italian Test Site and the highway on the Austrian side of the border, which has similar equipment to the Austrian Test Site described above. In Figure 10, the map of this test site is illustrated, with the cross-border being highlighted by a dark red box.

The capabilities and the equipment of this test site are included in the Austrian and Italian Test Sites description above. The goal of this test site is the implementation and testing of UC4 Cross-border interoperability (see section below for details).

Figure 10: Map of the cross-border Test Site

In the A22 hybrid approach, solutions based on ETSI ITS-G5 technology are combined and integrated with solutions based on mobile network technologies using a cloud-based solution.
ETSI messages are distributed through the TCP-IP stack, relying on the network infrastructure offered by the providers, to make the service available even in areas not directly covered by the G5.
The transport of ETSI messages takes place in ASN.1 UPER binary coding (represented in HEX) on AMQP protocol adopted for real-time communication in the creation of telemetry services and B2B applications.
The hybrid communication architecture foresees three players:

- the producer (typically a virtual RSU), delivering messages
- the consumer (typically the OBU, but also OEM or SPs Clouds), subscribing and receiving messages
- the broker: acting as a mediator and redistributing to consumers the messages obtained by the producers.

The Day-1 services presently available from the A22 path, according to the C-Roads specifications (both in Hybrid-LTE and in ETSI-G5 mode), are Road Works Warning (emergency Lane Closure, Transit Lane Closure, Overtaking Lane Closure and Exit Lane Closure), Other Hazardous Location Notification (Weather Condition Warning, Traffic Jam Ahead, Stationary Vehicle, Accident Zone, Obstacle on the Road), In-Vehicle Information (Other Signage Information, Embedded VMS Free Text, Dynamic Speed Limits Information).

3 ICT4CART Use Cases (UCs)

3.1 UC1 - Smart Parking & IoT services[3]

According to the European strategy for connected and automated mobility[4], parking services (belonging to Day 1.5 list) are a priority in the next period. ICT4CART, in total alignment with this EC communication, addresses parking service. An important aspect that will be investigated in this use case is the link to fleet management and relevant IoT services (e.g., self-refuelling, self-washing). These are closely related with automated parking services, e.g., parking the vehicle outside of the train station and the vehicle drives on its own to get charged or refuelled.

Scenarios (SCNs) of UC1 to be developed in ICT4CART (More details in Section 4)

- **SCN1.1: Smart Parking and IoT Services in City of Ulm, Germany (*SPIoTULM*).**
  This SCN will be led by **BMW**.
  Smart parking in the City of Ulm and fleet management with respect to mobility hubs (e.g., near a main station) and mobility demands as in car/ride sharing. Integrating also IoT services like charging/refuelling in combination with parking.
- **SCN1.2: Smart Parking and IoT management in City of Verona, Italy (*SPIoTCDV*).**
  This SCN will be led by **SWARCO**.
  On-street parking management will be implemented and tested in the city of Verona, based on SWARCO/City of Verona infrastructure. The reception of useful information to end-users (vehicles) will be demonstrated on CRF connected vehicles.

3.2 UC2 - Dynamic adaptation of vehicle automation level based on infrastructure information

The main goal of this use case is to enable comfortable and safe automated driving for SAE Level 3/4 vehicles. Generally speaking, the sensor range of a highly automated vehicle is extended with real-time information from the road infrastructure (e.g., traffic density, roadworks) using cellular and/or ad-hoc communications. This enables the automated vehicle to take decisions before reaching a potential critical situation and handover the control to the driver or come to a safe stop if needed. This is important both for the safety of the driver and passengers of this highly automated vehicle, and for enhancing the comfort features offered by L3 & L4 automated vehicles.

Scenarios (SCNs) of UC2 to be developed in ICT4CART (more details in Section 4)

- **SCN2.1: Dynamic clearance, adaptation and handover of vehicle automation level at special conditions in Graz (*DAVAGRZ*).**
  This SCN will be led by **BOSCH-H**.
  A vehicle driving with an active automated driving function L3 on the highway encounters a restricting condition and the function hands over to the driver, thereby performing an adaptation from L3 to L2. The function uses a data stream from the highway infrastructure to detect restricting conditions as early as possible in order to initiate an early in-time handover procedure.

[3] Even if cyber security mechanisms are described in every scenario, only the scenario SCN1.1 will be implemented with cyber security capacities. Cyber security descriptions in the other scenarios remain at a conceptual stage.

[4] COM(2016)766: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility.

- **SCN2.2: Dynamic adaptation of vehicle automation level on Trento motorway (*DAVATRN*).**
  This SCN will be led by **CRF**.
  The attention is focused on the exit ramp and on the approach of the vehicle to the toll station. Thanks to the information from the ICT4CART infrastructure, the connected and automated vehicle 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 disengaging automation).
- **SCN2.3: Dynamic adaptation of vehicle automation level in Verona, Italy (*DAVACDV*).**
  This SCN will be led by **CRF**.
  ICT4CART infrastructure monitors an urban intersection and is in charge to detect road users. The ICT4CART infrastructure communicates with the vehicle so that the second can adapt its behaviour to avoid dangers and possible collisions with other vehicles or vulnerable road users (VRUs) as pedestrians and bicycles.

3.3 UC3 - Intersection crossing (urban) & lane merging (highway) – "virtual mirror"

Intersection crossing and lane merging is one of the most challenging use cases and of significant importance, considering the increased frequency of traffic accidents in such situations. Deploying automated vehicles of L3 & L4 can significantly reduce those accidents while maintaining traffic efficiency. The intention here is to exploit hybrid connectivity and MEC to create a 360° awareness around the vehicle with very low latency, creating a kind of "virtual mirror" to support the automated vehicle while crossing an intersection or merging into a lane. Seamless integration of cellular networks and ITS-G5 in the infrastructure, e.g., on communicating traffic lights, to support all connected vehicles regardless of the communication interface, as well as precise localisation fusing GNSS with cellular network corrections, are key aspects of this use case.

This use case deals with both urban and highway environments. The goal of ICT4CART in this use case is to enable the crossing of the intersection and/or the lane merging in an automated way involving mixed traffic.
Scenarios (SCNs) of UC3 to be developed in ICT4CART (more details in Section 4)

- **SCN3.1: Virtual mirror to "see" surrounding traffic in urban environment**
  - **SCN3.1.a: In City of Ulm, Germany (*VMULM*)**
    This SCN will be led by **UULM.**
    Exploit hybrid connectivity and MEC to create a 360° awareness around the vehicle with very low latency, creating a kind of "virtual mirror" to support the automated vehicle while crossing an intersection. This "virtual mirror" consists of an environmental model of all road users at the intersection. The model is communicated to connected automated vehicles to improve their awareness of road users at the intersection.
  - **SCN3.1.b: In City of Verona, Italy (*VMCDV*)**
    This SCN will be led by **LINKS** (former ISMB)**.**
    An urban intersection in city of Verona is monitored by the ICT4CART infrastructure that is in charge to detect road users, to predict their dynamics and to broadcast an environment model of the road users present in the intersection, i.e., indicate the presence and position of road users that are in the intersection and where they are going.
- **SCN3.2: GLOSA (Green Light Optimized Speed Advisory) in City of Verona, Italy (*GLOSA*).**
  This SCN will be led by **SWARCO**.
  An urban intersection is monitored by the ICT4CART infrastructure. When a connected and

automated vehicle is approaching the intersection, based on the vehicle position, the infrastructure sends information regarding the time to the next green phase and on the optimal speed to maintain to reach it.

- **SCN3.3: Lane merging in Autostrada del Brennero, Italy (*LMBRE*).**
  This SCN will be led by **LINKS** (former ISMB)**.**
  The connected and automated vehicle is merging into the highway lane and it needs to avoid collisions and not to impede vehicles that are incoming on the highway lane. The intersection in monitored by the ICT4CART and the relative information is provided to the vehicle.
- **SCN3.4 Precise positioning in urban and highway location (*PPRTK*)**
  This SCN will be led by **NOKIA**.
  Precise Positioning will use standard GNSS (e.g., GPS) combined with correction information based on the Real Time Kinematic (RTK) technique in order to enhance the precision of positioning in rural environment, but also in more complex areas like urban environment (e.g., multi-path propagation).

3.4 UC4-SCN4.1 - Cross border interoperability between Italy-Austria (dynamic adaptation of vehicle automation level) at Brenner border (*DAVAXBR*)

The target of this use case is to test and demonstrate the cross-border interoperability and functionality of the developed ICT4CART infrastructure. In one country, an automated driving function may be using information received from the ITS-G5 network, while the neighbouring country may be using information from the cellular network. The purpose is to show that while crossing the border, the operation of this function is kept uninterrupted, due to the ICT4CART infrastructure capabilities. The initial idea is to test in this use case the accurate localisation while crossing the border, since this is one of the basic elements for supporting all automated driving use cases. However, this use case will be further elaborated, and instances of SCN2.1 will be demonstrated at the Cross-border Test Site too.

This UC and the corresponding SCN is led by **ASFINAG.**

4 ICT4CART Scenarios

In this section, more details per Scenario are provided. In general, ICT4CART will develop and demonstrate precise Urban UCs in Ulm Germany and City of Verona Italy, precise Highway UC in Italy, and low level Highway UCs in Italy and Austria.

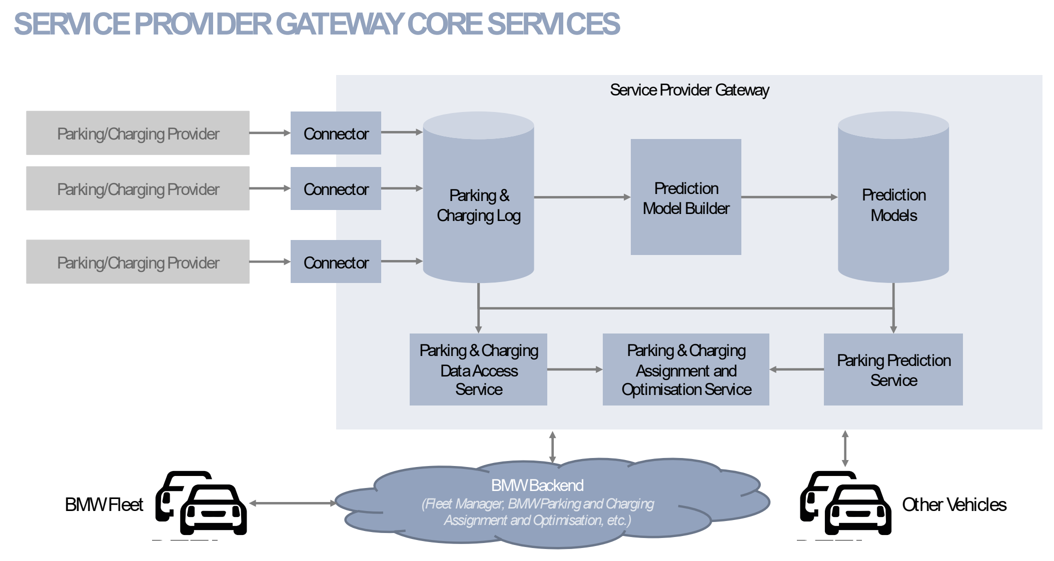
4.1 SCN1.1 - Smart Parking and IoT Services in City of Ulm, Germany

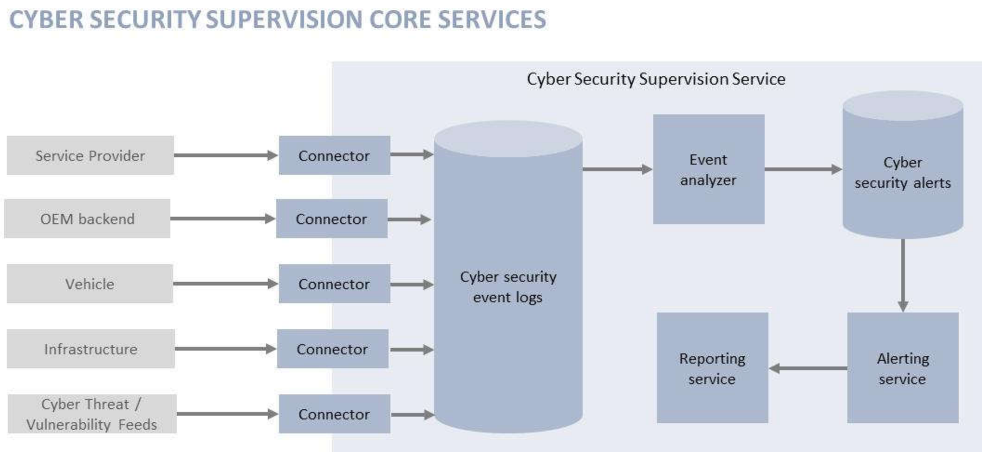
Name	**Smart Parking and IoT Services in Ulm, Germany**
Short name	**SPIoTUL**
ID	**UC1-SCN11-SPIoTULM**
Overview (abstract)	Smart Parking enables Fleet Managers to intelligently and securely relocate fleet vehicles by processing parking data from city or third-party providers. This requires a common data format and interface for seamless bilateral communication between, e.g., the Automotive OEM Cloud (Fleet Manager) and Service Provider Clouds, along with communication authentication and encryption. The interface will be specified along the development of the ICT architecture and it will be agreed on a common data exchange format. Furthermore, there will be developed a middleware

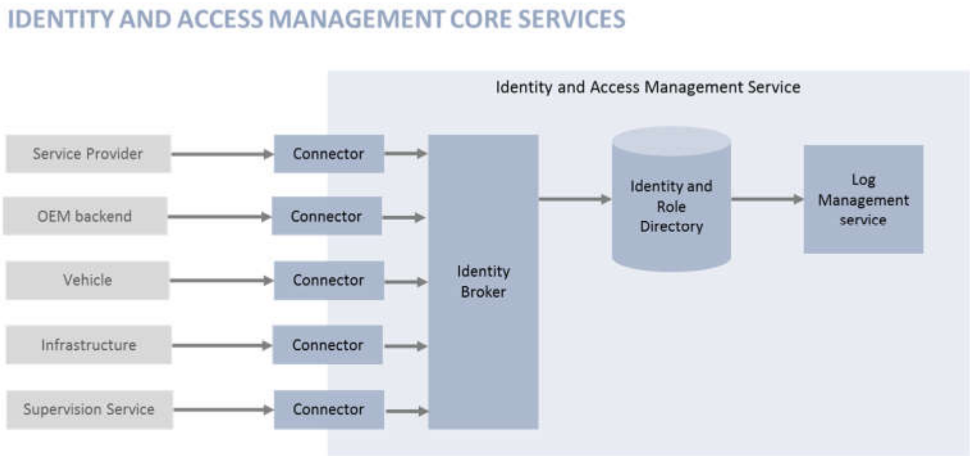
	with the provisional name "Service Provider Gateway". The Service Provider Gateway (SPG) enables e.g., automotive OEMs to communicate with providers offering parking or charging information or other services without knowing the interface or data format of every single provider. The Service Gateway Provider handles the communication between providers or OEM Clouds as well as necessary data transformations to satisfy the specified interface requirements for seamless communication. Also, it enables OEMs to get predictions for parking space availability in a specific area and time frame. It will also be possible that vehicles get assigned to certain parking spaces by the SPG, hence the algorithms and models within the gateway decide which vehicle gets assigned to which parking space.
Description	**1: One vehicle gets "sent to park and charge", another one will only be parked** The Fleet Manager checks the status of all fleet cars. It decides that one car needs to get charged. Based on the knowledge of demand prediction for that area it knows that the car should be parked there to immediately serve the demand. Subsequently, the Fleet Manager requests via the specified secured interface parking space information for that area from a parking service provider. The Fleet Manager receives the parking data. Based on the data it knows that parking spaces in that area that are available and those that also provide charging facilities. Hence, the car gets sent to that parking space to charge and minimize pickup time for customers. Another fleet car, gets relocated to the parking space but is not charged, since battery life is sufficient and possible immediate requests will be served by this car. Note: the Fleet Manager, the service providers and the SPG are registered in the IAM service. **2: Request charging data** The Fleet Manager checks the battery status of all fleet cars. It decides that one car needs to charge. The Fleet Manager requests information about Charging Stations in a preferred area by sending coordinates, a radius, a time frame, and the "wantCharging" attribute directly to the Service Provider, in an encrypted message. The Service Provider responds to Fleet Manager with a collection of Charging Stations. The Fleet Manager chooses a Charging Station and sends the vehicle to charge. The vehicle arrives at the Charging Station, gets plugged in and charges. **3: Relocation during idle time of fleet vehicles** The Fleet Manager decides that the idle time of the fleet cars should be used for relocation. It decides that vehicles shall be sent to different areas where high demand is expected (visualization of vehicle positions and high demand areas). It requests parking space for these areas with coordinates, radius, and time frame from a parking service provider (secured

	communication takes place via the commonly specified interface). The Fleet Manager receives the information and assigns the vehicles to the parking spaces in the different areas. The vehicles drive to the areas and park. **4: Customer dropped off. Vehicle must be parked. Request predictions from SPG.** A customer has just been dropped off at his target destination. The vehicle now needs to be parked since the destination location is only suited for disembarking only. The Fleet Manager decides that the vehicle should be parked in the nearby area and hence requests a parking slot/space from the Service Provider Gateway. The SPG identifies a parking data provider for that area and requests parking data. Based on free parking spaces and possible occupation in near time, made on predictions and travel time, the SPG identifies a suited parking space and replies to the Fleet Manager with the parking information and a time frame with the probability that the parking space will be available. The Fleet Manager directs the car based on the received parking information to that parking slot. The car arrives at the parking and parks. **5: Fleet Manager needs parking space predictions from SPG** The Fleet Manager decides to relocate fleet vehicles in the next few hours. The manager wants to make pre-calculations for the fleet distribution and therefore wants to take in consideration all the probabilities of the availability of parking spaces. The Fleet Manager sends a request to the SPG for a certain area with the attributes location (coordinates), radius, time frame and other attributes, within an encrypted message. The SPG replies with a collection of parking data and availability predictions. The Fleet Manager uses the data for further calculations and relocates the fleet vehicles accordingly. **6: Data transformation in SPG Cloud** The Fleet Manager requests parking data from the service provider gateway for a specific area and time. The SPG collects the parking data from a parking service provider. The data provided by this service is in a data format that is not compliant with the defined interface and the Automotive OEM Cloud is not able to process. Hence, the SPG transforms the data to comply with the interface and sends the data back to the Fleet Manager. The Fleet Manager allocates vehicles to the parking spaces based on the received data. The vehicles are on route to the parking space. The vehicles arrive and park.

	7: Fleet Manager asks SPG for Charging Stations with specific charging plug type The Fleet Manager checks the battery status of all fleet cars. The manager decides that one car needs to charge. The vehicle has a certain plug type for charging. The Fleet Manager requests information about charging stations that offer that specific charging plug in a preferred area by sending coordinates, a radius, a time frame, the “wantCharging” attribute, and the Plug type. The SPG collects the charging stations data from the provider(s) and sends them back to the Fleet Manager. The Fleet Manager chooses a charging station and sends the vehicle to charge. The vehicle arrives at the charging station, gets plugged in and charges. **8: Cyber security event in the Supervision Cloud** A registry failure by a “fake” Fleet Manager or service provider is reported by the IAM service to the Supervision service. Later on, authentication failures from either a “fake” Fleet Manager or Service Provider are reported, too. The Supervision service collects the event data, raises alerts and launches the cyber security analysis process. Cyber security dashboards are updated to take this situation into consideration. Concerned entities are contacted to get warned and resolve the cyber security issue. SPG = Service Provider Gateway (Middleware between OEM Clouds and Service Providers IAM = Identity and Access Management (authentication service)







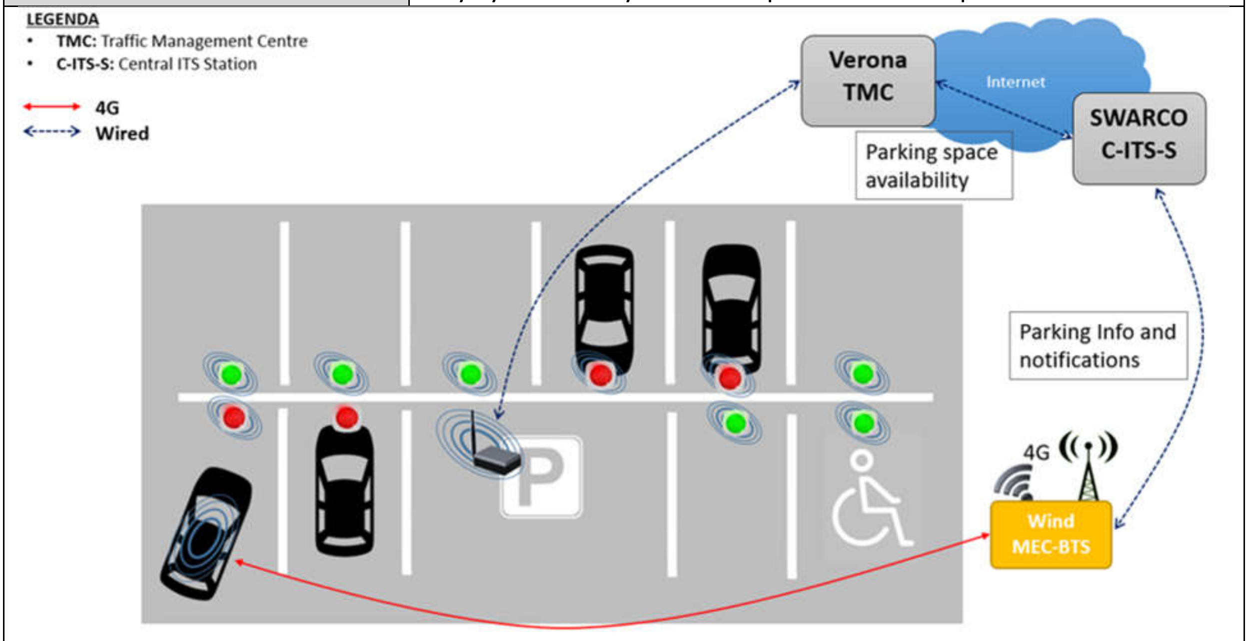
Key assumptions		• Fleet operation will be simulated. • Data (parking, charging) availability. • Mobile network availability. • Cyber security devices and services availability. • All communicating entities registered in the IAM service.
Actors and Relations		**BMW** – Data analytics, fleet provider. **City of ULM** – Provides parking spaces and data. **IBM-IE** – Develops and provides Service Provider Gateway. **AIRBUS** – Provides cyber security cloud services and embedded IAM components.
Realisation Prerequisites	**Physical infrastr.**	• On-street parking spaces (5-10) as well as public parking facilities. • Charging stations near the available parking spaces.
	Digital infrastr.	• Mobile Networks 4G/5G. • Cyber security cloud services (IAM and supervision).
	Data availability	• Parking space, charging capability & plug type information from City of Ulm. • Predicted parking space availability from SPG (IBM-IE). • Pickup/Drop-off capability of parking facilities and locations (City of Ulm -> Kiss&Ride).

Challenges/Barriers/ Open issues	**Technical**	• Data format - Connectors are complicated: Possible transformation between data formats within Service Provider Gateway to meet the interface specifications.
	Others e.g., operations, safety regulations	• Cybersecurity (Secure service provider to OEM registration and data exchange).
Target/Evaluation metrics		• **Pickup time deviation** – How much does the pickup time deviate from the desired one. • **Average pickup time** – Average pickup time for customers. (e.g., relocation efficiency). • **Fleet Idle time/Utilization time** – Is the fleet size appropriate for the demand (business area). • **Effective transportation distance ratio** – Ratio of distance driven with passenger(s) and without (deadheading).
Impact		Intelligent and efficient relocation of fleet vehicles to minimize customer pickup time and pickup time deviation which will allow people to use autonomous taxis over private cars and consequently reduce traffic congestion.
Initial and target TRL		Initial: TRL 1 – 2 Target: TRL 6 - 7

4.2 SCN1.2 - Smart Parking and IoT management in City of Verona, Italy

Name	**Smart Parking and IoT management in City of Verona, Italy**
Short name	**SPIoTCDV**
ID	**UC1-SCN12-SPIoTCDV**
Overview	The connected and automated vehicle is searching for a parking space in an outdoor parking lot. The ICT4CART infrastructure sends the information about the available spot, specifying the location. The vehicle can perform the driving actions according to the received information and go directly to the available space. To provide such information, the ICT4CART infrastructure exploits detection cameras and Vehicle-to-Infrastructure (V2I) communication, relying on cyber security mechanisms to preserve privacy and integrity.
Description	The vehicle is entering the parking area and needs to find an available space. The ICT4CART infrastructure receives a secured notification that a vehicle is entering the parking area and needs to find an available space. The OBU of the connected vehicle uses 4G to send this notification to the Traffic Management Centre (TMC). The ICT4CART infrastructure securely informs the vehicle entering the parking area about the availability of a parking space, sending precise coordinates of its location (The format of this information still needs to be decided during the project, since no standard exists

	yet). The OBU connects through 4G to retrieve parking information. At infrastructure level, the elaboration of the information gathered by the sensors can be initially performed at Traffic Management centre level. In case of multiple parking requests and responses, from several vehicles, it could be handled at Multi-access Edge Computing (MEC) server level, based on the rules of the infrastructure operators. Both options will use 4G/LTE mobile network for transmitting the information. The vehicle in the entrance of the parking area defines the driving actions to take, in order to avoid possible collisions with other vehicles situated in the parking area. In case of V2V communication, dedicated security mechanisms grant privacy and integrity. Any cybersecurity event is reported to the supervision service.



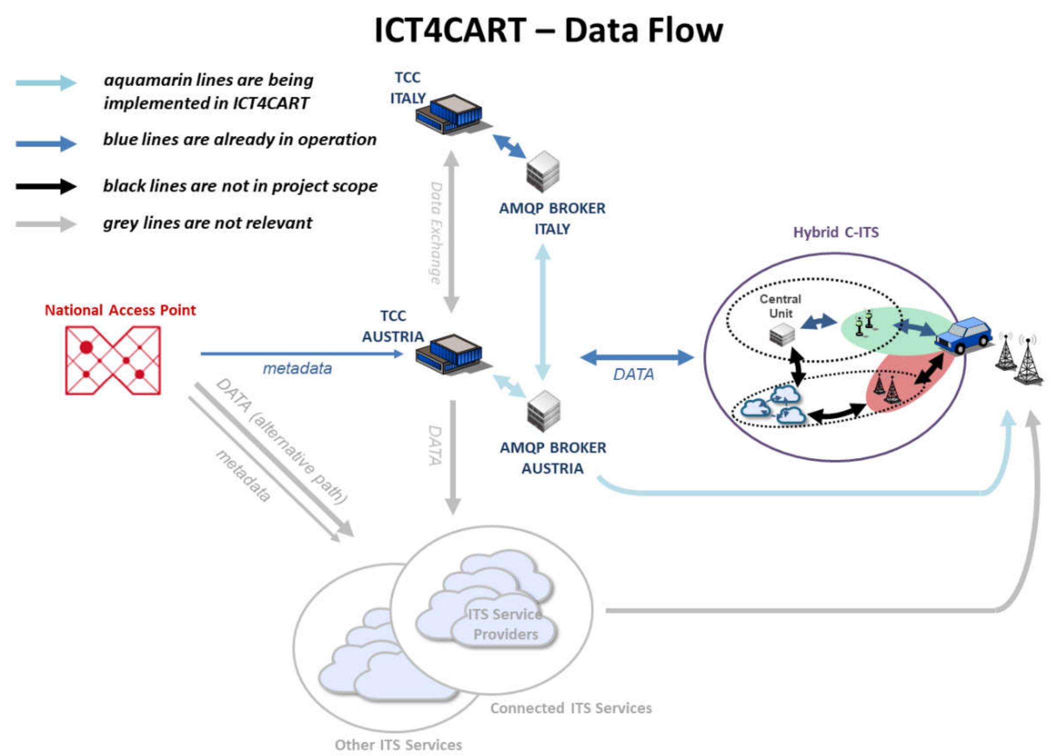
Key assumptions	• Availability of a surface parking, where management and ticketing system is already present. • Installation of sensors to detect the precise position of the available spaces. • IAM components (security module and access control gateway) integrated in both vehicle and infrastructure. • Cyber security cloud services up and running: IAM service and supervision. • Security modules and access control gateways must be able to connect to cyber security services. All communicating entities are registered in the IAM service.
Actors and Relations	**SWARCO:** provides the needed infrastructure to exchange the cooperative messages and process the messages to inform the vehicle of the available parking spaces. **Comune di Verona:** provides an outdoor parking lot, where management and ticketing system is present, to be used for the implementation of the scenario.

		CRF: provides support for the connected vehicle (viewing parking information). **WIND-Tre:** provides the MEC server on which the smart parking management service could be executed, as well as the 4G connectivity for the traffic management centre and OBUs (SIM and network configu-rations). **AIRBUS**: provides cyber security cloud services and embedded IAM components. **IBM-Z:** provides embedded encryption and authentication components (V2V communications).
Realisation Prerequisites	**Physical infrastr.**	• Electricity and detection cameras. • 4G and/or Fibre optics/others connection in the parking area.
	Digital infrastr.	• Communication technologies: 4G/LTE. • ITS services: smart parking. • Embedded encryption and authentication, IAM components. • Cyber security cloud services (IAM and supervision).
	Data availability	• Video flows from parking lot. • Position and dynamics of connected vehicle. • Parking availability information. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Definition of the data structures to enable the parking request from the vehicles. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastru-cture.
	Others e.g., operations, safety regulations	• Management of different parking requests from the vehicles. • The video flows and other sensors information gathered from the infrastructure of the parking lot could be transmitted to the MEC server if the MEC-based case is considered. The sharing of this information to the MEC server may not be possible due to security and privacy reasons.
Target/Evaluation metrics		• **Accuracy** of the vehicles detection. • **Average time** for the connected and automated vehicle to identify the closest free parking space.
Expected impact		Smooth and fast parking search for connected and automated vehicles. This can lead to an optimisation of space and time management in the parking area.
Initial and target TRL		Initial: TRL 3 Target: TRL 6

4.3 SCN2.1 - Dynamic clearance, adaptation and handover of vehicle automation level at special conditions in Graz, Austria

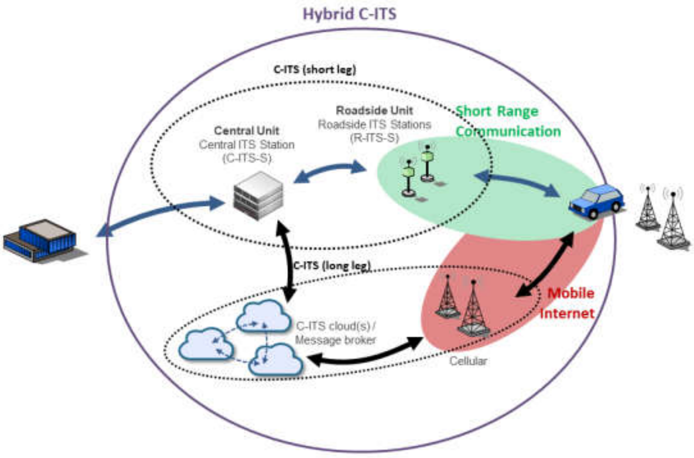
Name	**Dynamic clearance, adaptation and handover of vehicle automation level at special conditions in Graz, Austria**
Short name	**DAVAGRZ**
ID	**UC2-SCN21-DAVAGRZ**
Overview (abstract)	At the core of the Scenario is a vehicle driving with an active automated driving function L3 on the highway. The L3 function has a restriction regarding environmental conditions. Upon encountering a restricting condition, the function will hand over to the driver, thereby performing an adaptation from L3 to L2. The function uses a data stream from the highway infrastructure to detect restricting conditions as early as possible in order to initiate an early in-time handover procedure. Other automated driving functions with no such restrictions can use the same data stream to initiate early, in-time and comfortable reaction manoeuvers well ahead of encountering the difficult driving situation. The Scenario includes a data exchange with the traffic control centre via road-side infrastructure for Segment Clearance in order to determine, amongst other factors, whether the L3 function may be entered at all at the current vehicle location and the current time. The Use Case also includes an optional MEC server in the data stream to cater for future scalability and latency requirements. All data flows implemented for this use case will be available on the complete Austrian highway network, not just on the test site.
Description	The Use Case consists of three parts: Segment Clearance, Dynamic Adaptation, and MEC Supplement. **Segment Clearance** For Segment Clearance, ASFINAG infrastructure will provide data verification that the vehicle is located on a highway, this being a prominent safety issue for the automotive industry for prevention of false activations of L3 functions. Additionally, infrastructure will provide data from the operational control of the traffic control centre to enable clearance control for L3 activation for specific segments. The clearance will be either enforced manually by operators in charge or automatically by an algorithm following a defined set or rules for allowing L3 activation. The data stream will either be provided as a continuous broadcast or as a reply to an individual vehicle's requests. **Dynamic Adaptation** The focus is on establishing whether the vehicle is approaching roadworks or a traffic jam prior to the vehicles' own sensor detection, in order to allow for an acceptable handover to the vehicle or back to the driver. BOSCH will show a real handover to a driver and back in an automated

	vehicle. BOSCH's Traffic Jam Assistant hands over to driver in case of ahead roadworks. When the traffic jam ends, Assistant offers to drive at automated L3. ASFINAG/BOSCH will show a handover to a driver in the case of sudden black ice encounter. Black ice cannot be detected by the autonomous L3 function ahead of reaching it. This is a safety critical scenario, where latency is most important. The time difference between transmission via ITS-G5 and LTE-A will be shown. **MEC Supplement** To prepare for scalability in future scenarios of large scale usage of L3 functions, a MEC solution will be demonstrated. The MEC server will act as a cache for the infrastructure data stream. The MEC distributes the data in a defined relevance area. To demonstrate the use of MEC for latency-critical situations, ASFINAG/BOSCH will show a handover to a driver in the case of sudden black ice.



<table>
<tr><td colspan="3">

Detail: Hybrid C-ITS



</td></tr>
<tr><td colspan="2">Key assumptions</td><td>

The transmission of the infrastructure messages to the vehicles will be implemented according to the Geo-Hash concept. In this concept, the vehicle subscribes to a road section and then receives all infrastructure messages for that section from a Message Broker. The position of the vehicle is not recorded in this concept.
The Geo-Hash concept has been adopted to adhere to the C-Roads concept as far as possible while ensuring that the project timeline can be met by making use of the current implementation status where necessary.
Developments in the other C-Roads research projects will be adopted in ICT4CART wherever possible and could transform an “out of scope” data path in the diagram into an “implemented in ICT4CART”.
Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating entities are registered in the IAM service.

</td></tr>
<tr><td colspan="2">Actors and Relations</td><td>
ASFINAG: Test site leader, ITS-G5 on Austrian side.
T-MOBILE: LTE-A connectivity and MEC infrastructure.
BOSCH: Vehicles for testing, vehicle HAD application.
AIRBUS: provides cyber security cloud services and embedded IAM components.
</td></tr>
<tr><td rowspan="2">Realisation</td><td>Physical infrastr.</td><td>

ITS-G5, LTE base stations (3 sites will be upgraded to LTE-A by T-MOBILE).
MEC server.

</td></tr>
<tr><td>Digital infrastr.</td><td>
Vehicles

In car modem CAT6 or higher for LTE.
In car hybrid LTE/ITS-G5 Application.

</td></tr>
</table>

		• In car GNSS receiver and antenna. • In car positioning engine (HW, SW). • In car maps. **Highway infrastructure** • ASFINAG CONTENT realtime ITS-G5 Service for ITS-G5. • ASFINAG CONTENT realtime DATEX II Service for LTE. • ITS-G5 connectivity by ASFINAG. • LTE-A connectivity by TMA. • MEC by TMA, application by ASFINAG. • Precise Positioning service. • OP1: DATEX II (v2.3), Austrian Elementary Profiles http://www.datex2.eu/implementations/profile_directory • OP2: DATEX II (v2.3) http://www.mobilitaetsdaten.gv.at/en/data • OP3A: DATEX II (v2.3), ECo-AT Relesae 4.0, http://www.datex2.eu/implementations/profile_directory • OP3C: ETSI & ISO Messages, C-Roads-Release 1.4 • OP3D: ETSI & ISO Messages, C-Roads TF 4 – Hybrid • OP4: DATEX II (v2.3), Austrian Elementary Profiles http://www.datex2.eu/implementations/profile_directory • SP1: DATEX II (v2.3), SENSORIS, DATEX II over AMQP • SP2: AMQP / EDGE Computing Infrastructure • SPN: DATEX II (v2.3), Austrian Elementary Profiles http://www.datex2.eu/implementations/profile_directory Cyber security cloud services (IAM and supervision)
	Data availability	• ITS-G5 Day I by ASFINAG, already operational. • DATEX II Service Segment Clearance by ASFINAG. • DATEX II Service Unplanned Events by ASFINAG, already operational. • DATEX II Service Planned Events (Roadworks) by ASFINAG. • Technical Exercise, the functionality to send simulated incidents, by ASFINAG already operational. • Technical Exercise, the functionality to receive simulated messages in the vehicle. • OP1, OP2, OP3A, OP3B, OP3C, OP3D, OP4 operational. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open	**Technical**	• Modem CAT6 or higher needed in the vehicle. • Precise positioning via ITS-G5 is foreseen for DAY 1.5. It is not verified when the feature will be available. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastructure.
	Others e.g. operations, safety regulations	• Clearance for L3 for Test Site AUSTRIA GRAZ at AUSTRIATECH. • Booking of logging resources for Test Site AUSTRIA GRAZ at ALP.LAB.

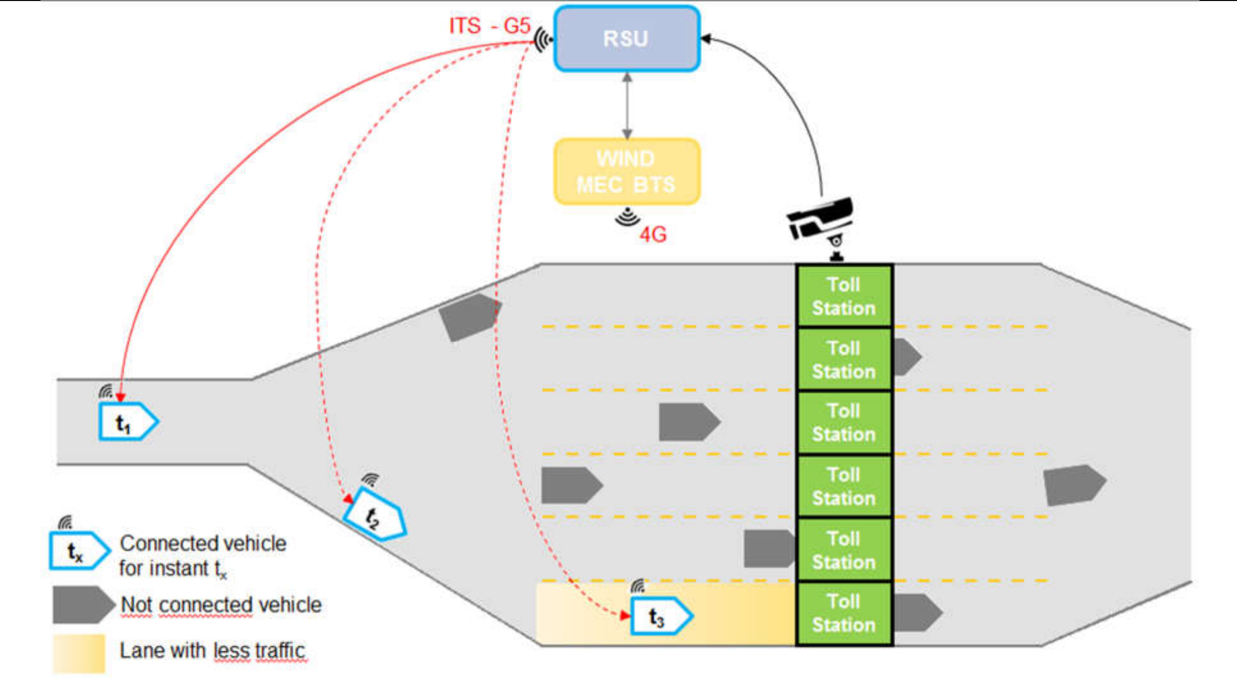
Target/Evaluation metrics	• **Response time:** The highway infrastructure messages of the incident location shall reach the vehicle 10 seconds before it reaches the incident location. Response time for sending the message is defined as the round trip time (RTT) (i.e., 2x one way). • **Percentage of vehicles receive the incident message** (10 + latency) seconds or more before reaching the incident. Target is 100% of possible candidates, i.e., vehicles which are more than (10 + latency) seconds away from incident when incident is created.
Impact	This SCN can improve the road safety and also increase the amount of time that a L3 vehicle spends in autonomous driving mode.
Initial and target TRL	Initial: TRL 2-3 Target: TRL 3

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.4 SCN2.2 - Dynamic adaptation of vehicle automation level on Trento motorway

Name	**Dynamic adaptation of vehicle automation level on Trento (Italy) motorway**
Short name	**DAVATR**
ID	**UC2-SCN22-DAVATRN**
Overview (abstract)	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 has to broadcast an environmental model considering the local map of the exit ramp and of the toll station, and the presence of involved vehicles, available toll lanes, and possibly the AD reserved one. Thanks to this information the connected and automated vehicle 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 could be the guidance of an autonomous vehicle toward a particular toll lane reserved to self-driving vehicles. Other applications can address gas stations and the approach of vehicles to the refuelling lane. The ICT4CART infrastructure can advise vehicles of possible dangers like trucks in manoeuver, wrong-way driving or broken down vehicles.
Description	The connected and automated vehicle is leaving the motorway and is approaching a toll station. Other vehicles are in the exit lane, on the way to the toll station. The ICT4CART infrastructure monitors the exit ramp and the toll station lanes considering the local map, exploiting information from sensors (e.g., cameras) and from CAMs sent by connected vehicles. An environment model is defined specifying the position of all identified vehicles and of their dynamics, using the approach in UC3-SCN33-LMBRE. All types of communications between ICT4CART architectural entities are

<table>
<tr><td></td><td>secured. Any cybersecurity event related to ICT4CART infrastructure is reported to the supervision service.</td></tr>
<tr><td colspan="2">



</td></tr>
<tr><td>Key assumptions</td><td>

Host Vehicle: main SCN demonstrator: vehicle equipped with ITS-G5 connectivity and automated functions, and secured communication mechanisms.
Remote Vehicles: at least one remote vehicle equipped with ITS-G5 connectivity, and secured communication mechanisms.
Infrastructure: the infrastructure required for the implementation of the SCN is installed in the proximity of the exit ramp and of the toll station in order to detect all the involved vehicles. It should include:

ETSI ITS-G5 roadside unit at the exit ramp;
Sensors (cameras, etc.);
Secured communication mechanisms.

Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating ICT4CART archictetural entitiesare registered in the IAM service.
Other: digital representation of road geometry at the exit ramp, in form of ETSI MAP message. Information of toll station lane availability.

</td></tr>
<tr><td>Actors and Relations</td><td>CRF: provide the connected and automated vehicle, and another connected vehicle where is implemented the decision logic on the vehicle, to take into consideration the information received by the CPM.

Autostrada del Brennero-A22: hosts the required infrastructure in the neighbourhood of the exit ramp and the toll station for the implementation of the SCN. Provide a digital map of the exit ramp until the toll station. Provide dynamic info of available toll lanes. Supply also to ICT4CART the C-ROADS Day 1 services that are of interest for this SCN (e.g., Traffic Jam Warning).</td></tr>
</table>

		LINKS: provide the OBUs for the connected vehicles; provide an ITS-G5 RSU to be used for the ITS-G5 communication services and for implementing the detection services on the exit ramp or at the toll station; implement the Collective Perception Service according to the ETSI TS 103 324; develop the required software tools for the detection and the dynamics prediction of all road users exploiting visual camera and other sensor information. **WIND-Tre:** provide the MEC server on which the Collective Perception Service can be executed and the 4G connectivity for ISMP RSUs and OBUs (SIM and network configuration). **AIRBUS:** provide cyber security cloud services and embedded IAM components. **IBM-Z:** provide embedded encryption and authentication components (V2V communications).
Realisation Prerequisites	**Physical infrastr.**	• Electricity, mounting facilities and 4G or other connection at the toll station and near the exit ramp. • Cameras or other sensors for detecting traffic/vehicles on lanes, or other places (gas station). • MEC server.
	Digital infrastr.	• **Communication technologies**: ITS-G5 and 4G/LTE. • **ITS services:** Collective Perception Service, Cooperative Awareness Service, Road and Lane Topology service. • **ETSI ITS messages**: CPM, CAM, MAP, DENM. • Embedded encryption and authentication, IAM components. • Cyber security cloud services (IAM and supervision).
	Data availability	• Video flows. • Vehicle information flows. • Position and dynamics information from the CAM of connected vehicles. • Data of available toll lanes. • HD Map of the exit ramp until the toll station. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Detection of both connected and non-connected vehicles, as well for the prediction of their dynamics is challenging due to the potentially high number of vehicles that may be present at the toll station. • Detection has to be timely performed since the information to the host vehicle has to be sent with low latency. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastructure.
	Others, e.g., operations, safety regulations	• Privacy issues may arise since visual cameras are installed. The implementation of the SCN will not identify any road users or drivers and it will use the video flow just to detect the road users. No sensible information, which may be gathered from the camera and other sensor, will be disclosed. • Available level of automation at exit lanes (longitudinal control

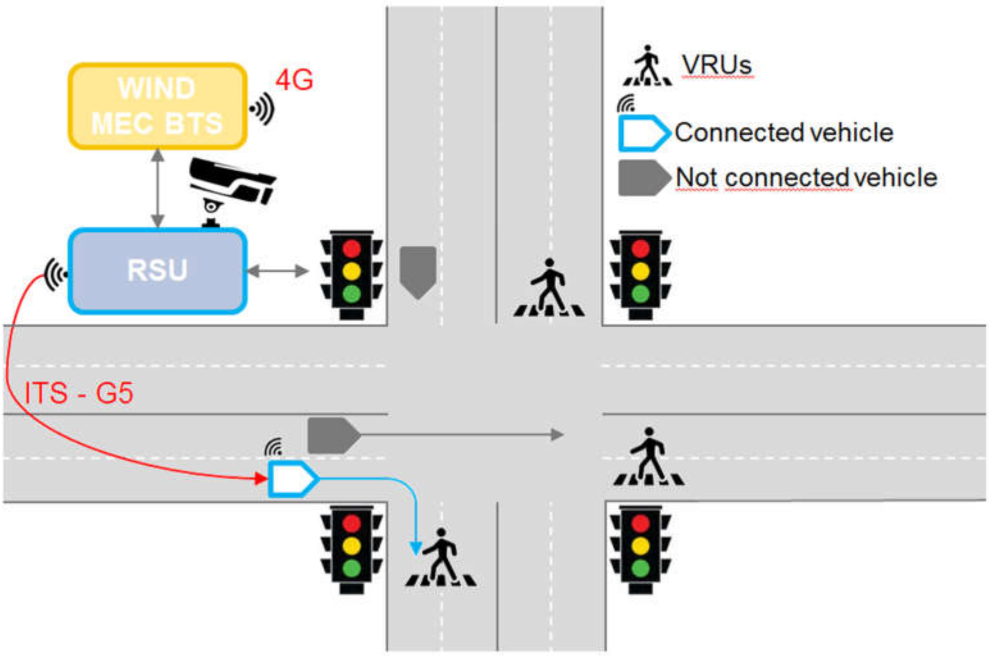
	only, manual, etc.) is to be investigated during the project. Legal constraints on public road tests.
Target/Evaluation metrics	• **Average time** and speed for the connected and automated vehicle to reach the toll station. • **Ratio** between traffic in the neighbourhood of the toll station and of traffic faced by the connected vehicle approaching the toll station. • **Accuracy** of the vehicles detection within the interest area.
Impact	Considering the traffic at the toll lanes, this proposal can improve the traffic congestion at the toll station with a betterment in fuel consumption, safeguarding the environment, and in time spend in traffic at the toll station.
Initial and target TRL	Initial: TRL 3 Target: TRL 6

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.5 SCN2.3 - Dynamic adaptation of vehicle automation level in Verona, Italy

Name	**Dynamic adaptation of vehicle automation level in Verona (Italy)**
Short name	**DAVACDV**
ID	**UC2-SCN23-DAVACDV**
Overview (abstract)	ICT4CART infrastructure monitors an urban intersection and it is in charge to detect road users, according also to UC3-SCN31b-VMCDV (the description is below). In particular, the infrastructure has to communicate with the vehicle so that it can adapt its behaviour to avoid dangers and possible collisions with other vehicles or vulnerable road users (VRUs) as pedestrians and bicycles. ICT4CART infrastructure has to provide GLOSA information, and Virtual mirror information. Based on this information, the vehicle can optimize longitudinal control and avoid dangerous situations.
Description	The connected and automated vehicle is about to cross an urban intersection. In the proximity of the intersection there are other vehicles and VRUs that probably are going to cross it too. The ICT4CART infrastructure monitors the intersection exploiting both information from sensors (e.g., visual cameras) and from CAMs sent by connected road users. An environmental model is defined specifying the position of all identified vehicles, VRUs and of their dynamics considering the local map and the geometry of the intersection. All types of communications are secured. Any cybersecurity event is reported to the supervision service. The environmental model will be defined according to ETSI Technical Specification 103 324, which publication is planned for May 2019, that standardizes the Collective Perception Service. This service will be based on the broadcasting of Collective Perception Message (CPM) that is a message that complements the CAM and it provides the position and

<table>
<tr><td></td><td>dynamics information of all the road users that the broadcasting ITS station is aware of. The environmental model can be elaborated either on a Road Side Unit (RSU) that is located close to the intersection, or on a Multi-access Edge Computing (MEC) server. The RSU will send the CPM using ITS-G5 communication, while the MEC server will use 4G/LTE for sending the information.

The connected and automated vehicle, considering the information contained in the CPM and GLOSA, can revise its velocity approaching the intersection. Optionally, the start-and-stop functionality of the vehicle will be modified to take the GLOSA information into account.</td></tr>
<tr><td colspan="2">
</td></tr>
<tr><td>Key assumptions</td><td>• Various sensors and/or visual cameras installed at the intersection in order to effectively detect all the road users.
• IAM components (security module and access control gateway) integrated in both vehicle and infrastructure.
• Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating entities are registered in the IAM service.</td></tr>
<tr><td>Actors and Relations</td><td>CRF: provide the connected and automated vehicle, possibly a connected vehicle for exhaustive verification of the SCN for the case of several connected road users (e.g., verify GLOSA-optimized speed in case of vehicles in queue). Implement the decision logic on the vehicle to take into consideration the information received by the CPM.

Comune di Verona: install the required facilities (electricity and fibre optic/others connection) at the intersection and install the required infrastructure for the implementation of the SCN.

LINKS: provide the OBUs for the connected vehicles; provide an ITS-G5 RSU</td></tr>
</table>

		to be used for the ITS-G5 communication services and for implementing the detection services at the intersection; implement the Collective Perception Service according to the ETSI TS 103 324; develop the required software tools for the detection and the dynamics prediction of all road users exploiting visual camera and other sensor information. **SWARCO:** provide information about the traffic lights to road users. **WIND-Tre:** provide the MEC server on which the Collective Perception Service can be executed and the 4G connectivity for LINKS RSUs and OBUs (SIM and network configuration). **AIRBUS:** provide cyber security cloud services and embedded IAM components. **IBM-Z** provides embedded encryption and authentication components (V2V communications).
Realisation Prerequisites	**Physical infrastr.**	• Electricity, mounting facilities and 4G and/or fibre optic/other connections at the intersection. • Connected traffic lights. • Visual cameras and depth sensors for monitoring the intersection. • Other potential traffic sensors (e.g., magnetic coils). • MEC server.
	Digital infrastr.	• **Communication technologies**: ITS-G5 and 4G/LTE. • **ITS services:** Collective Perception Service, Cooperative Awareness Service, Road and Lane Topology service. • **ETSI ITS messages**: CPM, CAM, SPAT, MAP, DEMN. • Embedded encryption and authentication, IAM components. • Cyber security cloud services (IAM and supervision).
	Data availability	• Video flows, depth information of the intersection from LiDAR and/or other depth sensors. • Vehicle flows information from other sensors such as magnetic coils. • Position and dynamics information from the CAM of connected road users. • Information about the traffic light phases and timing. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Vehicle control based on connectivity. • Evaluation strongly depends on traffic conditions (e.g., a vehicle with connected GLOSA service in the middle of the traffic where other vehicles are not equipped, may not receive any benefit from this GLOSA function). We may need to refer to simulation for the actual impact assessment, for instance making projections on the technology penetration in the future. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastructure.

	Others, e.g.,operations, safety regulations	• Regulations on automated driving in public roads.
Target/Evaluation metrics		• **Average time** for the connected and automated vehicle to go through the intersection. • **Average speed** of the connected and automated vehicle while going through the intersection. • **Acceleration/deceleration** (number of events and values) performed by the connected and automated vehicle while going through the intersection.
Impact		Information about traffic lights phases and timing can improve the flow of the traffic within urban intersection with a betterment in fuel consumption, safeguarding the environment, and in time spend in traffic.
Initial and target TRL		Initial: TRL 3 Target: TRL 6

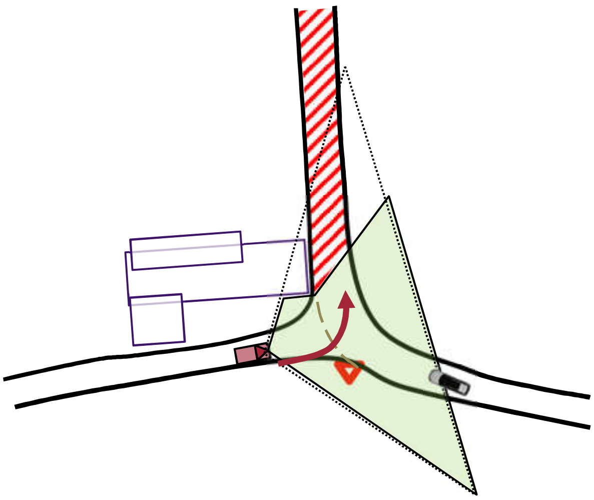
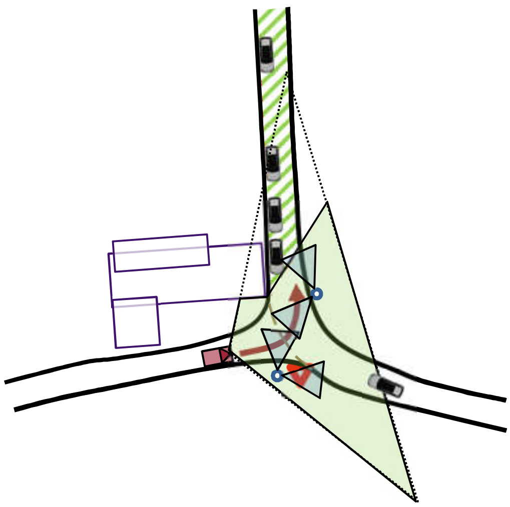
Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.6 SCN3.1 - Virtual mirror to "see" surrounding traffic in urban environment

SCN3.1.a: In City of Ulm, Germany

Name	**Virtual mirror to "see" surrounding traffic in city of Ulm, Germany**
Short name	**VMULM**
ID	**UC3-SCN31a-VMULM**
Overview (abstract)	This "virtual mirror" consists of an environmental model of all road users at the intersection. The model is calculated on a MEC server and uses information from connected infrastructure sensors and possibly from connected vehicles. The model is communicated to connected and automated vehicles to improve their awareness of road users at the intersection. Additionally, hybrid communication of the state per lane of a connected traffic light at another intersection is exploited. Seamless integration of cellular networks and ITS-G5 in the infrastructure is one of the key aspects of this scenario. This scenario is dealing with an urban environment in the city of Ulm in Germany. The goal of ICT4CART in this scenario is to enable the crossing of intersections in an automated way involving mixed traffic.
Description	**1. An Automated Vehicle crosses an intersection without traffic lights and has to yield right of way for main street** Depending on its connectivity options, the automated vehicle can connect to a MEC server via 5G/LTE and/or ITS-G5 (if it is within range). The MEC Server has access to all sensors which are deployed at the intersection and

	continuously calculates/updates an environmental model of the intersection along with predictions for future motions of all vehicles within sensor range (automated or non-automated). This environmental model is then distributed to automated vehicles (AVs) within range, which can integrate the model and the predictions into their own environmental model to improve their field of view. The predictions allow the AVs to optimize trajectory planning in order to allow smooth crossing of the intersection and to prevent unnecessary stopping. **2. An Automated Vehicle crosses an intersection with connected traffic lights** Depending on its connectivity options, the automated vehicle can connect to a traffic light control RSU via 5G/LTE or ITS-G5 (if it is within range). The traffic light control unit then sends information about the current traffic light signal for the lane that the vehicle is currently on, as well as predictions for when the traffic light signal will change. The automated vehicle can use this information to anticipate the traffic light change and thereby cross the intersection more smoothly. In both cases, all types of communications are secured, and any cybersecurity event is reported to the supervision service.

Intersection with poor visibility:	Visibility is enhanced through virtual mirror:
	

Key assumptions	• Conventional vehicles and other road users comply with the traffic rules. • IAM components (security module and access control gateway) integrated in both vehicle and infrastructure. • Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must

<table>
<tr><td colspan="2"></td><td>be able to connect to cyber security services. All communicating entities are registered in the IAM service.</td></tr>
<tr><td colspan="2">Actors and Relations</td><td>Ulm University (UULM): ICT infrastructure developer and operator (for test site), AV operator/user.

NOKIA: Telecom operator for test site, Telecom equipment manufacturer (5G/LTE).

City of Ulm: Road infrastructure operator.

SWARCO: Road infrastructure manufacturer.

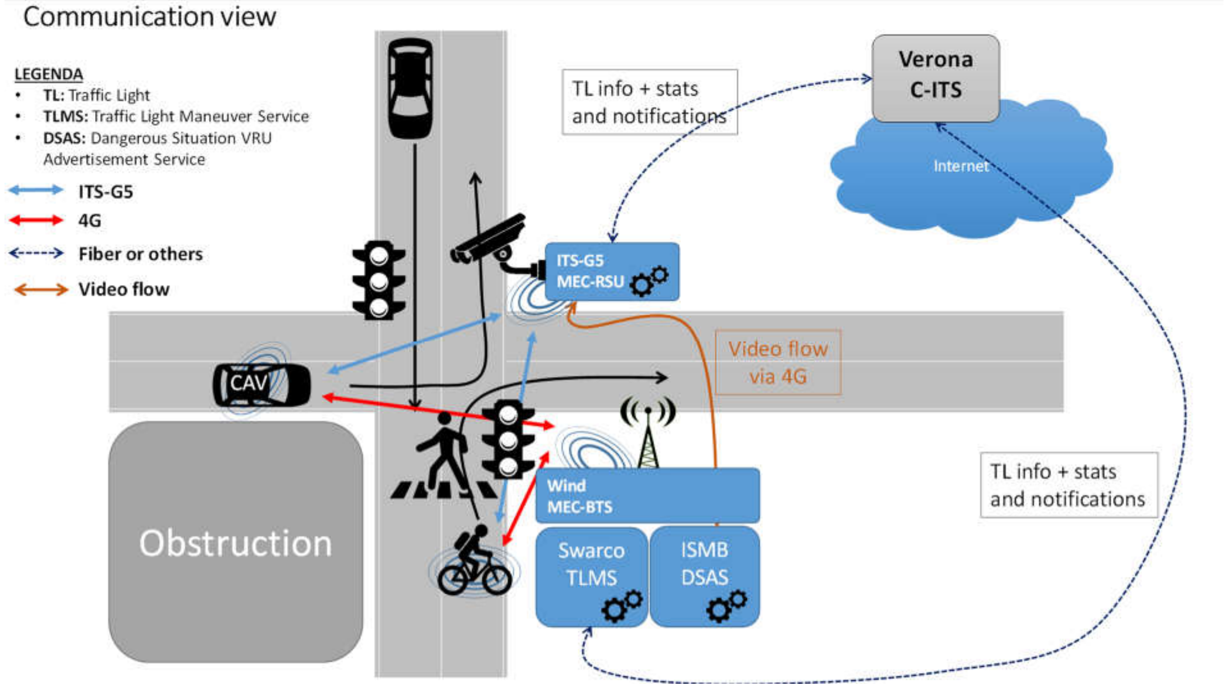
AIRBUS: provides cyber security cloud services and embedded IAM components.</td></tr>
<tr><td rowspan="3">Realisation Prerequisites</td><td>Physical infrastr.</td><td>Urban intersection with poor visibility in Ulm-Lehr, equipped with Cameras and LiDAR sensors to sense vehicles coming from various lanes.</td></tr>
<tr><td>Digital infrastr.</td><td>In vehicle: Either ITS-G5 or 5G/LTE is available (or both)
For intersection without traffic light:
MEC Server is available and either connected to ITS-G5 RSU or via 5G/LTE (or both).
Intersection is equipped with sensors which can be accessed by the MEC server.
Environmental model from sensor data fusion is available on MEC server.
For intersection with traffic light:
Traffic light control unit is connected with ITS-G5 RSU or via 5G/LTE (or both).
Traffic light state per lane are available via SPAT/MAP messages.
Embedded IAM components.
Cyber security cloud services (IAM and supervision).</td></tr>
<tr><td>Data availability</td><td>Sensor data from the sensors at the first intersection.
Environmental model created from sensor data.
Traffic light state and prediction.
Vehicle and infrastructure authentication data (e.g., credentials, right management model).</td></tr>
<tr><td>Challenges/Barriers/</td><td>Technical</td><td>Provide information on both information channels (ITS-G5 and 5G/LTE) in parallel with low latency and high reliability.
Provide highly accurate environmental model from sensor data.
Malfunction of Automated Vehicle.
Possibility to integrate security module and access control gateway in vehicles and infrastructure.</td></tr>
</table>

	Others, e.g., operations, safety regulations	• Weather conditions appropriate for infrastructure sensors to work (no fog/snow/heavy rain, etc.).
Target/Evaluation metrics		• **Percentage of intersection crossings** without the need of driver to take over control. • **Average latency** of infrastructure sensor data from capturing to reception in vehicle as part of infrastructure environmental model.
Impact		Enabling autonomous vehicles to cross intersections efficiently, reliably and safely is a key requirement for the future development and public acceptance of autonomous vehicles. Demonstrating a working prototype of this might increase adoption of autonomous vehicles.
Initial and target TRL		Initial: TRL 2 – 4 Target: TRL 6

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

SCN3.1.b: In City of Verona, Italy

Name	**Virtual mirror to "see" surrounding traffic in city of Verona, Italy**
Short name	**VMCDV**
ID	**UC3-SCN31b-VMCDV**
Overview (abstract)	An urban intersection in city of Verona is monitored by the ICT4CART infrastructure that is in charge to detect road users, to predict their dynamics and to broadcast an environmental model of the road users present in the intersection, i.e., indicate the presence and position of road users that are in the intersection and where they are going. The considered road users are not limited to vehicles, but they include also Vulnerable Road Users (VRUs) such as pedestrians and bicyclists (an example of connected bicycle will be tested among other legacy VRUs). The connected and automated vehicle can refine its driving action based on the information received by the ICT4CART infrastructure since it can be aware of road users even if they are in blind spots and the VRUs can be alerted about possible dangers.
Description	The connected and automated vehicle is going to cross an urban intersection. Other vehicles and VRUs are near the intersection or they are crossing the intersection too. The ICT4CART infrastructure monitors the intersection exploiting both information from sensors (e.g., magnetic coils, visual cameras) and from CAMs sent by the connected road users. The infrastructure defines an environmental model of the intersection specifying the position of all the identified road users as well as their dynamics. This service will be based on the broadcasting of CPMs that is a message that complements the CAM and it provides the position and dynamics information of all the road users that the broadcasting ITS station is aware of.

	The connected and automated vehicle can revise its driving trajectory when crossing the intersection based on the information contained in the CPM avoiding possible collisions and dangers. The ICT4CART infrastructure also informs the connected VRUs about possible dangers implementing a Dangerous Situation VRU Advertisement Service. Information about traffic lights phases and timings is taken into account for the trajectory definition and the identification of possible dangerous situations. The Traffic Light Manoeuvre Service is in charge to provide these details. All types of communications are secured. Any cybersecurity event is reported to the supervision service.
	
Key assumptions	• IAM components (security module and access control gateway) integrated in both vehicle and infrastructure. • Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating entities are registered in the IAM service.
Actors and Relations	**CRF**: provide the connected and automated vehicle, possibly provide a connected vehicle for an exhaustive verification of the SCN for the case of several connected road users, implement the decision logic on the vehicle to take into consideration the information received by the CPM. **Comune di Verona**: provide the required facilities (electricity and fibre optic/others connection) at the intersection and install the required infrastructure for the implementation of the SCN. **LINKS**: provide the OBUs for the connected vehicles; provide an ITS-G5 RSU to be used for the ITS-G5 communication services and for implementing the detection services at the intersection; provide a connected bicycle to verify the SCN considering also a connected VRU; implement the Collective

		Perception Service according to the ETSI TS 103 324; implement the Dangerous Situation VRU Advertisement Service; develop the required software tools for the detection and the dynamics prediction of all road users exploiting visual camera and other sensors' information. **SWARCO**: provide information about the traffic lights to the road users and to the Dangerous Situation VRU Advertisement Service. **WIND-Tre**: provide the MEC server on which the Collective Perception Service can be executed and the 4G connectivity for LINKS RSUs and OBUs (SIM and network configurations). **AIRBUS:** provide cyber security cloud services and embedded IAM components.
Realisation Prerequisites	**Physical infrastr.**	• Electricity, mounting facilities and 4G and/or fibre optic/other connections at the intersection. • Connected traffic lights. • Visual cameras and depth sensors for monitoring the intersection. • Other potential traffic sensors (e.g., magnetic coils). • MEC server.
	Digital infrastr.	• **Communication technologies**: ITS-G5 and 4G/LTE. • **ITS services**: Collective Perception Service, Cooperative Awareness Service, Traffic Light Manoeuvre Service, Road and Lane Topology Service. • **Additional services**: Dangerous Situation VRU Advertisement Service. • **ETSI ITS messages**: CPM, CAM, SPAT, MAP, DENM. • Embedded IAM components. • Cyber security cloud services (IAM and supervision).
	Data availability	• Video flows, depth information of the intersection from LiDAR and/or other depth sensors. • Vehicle flows information from other sensors such as magnetic coils. • Position and dynamics information from the CAM of connected road users. • Information about the traffic light phases and timing. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Detection of road users, as well as the prediction of their dynamics, is challenging due to the likely high number of road users that may be present at the intersection and due to the different types of road users involved in this SCN. • Detection has to be timely performed since the information to the road users has to be sent with low latency. • Possibility to integrate security module and access control gateway in vehicles and infrastructure.
	Others, e.g., operations, safety regulations	• Privacy issues may rise since visual cameras are installed in a public place. The implementation of the SCN too, will not identify any road user and it will use the video flow just to detect the road users. No sensible information, which may be gathered from the

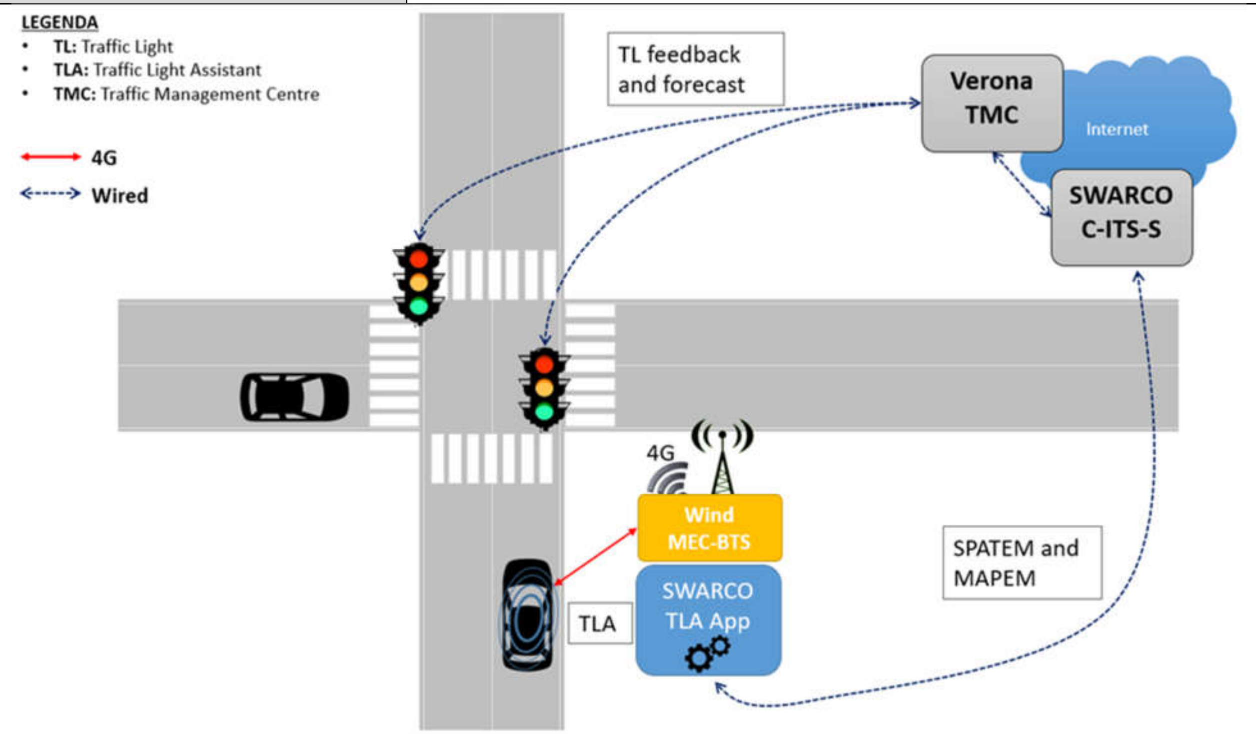
	camera and other sensors, will be disclosed.
Target/Evaluation metrics	• **Latency** of the information provided by the CPM perceived by road users. • **Accuracy** in the detection of the road users and in the prediction of their dynamics. • **Average time** for the connected and automated vehicle to go through the intersection. • **Average speed** of the connected and automated vehicle when going through the intersection. • **Accelerations/decelerations** (number of events and values) performed by the connected and automated vehicle when going through the intersection.
Impact	The Collective Perception Service can ease the crossing of an urban intersection performed by the connected and automated vehicle due to the information provided by the infrastructure. Furthermore, the Collective Perception Service can be extended to inform also VRUs about possible dangers. This SCN can influence the acceptance of autonomous vehicles by the society and it can motivate the importance of ICT and ITS also for VRUs since it provides a useful and tangible service to all road users.
Initial and target TRL	Initial: TRL 4 Target: TRL 6

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.7 SCN3.2 – GLOSA (Green Light Optimized Speed Advisory) in City of Verona, Italy

Name	**GLOSA in City of Verona, Italy**
Short name	**GLOSA**
ID	**UC3-SC32-GLOSA**
Overview	An urban intersection is monitored by the ICT4CART infrastructure. When a connected and automated vehicle 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 connected and automated vehicle can rely on the information received to reach it at the beginning of the next green phase and refine its driving action accordingly. The infrastructure will securely communicate with the vehicle using the 4G/LTE mobile network.
Description	The connected and automated vehicle is about to cross an urban intersection. The ICT4CART infrastructure is connected to the traffic lights of the intersection and receives feedback from the controllers about the traffic light status. The Traffic Management Centre sends a message pair to the TLA

	Application in the Multi-access Edge Computing (MEC) server: a MAPEM [MAP (topology) Extended Message, ETSI TS 103 301], containing intersection geometry and signal identifiers, and a SPATEM (Signal Phase and Timing Extended Message, ETSI TS 103 301), which contains real-time information of the traffic light signal phase and timing of the intersection. Using this information, the TLA Application 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 send the "time-to-green" countdown (TTG). The MEC server will use the 4G/LTE mobile network for sending the information to the vehicle. All types of communications are secured. Any cybersecurity event is reported to the supervision service. The connected and automated vehicle receives this information and can adjust its speed when crossing the intersection, to make the trip smoother. This information can be made available to the driver/vehicle through an HMI application, either using the vehicle's infotainment system or a customized application available in some handheld devices.



Key assumptions	• **Infrastructure installed:** intersection connected to the Traffic Management Centre, where SPATEM/MAPEM messages are generated. TLA application to be implemented/used at MEC server level and MEC server. • IAM components (security module and access control gateway) integrated in both vehicle and infrastructure. • Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All

<table>
<tr><td colspan="2"></td><td>communicating entities are registered in the IAM service.</td></tr>
<tr><td colspan="2">Actors and Relations</td><td>SWARCO: provision of the Traffic Light Forecast (TLF – SPATEM and MAPEM messages) enabling for the Traffic Light Assistance (TLA – including GLOSA and TTG services) service and of the application to be implemented in the MEC server. The TLA Application will elaborate the messages received from the TMC to provide the TLA service to the vehicles.

Comune di Verona: provide the required facilities (electricity and fibre optic/others connection) at the intersection and the urban traffic control system (i.e., traffic lights, communication capabilities and Traffic Management Centre).

CRF: provide the connected and automated vehicle to be used in the SCN.

WIND-Tre: provide the MEC server on which the TLA service can be executed and the 4G connectivity.

AIRBUS: provide cyber security cloud services and embedded IAM components.</td></tr>
<tr><td rowspan="3">Realisation Prerequisites</td><td>Physical infrastr.</td><td>• Electricity, mounting facilities and 4G and/or fibre optics/other connections at the intersection.
• Connected traffic lights.
• MEC server.</td></tr>
<tr><td>Digital infrastr.</td><td>• Communication technologies: 4G/LTE.
• ITS services: Traffic Light Assistant.
• ETSI ITS messages: SPATEM, MAPEM.
• Embedded IAM components.
• Cyber security cloud services (IAM and supervision).</td></tr>
<tr><td>Data availability</td><td>• Feedback from connected traffic lights.
• SPATEM messages and intersection topology (MAPEM) from the Traffic Management Centre.
• Position and dynamics of connected vehicle.
• GLOSA and TTG services to be sent to the vehicle.
• Vehicle and infrastructure authentication data (e.g., credentials, right management model).</td></tr>
<tr><td rowspan="2">Challenges/Barriers/ Open issues</td><td>Technical</td><td>• Traffic light forecast for intersections with actuated traffic control.
• Possibility to integrate security module and access control gateway in vehicles and infrastructure.
• Scalability; number of vehicles and number of messages to disseminate is too large.</td></tr>
<tr><td>Others, e.g., operations, safety regulations</td><td>• GLOSA needs to respect specific speed limitations.
• No sensible information, which may be gathered from the vehicle, will be disclosed.</td></tr>
</table>

Target/Evaluation metrics	• **Latency of the information** from the time the Traffic Light Controller (TLC) sends the feedback to the TMC to the reception of the TLA service by the vehicle at the intersection. • **Availability** and **accuracy** of the traffic light forecast.
Expected impact	Smooth trip across urban corridors, due to optimised crossing of signalised intersections. This SCN can influence the acceptance of autonomous vehicles by the society and decrease traffic congestion instances.
Initial and target TRL	Initial: TRL 6 Target: TRL 8

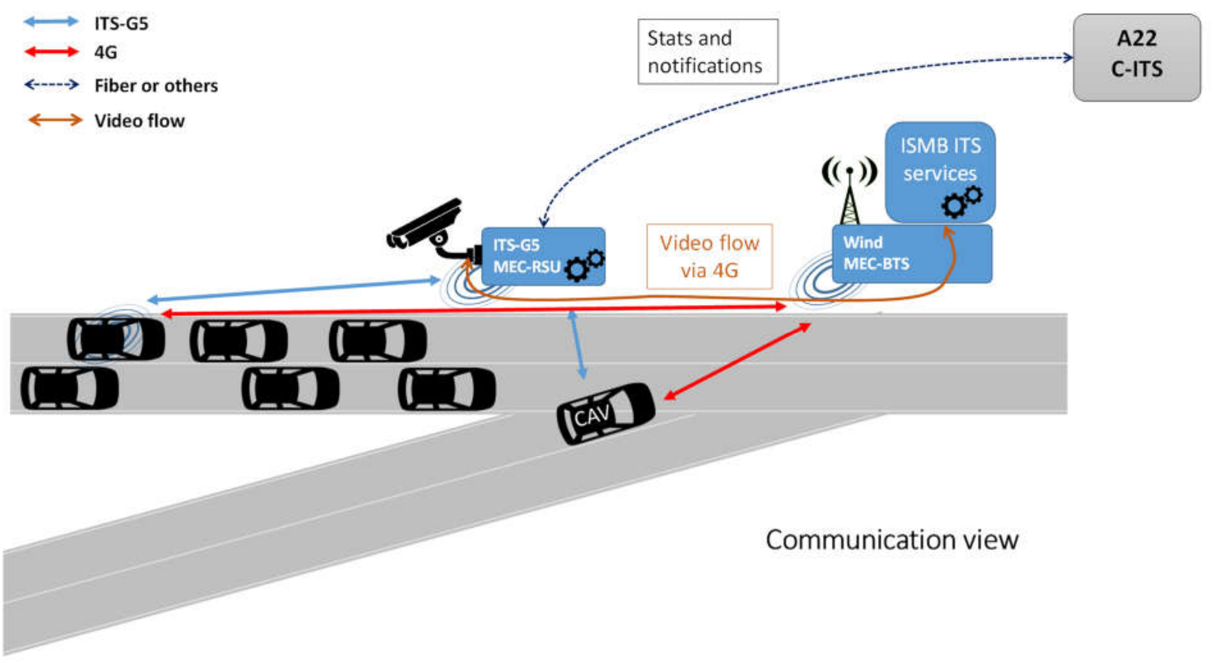
Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.8 SCN3.3 - Lane merging in Autostrada del Brennero, Italy

Name	**Lane merging in Autostrada del Brennero, Italy**
Short name	**LMBRE**
ID	**UC3-SCN33-LMBRE**
Overview (abstract)	The connected and automated vehicle is merging into the highway lane and it needs to avoid collisions and not to impede vehicles that are incoming on the highway lane. The ICT4CART infrastructure informs the vehicle in entrance about the incoming vehicles on the highway lanes and the vehicle can perform the driving actions according to the received information. The ICT4CART infrastructure exploits several sources of information, such as, traffic sensors, detection cameras, Vehicle-to-Infrastructure (V2I) communication, etc., to provide a full and accurate picture of the situation on the highway lanes. The vehicle in entrance has a higher level of information available with respect to relying only on the information gathered by the sensors that are on-board.
Description	The vehicle is in the entrance ramp of the highway and it is going to merge into the highway lane. The ICT4CART infrastructure monitors the highway lanes using different sensors (e.g., magnetic coils, visual cameras) to detect incoming vehicles and to predict their dynamics (i.e., speed and heading). Furthermore, it collects the information from Cooperative Awareness Messages (CAM) sent by the connected vehicles that are incoming on the highway lanes and that cannot be received by the autonomous vehicle. The ICT4CART infrastructure informs the vehicle on the entrance ramp about the presence of incoming vehicles providing details about the vehicles dynamics (e.g., position, speed and heading). The information about the vehicles and their dynamics can be provided using Collective Perception Messages (CPM).

<table>
<tr><td></td><td>The elaboration of the information gathered by the available sensors can be performed either on a Road Side Unit (RSU) that is located close to the entrance ramp either on a Multi-access Edge Computing (MEC) server that is located within the premises of a mobile network’s base station. The RSU will send the CPM using ITS-G5 communication, while the MEC server will use 4G/LTE mobile network for sending the same information.

The vehicle on the entrance ramp defines the driving actions to take, in order to avoid possible collisions and not to impede the incoming vehicles, based on the information contained in the CPM.

All types of communications between ICT4CART archictetural entities are secured. Any cybersecurity event related to ICT4CART infrastructure is reported to the supervision service.</td></tr>
<tr><td colspan="2">
</td></tr>
<tr><td>Key assumptions</td><td>IAM components (security module and access control gateway) integrated in both vehicle and infrastructure.
Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating ICT4CART architectural entities are registered in the IAM service.</td></tr>
<tr><td>Actors and Relations</td><td>CRF: provide the connected and automated vehicle to be used as vehicle on entrance; provide a connected vehicle to be used as incoming vehicle to check that ICT4CART infrastructure creates the CPM message also exploiting information received by the CAM sent by the incoming vehicles; implement the decision logic on the vehicle on entrance to take into consideration the information received by the CPM.

Autostrada del Brennero: provide the required facilities (electricity and possibly fibre optic/other connection) and hosts the required infrastructure for the implementation of the SCN.</td></tr>
</table>

		LINKS: provide the OBUs for the connected vehicles; provide an ITS-G5 RSU to be used for the ITS-G5 communication services and for implementing the vehicles detection services; implement the Collective Perception Service according to the ETSI TS 103 324; develop the required software tools for the vehicles detection and vehicles dynamics prediction exploiting visual cameras and other sensors' information. **WIND-Tre**: provide the MEC server on which the Services can be executed and the 4G connectivity for LINKS RSUs and OBUs (SIM and network configurations). **AIRBUS:** provides cyber security cloud services and embedded IAM components.
Realisation Prerequisites	**Physical infrastr.**	• Electricity and mounting pole close to the entrance ramp. • 4G and/or Fibre optics/others connection close to the entrance ramp. • Visual cameras and depth sensors for monitoring the highway lanes to detect incoming vehicles. • Other potential traffic sensors (e.g., magnetic coils). • MEC server (just in the MEC-based case).
	Digital infrastr.	• **Communication technologies**: ITS-G5 and 4G/LTE. • **ITS services**: Collective Perception Service, Cooperative Awareness Service. • **ETSI ITS messages**: CPM, CAM • Embedded IAM components. • Cyber security cloud services (IAM and supervision).
	Data availability	• Video flows, depth information of the highway lanes from LiDAR and/or other depth sensors. • Vehicle flows information from other sensors such as magnetic coils. • Position and dynamics of connected vehicle from CAM. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Detection of incoming vehicle is challenging since it has to be performed on targets that move at very high speed (i.e., up to 130 km/h). • Detection has to be performed very fast since the vehicle on the entrance ramp has to receive the information with very low latency. • Possibility to integrate security module and access control gateway in vehicles and infrastructure.
	Others e.g. operations, safety regulations	• The video flows and other sensors information gathered from the infrastructure on the highway should be transmitted to the MEC server if the MEC-based case is considered. The sharing of this information to the MEC server may not be possible due to security and privacy issues.

Target/Evaluation metrics	• **Latency** for the transmission of the information from the cars detection to the reception of the CPM messages by the vehicle on the entrance ramp. • **Accuracy** of the vehicles detection and of the prediction of vehicles dynamics. • **Average time** for the connected and automated vehicle to merge into the lane. • **Average distance** at the lane merge between the connected and automated vehicle and the first incoming vehicle (considering specific traffic conditions). • **Average speed** of the connected and automated vehicle when merging the lane. • **Accelerations/decelerations** (number of events and values) performed by the connected and automated vehicle when merging the lane.
Impact	Smooth and safe lane merging of a connected and automated vehicle can lead to a faster acceptance of autonomous vehicles by the society.
Initial and target TRL	Initial: TRL 4 Target: TRL 6

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.9 SCN3.4 - Precise positioning in urban and highway location

Name	**Precise positioning in urban and highway location**
Short name	**PPRTK**
ID	**UC3-SCN34-PPRTK**
Overview (abstract)	Precise Positioning will use standard GNSS (e.g., GPS) combined with correction information based on the Real Time Kinematic (RTK) technique in order to enhance the precision of positioning in rural environment, but also in more complex areas like urban environment (e.g., multi-path propagation). The correction information is provided either by physical or virtual Reference Stations and is distributed through the cellular network via Mobile Edge Computing (MEC). RTK can provide sufficient accuracy enhancements only up to a distance of about 10 km from a physical Reference Station. Otherwise, Network RTK has to be used, in order to calculate correction information for a so-called virtual Reference Station.
Description	**1. Precise Positioning using Physical Reference Stations** The correction information is provided directly from physical Reference Stations. If the Reference Stations are collocated with 4G/5G Radio Sites, the distance between the Reference Stations is typically far below 10 km. In this case, the MEC-Server can simply distribute the correction information provided by the nearest Reference Station (Physical Reference

		Stations collocated with 4G/5G Radio Sites are deployed in the German Test Site). **2. Precise Positioning using Virtual Reference Stations** The correction information is provided by a virtual Reference Stations using publicly available services (e.g., SAPOS in Germany) and can directly distributed by the MEC Server. In this case the distance between the physical Reference Stations are typically more than 50 km. Therefore, the correction information for a virtual Reference Station has to be calculated from the correction information provided by the physical Reference Stations (In the Austrian, the Italian and the Cross-Border Test Site, virtual Reference Stations are used). All types of communications are secured and any cybersecurity event is reported to the supervision service.
Key assumptions		• Comparing accuracy enhancements of RTK (physical Reference Stations) versus Network RTK (virtual Reference Station). • Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating entities are registered in the IAM service.
Actors and Relations		**NOKIA**: Telecom operator for the German Test Site, including RTK infrastructure/application. **T-MOBILE**: Telecom operator for the Austrian Test Site. **WIND-Tre**: Telecom operation for the Italian Test Site. **Ulm University (UULM)**: Demonstration of RTK application in a vehicle in German test site. **AIRBUS:** provides cyber security cloud services and embedded IAM components.
Realisation Prerequisites	**Physical infrastr.**	• Physical RTK Reference Stations collocated with 4G/5G Radio Sites (German Test Site).
	Digital infrastr.	• 4G/5G Cellular Radio Network, in order to connect the physical or virtual Reference Stations with an RTK Rover via a MEC-Server. • Cyber security cloud services (IAM and supervision).
	Data availability	• Correction information compliant to RTCM (Radio Technical Commission for Maritime Services) provide by a NTRIP (Network Transport of RTCM via Internet Protocol) Server. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).

Challenges/Barriers/Open	Technical	• Accuracy enhancements provided by RTK (Physical Reference Stations) and Network RTK (Virtual Reference Stations) has to be investigated and analysed, respectively. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastructure.
	Others e.g. operations, safety regulations	• Impact of weather and topology conditions on accuracy enhancements. • Deployment cost.
Target/Evaluation metrics		• Absolute accuracy of the enhancements provided by (Network) RTK.
Impact		Enabling road users to provide position information with sufficient accuracy for automated driving.
Initial and target TRL		Initial: TRL 3 - 5 Target: TRL 7

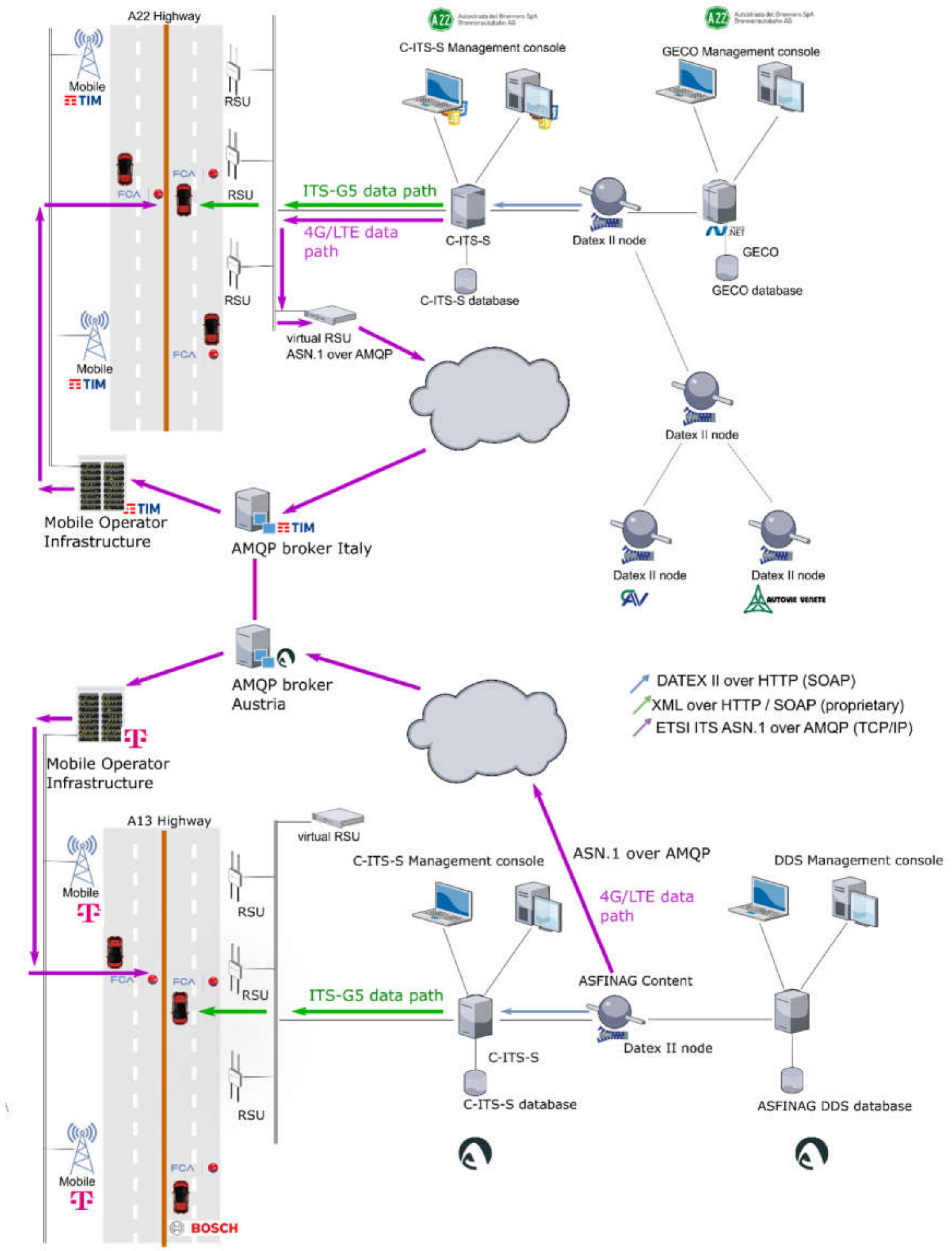
Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

4.10 SCN4.1 - Cross border interoperability between Italy-Austria (dynamic adaptation of vehicle automation level) at Brenner border

Name	**Cross border interoperability between Italy-Austria (dynamic adaptation of vehicle automation level) at Brenner border**
Short name	**DAVAXBR**
ID	**UC4-SCN41-DAVAXBR**
Overview (abstract)	Hybrid communication is included in the roadmap of EC and is mentioned in the Delegated Act. C-ROADS TF4-TF5 are addressing respectively the hybrid communication and the cross-border testing all across Europe. It is essential to build on C-ROADS harmonization efforts to progress with the ICT interoperability across countries (handover, etc.). While C-ROADS is currently addressing driving cases that are connected to the same back-end which synchronises with other back-ends, ICT4CART will address the handover between different back-ends, aiming at the development of a pan-European solution. The basic feature will be to seamlessly change back-end connections while driving between Austria and Italy and vice versa. The most relevant scenarios to showcase and validate this aspect will be selected. A major challenge is the agreement of the stakeholders in the projects ICT4CART, C-ROADS and ICT-18 5G-CROCO, 5G-MOBIX and 5G-CARMEN, which also address cross border interoperability. Developments in these other research projects will be adopted in ICT4CART wherever possible.

	This scenario will encompass cross border tests for: • Precise Positioning • ITS-G5 Day 1 • 4G/LTE tests analogous to ITS-G5 Day 1 • Dynamic adaptation of vehicle automation In all of these cases, the characteristics for handovers with **no transmission technology change** while crossing the border will be tested: • ITS-G5 to ITS-G5 • 4G/LTE to 4G/LTE In all of these cases the characteristics for handovers **with a change in transmission technology** while crossing the border will be tested: • ITS-G5 to 4G/LTE • 4G/LTE to ITS-G5
Description	The Scenario consists of three parts: 1) transition between ITS-G5 installations in two neighbouring countries, 2) transition between LTE infrastructure between two neighbouring countries, 3) transition from ITS-G5 to LTE or vice versa between two neighbouring countries. The tests of SCN2.1 will be performed while crossing the border with the vehicle from Italy to Austria and vice versa. **ITS-G5** This part involves the vehicle moving from one WLAN area to the next. There is no transition as such, but the identical implementation of the ITS-G5 standard in country 1 and country 2 is required and will be tested (C-Roads specifications). **LTE** The general approach is that a traffic information broker in each country provides the traffic information as a subscriber service. When requesting a subscription, the vehicle is directed to the broker in the respective country. When the vehicle crosses the border from country 1 to country 2, the vehicle subscribes relevant road section information with two traffic information brokers, one from country 1, and the other from country 2. The research will focus on how to achieve a seamless subscription handover at all times, and whether the handover to the mobile network operator of country 2 causes any disruptions. **ITS-G5 to LTE and vice versa** Similar to the ITS-G5 case, this is about entering/leaving an ITS-G5 WLAN area. The testing will focus on whether there are any unforeseen effects when the new provider is in a different country. **Side scenarios** • Precise Positioning, i.e., crossing the border without losing position information. • Prevention of L3 activation by the vehicle because of an incident right after the border. • Seamless Reception of in vehicle information.

	• Seamless reception of highway infrastructure road events (CAM, DENM – C-Roads specifications). • All types of communications between ICT4CART architectural entities are secured and any cybersecurity event related to ICT4CART infrastructure is reported to the supervision service.



Key assumptions		• The transmission of the infrastructure messages to the vehicles will be implemented according to the Geo-Hash concept. In this concept the vehicle subscribes to a road section and then receives all infrastructure messages for that section from a Message Broker. The position of the vehicle is not recorded in this concept. • The data from the infrastructure provider will be provided to the Message Broker either via a Virtual RSU from the ITS-G5 system or from the DATEX II node of the Traffic Control Centre. • C-ROADS is currently designing and specifying the C-ITS Hybrid Architecture,. It will be an AMQP Broker architecture,. The C-ROADS AMQP Broker will serve as basis for the exchange of C-ITS content over IP between any two parties. • Cyber security cloud services up and running: IAM service and supervision. Security modules and access control gateways must be able to connect to cyber security services. All communicating ICT4CART architectural entities are registered in the IAM service.
Actors and Relations		**ASFINAG**: Test site leader, ITS-G5 on Austrian side, Application for cross border communication. **A22 - AUTOSTRADA DEL BRENNERO:** Test site ITS-G5 on Italian side, Application for cross border communication. **LINKS**: Hybrid communication. **T-MOBILE**: LTE connectivity and MEC infrastructure at the Austrian side. **BOSCH**: vehicles for testing, vehicle HAD application, application for session handover. **CRF**: vehicles for testing, vehicle HAD application, application for session handover. **AIRBUS**: provides cyber security cloud services and embedded IAM components. **SWARCO**: Technology provider of ITS-G5 equipment and extended functionality of roadside equipment for Day 1.5 use cases.
Realisation Prerequisites	**Physical infrastr.**	• CRF vehicles with LINKS equipment and BOSCH vehicles (BMW or Mercedes) with BOSCH equipment. • ITS-G5, already deployed with current Day 1 functionality. • LTE base stations, already deployed.
	Digital infrast.	**Vehicles** • In car modem CAT6 or higher for LTE. • In car hybrid LTE/ITS-G5 Application. • In car GNSS receiver and antenna. • In car positioning engine (HW, SW). • In car maps. **Highway infrastructure** • ASFINAG CONTENT real-time ITS-G5 Service for ITS-G5.

		• ASFINAG CONTENT real-time DATEX II Service for LTE. • A22 CONTENT real-time ITS-G5 Service for ITS-G5. • A22 CONTENT real-time ETSI Service for LTE. • ITS-G5 connectivity. • LTE-A connectivity. Cyber security cloud services (IAM and supervision).
	Data availability	• ITS-G5 Day I by ASFINAG, already operational. • ITS-G5 Day I by A22, already operational. • DATEX II Service Segment Clearance by ASFINAG. • ETSI service (planned and unplanned events) by A22. • DATEX II Service Unplanned Events by ASFINAG, already operational. • DATEX II Service Planned Events (Roadworks) by ASFINAG. • Technical Exercise, the functionality to send simulated incidents, by ASFINAG already operational. • Functionality to send simulated incidents, by A22 already operational. • Technical Exercise, the functionality to receive simulated messages in the vehicle. • Vehicle and infrastructure authentication data (e.g., credentials, right management model).
Challenges/Barriers/Open issues	**Technical**	• Modem CAT6 or higher is needed in the vehicle. • Precise positioning via ITS-G5 is foreseen for DAY 1.5 use cases. • Possibility to integrate encryption and authentication, security module and access control gateway in vehicles and infrastructure.
	Others e.g. operations, safety regulations	• Clearance for level 3 for Test Site AUSTRIA GRAZ at AUSTRIATECH. • Clearance for level 3 for Test Site ITALY A22 at CRF. • Clearance for level 3 for Test Site AUSTRIA X-BORDER at AUSTRIATECH.
Target/Evaluation metrics		• **Latency:** The highway infrastructure messages of the incident location shall reach the vehicle 10sec before it reaches the incident location. Latency for sending the message is defined as round trip time (RTT) (i.e. 2x one way). • **Percentage of vehicles receive the incident message:** (10 + Latency) seconds or more before reaching the incident. Target is 100% of possible candidates, i.e., vehicles which are more than (10 + Latency) seconds away from incident when incident is created. • **Handover Gap:** The vehicle shall experience a maximum acceptable interruption of connected-status of no more than 10s.
Impact		Smooth transition between the two countries will allow the L3 functionalities to remain activated for longer periods of time, allowing safer driving conditions.
Initial and target TRL		Initial: TRL 3 Target: TRL 4

Note: the proposed cyber security capacities are only conceptual; no implementation will be done in this scenario.

5 ICT4CART UCs’ Functional Requirements

In this section, the functional requirements (required functions in order to realise the use cases and the corresponding scenarios) describe the features, behaviour, and general functionality that the proposed infrastructure’s system must support.

Requirement ID	Functional requirement	Core service
UC1-SCN11-SPIoTULM-F01	Automotive OEM Clouds should be able to communicate (registration and data exchange) with parking service providers through a common interface. That means the Fleet Manager (implemented in the BMW Cloud) sends a position and radius through the interface to a parking service provider and receives a collection of parking data for that area.	This interface is needed in UC1-SCN11-SPIoTULM for the exchange of parking/charging data.
UC1-SCN11-SPIoTULM-F02	Automotive OEM Clouds should be able to communicate (registration and data exchange) with a charging service provider through a common interface. That means the Fleet Manager (implemented in the BMW Cloud) sends a position and radius through the interface to a charging service provider and receives a collection of Charging Stations for that area.	This interface is needed in UC1-SCN11-SPIoTULM for the exchange of parking/charging data.
UC1-SCN11-SPIoTULM-F03	Automotive OEM Clouds should be able to request a) availability of parking space(s) within a given area and receive specific parking space(s) info for that area. This means the mentioned service provider gateway allocates appropriate parking space(s) to the requests sent by the Fleet Manager (BMW Cloud) and returns the parking space data.	This interface is needed in UC1-SCN11-SPIoTULM for the exchange of parking/charging data.
UC1-SCN11-SPIoTULM-F04	The interface should enable the Fleet Manager to ask for parking space predictions for a certain area, day and timeframe. The service provider gateway delivers those predictions (space, time, probability) to the Fleet Manager.	This interface is needed in UC1-SCN11-SPIoTULM for the exchange of parking/charging data.
UC1-SCN12-SPIoTCDV-F01	A connected vehicle shall be able to communicate via 4G/LTE.	Core requirement for the realization of UC1-SCN12-SPIoTCDV.
UC1-SCN12-SPIoTCDV-F02	The TMC shall provide parking space availability.	Core requirement for the realization of UC1-SCN12-SPIoTCDV.
UC1-SCN12-SPIoTCDV-F03	The TMC shall provide parking lot mapping in ETSI standard MAP format.	Core requirement for the realization of UC1-SCN12-SPIoTCDV.
UC1-SCN12-	The C-ITS-S shall be able to elaborate	Core requirement for the

SPIoTCDV-F04	parking request notifications coming from connected vehicles and provide parking information	realization of UC1-SCN12-SPIoTCDV.
UC2-SCN21-DAVAGRZ-F01 **UC2-SCN22-DAVATRN-F01** **UC2-SCN23-DAVACDV-F01** **UC4-SCN41-DAVAXBR-F01**	The TMC should be able to communicate with the vehicles through ITS-G5 messages.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.
UC2-SCN21-DAVAGRZ-F02 **UC2-SCN22-DAVATRN-F02** **UC2-SCN23-DAVACDV-F02** **UC4-SCN41-DAVAXBR-F02**	The TMC should be able to communicate with the vehicles through 4G/LTE messages.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.
UC2-SCN21-DAVAGRZ-F03 **UC4-SCN41-DAVAXBR-F03**	The TMC should be able to send Roadworks messages via ITS-G5.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.
UC2-SCN21-DAVAGRZ-F04 **UC4-SCN41-DAVAXBR-F04**	The TMC should be able to send Roadworks messages via 4G/LTE.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.
UC2-SCN21-DAVAGRZ-F05 **UC2-SCN22-DAVATRN-F03** **UC2-SCN23-DAVACDV-F03** **UC4-SCN41-DAVAXBR-F05**	The TMC should be able to send Traffic Incident messages via ITS-G5.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.
UC2-SCN21-DAVAGRZ-F06 **UC2-SCN22-DAVATRN-F04**	The TMC should be able to send Traffic Incident messages via 4G/LTE.	Core requirement for the realization of UC2-SCN21-DAVAGRZ and UC4-SCN41-DAVAXBR.

UC2-SCN23-DAVACDV-F04 **UC4-SCN41-DAVAXBR-F06**		
UC2-SCN21-DAVAGRZ-F07	There should be an AMQP Message Broker Austria within the ICT which holds traffic information in a geohashed structure, which can be subscribed to from the internet and which pushes messages to subscribers according to the subscribed geohash-tag.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC2-SCN21-DAVAGRZ-F08	The AMQP Message Broker should be able to process the Traffic Incident messages from the TMC.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC2-SCN21-DAVAGRZ-F09	The AMQP Message Broker should be able to process the roadworks messages from the TMC.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC2-SCN21-DAVAGRZ-F10	The vehicles should be able to subscribe to the AMQP Message Broker.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC2-SCN21-DAVAGRZ-F11	The MEC Server should have an AMQP Message Broker implemented on it.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC2-SCN21-DAVAGRZ-F12	The vehicles should refer to the MEC server if subscribed to the AMQP Austria server and in the relevance radius of the MEC server.	Core requirement for the realization of UC2-SCN21-DAVAGRZ
UC3-SCN31a-VMULM-F01	Automated cars should be able to communicate using ITS-G5.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F02	Automated cars should be able to communicate using 5G/LTE.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F03	The MEC server should be able to push a current/updated environment model to automated vehicles which are near the intersection.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F04	Automated vehicles should be able to push their own perceived environmental model to the MEC server, in order to extend its field of view and to increase accuracy.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F05	Connected Traffic lights should be able to communicate via ITS-G5.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F06	Connected Traffic lights should be able to communicate via 5G/LTE.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31a-VMULM-F07	Connected Traffic lights should broadcast traffic light state per lane and predictions via SPATEM/MAPEM messages.	Core requirement for the realization of UC3-SCN31a-VMULM
UC3-SCN31b-VMCDV-F01	The Collective Perception Service (CPS) should be able to gather position and	Core requirement for the realization of UC3-SCN33-LMBRE

UC3-SCN33-LMBRE-F01	motion information from sensors, such as visual cameras, depth sensors and other monitoring sensors.	and of UC3-SCN31b-VMCDV
UC3-SCN31b-VMCDV-F02 **UC3-SCN33-LMBRE-F02**	The Collective Perception Service (CPS) should be able to locate and predict dynamics of the road users based on the available environmental information.	Core requirement for the realization of UC3-SCN33-LMBRE and of UC3-SCN31b-VMCDV.
UC2-SCN21-DAVAGRZ-F13 **UC3-SCN31b-VMCDV-F03** **UC3-SCN33-LMBRE-F03**	The road-side infrastructure should be able to communicate with the MEC server.	Needed by all the MEC-based applications developed in the ICT4CART project.
UC3-SCN31b-VMCDV-F04 **UC3-SCN33-LMBRE-F04**	The Collective Perception Service (CPS) should be able to communicate with connected road users through standard ITS-G5 message.	Needed by all ITS services implemented in the ICT4CART project.
UC3-SCN31b-VMCDV-F05 **UC3-SCN33-LMBRE-F05**	The Collective Perception Service (CPS) should be able to communicate with connected road users using ITS-G5 communication stack.	Needed by all ITS services implemented in the ICT4CART project.
UC3-SCN31b-VMCDV-F06 **UC3-SCN33-LMBRE-F06**	The Collective Perception Service (CPS) should be able to communicate with connected road users using 4G/LTE communication technology.	Needed by all ITS services implemented in the ICT4CART project.
UC3-SCN31b-VMCDV-F07	The Traffic Light Maneuver Service and the Road and Lane Topology Service should be able to communicate with connected road users using ITS-G5 communication stack.	Needed by all ITS services implemented in the ICT4CART project.
UC3-SCN31b-VMCDV-F08	The Traffic Light Maneuver Service and the Road and Lane Topology Service should be able to communicate with connected road users using 4G/LTE communication technology.	Needed by all ITS services implemented in the ICT4CART project.
UC3-SCN31b-VMCDV-F09	The Dangerous Situation VRU Advertisement Service should be able to communicate with connected VRUs.	Core requirement for the realization of UC3-SCN31b-VMCDV.
UC3-SCN31b-VMCDV-F10	The Dangerous Situation VRU Advertisement Service and the Collective Perception Service should be able to communicate with the Traffic Light Maneuver Service and the Road and Lane Topology Service.	Core requirement for the realization of UC3-SCN31b-VMCDV
UC3-SCN31b-	The Dangerous Situation VRU	Core requirement for the

VMCDV-F11	Advertisement Service should be able to gather position and motion information from sensors, such as visual cameras, depth sensors and other monitoring sensors.	realization of UC3-SCN31b-VMCDV
UC3-SCN31b-VMCDV-F12	The Dangerous Situation VRU Advertisement Service should be able to locate and predict dynamics of the road users based on the available environmental information.	Core requirement for the realization of UC3-SCN31b-VMCDV
UC3-SCN32-GLOSA-F01	Connected vehicle shall be able to communicate via 4G/LTE	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN32-GLOSA-F02	TMC shall be connected to the traffic light controllers to retrieve traffic light feedback and forecast information	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN32-GLOSA-F03	C-ITS-S shall receive traffic light feedback and forecast information from TMC and elaborate MAPEM and SPATEM messages	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN32-GLOSA-F04	C-ITS-S shall send MAPEM and SPATEM messages to the TLA App in MEC server	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN32-GLOSA-F05	TLA App shall be able to elaborate MAPEM and SPATEM messages to generate GLOSA and TTG services to the connected vehicle	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN32-GLOSA-F05	Connected vehicle shall send GPS coordinates to the TLA App to enable generation of GLOSA and TTG services	Core requirement for the realization of UC3-SCN32-GLOSA
UC3-SCN34-PPRTK-F01	Physical RTK Reference Station available (German Test Site)	
UC3-SCN34-PPRTK-F02	RTK Rover (for automated Cars) are available	
UC3-SCN34-PPRTK-F03	RTK Rover (in automated cars) should be able to connect to Physical RTK Reference Station via 4G/5G Radio Network (German Test Site)	
UC3-SCN34-PPRTK-F04	RTK Rover (in automated cars) should be able to connect to Virtual RTK Reference Station (e.g., SAPOS) via 4G/5G Radio Network	
UC3-SCN34-PPRTK-F05	Network of Physical RTK Reference Station available (German Test Site)	
UC3-SCN34-PPRTK-F06	RTK Rover (in automated cars) should be able to connect to Network of Physical RTK Reference Stations via 4G/5G Radio Network (German Test Site)	

6 ICT4CART UCs' Non-Functional Requirements

In this section the non-functional requirements that will ensure the correct operation of the ICT4CART Use Cases and the corresponding Scenarios are presented. The term non-functional requirements is used to describe the requirements that ensure the correct operation of the various ICT4CART components in the system, e.g., performance, operation conditions, scalability requirements, etc. Generally, non-functional requirements answer the question on how, in technological terms, functional requirements are achieved.

Requirement ID	Non-functional requirements	Comments
UC1-SCN11-SPIoTULM-NF01	For the exchange of parking data via the interface, that is to be specified, the "mobivoc" data format should be used (and if necessary extended) for the purpose of this Use Case.	Standardized (mobility) vocabulary using Semantic Web technologies and ontologies. (www.mobivoc.org)
UC1-SCN12-SPIoTCBV-NF01	V2V communication means must integrate authentication and encryption components.	
UC1-SCN12-SPIoTCBV-NF02 **UC3-SCN31b-VMUCDV-NF01** **UC3-SCN33-LMBRE-NF01**	Vehicle-Infrastructure communication means must integrate authentication and encryption components.	
UC1-SCN11-SPIoTULM-NF02 **UC1-SCN12-SPIoTCBV-NF03** **UC2-SCN22-DAVATRN-NF01** **UC2-SCN23-DAVACDV-NF01** **UC3-SCN31a-VMULM-NF01** **UC3-SCN31b-VMUCDV-NF02** **UC3-SCN32-GLOSA-NF01** **UC3-SCN33-**	Vehicle – Cloud service communication means must integrate authentication and encryption components.	At the very least, there will be communications to the cloud based supervision service. All FR depending on NFR related to vehicle – MEC server communications apply if the use case implementation also deploys cloud services instead of MEC server hosted services.

LMBRE-NF02		
UC1-SCN12-SPIoTCBV-NF04 **UC2-SCN22-DAVATRN-NF02** **UC2-SCN23-DAVACDV-NF02** **UC3-SCN31a-VMULM-NF02** **UC3-SCN31b-VMUCDV-NF03** **UC3-SCN32-GLOSA-NF02** **UC3-SCN33-LMBRE-NF03**	Vehicle – MEC server communication means must integrate authentication and encryption components.	
UC3-SCN31a-VMULM-NF03	Vehicle – RSU communication means must integrate authentication and encryption components.	
UC1-SCN12-SPIoTCBV-NF05 **UC2-SCN22-DAVATRN-NF03** **UC2-SCN23-DAVACDV-NF03** **UC3-SCN32-GLOSA-NF03** **UC3-SCN33-LMBRE-NF04** **UC3-SCN31a-VMULM-NF04** **UC3-SCN31b-VMUCDV-NF04**	RSU – Service communication means must integrate authentication and encryption components.	At the very least, there will be communications to the cloud based supervision service. All FR depending on NFR related to RSU – MEC server communications apply if the use case implementation also deploys cloud services instead of MEC server hosted services.
UC3-SCN31a-VMULM-NF05	MEC Server – Service communication means must integrate authentication and encryption components.	At the very least, there will be communications to the cloud based supervision service.
UC1-SCN12-SPIoTCBV-NF06	RSU - MEC server communication means must integrate authentication and encryption components.	

UC2-SCN22-DAVATRN-NF04 **UC2-SCN23-DAVACDV-NF04** **UC3-SCN31b-VMUCDV-NF05** **UC3-SCN33-LMBRE-NF05**		
UC1-SCN11-SPIoTULM-NF03 **UC3-SCN31b-VMUCDV-NF06** **UC3-SCN32-GLOSA-NF04**	Service to service communication means must integrate authentication and encryption components.	There will also be communications to the cloud based supervision service.
UC1-SCN11-SPIoTULM-NF04 **UC1-SCN12-SPIoTCBV-NF07** **UC2-SCN22-DAVATRN-NF05** **UC2-SCN23-DAVACDV-NF05** **UC3-SCN31b-VMUCDV-NF07** **UC3-SCN32-GLOSA-NF05** **UC3-SCN33-LMBRE-NF06**	Any communicating entity must be registered in the IAM service, along with its rights.	
UC1-SCN11-SPIoTULM-NF05 **UC1-SCN12-SPIoTCBV-NF08** **UC2-SCN22-DAVATRN-NF06** **UC2-SCN23-DAVACDV-NF06**	Any cyber security issue regarding authentication and access within a vehicle should be reported by the vehicle to the supervision service as an event.	The message format and protocol has not been defined yet.

UC3-SCN31a-VMULM-NF06 **UC3-SCN31b-VMUCDV-NF08** **UC3-SCN32-GLOSA-NF06** **UC3-SCN33-LMBRE-NF07**		
UC1-SCN12-SPIoTCBV-NF09 **UC2-SCN22-DAVATRN-NF07** **UC2-SCN23-DAVACDV-NF07** **UC3-SCN31a-VMULM-NF07** **UC3-SCN31b-VMUCDV-NF09** **UC3-SCN32-GLOSA-NF07** **UC3-SCN33-LMBRE-NF08**	Any cyber security issue regarding authentication and access within a RSU should be reported by the RSU to the supervision service as an event.	The message format and protocol has not been defined yet.
UC1-SCN12-SPIoTCBV-NF10 **UC2-SCN22-DAVATRN-NF08** **UC2-SCN23-DAVACDV-NF08** **UC3-SCN31a-VMULM-NF08** **UC3-SCN31b-VMUCDV-NF10** **UC3-SCN32-GLOSA-NF08** **UC3-SCN33-LMBRE-NF09**	Any cyber security issue regarding authentication and access within a service (MEC server) should be reported by the service to the supervision service as an event.	The message format and protocol has not been defined yet.

UC1-SCN11-SPIoTULM-NF06 **UC1-SCN12-SPIoTCBV-NF11** **UC3-SCN31a-VMULM-NF09** **UC3-SCN32-GLOSA-NF09**	Any cyber security issue regarding authentication and access within a cloud service should be reported by the service to the supervision service as an event.	The message format and protocol has not been defined yet.
UC2-SCN21-DAVAGRZ-NF01 **UC4-SCN41-DAVAXBR-NF01**	ITS-G5 communication (air interface) should have a latency of less than 10 seconds.	
UC2-SCN21-DAVAGRZ-NF02 **UC4-SCN41-DAVAXBR-NF02**	4G/LTE communication TMC to vehicle should have a latency of less than 10 seconds.	

7 Conclusions

This deliverable provides a description of the facilities to be used in the four test sites involved in the ICT4CART project, as well as a thorough presentation of the Use Cases and the associated Scenarios that are to be developed and demonstrated in order to evaluate the ICT4CART unified architecture.

More specifically, for each use case, a short description, sequence of actions, prerequisites, required components, challenges (technical, operational, etc.), evaluation targets/metrics and other relevant information are included. Additionally, a list of high-level functional and non-functional requirements linked to each use case and scenario is extracted, which will feed the system requirements subtasks of Task 2.3. Overall, the defined requirements will serve as an input to the following project work such as specification and definition of its architecture, and subsequently to the development work.

For each of the Use Cases, the project focuses on several representative traffic situations, which demonstrate the influence of the project outcome to the most critical traffic conditions with respect to safety and performance. For each Scenario the realisation prerequisites, the required physical and digital equipment, are considered.