Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D. 1.7
INITIAL SPECIFICATION OF COMMUNICATION SYSTEM FOR IoT ENHANCED AD

Due delivery date: 30/9/2017

Actual delivery date: 29/09/2017

Organization name of lead participant for this deliverable: TIM

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)	

AUTOPILOT

Document Control Sheet

Deliverable number:	D1.7
Deliverable responsible:	TIM
Workpackage:	T1.4 “Communication Specification”
Editor:	TIM

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Almeida, Miguel	NEC	miguel.almeida@neclab.eu
Alen, Silvia	CTAG	silvia.alen@ctag.com
Bastianelli, Andrea	Thales	andrea.bastianelli@thalesgroup.com
Ben Alaya, Mahdi	Sensinov	benalaya@sensinov.com
Brevi, Daniele	ISMB	brevi@ismb.it
Bianco Levrin, Federico	TIM	federico.biancolevrin@telecomitalia.it
Buracchini, Enrico	TIM	enrico.buracchini@telecomitalia.it
Chapuis, Cedric	Continental	Cedric.Chapuis@continental-corporation.com
Chiocchetti, Ezio	TIM	ezio.chiocchetti@telecomitalia.it
Cuenot, Philippe	Continental	Philippe.Cuenot@continental-corporation.com
Falcitelli, Mariano	CNIT	mariano.falcitelli@cnit.it
Ferrera, Enrico	ISMB	ferrera@ismb.it
Fiammengo, Anna	TIM	annamaria.fiammengo@telecomitalia.it
Gatti, Fabrizio	TIM	fabrizio1.gatti@telecomitalia.it
Gavilanes Castillo, Guido Alejandro	ISMB	gavilanes@ismb.it
Jansen, Sven	TNO	sven.jansen@tno.nl
Larini, Giovanna	TIM	giovanna.larini@telecomitalia.it
Marcasuzaa, Herve	Valeo	herve.marcasuzaa@valeo.com
Long, Daniela	TIM	daniela.long@telecomitalia.it
Martinez, Vincent	NXP	vincent.martinez@nxp.com
Martinez, Jose Manuel	CTAG	josemanuel.martinez@ctag.com
Noto, Sandro	CNIT	snoto@cnit.it
den Ouden, Jos	TUE	j.h.v.d.ouden@tue.nl
Petrescu, Alexandre	CEA	alexandre.petrescu@cea.fr
Scholliers, Johan	VTT	Johan.Scholliers@vtt.fi
Solmaz, Gurkan	NEC	gurkan.solmaz@neclab.eu
van de Sluis, Jacco	TNO	jacco.vandesluis@tno.nl
van Eert, Marc	Technolution	marc.van.eert@technolution.eu
Vermesan, Ovidiu	Sintef	Ovidiu.Vermesan@sintef.no

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	02/03/17	Table of Contents	TIM
V0.11	28/03/17	Integration of table of contents and structure with received contributions: NXP, TNO, CEA, Continental and Sensinov	TIM
V0.12	31/03/17	Rationalization of ToC	TIM
V0.13	11/04/7	Section 3.3 Communication interfaces	TIM
V0.15	26/04/17	Section 2.2 & Section 4	TIM, Sensinov, TNO
V0.16		Contributions from NXP for the sections 3.3 and 4.2.3.	NXP
V0.2	16/05/17	Update of chapter 2,3,4 and 5	TIM, NXP, CEA, Sensinov, CNIT
V0.25	29/05/17	Contribution arrived in the time range: 16/05 → 28/06	TIM, CNIT and TNO
V0.3	08/06/17	Contribution arrived in the time range: 29/05 → 08/06	TIM, NXP, NEC, VTT, TNO
V0.4	28/06/17	Contribution arrived in the time range: 08/06 → 28/06	TIM, NEC, TNO, TUE, CONTI
V0.5	19/07/17	Contribution arrived in the time range: 28/06 → 18/07	TIM, NEC, CTAG
V0.6	25/07/17	Contribution arrived in the time range: 18/07 → 25/07	CEA, SINTEF, TNO
V0.7	28/07/17	Contribution arrived in the time range: 25/07 → 28/07	SINTEF and ISMB
V0.8	03/08/17	Final Revision, draft for Internal Reviewers	TIM
V0.93	28/09/17	Final revision after peer review	TIM
V1.0	29/09/17	Format for submission	Rita Bhandari, ERTICO

Abstract
This document presents the specification of requirements concerning communication means and in particular the capabilities necessary for IoT and AD use case – initial release.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
3GPP	Third Generation Partnership Project
5GAA	5G Automotive Alliance
3G, 4G, 5G	3GPP mobile technologies
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AAS	Active Antenna System
AD	Automated Driving
ADASIS	Advanced Driver Assistance System
AE	Application Entity
AIOTI	Alliance for IoT Innovation
BC	Business Case
BLE	Bluetooth LowEnergy
BTS	Base Transceiver Station
CA	Carrier Aggregation
CC	Component Carrier
C-ITS	Cooperative ITS
CAM	Cooperative Awareness Message
CEN	European Committee for Standardization
CSE	Common Services Entity
CSI	Channel State Information
D2D	Device-to-Device
DENM	Distributed Environmental Notification Message
DITCM	Dutch Integrated Testsite Cooperative Mobility
DL	Downlink
DM RS	Demodulation Reference Signal
eMTC	enhanced Machine Type Communication
eNodeB	Evolved Node B
E2E	End-to-End
EC	European Commission
EN	European Standard
ERM	EMC and Radio Spectrum Matters
ETSI	European Telecom Standardisation Institute
EG	ETSI Guide
ES	ETSI Standard
FD-MIMO	Full-Dimension MIMO Carrier Aggregation
GN	GeoNetworking
GSM	Global System for Mobile Communications (3GPP technology)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

Acronym	Definition
IMT- Advanced	International Mobile Telecommunications-Advanced
IoT	Internet of Things
ISO	International Organization for Standardization
IP	Internet Protocol
ITS	Intelligent Transport Systems
ITU-R	International Telecommunication Union Radio Sector
KA	Knowledge Area
KPI	Key Performance indicator
LDM	Local Dynamic Map
LTE	Long Term Evolution (3GPP technology)
LTE-A	LTE-Advanced
M2M	Machine-to-Machine
MAP	Map data
Mca, Mcc, Mcn	oneM2M standard interfaces
MCT	Machine Type Communication
MIMO	Multiple Input/Multiple Out
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrow Band Internet of Things
NFC	Near Field Communications
NGSI	Next Generation Service Interfaces
NSE	Network Services Entity
OCB	Outside the Context of a BSS
OMA	Open Mobile Alliance
OBU	On-Board-Unit
oneM2M	Organization to develop technical specifications for Machine-to-Machine and Internet of Things services
PC5	Interface between two UEs
PDU	Packet Data Unit
PF	Platform
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
SPAT	Signal Phase and Time
TC	Technical Committee
TCC	Traffic Control Center
TM	Transmission Mode
TR	Technical Report
TS	Technical Specification
TTT	Transport and Traffic Telematics
TX	Transmission
UC	Use case
UE	User Equipment
UL	Uplink

Acronym	Definition
Uu	UMTS Air Interface
V2X, V2I, V2V	Vehicle-to: X= everything, I=Infrastructure, V= Vehicle
WG	Working Group
WP	Working Package

Table of Contents

List of Figures

List of Tables

Executive Summary

This document, D1.7, provides the initial specification of requirements concerning communication means and in particular the capabilities necessary for Internet of Things (IoT) and Automated Driving (AD) use cases. It is delivered in M09. It is produced based on the activities of T1.4 – Communication Specification task. The activities of T1.4 continue until M14, and between M32-35. An update of this document is planned by M30 on the base of: T1.4 activities, use case definitions by T1.1, IoT Architecture and Specification by T1.2 as well as the pilot sites experience.

The main target of the AUTOPILOT project is leveraging IoT to have progress in AD. This document is an outcome of T1.4 activities and it consists of inputs received by all participant organizations of the task. As various participants span a wide-range of technical domains, the document reflects this in the sense that it covers various communication domains in the field of AD and IoT.

IoT is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. The IoT brings a new paradigm where the devices are things that are connected and communicating with other things. The interaction will be with a heterogeneous continuum of users, things and real physical events and the Internet is the common convergence connectivity capability, replacing the previous independent systems.

The concept of Internet of Vehicles (IoV) or Vehicle-to-Everything (V2X) communications applied for autonomous transportation and mobility applications, requires creating mobile ecosystems based on trust, security and convenience to connectivity services and transportation applications in order to ensure security, mobility and convenience to consumer-centric transactions and services. In this context for autonomous vehicle applications, 5 communication domains are defined covering the communications of vehicle to everything (V2X) that includes vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), vehicle to device (V2D) vehicle to grid (V2G) and vehicle to vehicle (V2V) as important communication building blocks of the IoT ecosystems.

Task1.4 is devoted to the identification and analysis of the communications-related requirement relevant for the use cases selected in Task1.1 Having as a reference the layered end-to-end architecture specified in Task1.2 and the consolidated communications standards related to IoT, ITS, V2X and all the related communications technologies, D1.7 provides an overview about the various communications technologies and protocols that are considered applicable for AUTOPILOT.

The identification of the significant communication requirements for the 5 AUTOPILOT large scale pilots has been carried out analysing them on the base of 7 different essential parameters (End-to-end latency, Reliability, Bandwidth, Communication range, Node mobility, Network density and Security), considered relevant by scientific literature. This activity has been performed to guarantee a credible reality check and to properly address/prioritize the development and deployment tasks in other WPs.

1 Introduction

1.2 Purpose of document

This document represents the Deliverable D1.7 “Initial specification of Communication System for IoT enhanced AD”, first output carried out within Task 1.4 “Communication Specification” of project AUTOPILOT. According to project Technical Annex, the D1.7 purpose is to present the “Specification of requirements concerning communications means and in particular the capabilities necessary for IoT and AD use cases”.

1.3 Intended Audience

This deliverable (D1.7) is a Public document and therefore, the intended audience for this document is considered to be anyone that is interested in Communication System requirements and capabilities applied in automated driving progressed by IoT.

Within the AUTOPILOT project, the main intended audience for this deliverable is considered to be all the AUTOPILOT participants and in particular, the AUTOPILOT participants involved in Task 2.4 “Development and integration of IoT devices” and in Task 2.5 “Pilot Readiness verification”.

1.4 Process

The specification described in this document, was made following a process that included several meetings amongst task partners. In a first phase the group addressed an information collection activity focusing a general overview about the use cases considered within AUTOPILOT Task 1.1, a description of the communication infrastructure of the pilot sites and a detailed State Of the Art regarding communications technologies of interest for the project. In a second phase, considering the architecture framework worked out by T1.2, the communication interfaces have been identified and described. Finally basing on the analyses carried out in the previous phases] and the guidelines available on document "5G Automotive Vision” [99], the identification and the evaluation of the relevant communication requirements has been performed.

1.5 Outline of the document

The deliverable has been organized into 6 different sections:

- The aim of chapter 2 “AUTOPILOT Project ecosystem” is to provide a general overview of the Autopilot project scenario summarising the use cases addressed by the project (please consider D1.1 [1] for a complete description of them) and a clear picture of the communication infrastructure currently present in the various pilot sites.
- The aim of chapter 3 “Communication technologies review and description” is to provide a general overview about the various communications technologies that can be used within Autopilot project. For each of these technologies some basic points have been covered such as the overview about main features and basic indicators representing the technology key performances.
- Section 4 “Autopilot Infrastructure Architecture” aims to provide:
    - a general reference architecture scheme that can be in principle applied to all the pilot sites trials;
    - a description of all the macro elements that are part of the reference architecture;
    - the identification of the communication interfaces and their general description.

The work for this chapter is based on the outputs of task 1.2 “IoT Architecture and Specification” and task 1.3 “Vehicle IoT platform specification”, having the focus to highlight mainly communications aspects involved by the project.

- In section 5 “Communication requirements” the identification and the description of the communication requirements necessary to allow chapter 1 use cases to be executed within the various pilot sites has been carried out basing on the critical key parameters highlighted in Project Proposal (e.g. end-to-end latency, throughput, reliability…).
- Section 6, finally reports the conclusions for all the work done.

2 AUTOPILOT Project ecosystem

2.1 AD use cases to be considered

As reported in AUTOPILOT D1.1 [1], the main use cases considered in the project are:

- Automated Valet Parking

The main research questions for Automated Valet Parking concern positioning and control, and prevention of conflicts with other (legacy) cars and vulnerable road users (i.e. safety and efficiency improvements). This requires scenarios with legacy traffic and route obstructions in a variety of environments (e.g. indoor and outdoor) and different configurations of IoT sourcing for local dynamic maps. Assessment criteria should consider (at least) the traffic flow on parking areas, vehicle control performance and duration of the parking operation.

- Highway Pilot

The main research questions for Highway Pilot relate to the detection of road (infrastructure) obstructions and road defects relevant for automated driving operation and assess when human interventions are required. Scenarios focus at motorway application environments (with a variety of types of obstructions) and at driving speeds where the range of vehicle mounted sensors is a limiting factor. The assessment data needs to indicate the detection potential of vehicle mounted systems and data exchange timing requirements.

- Platooning

The main research questions for Platooning concern scheduling and organisation of platoons (from complex road networks towards motorway platooning), interactions with legacy traffic, and driving efficiency and comfort. The scenarios need to include a variety of starting configurations of the platoon assembly process and vehicle types, congestion levels of traffic, different penetration rates of legacy traffic connected to the platooning system, and specific (potential) interactions with legacy traffic. Assessment data should indicate the efficiency of the platoon assembly, platooning driving performance (e.g. in terms of safety and comfort), and detection and prediction capability of legacy vehicle manoeuvres.

- Urban Driving

The main research questions for Urban Driving relate to the interaction with traffic lights and legacy traffic, robustness and safety when dealing with vulnerable road users, and positioning. The scenarios involve intersections, locations with presence of (large groups of) vulnerable road users, and different levels of congestion. Assessment data criteria needs to include changes in traffic efficiency (including vulnerable road users), as well as a comparison of functional performance of current AD systems and IoT-extended AD systems in real-traffic conditions.

- Car Sharing

The main research questions for car sharing are in which extent heterogeneous IoT sources can provide event detections and support traffic predictions, which penetration rate of IoT devices is required, how to address scalability (geographical and users/sources), and how to support fleet and vehicle maintenance. The scenarios should involve a scalable IoT-enabled population and heterogeneity, and a significant geographical area needs to be considered. Car sharing should be deployed for a large community of users in operational situations (real traffic conditions), targeting

to capture occurring incidents (e.g. road closure, sports events, etc.), and involve a significant fleet of vehicles to be connected to the car sharing service. Assessment data should allow for comparison of predicted and actual travel times of vehicles, and as well as provide indications on how users' comfort (e.g. waiting time) is affected using IoT.

The use cases analysis from the communication requirements point of view is one of the goals of the task activities and it is reported in section 5.

2.2 Pilot sites infrastructure

2.2.1 Pilot site Finland - Tampere

The Autopilot Pilot Site in Finland is located in Tampere, in the town district of Hervanta, at the premises of VTT.

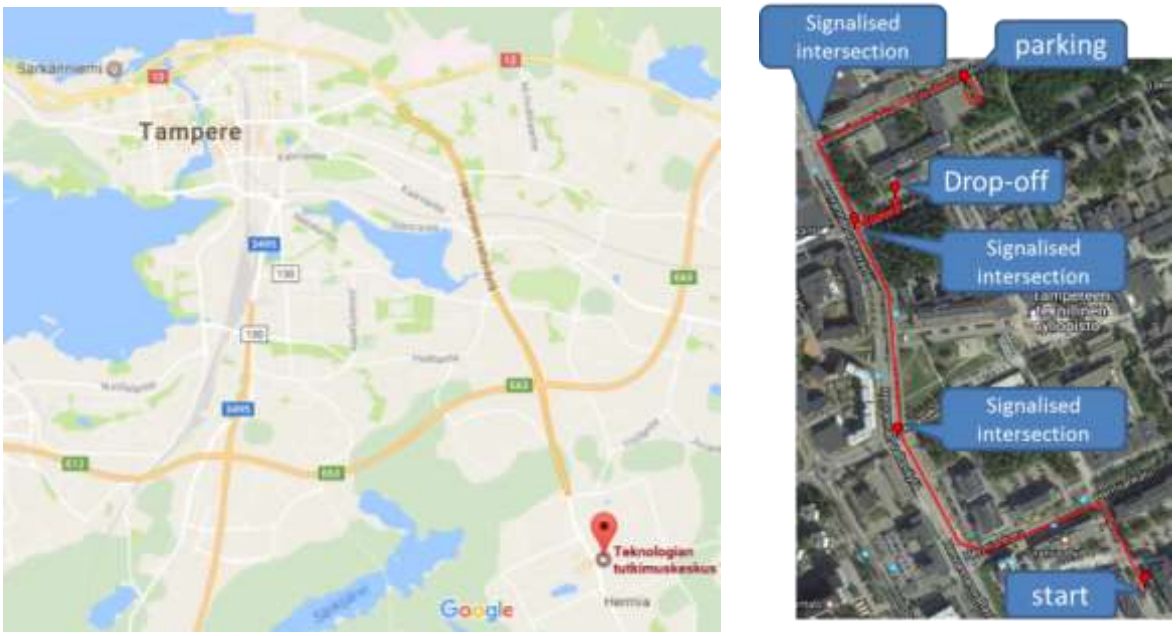


Figure 1 - Location of the test site in Tampere and draft test route

The pilot is located on the premises of VTT and on the public roads in the neighbourhood.
The major road (Hervannan Valtaväylä) connecting Hervanta to the city centre is a road with two lanes in each direction, with maximum speed limit of 50 km/h. There is a separate cycle track at the east side of the road, which is used by students and personnel working in the Hermia region.

Traffic lights are connected to the network of the city of Tampere and real-time information is publicly available for selected traffic lights. Traffic lights in Finland have a pre-green amber phase. The city of Tampere is also installing traffic cameras at major intersections.

The vehicles which will be used in the AUTOPILOT test site are research vehicles from VTT. VTT has 2 research vehicles, a Citroen C4 which has been converted by VTT for automated driving and acts as an innovation environment where industry can test sensors and applications, and a Volkswagen Touareg, which is equipped with V2X equipment. If available, other V2X enabled vehicles will be included in the test site. VTT has also a mobile station on which roadside infrastructure, such as V2X equipment and cameras can be installed. This equipment will be used for the traffic cameras used in the pilot use cases. Another camera may be installed at the VTT premises.

On the Tampere Pilot site two use cases are considered:
1) Urban driving with intersection support, for the intersections on the Hervannan Valtaväylä.
2) The Automated Valet Parking (AVP) use case will be executed on the VTT facilities. A special area will be reserved for the valet parking service.

IoT utilization
- Automated driving support using traffic cameras
- Signalised intersection support - The Finnish pilot will assess how the vehicle can communicate with the traffic light control system, by using cellular communications.

2.2.2 Pilot site France - Versailles

Versailles Use Cases
According to the AUTOPILOT objectives, several AD use case will be tested in order to evaluate the added value of IoT Technologies in AD functions. These use cases will be implemented on VEDECOM's vehicles within the French business cases framework:
- Point of Interest notification
- Fleet management
- Platooning
- Automated valet de parking
- Collaborative perception

Use cases and business cases matrix

Uses Cases	PoI	Fleet. Man	Platooning	AVP	Coll. Per
Connected urban driving	X	X			
Fully autonomous driving	X	X			X
Automated rebalancing fleet		X	X	X	

Table 1: UC/BC matrix

IoT utilization
Several IoT devices will be used on the French pilot site:
- Connected traffic lights cross roads (using Road Side Units)
- Road Side Camera
- IoT sensors (infrastructure)
- Wearables
- Connected bicycles
- Smartphones

2.2.3 Pilot site Italy - Livorno

The Italian Pilot Site is a testing infrastructure encompassing the Florence – Livorno freeway together with road access to the Livorno sea port settlement.

Figure 2 - Livorno Pilot site

The testbed consists of three zones:

1) The Livorno – Florence freeway
The Livorno – Florence is a highway also known as FI-PI-LI. Renowned as one of the most important arteries and heart to the Tuscany road system, it is comprised of 31 junctions connecting some of the biggest economic and civil conglomerates of the region like Firenze, Pisa and Livorno, but also Empoli and Pontedera. Highway with dual carriage on a length of 100 km, and 2 lanes per direction. It is of high value on the territory and well regarded by the public administration. The Livorno – Florence highway is provided with ITS technology for control and data analysis in real time, with 44 VMS spanning over the whole length of the road system and 32 Full-HD cameras.

2) The TCC in Empoli
The Traffic Control Center is located in Empoli which acts as the centre of information and data analysis for the whole system. Built with the latest technologies, it follows the best practices with a state of the art system. A monitor wall follows the development of the traffic from point Firenze to point Livorno and Pisa and viceversa, enabling real time monitoring by the staff of the TCC. Several ITS appliances are in use to keep track of the events and change the VMS accordingly to the needs of the users and road system.

3) The port landside
The test track in the harbor is just in front of the cruise terminal. It is equipped with several service points providing electric sockets and Ethernet connectivity that can be used for a quick setup of testing equipment on the field. Full WiFi coverage of the installation points is provided by means of high power integrated antennas with Gigabit Ethernet ports.

The vehicles which will be used in the Italian AUTOPILOT test site are FCA Jeep Renegade with different functions and roles: two vehicles by CRF with automated driving functions and five service vans (2 by CRF, 3 by AVR) with advanced V2X communication capabilities. The latter are used for tuning and pre-testing the systems and the services for the vehicles in the IoT enhanced ITS environment, the former are used to demonstrate the performance of the IoT-ITS ecosystems when the automated driving scenarios beyond SAE 3 levels are running.

Use cases:

- Highway
    - Hazard on the roadway
    - Roadway works with TCC in the loop

- Urban
  - Pedestrian detection with camera
  - Connected bicycle
- Highway/Urban
  - Potholes detection/Surface road condition
  - Data crowdsourcing from IoT (Urban and Highway)

IoT utilization:

- Road hazard sensors (flooding, smart tracer roadworks)
- Connected traffic lights cross roads (using Road Side Units)
- IoT enhanced RSUs
- IoT enhanced OBUs
- Smart Road Side Cameras
- In-car IoT sensors (pothole detector)
- Connected bicycles

2.2.4 Pilot site Netherlands - Brainport

The Brainport Pilot site located in the region of Helmond-Eindhoven in the Netherlands, as depicted in Figure 3. The region comprehends 3 campuses (Eindhoven University, Automotive Campus, High-Tech Campus) and Eindhoven airport. The main road between the cities of Eindhoven and Helmond is the A270 motorway, which is part of the DITCM test site.

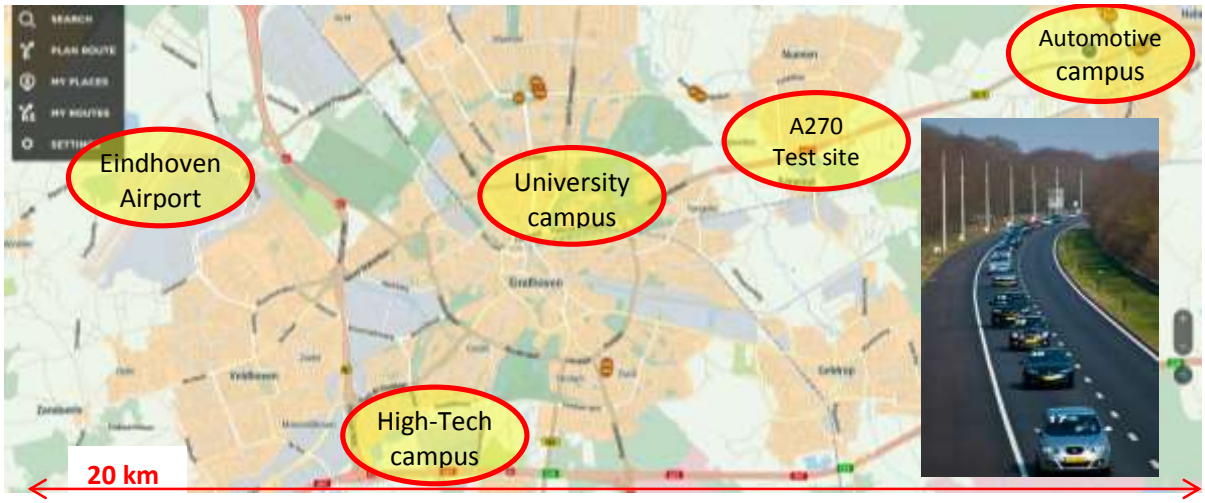


Figure 3 - Brainport Pilot site.

This DITCM test site is a purpose-built facility for the development, testing and validation of Intelligent Transport Systems (ITS) and cooperative driving technologies. It consists of both a motorway (A270 and N270) and urban environments. The DITCM test site is 8 km long, with 6 km of motorway.

DITCM Test site:

- 6km highway, 2km urban road & 2 traffic light controllers, 2 additional controllers to be added this year
- 20 dual channel ITS G5 roadside units

    - Some related C-ITS standards deployed (EN 302 663 [71], EN 302 636-4-1 [68], EN 302 636-5-1 v1.2.1 [109]
    - At facilities layer: EN 302 637-2 [69], EN 302 637-3 [70]. In addition pre-standards or non-standard ITS messages can be deployed for testing and piloting.
- 56 cameras for real-time vehicle detection and tracking, 11 dome cameras
- Cellular Communication from multiple networks (up to 4G/LTE)
- dGPS base station
- Integration of 3rd party hardware and software for testing

Vehicles at Brainport:

- AVP: NEVS, DLR, TASS
- Highway Pilot: Valeo
- Platooning: NEVS, TASS
- Urban driving: TASS/TUE/other

TNO/TASS: 2 equipped test vehicles (Prius): instrumented with extendable in-car platforms. Vehicles are (partly) equipped with radar, camera, lidar, DSRC, GPS, 3G; Software toolkit to rapidly create and test application software; Communication unit with ITS-G5. To be extended with LTE cellular communication.

TUE: probably 3 vehicles (eg Renault Twizzy). Communication channels using TU/e high-speed Wi-Fi network, extend with cellular connectivity.

NEVS vehicles: currently not equipped with communication technology.

DLR: Drone with video camera and cellular link (optionally a base station).

Use cases:

1) Platooning from Helmond to Eindhoven will be done on the A270 motorway (2 x 2 lanes) utilizing its emergency lane. For a large extent, it is equipped with ITS-G5 communication and monitoring cameras. The speed limit is 100 km/h.
2) A driverless car rebalancing service will be used on the Eindhoven University campus. The University Campus has a 2-km road network and a 30 km/h speed limit. On the campus, there are neither cross walks nor traffic lights.
3) The Automated Valet Parking (AVP) use case will be executed on the Automotive campus, involving a parking which can host 200 vehicles, and several access roads. The speed limit is 15 km/h.
4) The Highway Pilot use case will be carried out on the A270 motorway (see Platooning use case).
5) A car sharing service covering the whole Brainport area, interacting with the various automated driving use cases.

IoT utilization (AVP–only):

- Cameras at fixed positions in and around parking area
- Parking spot detection sensors
- Using camera/radar information from other (driving and/or parked) vehicles
- Car-following drones that can aid less-equipped vehicles, or can be used at less equipped parking lots
- Inductive-loop traffic detectors (such as commonly used for traffic lights)
- Usage of statistic models in traffic management systems to avoid congestions

Cellular Connectivity Brainport:
In the Netherlands LTE connectivity is provided by 4 parties: KPN, Vodafone(Ziggo), T-Mobile and Tele2 [106]:

- KPN: mainly operating at 800 MHz, also 1800 and 2600Mhz. Also 4G+. Coverage: population 98.4%, area 96%
- Vodafone: mainly operating at 800 MHz, also 1800 and 2600Mhz. Also 4G+. Coverage: population 91.6%, area 90%[Error! Bookmark not defined.]
- T-Mobile: mainly operating at 1800Mhz, also 900 and 2600Mhz. Coverage: population 96%, area 97.6%[Error! Bookmark not defined.]
- Tele2: mainly operating at 800 MHz, also 2600Mhz. Coverage: population 76.34%, area 67%

2.2.5 Pilot site Spain - Vigo

PS of Vigo is located in the north west of Spain. It is integrated in the urban section of SISCOGA corridor. It is extended along more than 100 Km of urban and interurban roads in A55, A52, VG20 and AP9 highways. The access to Vigo from AP9, A55 and VG20 are linked across the city roads through the main city streets.

SISCOGA facilities have enabled testing and development of multiple ITS solutions from C-ITS systems, ADAS, eCall and Electro mobility, especially those involving V2X communications. Some examples of local and European projects, which have been tested in SISCOGA facilities, are: DriveC2X, Compass4D, CO-GISTICS, CO2PerautoS2, OpEneR, Mobinet, HeERO2, etc.

Both, urban and interurban sections are connected to management infrastructures from the competent road authorities, Vigo Movility and Safety Area and DGT respectively.

Figure 4 - Vigo Pilot Site testing scenarios

Nevertheless, CTAG test tracks will be used to early testing and fine tuning of connectivity and AD functions before starting pilot in real environment. In these sense the main scenarios will be early reproduced in controlled conditions.

Use cases:
1) Urban autopilot: this will be piloted in the middle section of Gran Via avenue
2) Automated Valet Parking: this will be piloted in City Council Parking.

IoT utilization

- The Traffic light Control Unit acts as an IoT device integrated in IoT ecosystem and connected to IoT platform
- Vehicle IoT platform connects to City IoT platform and request relevant information according its position and heading (and/or route)
- IoT platform sends data relevant according the position, heading and (and/or route) using the most suitable communication channel: In this case traffic light status and time to change for the next intersection(s) according heading (route)
- The vehicle establishes connection with parking infrastructure (through IoT platforms) and manoeuvers are supported by information from parking cameras and sensors together with parking mapping and instructions according internal traffic.

2.2.6 Pilot site South Korea

The information relating the South Korean pilot site is not currently available. The description will be included in the next version of the deliverable, D1.8.

2.2.7 Pre – existing communication infrastructure

In Section 2.2.7 the communication infrastructure used in the pilot sites is described; this section report the information available at the writing time of this deliverable.

2.2.7.1 Pilot site France – Versailles

The pilot site in France is situated in the city of Versailles. The use-cases featured in the city of Versailles relate to the tourist services. In these use-cases, automated vehicles and fleet of automated vehicles will be demonstrated as service for travelers visiting Versailles' tourist areas. Some of the tourist areas include the Versailles Castle and historic monuments, churches and walk paths. An overview map of the area, together with potential itineraries, is illustrated in Figure 5:

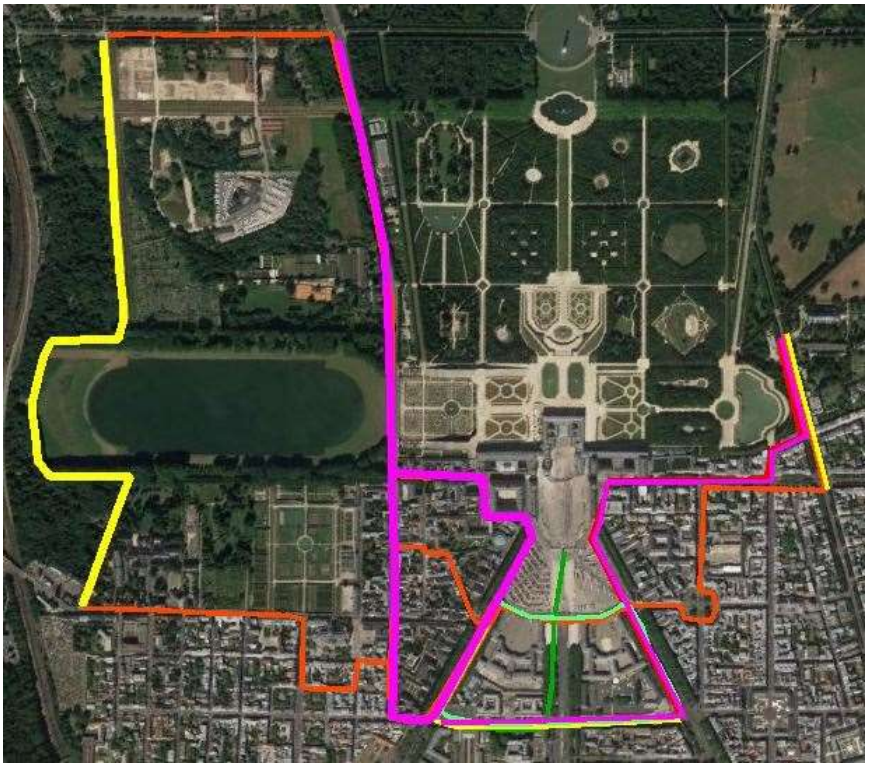


Figure 5: - Versailles automated routes

In Figure 5 aerial view depicts a tourist area in the city Versailles. The colored lines represent the itineraries considered currently for deploying vehicles for different use-cases. There are 14 intersections that are all equipped with Traffic Lights.

The communication devices present at the site includes the following:

- Cellular network coverage ensured by 21 base stations for 2G, 3G and 4G technology.
- WiFi network coverage for tourist is given by 2 WiFi Access Points.
- ETSI ITS G5 radio given by 5 Road-Side Units.
- Bus detectors (coils), on some lanes.
- Remote management of traffic lights controllers on GPRS modules equipped with SIM cards, on some traffic lights.

The precise location and detail of this equipment is available to the partners involved in the Versailles site.

New equipment will potentially be installed, with the goal to realize the use-cases of project at the test-site. This equipment includes but is not limited to:

- When cellular coverage improvement is necessary, new cellular base stations will be installed, permanently, or on a temporary basis.
- New Road-Side Units connected to the IPv6 Internet.
- Point-to-point communication links between RSUs, where necessary.
- Built-in RFIDs or Bluetooth Beacons to help with POI detection, or with traffic light control for automated driving.
- Interfaces to traffic light controllers.
- Potentially other communication equipment.

2.2.7.2 Pilot site Finland – Tampere

The pilot site in Tampere is located in the city district of Hervanta, near several technological advanced organisations are located, such as the Tampere University of Technology, VTT and the Hermia Technology park. The communication channels which will be used between the vehicle and the backend in Tampere are:

- Cellular communication is the major communication channel.
    - Commercial Mobile Network operators (Telia, Elisa, DNA) provide 4G over the whole test area. Frequency band used are 800 DD, 1800+ and 2600 MHz. Telia and Elisa also have commercial LTE-A networks, but parts of the test network may not be covered.
    - Elisa has announced to roll out a 5G ready network in Tampere during the end of 2017.
    - In the framework of the national 5G-SAFE project, VTT is planning to test the 5GTN test network, which VTT is developing in Oulu, near VTT facilities in Tampere.

Both the vehicles and the mobile road side unit will be equipped with cellular communications. Through cellular communications the vehicles will receive information from the traffic lights, which transfer status data in real time to the city network through wired connection, and from the traffic cameras, installed at the mobile road side unit.

- ITS-G5.
    - Both the vehicles and the mobile road side unit, have ITS-G5 communication capabilities, for communication of safety critical information.
- Bluetooth communication could be used to determine whether the driver has left the vehicle, e.g. through pairing of the driver's smartphone with the in-vehicle OBU.

2.2.7.3 Pilot site Italy – Livorno

The Italian permanent Pilot Site is a unique location in Tuscany encompassing the Florence – Livorno highway together with road access to the Livorno sea port and its urban like environment. It was used by ETSI/ERTICO in November 2016 for the 5th ITS Cooperative Mobility Services Plugtest™ (1st C-ITS ETSI Plugtest™ with real-world test scenarios) and currently it is used by CNIT, Livorno Port Authority and AVR (the latter on behalf of Regional Government Authorities) for developing research and innovation activities.

The pre-existing communication infrastructure of the Italian PS is made by three segments: the highway (with TCC), the seaport (with CNIT/APL lab) and the cars. The pre-existing communication infrastructure is the one set up for the Plugtest™, to which it has been added the LTE coverage, since 3G/4G and even 3GPP V2X (when this technology is available) shall be considered for AUTOPILOT experimentations.

1) Highway segment:

The following definitions apply:

- **Highway SGC Fi-Pi-Li**: Highway (without tolling stations) operated by AVR and flowing from Firenze to Livorno, as shown in Figure 6.
- **RTRT3 network**: Regional wide network infrastructure, operated by the Regional Government
- **AVR Control Room in Empoli**: The operator of the **SCG Fi-Pi-Li** hosts in Empoli a control room connected with Road Side Equipment along the highway.

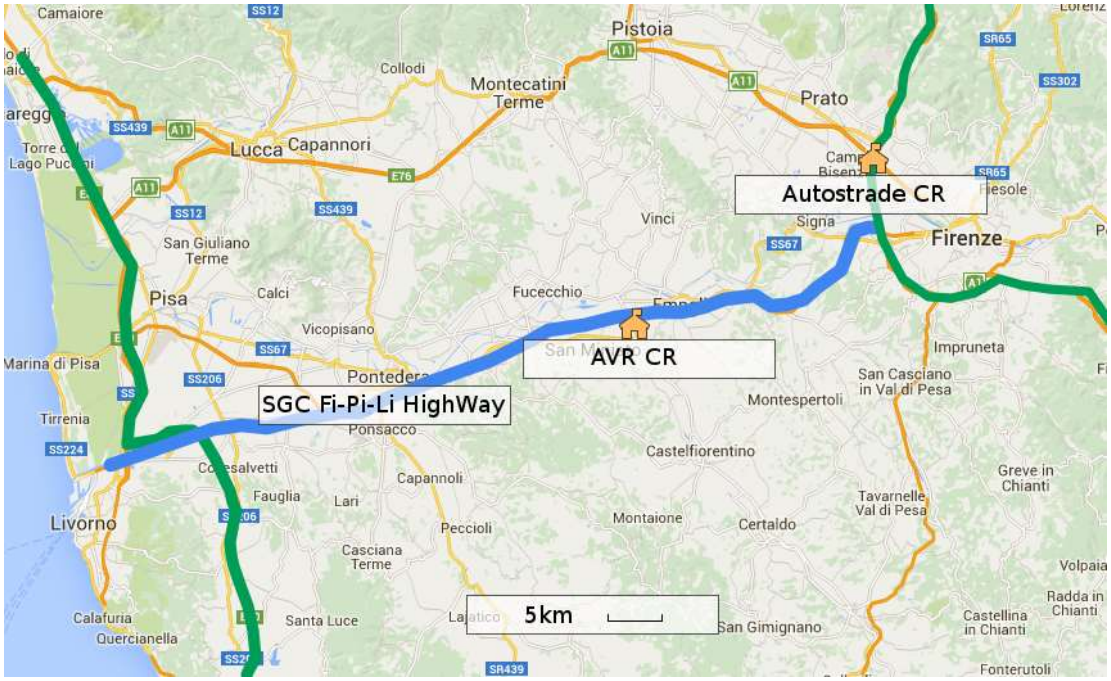


Figure 6 – Geographic locations of Highway settlements

2) Seaport segment:

The test track in the harbour is just in front of the cruise terminal. It is equipped with several service points providing electric sockets and Ethernet connectivity that can be used for a quick setup of testing equipment on the field. Full WiFi coverage of the installation points is provided by means of high power integrated antennas with Gigabit Ethernet ports.

The Internet connectivity is managed by CNIT (and turned on when needed) with proper QoS for the intended use.

In the Seaport there is also a jointly managed laboratory by CNIT and Port Authority, dedicated to pre-conformance tests of AUTOPILOT equipment. The room of about 70 square meters is equipped with rack, servers, switch, routers, Internet connectivity and WiFi WLAN. Outside the lab there is a permanent installation of a ITS System (RSU and a smart camera network) communicating by IEEE 802.11p ETSI G5, 6LoWPAN, 3GPP and WiFi protocols, for parking lot monitoring.

LTE coverage:

Since LTE communication network is a fundamental infrastructure for AUTOPILOT experimentation, the coverage of the “in-car” signal is guaranteed along the test track. Also the traffic control center and Florence area are well covered by the signal. The deployment of road side equipment that needs LTE connectivity shall exclude the few zone between Empoli and Pontedera not covered by the signal.

2.2.7.4 Pilot site Spain – Vigo

As aforementioned in previous section, AUTOPILOT use cases Urban Autopilot and Automated Valet Parking will be tested in SISCOGA facilities. The origin of SISCOGA is a C-ITS corridor aimed, in the very beginning, to test in real environment the first Cooperative ITS Systems with early On Board Units and Road Side units developed by CTAG in the framework of SISCOGA FOT project. SISCOGA facilities grew up as test bed in the framework several aforementioned National and European initiatives until becoming complete urban and interurban environment for testing connected and

automated driving (CAD) systems and services SISCOGA[4CAD]

The current infrastructure comprehends 120 km of interurban roads including AP9, A55, and A52 and 10 Km of urban roads within the city of Vigo (Figure 7).

- Interurban infrastructure is connected to DGT Traffic Control Centre North west (National Authority) comprehending:
  - 30 Road Side Units
  - 21 Cameras
  - 19 Variable Message signs
  - 10 High Precision Meteorological Stations
  - All network components linked by an optic fiber ring

- The urban infrastructure is connected to Mobility Management Centre in the City of Vigo and comprehends:
  - 50 Road side units
  - 43 Traffic detectors
  - 5 cameras
  - 60 Bluetooth sensors for traffic monitoring
  - 10 Bluetooth sensors for VRU detection
  - City services platform and citizen app.
  - Optic fiber ring connecting all infrastructure Mobility Management Centre

In such infrastructure has been tested and deployed a long list of C-ITS services including those named by the European Commission C-ITS platform as day 1 cooperative services

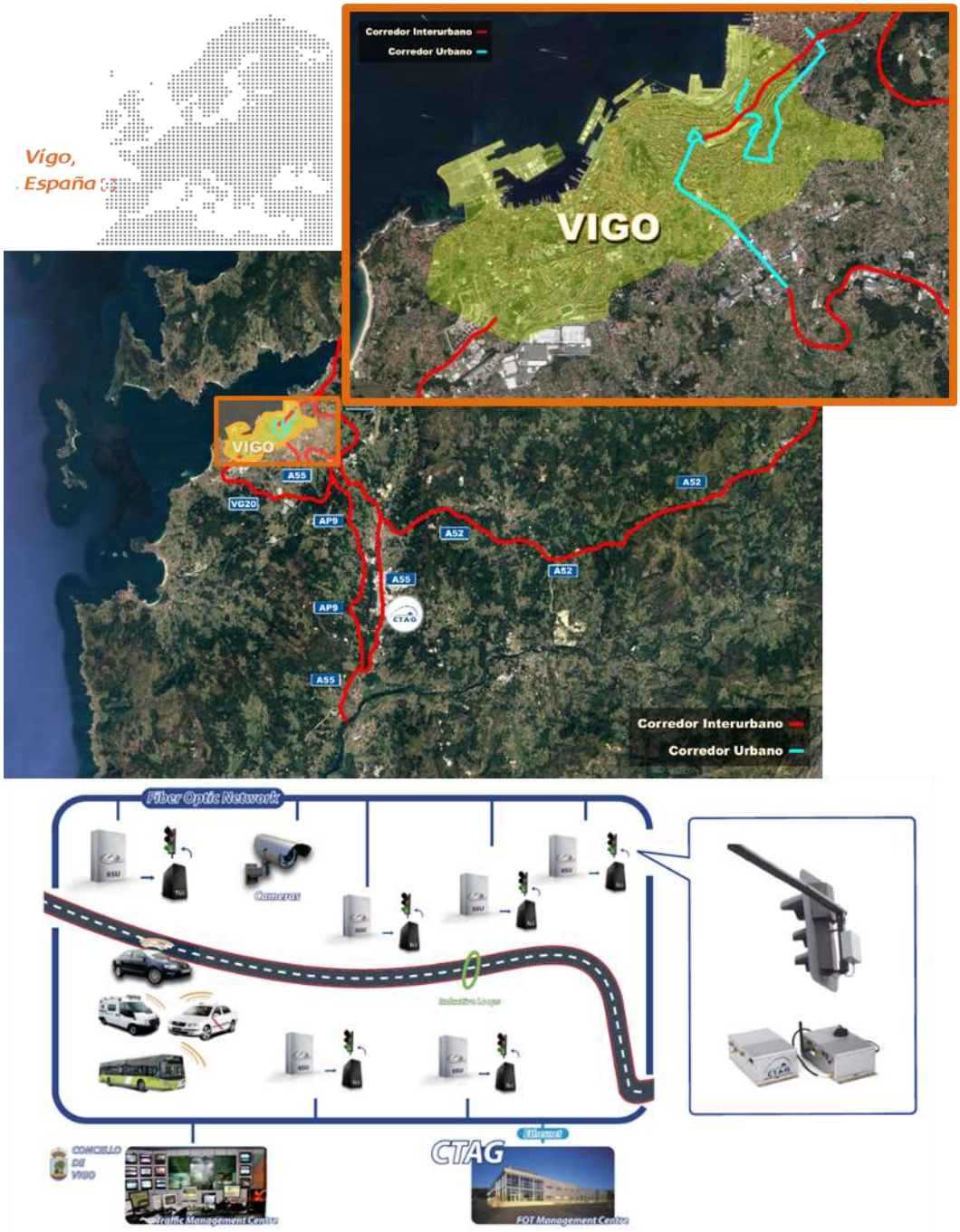


Figure 7 – SISCOGA[4CAD] Test bed infrastructure

With regards to V2I connectivity capabilities **ITS G5 and cellular** communication are available with city infrastructure through OBU – RSU (802.11p) and the connection to a centralized server, respectively.

The pilot will test in urban roads 2 use cases:

Urban autopilot with:

- Access to phase and remaining time of traffic lights
- Information of Hazards from Traffic management centre

- Information of pedestrian presence detected by V2X

Automated VALET Parking, where the connection with parking management infrastructure will enable and support the admission, positioning, routing, guidance and parking maneuvers inside an indoors parking lot.

Several Connected automated driving tests have been carried out in controlled environment using ITS G5 communication. The main objective of AUTOPILOT in Vigo is enhance existing infrastructure with the IoT approach in order to test the benefits of wider range of information available for the automated vehicle and, thus, extend the perception horizon.

The use cases of Vigo will be tested in Gran Via for urban autopilot. The main route will use four of its intersections to design the different scenarios. In such route all existing infrastructure aforementioned is available.

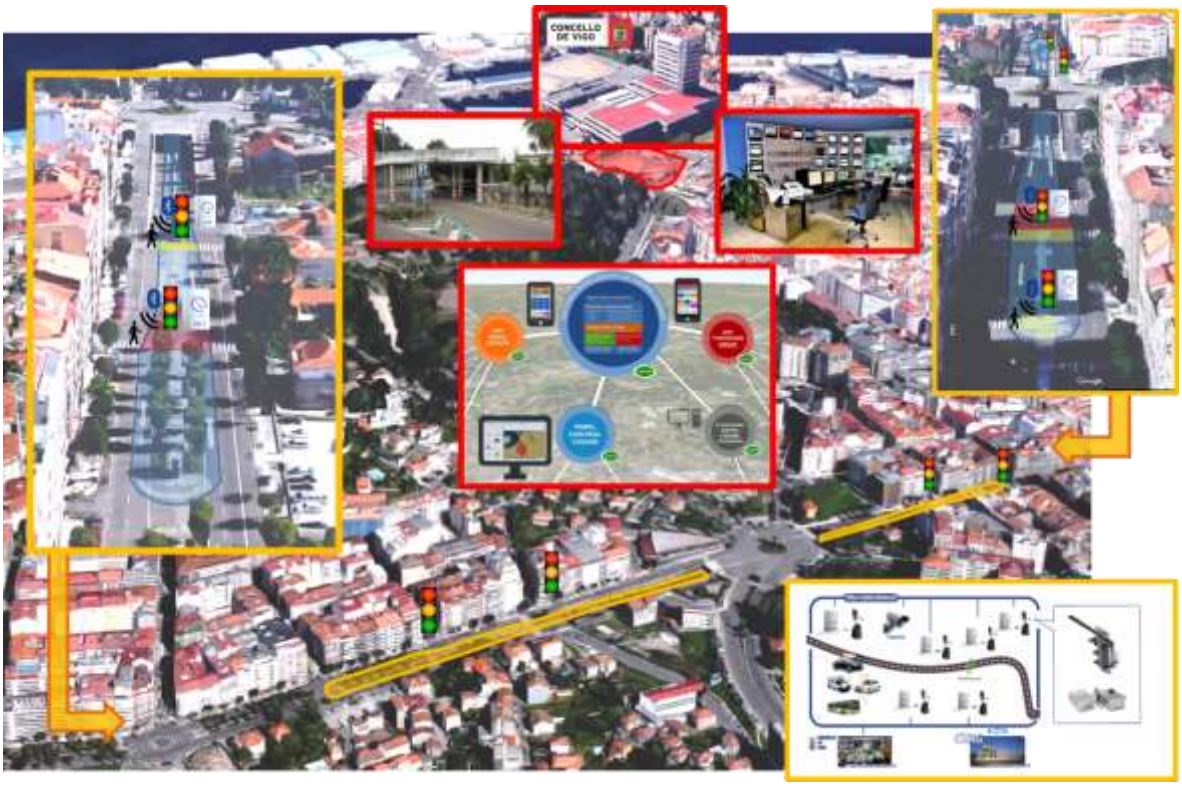


Figure 8 – Location of testing areas of AUTOPILOT in Vigo

The parking IoT infrastructure will mainly extended and adapted in the framework of AUTOPILOT being V2I communication limited by the moment.

2.2.7.5 Pilot site Netherlands – Brainport

In Brainport Pilot site the roadside equipment is responsible for vehicle detection and V2X communication. All other equipment is placed indoor and includes sensor fusion facilities, application platforms and a traffic management centre. The test site is connected to neighboring urban sections and other information sources via a high-speed internet connection. Besides, the DITCM control room also the Traffic Innovation Centre is located on the Automotive Campus.
The DITCM control room will be extended with an interface/connection to the IoT platform(s). Also

RTK-GPS corrections which are normally provided via a radio-modem only, will be extended. Further, deployments using LTE and ITS-G5 communication to provide the RTK-GPS corrections are foreseen. At some of the DITCM intersections real-time information from the traffic light controllers will be provided via Roadside units using SPAT/MAP messages conform ISO TS 19091: Intelligent transport systems -- Cooperative ITS -- Using V2I and I2V communications for applications related to signalized intersections:

- SPaT: Signal Phase and Timing of traffic light, status of traffic controller, prediction of duration and phases.
- MAP: Topological definition of lanes within an intersection, type of lanes, restrictions of lanes.

What actually can be deployed at the DITCM intersections is currently under investigation. LTE communication is planned to be extended by deployment of a pre-5G core network (TNO). Note that 3GPP (3gpp.org) is currently working on 5G standard for mobile networks, covering both core and radio access parts. Radio access is provided by using eNB (one or multiple) connected to a pre-5G core network (supporting SDN, NFV and slicing). In addition, work is ongoing on a Mobile Edge Computing unit next to the eNB to support local breakouts from the eNB.

3 Communication technologies review and description

IoT is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [112]. The technological trend is a move from systems where there are multiple users per device, providing the ability for vehicle to interact with vehicle, infrastructure, devices and people [114]. The IoT brings a new paradigm where the devices are things that are connected and communicating with other things. The interaction will be with a heterogeneous continuum of users, things and real physical events and the Internet is the common convergence connectivity capability, replacing the previous independent systems.

The concept of Internet of Vehicles (IoV) or Vehicle-to-Everything (V2X) communications applied for autonomous transportation and mobility applications, requires creating mobile ecosystems based on trust, security and convenience to connectivity services and transportation applications in order to ensure security, mobility and convenience to consumer-centric transactions and services [115].
In this context for autonomous vehicle applications 5 communication domains are defined as presented in Figure 9. The domains cover the communications of vehicle to everything (V2X) that covers vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), vehicle to device (V2D) vehicle to grid (V2G) and vehicle to vehicle (V2V) as important communication building blocks of the IoT ecosystems.

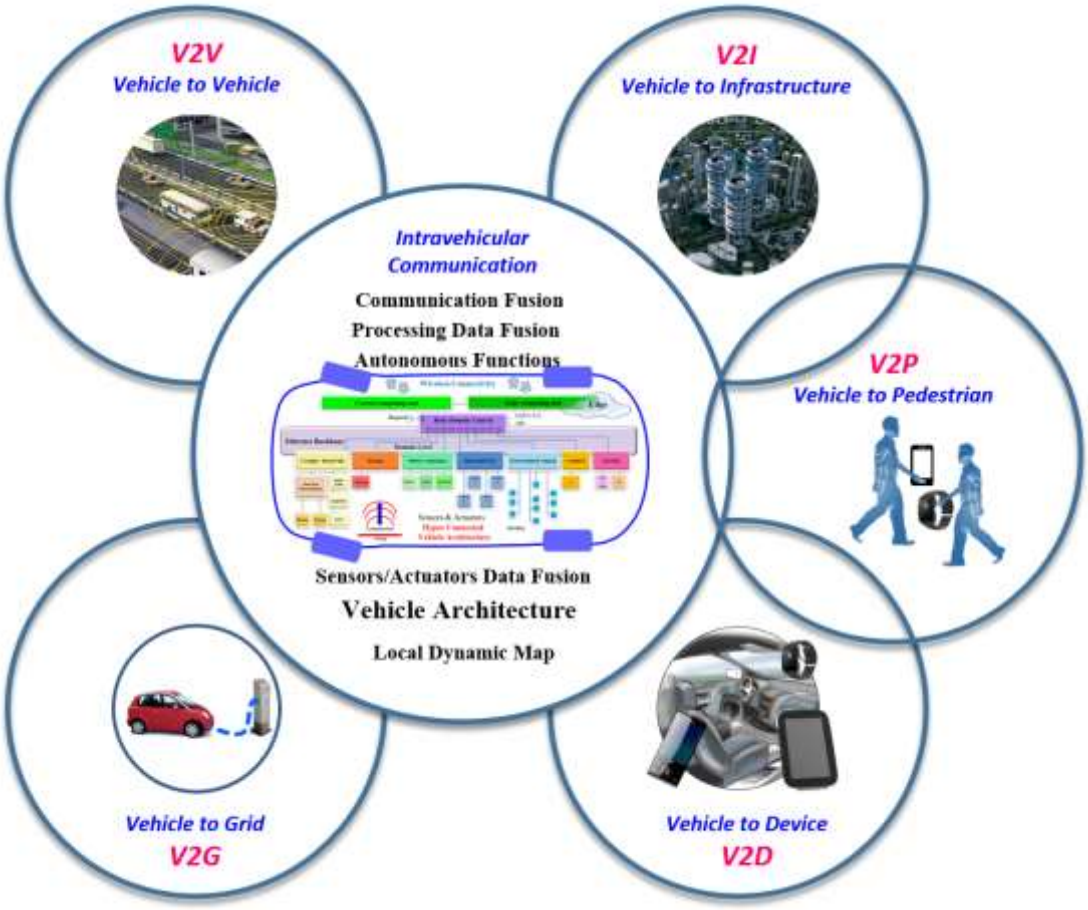


Figure 9 – Communication domains in autonomous vehicle applications (from [113])

Smart sensors and actuators in the vehicles, roads and traffic control infrastructures collect a variety of information to serve enhanced automated driving [113]. These requires robust sensor, actuators and communication solutions, which are able to communicate with the control systems while considering the timing, safety and security constraints. Redundancy and parallel systems are required in all safety and security critical applications. It is worth noting that power saving mode (e.g. sensors, actuators) can be a barrier to real-time information. For battery-powered equipment, it will always be a trade-off between power consumption and communication latency.

The integration needs of the communication gateways into vehicles are illustrated in Figure 10. The expected high amount of data collection, interpretation and exploitation will require edge computing and sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles.

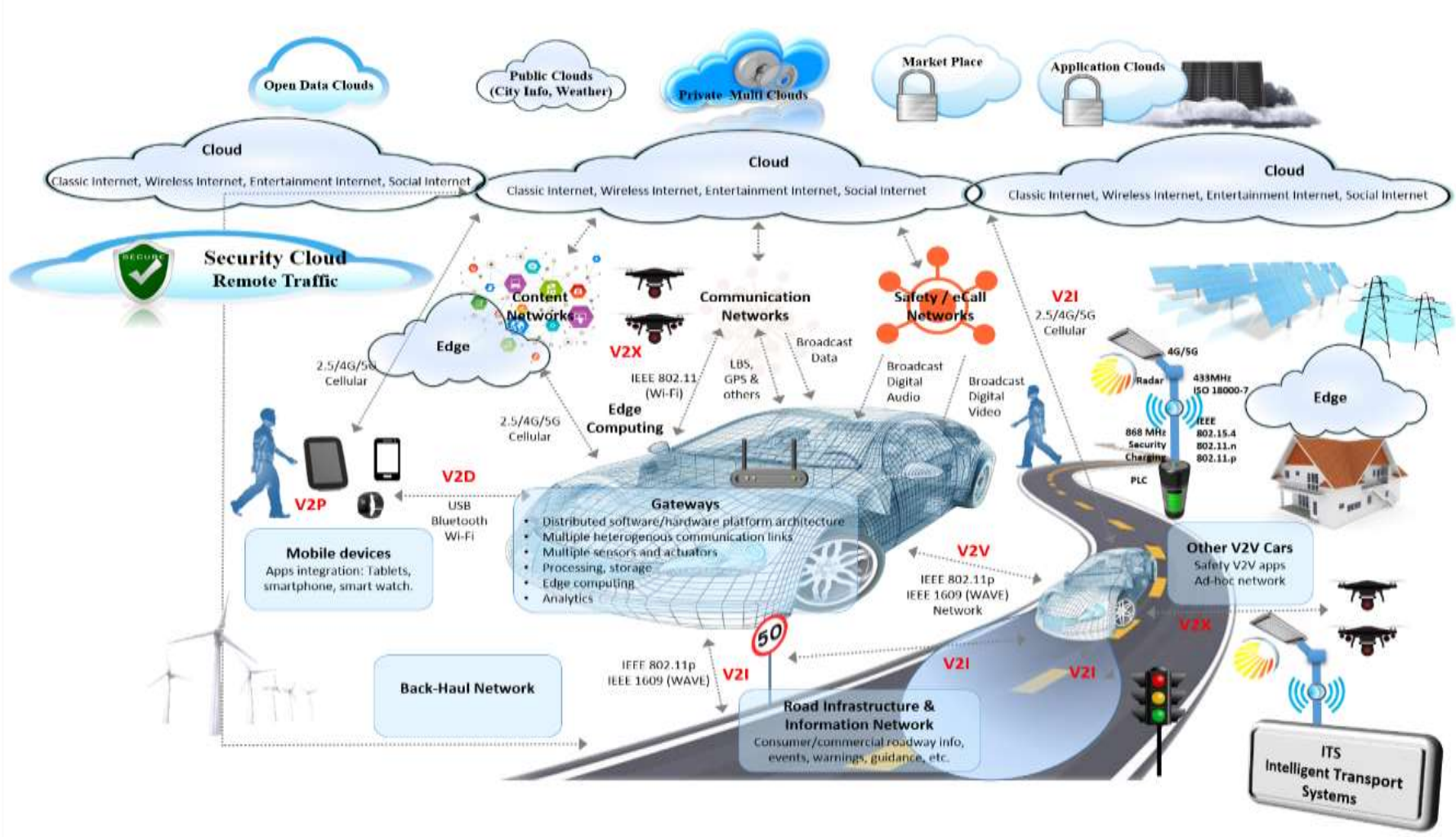


Figure 10 – Overall Vehicle to Everything (V2X) IoT ecosystem (from [113])

The IoT ecosystem relies on interaction among vehicles, pedestrians, devices, drones and infrastructure, to improve traffic management (increase efficiency, security and safety).

The aim of this section is to provide a general overview about the various communications technologies used within Autopilot project. For each of these technologies some information is given, such as: reference standards, overview about main features and basic indicators representing the technology key performances.

The communication technologies used in autonomous connected vehicles present varying characteristics and address different requirements as following:

- Autonomous oriented (i.e. real-time traffic communication, personalized roadside assistance, monitor and adjust position on highways, alerts for drifting out of lane, slowing down if too close to the vehicle around, robust security communication)
- Safety oriented (i.e. stopped or slow vehicle advisor, emergency electronic brake light, V2V post-crash notification, road feature notification, and cooperative collision warning)
- Convenience oriented (i.e. congested road notification, traffic probe, free flow tolling, parking availability notification, and parking spot locator)
- Commercial oriented (i.e. remote vehicle personalization/diagnostics, service announcement, content download, and real-time video broadcasts)
- IoT oriented (i.e. heterogeneous communication multi-layer approach with interfacing to sensors/actuators cameras, maps and federation with IoT platforms, cognitive networks and AI)

An overview of the wireless technologies used in autonomous vehicles ranging from AM/FM, satellite, Bluetooth, Wi-Fi, cellular 2G-4G and DSRC technologies that supports both V2V and V2I applications and use for vehicle commutations, navigation and active sensors is presented in Figure 11. Different applications have different networking criteria, network attributes and communication protocols parameters.

Vehicular communication systems are used complementary with of Radar/LiDAR/active sensing systems. The IEEE 802.11p-based dedicated short-range communications - DSRC using the two wireless modes, V2I and V2V, allow the autonomous vehicles to acquire traffic data to optimize their driving strategy. In addition, the use of Wi-Fi, Bluetooth, ZigBee, WiMax, and cellular 2G-4G technologies into vehicles enhance the functions provided to support the autonomous vehicles. Conventional wireless communications have limited bandwidth (i.e. maximal bit rate of DSRC is 27 Mb/s) and the next generation wireless technology, millimeter-wave (mmWave) that works at up to 300 GHz with channel bandwidth up to several gigahertz can achieve multi-gigabit transmission for high data rate delivery.

The wireless protocol functions are covered by the seven-layer OSI model with many standards activities related to layers:

- Layer 1 (Physical): IEEE 802.11 wireless [66], ISO 11898 CAN [72]
- Layer 2 (Data Link): IEEE 802.11 wireless [66], ISO 11898 CAN [72]
- Layer 3 (Network): IETF RFC 1122 Internet protocol (IP) [73]
- Layer 4 (Transport): IETF RFC 793 transmission control protocol (TCP) [74] and IETF RFC 768 user datagram protocol (UDP) [75]
- Layer 5 (Session): IETF RFC 793 transmission control protocol (TCP) [74] and IETF RFC 768 user datagram protocol (UDP) [75]

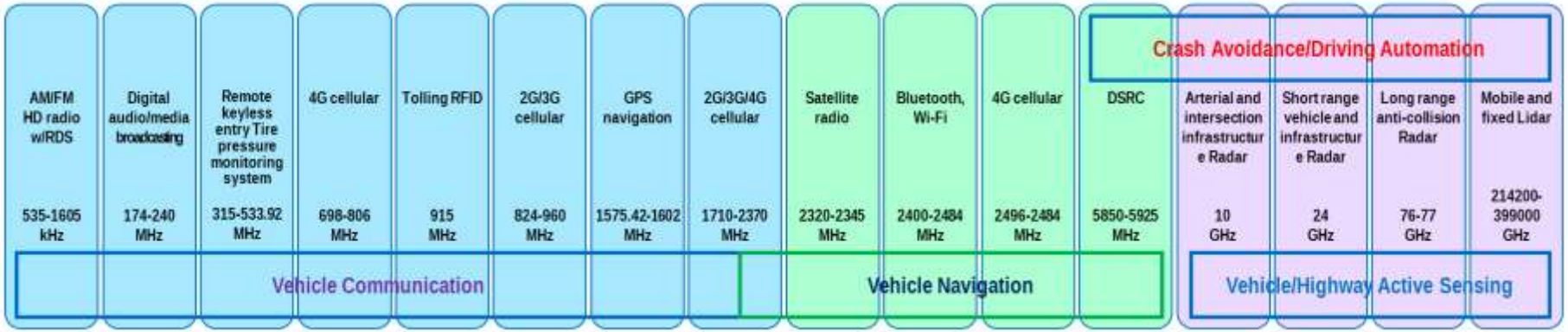
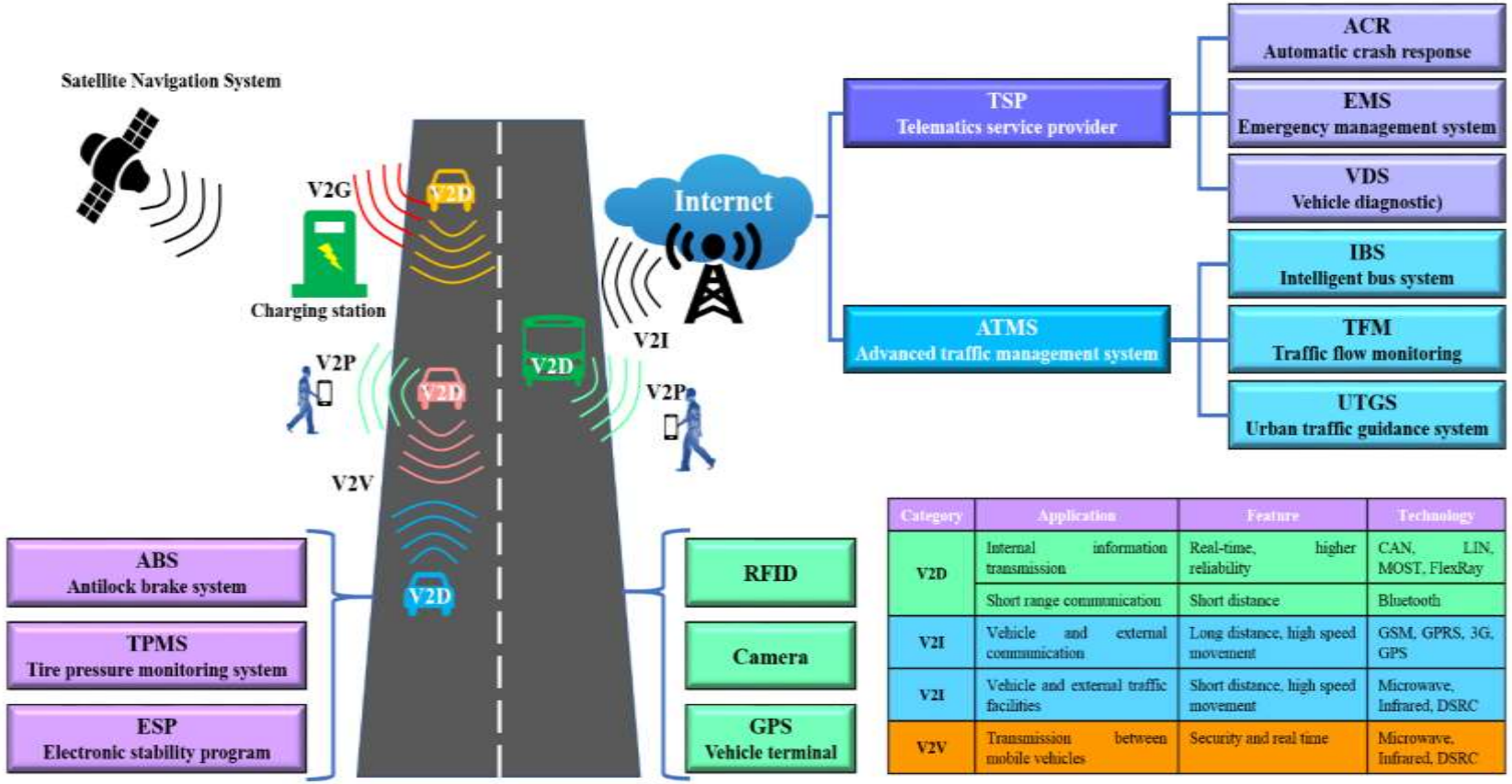


Figure 11 – Overview of the wireless technologies used in autonomous vehicles (from [113])

Parameters	DSRC mmWave	Wi-Fi	Bluetooth	ZigBee	DSRC	LTE	4G/WiMax	3GPP LTE-V2X
Spectrum	57-64 GHz	2.4/5.8 GHz	2.4 GHz	868/915 MHz, 24 GHz	5.9 GHz	1880-2650 MHz	2-6 GHz	700MHz/1,8, 2,6 GHz
Standard		802.11 a/b/g/n	802.15.1	802.15.4	802.11p	LTE	802.16e	C-V2X Rel-17
Bandwidth	2.16 GHz	20/40 MHz	1 MHz	2 MHz	10 Mbps	20 MHz	1.75-20 MHz	20 MHz
Bit rate	0.693-6.76 Gbps	6-600 Mbps	1-24 Mbps	250 kbps	3-27 Mbps	75/300 Mbps (Up/Down)	56/128 Mbps (Up/Down)	
Modulation	OFDM	OFDM, MIMO	FHSS, GFSK, π/4-DPSK, 8-DPSK	DSSS, O-QPSK	OFDM	OFDMA, MIMO	OFDMA, MIMO	OFDMA
TX range	< 10 m (Omni antenna)	< 100 m	< 75 m	< 100 m	< 500 m	< 2 km	< 10 km	Cellular + sidelink

Figure 12 – Communication technologies for autonomous vehicle applications (from [113])

The interaction of the autonomous vehicles and the use of communication technologies on the road use case scenario is presented in Figure 13.



Category	Application	Feature	Technology
V2D	Internal information transmission	Real-time, higher reliability	CAN, LIN, MOST, FlexRay
	Short range communication	Short distance	Bluetooth
V2I	Vehicle and external communication	Long distance, high speed movement	GSM, GPRS, 3G, GPS
V2I	Vehicle and external traffic facilities	Short distance, high speed movement	Microwave, Infrared, DSRC
V2V	Transmission between mobile vehicles	Security and real time	Microwave, Infrared, DSRC

Figure 13 –Interaction of the autonomous vehicles and use of communication technologies on the road use case scenario (from [113]

The communication interfaces of the autonomous vehicle with the V2V, V2I, V2D, V2P through the vehicle communication gateway is presented in Figure 14 and Figure 15.

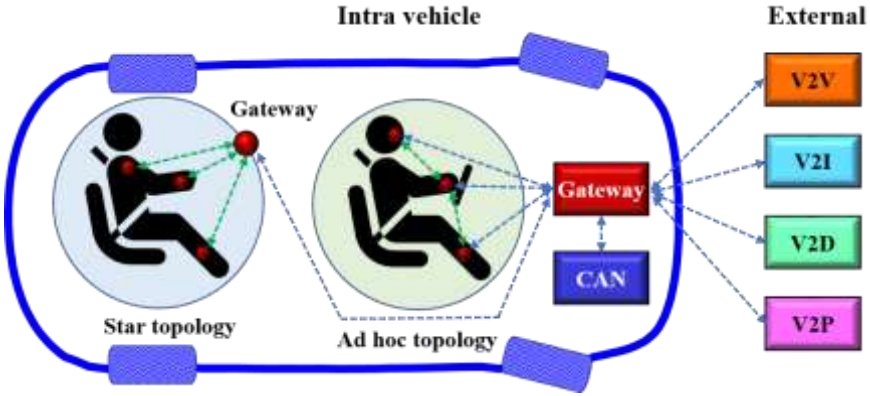


Figure 14 – Communication interfaces of the autonomous vehicle (from [113])

Communication scenario	Communication technologies	Frequency bandwidth	Data rate	Transmission range	Power consumption	Topology
Intra vehicle	Bluetooth	2.4 GHz	1-24 Mbps	< 75 m	Low (1 mW)	Star
	ZigBee	2.4 GHz, 868 MHz, 915 MHz	250 kbps	< 100 m	Low (< 1 mW)	Star, Mesh
	UWB	3.1 - 10.6 GHz	1 Gbps	< 10 m	Low (< 1 mW)	Peer-to-peer
V2V, V2D, V2P	DSRC	5.8 GHz, 915 MHz, 2.45 GHz	250 - 500 kbps	< 500 m	Low (10 mW)	Peer-to-peer
V2V, V2D, V2P, V2I	LoRaWAN	Sub GHz (varies)	0.3 - 50 kbps	2 - 5 km urban 15 km suburban 45 km rural	Low (< 25 mW)	Star
	NB-IoT	Variable	250 kbps	3 km	Medium (200 mW)	Star
	LTE-V	900, 1800, 1900, 2100 MHz	3 - 10 Mbps	2 km	Medium (300 mW)	Star, Peer-to-peer

Figure 15 – Communication interfaces of the autonomous vehicle: technical characteristics (from [113])

Cellular V2X (C-V2X) technologies as presented in and Figure 16 are designed to connect V2V, V2P, V2I, to the network V2N with different modes of operations.

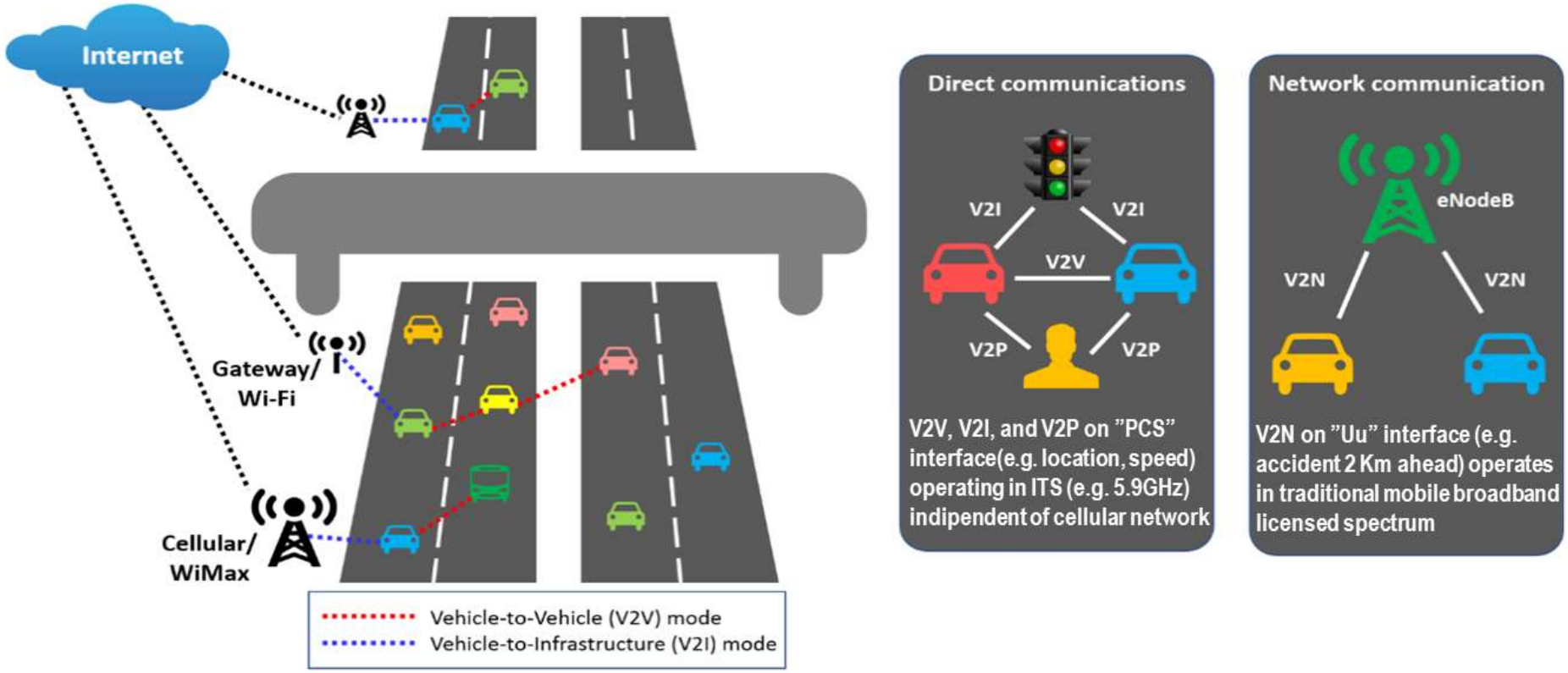


Figure 16 – Two transmission modes available through C-V2X (Adapted from Qualcomm [76]

3.1 Long range wireless communication network

3.1.1 Overview of LTE

Long-Term Evolution (LTE) is recognized as the fastest growing mobile broadband technology, and is becoming the most widely adopted cellular standard worldwide.

3GPP started to work on LTE since 2004, beginning the study item on it based on this main rationale (from [121]):

- "… to ensure competitiveness in an even longer time frame, i.e. for the next 10 years and beyond, a long-term evolution of the 3GPP radio-access technology needs to be considered.
- …Important parts of such a long-term evolution include reduced latency, higher user data rates, improved system capacity and coverage, and reduced cost for the operator. In order to achieve this, an evolution of the radio interface as well as the radio network architecture should be considered.
- ….Considering a desire for even higher data rates and also taking into account future additional 3G spectrum allocations the long-term 3GPP evolution should include an evolution towards support for wider transmission bandwidth than 5 MHz. At the same time, support for transmission bandwidths of 5 MHz and less than 5 MHz should be investigated in order to allow for more flexibility in whichever frequency bands the system may be deployed".

The main objective was to develop a framework for the evolution of the 3GPP radio-access technology towards a high-data-rate, low-latency and packet-optimized radio-access technology, with the following targets for the evolution of the radio-interface and radio-access network architecture (from [121]):

- Significantly increased peak data rate e.g. 100 Mbps (downlink) and 50 Mbps (uplink)
- Increase "cell edge bitrate" whilst maintaining same site locations as deployed today
- Significantly improved spectrum efficiency (e.g. 2-4 times over UMTS/HSPA Release 6)
- Possibility for a Radio-access network latency (user-plane UE – RNC (or corresponding node above Node B - UE) below 10 ms
- Significantly reduced C-plane latency (e.g. including the possibility to exchange user-plane data starting from camped-state with a transition time of less than 100 ms (excluding downlink paging delay)
- Scalable bandwidth
    - 5, 10, 20 and possibly 15 MHz
    - allow flexibility in narrow spectral allocations where the system may be deployed

LTE Rel-8 main requirements are summarised in Figure 17.

LTE key enabling solutions and technologies are summarized in Figure 18. For more information please refer to section 7.4 - Annex 4

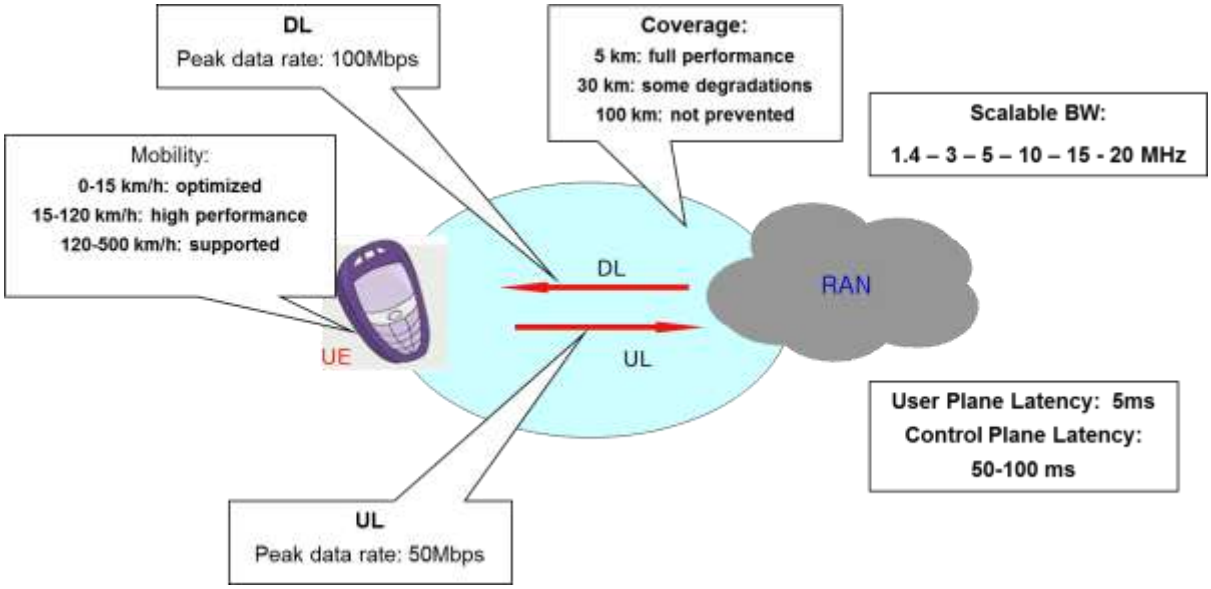


Figure 17 – LTE Rel-8 main requirements (from [121])

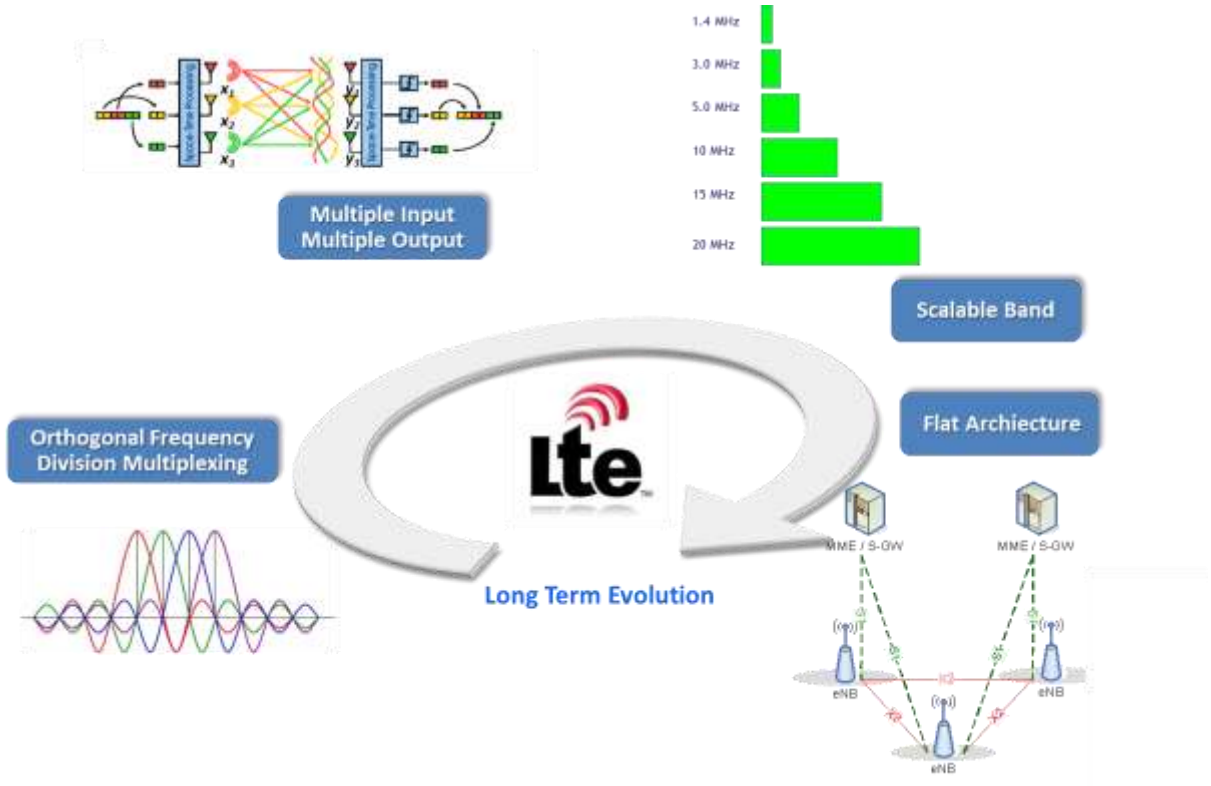


Figure 18 – LTE main technology enablers (Source 3GPP [4])

3.1.2 Overview of 5G

The telecommunications sector is characterized by an overwhelming evolution, favoured by the evolution of semiconductor technologies and their respective processing and memory capabilities,

optics, radio and information technology [77].

The development of the Internet as a global network has changed many telecoms usage scenarios and, along with the spread of broadband and then ultra-wide, has begun innovation through pervasive digitization in all industries, as well as in the media, Information, work and study, to which exponential growth of traffic and services is followed.

In the past, the evolution of mobile radio systems has occurred with two elements in mind: migration to transmission and control IP, and performance growth (bitrate and latency). The 5G is a more complex phenomenon that includes many innovations in technology:

- software networking, which aims at simplifying and developing and deploying agility, also has the ability to allow platforms to be increasingly opened by transforming Telco vertical systems into flexible programmable platforms, whose features are open to third parties;
- the development of wireless access that allows you to exploit new bandwidths and to achieve conditions comparable to those of fixed access.
- the evolution of transport networks based on an increasingly integrated and flexible use of fiber and IP technology;
- the development of the "Internet of Things" revolution, the world of "connected" sensors and actuators, which includes many sectors: smart cities, healthcare, our homes; Scenarios where potentially each subject is connected to Digital Life;
- a new development mode, where in addition to standardization bodies, Telco work directly with industries, both to reduce time between standardization, development and market to meet and develop their requirements, to be brought back to standards to ensure market success.

5G is the next generation of mobile communication technology. It is expected to be defined by the end of this decade and to be widely deployed in the early years of the next decade. There are a great many researchers studying 5G and its component technologies – in funded EU projects, in national programs, in individual companies and in research institutions.

Annex 1 describe how and where the standardization of 5G is carried out, by identifying the “three phases” of the process: vision, technical specifications and policy and profiling. An overview of the main players is given, followed by an in-depth of the two major players: ITU-R [5] and 3GPP [1], who will shape the technical characteristics of the new system. Other authors provided an overview of the standardization process [6], [7], [8], [9], [11], [12], but the idea behind this document is to provide a view of the process leading to success of a technology, by means of high quality standards.

3.2 IoT wireless communication technologies

3.2.1 Low Power Wide Area Network technologies

The standardization activities covered by different standardization organisations in the area of Low Power Wide Area Network technologies are presented in Figure 19.

Figure 19 – LPWA standards (from [113])

LPWA networks have several features that make them particularly attractive for IoT devices and applications that require low mobility and low levels of data transfer [113]:

- Low power consumption that enable devices to last up to 10 years on a single charge
- Optimised data transfer that supports small, intermittent blocks of data
- Low device unit cost
- Few base stations required to provide coverage
- Easy installation of the network
- Dedicated network authentication
- Optimised for low throughput, long or short distance
- Sufficient indoor penetration and coverage

3.2.2 3GPP technologies

In Release-13 3GPP [79] has made a major effort to address the cellular IoT market (see Figure 20); the portfolio of 3GPP technologies to address different market requirements include:

- **NB-IoT (a.k.a. UE Cat NB1):** New radio added to the LTE platform optimized for the low end of the market
- **LTE-M (a.k.a. UE Cat M1, or eMTC):** LTE enhancements for Machine Type Communications, building on the work started in Release-12 (UE Cat 0)
- **EC-GSM-IoT:** EGPRS enhancements for IoT

In the following paragraphs, the main characteristics of NB-IoT and LTE-M are described.

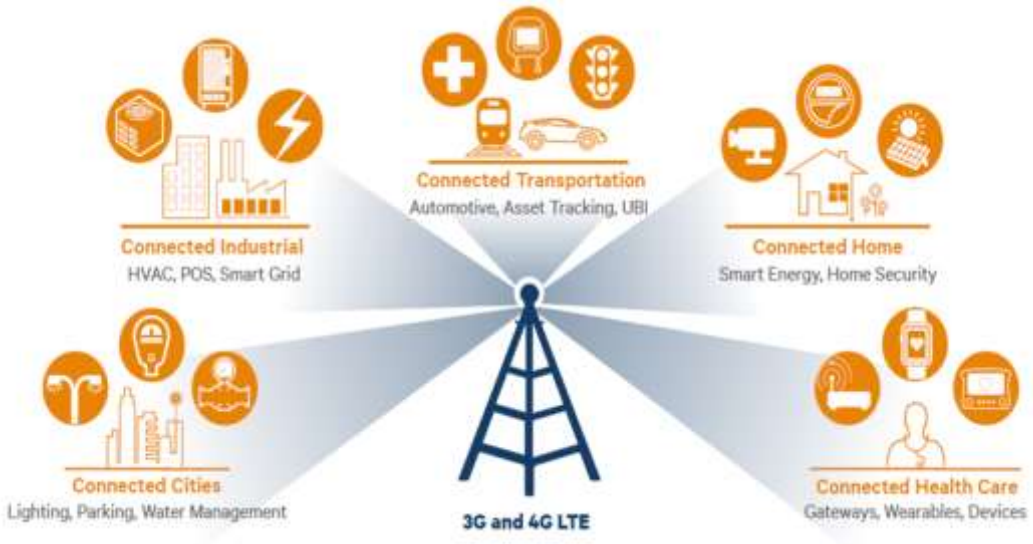


Figure 20 - IoT & 3GPP Systems (source Qualcomm [80])

3.2.2.1 NB-IoT

NB-IoT (Narrow Band Internet of Things [79]) has been introduced in Release 13 of the 3GPP specification enabling IoT services in the mobile domain. In particular, NB-IoT applications focus mainly on devices placed in locations where a substantial extension of the radio coverage is required and battery life is an extremely important factor since it is not easy or even economically convenient, to replace the battery; In these cases, the life cycle of the devices corresponds de facto to the life of their battery. At the same time, the amount of data to be transferred and received by these devices is very small (in the order of several tens of bytes per day as average or even smaller), so NB-IoT is an optimized solution for specific applications such as smart metering.

It should be noted that for NB-IoT there is no handover defined. Anyway a fast resume procedure of the UE is executed by two eNBs after it goes in the idle state [55].

NB-IoT technology allows three different forms of deployment:

- **"stand-alone ":** it works in spectrum portions made available, for example, by re-farming one or more GSM carriers, using one or more nominal 200 kHz channels, 180 kHz effective.
- **“guard-band”:** it works by using one or more 180 kHz PRB allocated in the guard(s) band of a LTE channel.
- **"in-band":** NB-IoT can be deployed on an LTE channel by using one or more 180 kHz spectrum portions, called Physical Resource Blocks (PRBs), allocated directly inside it;

Figure 21 shows the three modes described above.

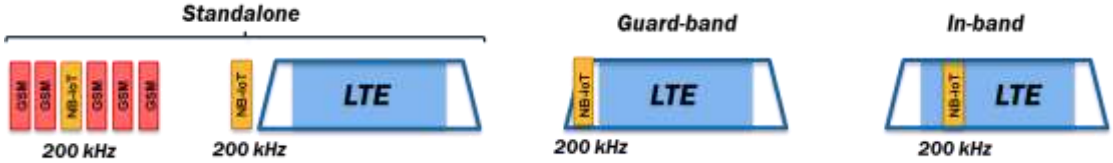


Figure 21 - NB-IoT deployment modes (from [77])

The NB-IoT system is self-contained, as it provides dedicated control channels and synchronization signals, separate from LTE. It is precisely this feature that also allows NB-IoT to be deployed in "guard-band" or "stand-alone" mode, since for broadcasting and synchronization purposes it does not depend on an existing legacy system.

The main requirements fulfilled by NB-IoT can be summarized as follows:

- deployment in an extremely low bandwidth (180 kHz) and easily scalable to the growth of IoT traffic (with multiple allocations of 180 kHz channels);
- Radio coverage extension of at least 20 dB compared to a legacy GSM/GPRS network, corresponding to a 164 dB MCL (Maximum Coupling Loss), to cover scenarios where devices are placed in places that are not easily accessible, such as basements, and/or are protected in metal containers;
- 23 dBm or 20 dBm UE TX power, allowing power amplifier to be integrated into the System-on-Chip (SoC) design; just for comparison purposes, a GPRS UE transmits at 33 dBm, i.e. at a value of at least 10 dB higher, even reaching a radio coverage of 20 dB lower than NB-IoT one;
- UE battery life of more than 10 years, adopting a traffic model based on up to 200 bytes transmission per day;
- reduced data rate of about 10 kbps in both UL and DL, with peak values of 250 kbps in UL and 170 / 226.7 kbps in DL in-band / stand-alone deployment (and average data values of 62.5 kbps in UL and 21.25 kbps in DL);
- Extremely reduced complexity and presumably extremely low cost of the terminals (e.g. lower than the legacy GPRS-only devices of Release 97);
- support for a large number of terminals/sensors (over 50,000) in each sector of a three-sector site, with the allocation of a PRB per sector;
- Absence of stringent requirements in latency, however, not exceeding 10 seconds in the case of applications requiring alarms from devices in places requiring the maximum coverage extension of 20 dB. The delay is evaluated between the instant in which the event that determines the alarm signal and the instant in which this signal is available at the base station to be sent to the core network occurs.

In Figure 22 the adopted techniques to increase battery life are briefly summarised.

Figure 22 - IoT & 3GPP Systems (source Qualcomm [80])

3.2.2.2 eMTC

eMTC (enhanced Machine Type Communication), often referred to as LTE-M, is a radio LTE feature, designed to enable IoT before of NB-IoT, initially in Release 12 (aka cat-0) and after in Release 13 (aka cat M1) of the 3GPP specifications [79].

eMTC works within a LTE carrier and uses a minimum 6 contiguous PRBs (Physical Resource Blocks) of LTE allocated radio resources. It also reuses broadcast, common channels and LTE synchronization signals, and can work in a LTE channel of 1.4 MHz, i.e. the minimum channel bandwidth specified for an LTE.

The flexibility of the system is such that eMTC works properly, regardless of the LTE band in which it is deployed (1.4 MHz, 5 MHz, 10 MHz, 15 MHz or 20 MHz). Unlike NB-IoT that only supports Duplex Duplexing (Half Duplex - Frequency Division Duplex), eMTC is versatile and supports HD-FDD, Full Duplex (Frequency Division Duplex) and TDD (Time Division Duplex).

The peak data rate reached in both DL and UL is 1 Mbps. Nominal mediated values are 800 Kbps in DL and 1 Mbps in UL in FD-FDD mode, while in HD-FDD mode they are 300 kbps in DL and 375 kbps in UL. The terminal output power is 20 dBm or 23 dBm.

Due to a higher channel bandwidth (minimum 1.4 MHZ) and to a higher reachable bit rate (up to 1 MBps), eMTC does not reach NB-IoT's radio coverage extension levels: the value of MCL (Maximum coupling Loss) reachable by eMTC is 155.7 dB compared to 164 dB of NB-IoT, even if the Tx power is 20 dBm for eMTC and 23 dBm for NB-IoT. The requirement for battery life of the terminals/sensors is also lower than NB-IoT one, although the same mechanisms of DRX and PSM used by NB-IoT.

The complexity of terminals for eMTC, and presumably their consequent cost, is higher than expected for NB-IoT. It follows that the use cases for eMTC are complementary to those foreseen for NB-IoT, e.g. services having different requirements, such as higher bit rates up to 1 Mbps, limited or moderate mobility or others (e.g. wearable categories) that cannot be satisfied with NB-IoT solutions. Table 2 compares the main features of an LTE UE category 1, of catM1 and of NB-IoT.

Supported Features	LTE Cat 1	Cat M1 (LTE-M)	Cat NB1 (NB-IoT)
UE RF Bandwidth	Up to 20 MHz	1.4 MHz	200 KHz
DL Peak Data Rate	10Mbs	~ 1 Mbps	~200 kbps
UL Peak Data Rate	5 Mbps	~ 1 Mbps	~200 kbps
No of RF Rx chains	2	1	1
Max UE Tx power	23 dBm	20 / 23 dBm	23 dBm
Duplex Mode	Full	Half (optional)	Half (mandatory)
Other Features		Coverage Enhancement, Power saving	Stand alone, guard band, in band modes, Coverage Enhancement (20dB), Power saving

Table 2: Sensors Networks (IEEE 802.15.4 [81])

3.2.3 Wireless Sensors Networks (IEEE 802.15.4)

3.2.3.1 Zigbee

ZigBee is a low-cost and low power wireless communication technology, maintained by the Zigbee Alliance, for low-data rate and short-range applications [51]. The ZigBee protocol stack is composed of four main layers: the physical (PHY) layer, the medium access control (MAC) layer, the network (NWK) layer, and the application (APL) layer. In addition, ZigBee provides security functionality across layers. The two lower layers of the ZigBee protocol stack are defined by the IEEE 802.15.4 standard [81], while the rest of the stack is defined by the ZigBee specifications.

The main contribution of Zigbee technology is giving mesh network capabilities to 802.15.4 applications. Mesh networking allows reconfiguration around blocked paths by hopping from node to node until the data reaches the destination. Moreover, Zigbee specifications define a beacon-enabled tree-based topology, as a particular case of the IEEE 802.15.4 peer-to-peer networks. Usually, to deploy Zigbee network, additional equipments such as a Zigbee coordinator and a Zigbee router are required in addition to the Zigbee end-devices. Standard ZigBee node needs an 802.15.4/IP gateway to communicate with an IP network. Hence, ZigBee is good for WSN applications that do not require interfacing with IP devices. However, the new ZigBee IP specification provides an IPv6-based wireless mesh networking solution. It enriches IEEE 802.15.4 by adding network and security layers and an application framework, offering a scalable architecture with end-to-end IPv6 networking.

3.2.3.2 6LoWPAN

The 6LoWPAN standard (RFC 4944) [52] has been defined by IETF to adapt IPv6 communication on top of IEEE 802.15.4 networks. 6LoWPAN refers to IPv6 over Low Power Wireless Personal Area Networks. It enables IPv6 packets communication over low power and low rate IEEE 802.15.4 links and assures interoperability with other IP devices. 6LowPAN devices can communicate directly with other IP-enabled devices.

IP for Smart Objects (IPSO) Alliance [53] is promoting the use of 6LowPAN and embedded IP solutions in smart objects. 6LoWPAN provides an adaptation layer, new packet format, and address management to enable such devices to have all the benefits of IP communication and management. Since IPv6 packet sizes are much larger than the frame size of IEEE 802.15.4 [81], the adaptation layer is introduced between MAC and the network layers to optimize IPv6 over IEEE 802.15.4. The

adaptation layer provides mechanisms for IPv6 packet header compression, fragmentation and reassembly allowing IPv6 packets transmission over IEEE 802.15.4 links.

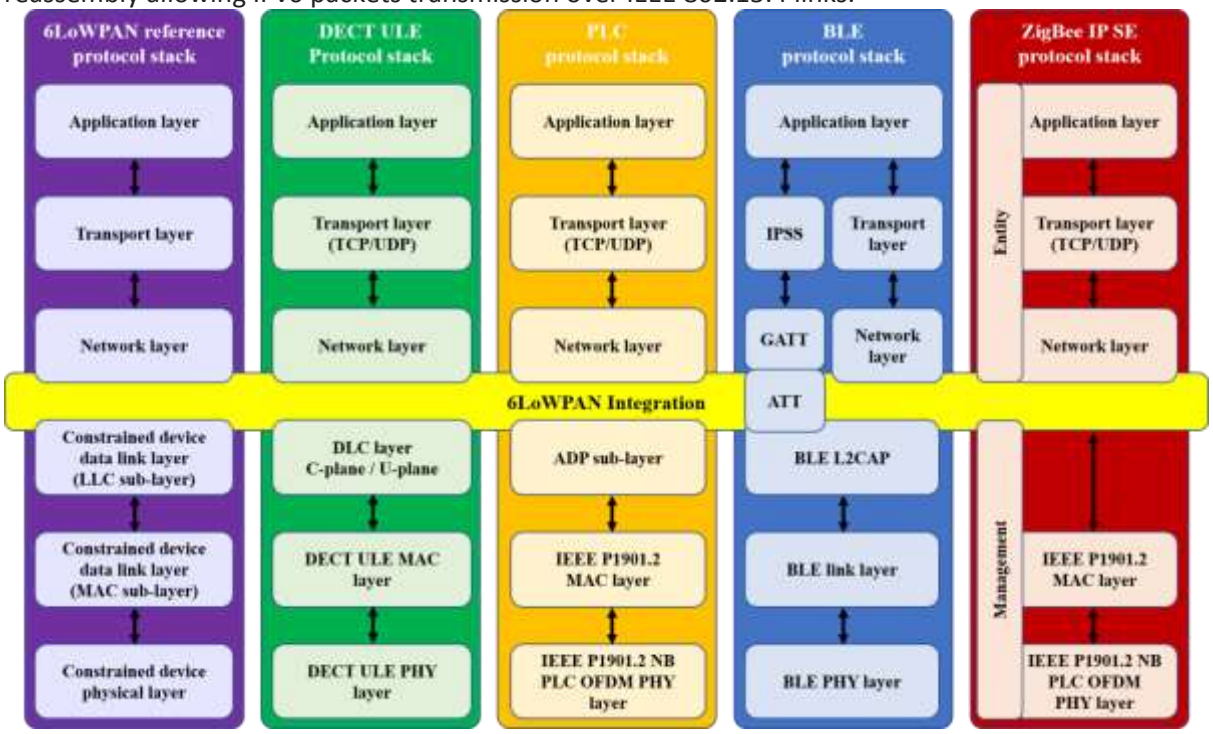


Figure 23 - 6LowPAN integration and adoption over other protocols

The fundamental difference between 6LowPAN and Zigbee is the IP interoperability of the first. 6LowPAN devices are capable of communication with other IP-enabled devices whereas Zigbee node needs an 802.15.4/IP gateway to interact with an IP network. The decision to select one standard versus another should be determined by the target application. For an application in which there is no need to interface with IP devices or the packet size is small, it is not necessary to implement 6LowPAN, which performs fragmentation. Zigbee can achieve better overall performance in such an application.

3.2.3.3 BLE

Bluetooth Low Energy (BLE) [82] is considered as an attractive technology for WSN applications demanding higher data rates, but short range. BLE technology [54] enables new low-cost Bluetooth Smart devices to operate for months or years on tiny, coin-cell batteries. Potential markets for BLE-based devices include healthcare, sports and fitness, security, and home entertainment. BLE operates in the same 2.45 GHz ISM band as classic Bluetooth, but uses a different set of channels. Instead of Bluetooth's 1-MHz wide 79 channels, BLE has 2-MHz wide 40 channels. As compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and lower cost, with enhanced communication range. BLE allows 1 Mbps data rates with 200 m range and has two implementation alternatives; single-mode and dual-mode. Single-mode BLE devices support only new BLE connections, whereas dual-mode devices support both classic Bluetooth as well as new BLE connections and have backward-compatibility.

3.2.4 Intelligent Transport Systems wireless technologies

3.2.4.1 V2X Technologies

3.2.4.1.1 ITS reference architecture

The General standards in ITS Communication Architecture document [83] gives a reference architecture for an ITS station with examples of possible elements in such a station, picture which is

somehow outdated, since new technologies like 3GPP LTE-V2X are not mentioned.

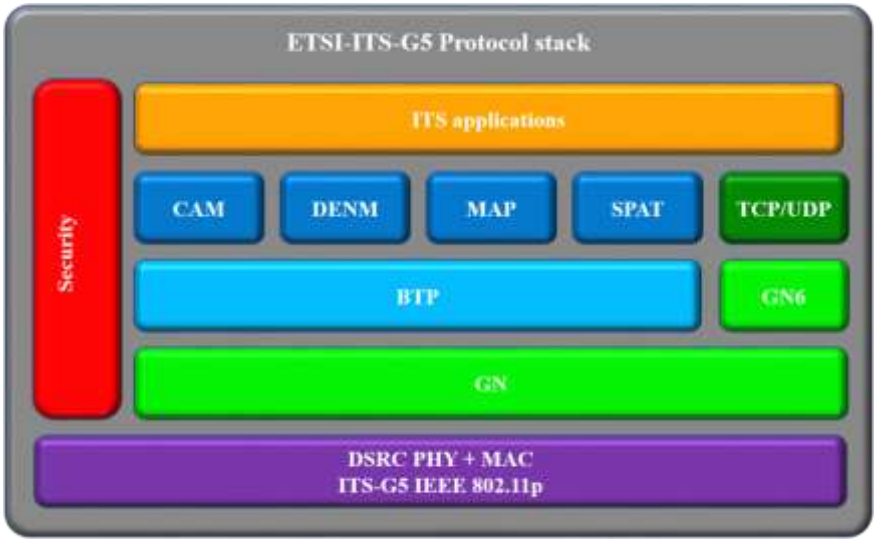


Figure 24 - ETSI-ITS-G5 Protocol stack

The three lower blocks in the middle of Figure 25 contain functionality of the OSI communication protocol stack with:

- "Access" representing OSI layers 1 and 2,
- "Networking & Transport" representing OSI layers 3 and 4,
- "Facilities" representing OSI layers 5, 6 and 7.

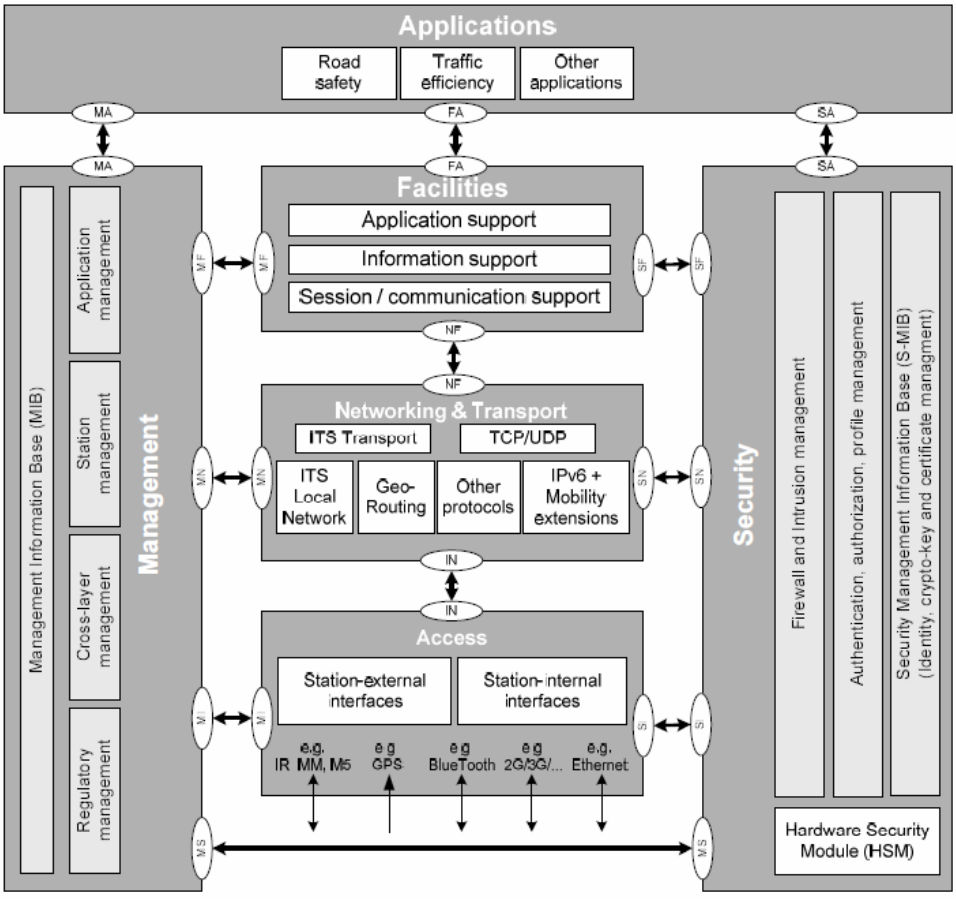


Figure 25 - ITS reference architecture (from [83])

3.2.4.1.2 Access Layer

C-ITS defines physical layer access based on different technologies. ITS-G5 used for V2X communications, formerly addresses as 802.11p is now part of the IEEE 802.11standard [66]. Regarding V2X communications the possibility to use 3GPP technology will be further analysed in section 3.2.4.2.2; in order to have a comparison between these two technologies please refer to [103]. More details are available in ETSI ES 202 663 [104] and EN 302 663 [105]. The spectrum available is the European ITS-ITS-G5A band ranging from 5875 – 5905 MHz with 10 MHz channels (Control Channel and 2 Service Channels). The ITS-G5A frequency band is set aside for ITS road traffic safety applications and it is only allowed to be used by ITS-G5 compliant stations.

Channel Type	Center frequency	Channel number	Channel spacing	Default data rate	Tx Power limit	Tx Power Density limit
G5-CCH	5 900 MHz	180	10 MHz	6 Mbit/s	33 dBm EIRP	23 dBm/MHz
G5-SCH2	5 890 MHz	178	10 MHz	12 Mbit/s	23 dBm EIRP	13 dBm/MHz
G5-SCH1	5 880 MHz	176	10 MHz	6 Mbit/s	33 dBm EIRP	23 dBm/MHz

Table 3: European channel allocation

3.2.4.1.3 Networking and Transport layer

The networking and transport layers must provide low-latency communications and keep signalling, routing and packet forwarding overhead low. Also, it must provide reliable communications with fairness among different nodes with respect to bandwidth or priority type. C-ITS standard defines support to different protocols in this layer. GeoNetworking (GN) is used for communications in the ITS-domain (ETSI EN 302 636), and TCP/UDP/IP protocols in the IP domain e.g. for management purposes. For usage of GN over different ITS access technologies the protocol is split into a media-independent and a media-dependent part for ITS-G5.
Basic Transport Protocol (BTP) is used as transport protocol (part 5 of the standard). BTP provides an end-to-end connectionless transport service for transmission of packets via GN.

3.2.4.1.4 Facilities layer

Facilities provide services and common functionalities to enable different ITS applications. The main components of the facilities are Cooperative Awareness (CA) service that generates CA Messages [69], and Decentralized Environmental Notification (DEN) service that generates DEN Messages [70]. Related to roadside system at intersection also SPAT (Signal Phase and Time) and MAP (map data) are of importance and are standardized in [84]. Also, the Local Dynamic Map (LDM) is part of the facilities layer [85].

3.2.4.1.5 Application layer

On top of this all is the application layer with a focus on ITS road traffic safety applications. A subset of applications is defined in the Basic Set of Applications (BSA) in [86]. Often use cases are descripted in an Urban setting or in a Highway setting, using V2I, I2V, and/or V2V communication.

- Driving assistance – Cooperative awareness
- Driving assistance – Road Hazard Warning
- Speed management

In the AUTOPILOT context this layer must support the different AD use cases. As at this time the focus within C-ITS is on cooperative awareness and environmental notifications. Current available standardized messages set are not directly designed to support ADAS/AD applications. So, new message sets have to be designed or existing has to be adopted/extended. Related to platooning ETSI TR 103 299 “C-ACC pre-standardization study” [87] and TR 103 298 “Platooning pre-standardization study” [88] are of interest. But also other are of interest TS 103 324 “Collective Perception Service” [89], ETSI TS 103 301 “Infrastructure services” [90].

3.2.4.1.6 ETSI G5

The ETSI G5 V2X technology builds upon IEEE 802.11-OCB PHY/MAC layers [66], and describes additional upper layers protocols such as GeoNetworking [68]. OCB stands for "Outside the Context of a BSS". Even though the term “802.11p” is still widely used in the industry, “802.11-OCB” is a more technically correct terminology. In the early versions of IEEE 802.11 standard, the term “p” appeared as an amendment, but since 2005 the 'amendments' like b, g, n, etc…, were rolled into a single 802.11 document ("IEEE 802.11-2016"). This term can be found in new standard documents like ETSI specifications.

The ETSI G5 is a short-range communication system between cars and roadside infrastructure. The “WiFi-like link” have been upgraded for high speed automotive in IEEE 802.11-OCB. ETSI G5 is optimized for mobile conditions, including multi-path reflection situations. It uses a dedicated reserved frequency band at 5.9 GHz (several 10 MHz channels): one channel reserved for safety messages, the remaining channels open for extra services. The typical range is at least 500 meters, and is meant to “look around corners” thanks to multipath fading-channel reflections. It has been shown that with state of the art technology, meanwhile also offered as products, larger ranges of 1 km and more are routinely achievable. IEEE 802.11-OCB focuses on short range low latency applications (<300 ms sensor-to-actuator, where the actual latency from network layer to network layer is only a small portion, typically in the order of 2 ms).

C-ITS does not exclude other communication channels (such as cellular-based channels). As an example of use cases enabled by C-ITS, the below tables are taken from the EU commission report “C-ITS Platform final report” [91]. The targeted applications can be separated between Day 1 and Day 1.5 use cases.

#	Day 1 Services (2019?)			Bundle
1	Emergency electronic brake light	V2V	Safety	1
2	Emergency vehicle approaching	V2V	Safety	1
3	Slow or stationary vehicle(s)	V2V	Safety	1
4	Traffic jam ahead warning	V2V	Safety	1
5	Hazardous location notification	V2I	Motorway	2
6	Road works warning	V2I	Motorway	2
7	Weather conditions	V2I	Motorway	2
8	In-vehicle signage	V2I	Motorway	2
9	In-vehicle speed limits	V2I	Motorway	2
10	Probe vehicle data	V2I	Motorway	2
11	Shockwave damping	V2I	Motorway	2
12	GLOSA / Time To Green (TTG)	V2I	Urban	3
13	Signal violation/Intersection safety	V2I	Urban	3
14	Traffic signal priority request (designated veh.)	V2I	Urban	3

Table 4: Day 1 targeted applications

#	Day 1.5 Services			Bundle
1	Off street parking information	V2I	Parking	4
2	On street parking information and management	V2I	Parking	4
3	Park & Ride information	V2I	Parking	4
4	Information on AFV fuelling & charging stations	V2I	Smart Routing	5
5	Traffic information and smart routing	V2I	Smart	5

			Routing	
6	Zone access control for urban areas	V2I	Smart Routing	5
7	Loading zone management	V2I	Freight	6
8	VRU protection (pedestrians and cyclists)	V2X	VRU	7
9	Cooperative collision risk warning	V2V	Collision	8
10	Motorcycle approaching indication	V2V	Collision	8
11	Wrong way driving	V2I	Wrong Way	9

Table 5: Day 1.5 targeted applications

3.2.4.1.7 IEEE802.11-OCB

Standard IEEE802.11-OCB [66] is the proposed PHY&MAC layers of several V2X applications such as U.S. V2X or ETSI G5. The latest version to date is 802.11-2012 and should be used unless explicitly mentioned otherwise.

3.2.4.1.7.1 IEEE802.11-OCB MAC

The Medium Access Control (MAC) layer governs how the shared communication channel is divided among users (either vehicles, road-side units, personal devices). In the case of IEEE802.11-OCB, this functionality is fully distributed to the end users, meaning there is no central entity such a base-station or road-side unit network that provides a time reference nor an access policy to the network. The IEEE802.11-OCB MAC layer is based on CSMA (Carrier Sense Multiple Access), which is a "listen-before-talk" scheme. A user that wants to transmit must first sense the medium, measure its occupancy rate, and derive when appropriate to send his message.

This scheme deals efficiently with congestion in the wireless channel. This mechanism is called DCC (Decentralized Congestion Control). In a standardized way, data-rate, power and a number of other parameters can be automatically modified so that congestion in the channel reduces, causing the relevant nearby messages to still arrive. This scheme mitigates interferences between users. Such channel access procedure in IEEE 802.11 [66] is summarized in Figure 26 of ETSI EN 302 663 [71].

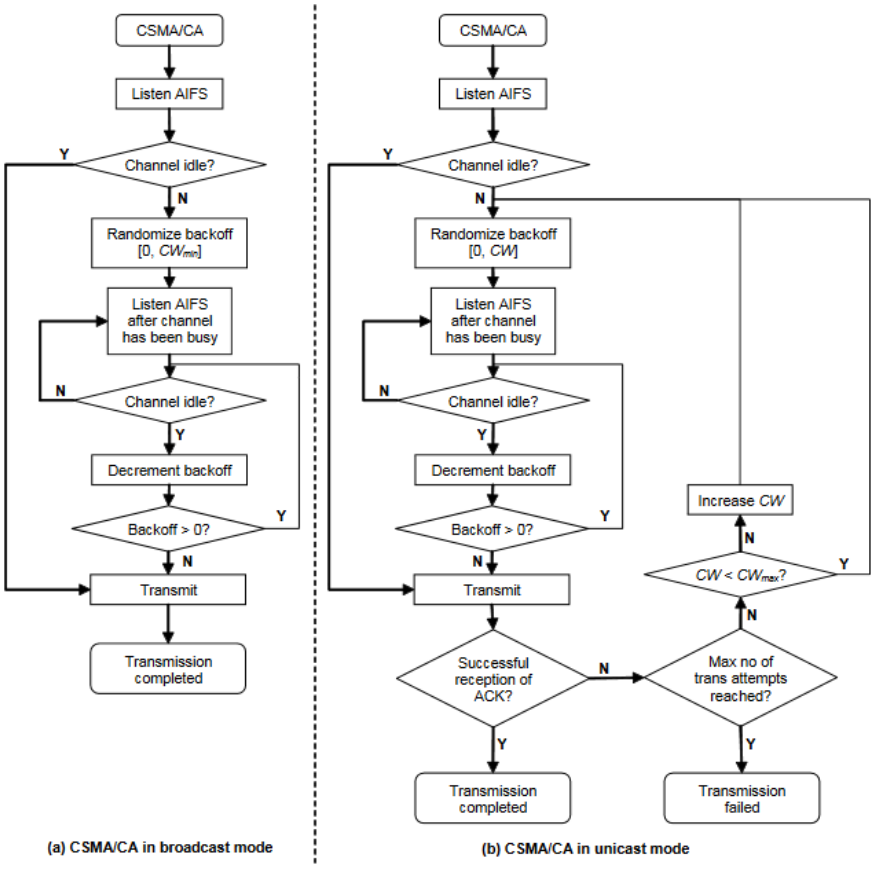


Figure 26 Channel Access Procedure 802.11-OCB (from [71])

The IEEE802.11-OCB MAC layer introduces several quality of service (QoS) classes, to provide a higher bandwidth to the safety-critical message.

3.2.4.1.7.2 IEEE802.11-OCB PHY

The PHY layer of IEEE802.11-OCB standard takes roots from the long-standing and mature IEEE802.11a/c technology. It is based on OFDM technology, as described in IEEE802.11-2012, chapter 18 “Orthogonal frequency division multiplexing (OFDM) PHY specification”.

The PHY layer is responsible for the encoding of the bit payloads provided by higher layers into a given modulation (e.g. QPSK), and generating the time-domain IQ samples waveform.

- A preamble is sent as a training sequence. It is composed of 12 training symbols (ten short training sequences, and two long training sequences). Their purpose is to calibrate the receiver’s AGC, get a good time and frequency synchronization between the transmitted messaged and the receiver, and for channel estimation purposes. Channel estimation is needed for the receiver to estimate the amplitude and phase distortions and Doppler shifts that may arise from the wireless multipath fading-channel.
- Users data (PDU) are encoded with convolution codes and rate-matching. Then, a modulation mapper transforms groups of bits into complex-values symbols (e.g. QPSK, 16QAM), and are placed into a frequency domain grid together with some pilot-subcarrier tones.

Parameters	IEEE 802.11a	IEEE 802.11-OCB
bit rate	6-54 Mbps	3-27 Mbps
modulation	BPSK, QPSK, 16/64QAM	BPSK, QPSK, 16/64QAM
code rate	1/2,2/3,3/4	1/2,2/3,3/4
number of subcarriers	52	52
symbol duration	4 usec	8 usec
cyclic prefix	0.8 usec	1.6 usec
FFT duration	3.2 usec	6.4 usec
subcarrier spacing	312.5 kHz	156.25 kHz

Table 6: Recap of the main PHY parameters of 802.11-OCB

3.2.4.2 3GPP technologies

3.2.4.2.1 LTE D2D

One of the vertical areas 3GPP Rel 14 ([92], [93]) will be looking at is Device to Device (D2D) and device-to-network relays for IoT and Wearables. This really means looking at how remote devices, like wearables, connect to other devices that in turn connect to the access network. An example might be a wearable device of some kind that relays back to the network via a connection to a smartphone.

Work on enabling Proximity Services started in R12 with the focus on Public Safety applications and continued in R13. The 3GPP proposal says there is a lot of interest in using LTE technology to connect and manage low cost MTC devices, such as wearables, “which also have the benefit of almost always being in close proximity to a smartphone that can serve as a relay”.

One study item is to give networks the ability to differentiate between traffic coming from a wearable and from the relay device (e.g. smartphone) in the access layer. Achieving that differentiation would allow the operator to treat the wearable or remote device as separate devices, say for billing or security. In particular, 3GPP security associations never reach end-to-end between the network and the remote device, meaning that the relay (smartphone) has clear text access to the remote device’s communications. 3GPP would like UE-to-Network relaying to be enhanced to support end-to-end security through the relay link, service continuity, E2E QoS where possible, efficient operation with multiple remote UEs, and efficient path switching between Uu and D2D air-interfaces.

A second strand in the study item is to look at enhancements to give remote devices the ability to operate at lower power, rate and complexity. The idea is to reuse the ideas developed during NB-IoT and eMTC studies, e.g. the NB-IoT/eMTC uplink waveform can be reused for D2D. Such devices will potentially use a single modem for communicating with the internet/cloud and for communicating with proximal devices. The current PC5 link design – the interface between devices – is inherited from the design driven by public safety use cases and represents a bottleneck that prevents low power and reliable D2D communication, due to lack of any link adaptation and feedback mechanisms. These shortcomings will not enable designers to achieve the required performance metrics for wearable and MTC use cases in terms of power consumption, spectrum efficiency, and device complexity [94].

Therefore, Rel14 will see 3GPP look to study and define a generic UE-to-Network Relay architecture, including methods for the network to identify, address, and reach a remote UE via a relay UE.

3.2.4.2.2 Cellular V2X

As part of the expansion of the LTE platform to new services, and to keep track with the increasing needs of the automotive industry, 3GPP is developing functionality to provide enhancements specifically for vehicular communications - both in terms of direct communication (between vehicles, vehicle to pedestrian and vehicle to infrastructure) and for cellular communications with networks [95].

The initial Cellular Vehicle-to-Everything (V2X) standard, for inclusion in the Release 14, was completed in September 2016 during the 3GPP RAN meeting in New Orleans. It focuses on Vehicle-to-Vehicle (V2V) communications, with further enhancements to support additional V2X operational scenarios to follow, in Release 14, targeting completion during March 2017.

The 3GPP Work Item Description can be found in RP-161894 [96].

V2V communications are based on D2D communications defined as part of ProSe services in Release 12 [97] and Release 13 [79] of the specification. As part of ProSe services, a new D2D interface (designated as PC5, also known as sidelink at the physical layer) was introduced and now as part of the V2V WI it has been enhanced for vehicular use cases, specifically addressing high speed (up to 250Kph) and high density (thousands of nodes) .

To that end, a few fundamental modifications to PC5 have been introduced. Firstly, additional DMRS symbols have been added to handle the high Doppler associated with relative speeds of up to 500 kph and at high frequency (5.9GHz ITS band being the main target). This results in the sub-frame structure illustrated in Figure 27.

As illustrated the V2V sub-frame for PC5 interface has 4 DMRS symbols, in addition to the Tx-Rx turnaround symbol at the end, allowing for better tracking of the channel at high speed.

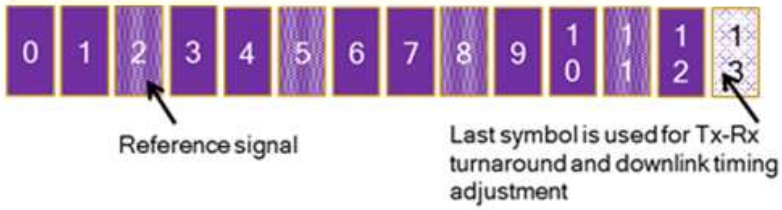


Figure 27 – V2V sub-frame (from [95])

Secondly, a new arrangement of scheduling assignment and data resources has been agreed. The arrangement is illustrated in Figure 28 and is designed to enhance the system level performance under high density while meeting the latency requirements of V2V. Scheduling assignments (SA or PSCCH) are transmitted in sub-channels using specific RBs across time. Data transmissions associated with said scheduling assignments are occupying adjacent RBs in the same sub-frame. Note that another variant where SA and associated data transmissions are not necessarily transmitted on adjacent RBs has also been standardized.

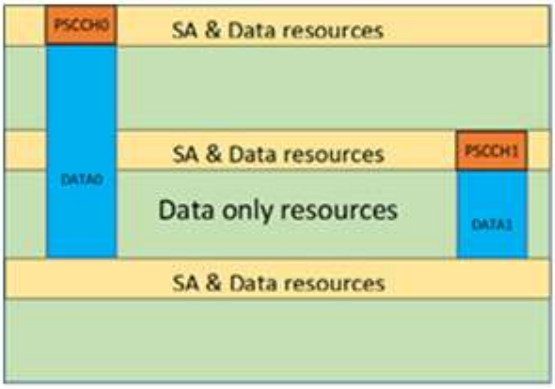


Figure 28 - Scheduling assignment and data resources (from [95])

Finally, for distributed scheduling (a.k.a. Mode 4) a sensing with semi-persistent transmission based mechanism was introduced. V2V traffic from a device is mostly periodic in nature. This was utilized to sense congestion on a resource and estimate future congestion on that resource. Based on estimation resources were booked. This technique optimizes the use of the channel by enhancing resource separation between transmitters that are using overlapping resources.

The design is scalable for different bandwidths including 10 MHz bandwidth. Based on these fundamental link and system level changes there are two high level deployment configurations currently defined, and illustrated in Figure 29.

Both configurations use a dedicated carrier for V2V communications, meaning the target band is only used for PC5 based V2V communications. Also in both cases GNSS is used for time synchronization.

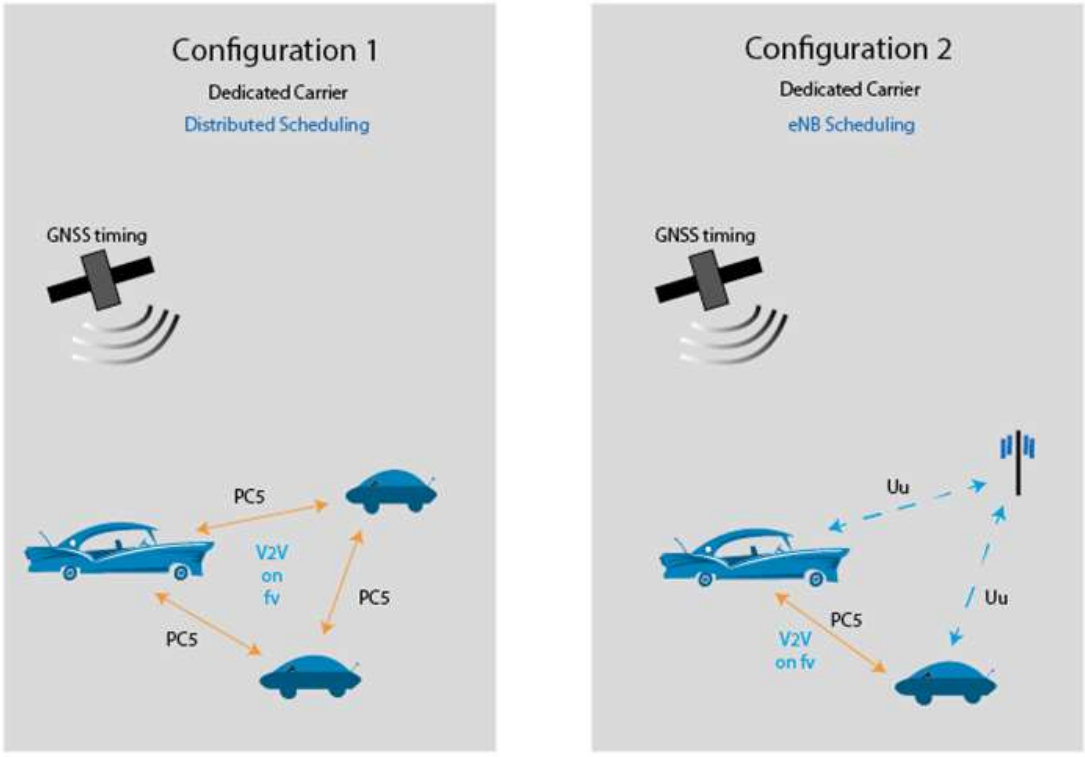


Figure 29 – High level deployment configurations (from [95])

In “Configuration 1” scheduling and interference management of V2V traffic is supported based on distributed algorithms (Mode 4) implemented between the vehicles. As mentioned earlier the distributed algorithm is based on sensing with semi-persistent transmission. Additionally, a new mechanism where resource allocation is dependent on geographical information is introduced. Such a mechanism counters near far effect arising due to in-band emissions.

In “Configuration 2” scheduling and interference management of V2V traffic is assisted by eNBs (a.k.a. Mode 3) via control signalling over the Uu interface. The eNodeB will assign the resources being used for V2V signalling in a dynamic manner.

3.3 IP Communication

This section will describe the IP communication based on the AD use cases requirements defined in deliverable D1.1 [1]. For example the Versailles use-cases exhibit the need of using scalable IP communication protocols involving vehicles, fixed infrastructure along the road, and Internet connectivity. The communication architecture relies on a basis of existing Road-Side Units, traffic light controllers and cellular network access to the Internet. New entities will be deployed, namely vehicle On-Board Units, new Road Site Units, point-to-point links and potentially RFIDs.

Before describing the IP communication system, it is necessary to introduce the simple use-case where this system is used.

Deliverable D1.1 lists the high-level overview of the Versailles use-cases for tourist applications. The use-cases are “Automated Fleet Rebalancing”, “Autonomous Valet Parking”, “Connected Urban Driving”, “Fully Autonomous Driving”, and potentially others.

In order to express the need of IP communication, we show here a simple use-case issued from the current study of an initial phase during the use-cases “Fully Autonomous Driving” and “Automated Fleet Re-balancing”.

In “Fully Autonomous Driving”, it is considered that a VFLEX vehicle together with passengers/driver leaves its parking slot situated in the front of the town hall. A succession of 5 steps synchronizes the vehicle with the traffic lights, as illustrated in Figure 30:

Figure 30: Use-case Autonomous Driving and Traffic Lights

This figure depicts, from bottom to up:

1. The car quits the parking lot
2. Car ensures nobody on the crosswalk
3. Car detects stop line painted on the ground and stops, commands lights, and waits for data
4. Car passes, then waits for data
5. Car turns left into traffic

On the bottom line (near step 1), it is possible to insert an RFID into ground that is useful for precise localization. Several “Feux” (traffic lights) are depicted as yellow pins, whose numbers correspond to the traffic lights controller’s identification. In the upper left corner is indicated the presence of an existing Road Side Unit, that is disconnected from the Internet and from the traffic lights controller. This represents an example under study.

In order to realize the above use-case, several data paths over various communication technologies are necessary.

RFID detection: certain points are of high importance to the vehicle. It is required to be detected with high precision, and reliably. It is the case for the stop line painted on ground, or for the crosswalk lines. In this particular setting of small dimensions, and where it is possible to control the points, the RFID technology is probably the most reliable and precise method compared to satellite reception, inertial station, video camera recognition, and similar.

In Figure 31 the IP networking topology for RFID detection by the vehicle is described.

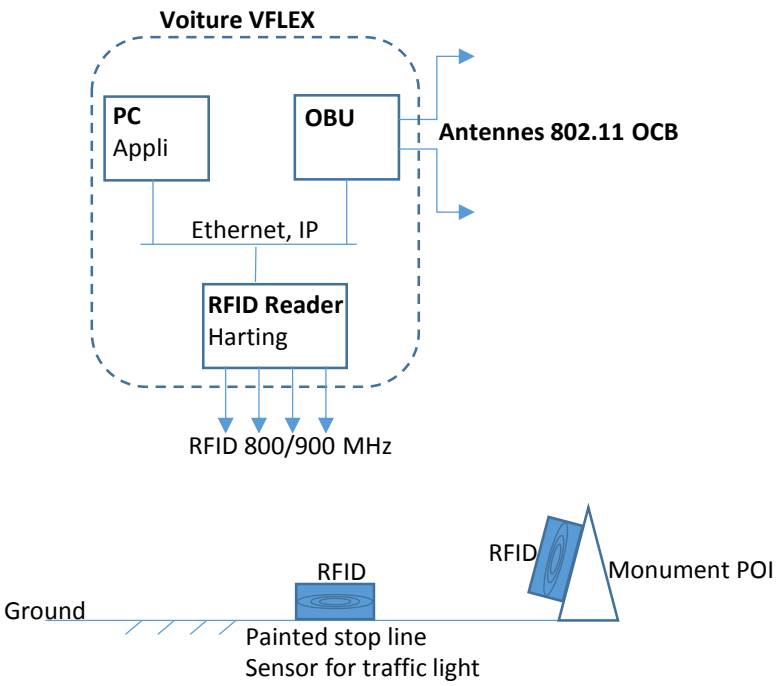


Figure 31: IP Networking Topology for RFID-based detection

In particular an automated car model "VFLEX" is illustrated. The network deployed in the car consists of an Application PC, an On-Board Unit (OBU) and an Ethernet-enabled RFID Reader of brand "Harting". These three entities are connected together with wired Ethernet that supports IP protocols.

Depending on the application requirements it could be possible to offer both IP protocols versions, namely IPv4 [116] and IPv6 [117]. The latter would be preferable in vehicular environment because of features that fit the fast connection-establishment requirements of the case. The SLAAC auto-configuration is usually faster than DHCP most of the times. Additionally the large addressing space of IPv6 can accommodate a large number of new network in new vehicles.

The communication among the entities inside the car will be done through a wired Ethernet network. The "IoT Platform" (aka OBU) device will be in charge to give the access to the external world (vehicles and infrastructures), while the other entities, as PCs for applications and RFID Reader, will utilize this connection to perform all the message exchanges required using the IP technologies indicated above.

Depending on the application, the the transport protocol used could be TCP [74] as well as UDP [75] or others running over IP. For example, one of the applications will be RTMaps. This software communicates with sockets on IP, including IPv6.

Regarding the choice of the application protocols a certain freedom can be allowed. The RFID devices are deployed on the ground, for example near the ground-painted Stop line, or otherwise in the pavement or on its border. The same type of device can be attached on a monument that needs to be signaled as a tourist Point of Interest.

The RFID uses RFID radio technology (e.g. EN 302 208 at 800/900 MHz [118]). Depending on the range needs, it could use also NFC (Near Field Communications). It is possible to use IP to carry data packets over these kinds of links (e.g. IPv6-over-NFC [119]).

Once the tag is detected, this information can be sent by the RFID reader directly to the traffic light controller, in an end-to-end manner. This transmission can happen over the OBU. The OBU is connected to the outside of the car by using IEEE 802.11 OCB technology [66].

In this case an IPv6 communication would be preferable. The availability of a link local address would make a vehicle immediately reachable inside the wireless channel. Up to IP, depending on the application that is going to send the message, could be used TCP as well as UDP or others. If the OBU needs to maintain TCP connection, then MobileIP can be used.

Communication with the Traffic Lights Controller: in the steps 3 and 4 of the small use-case described above (automated car getting out of parking slot) there is a need to issue commands from the car to the traffic lights, and wait for the car to receive status reports from the traffic lights.
An initial design of the communication system between the car and the traffic lights is illustrated in Figure 32.

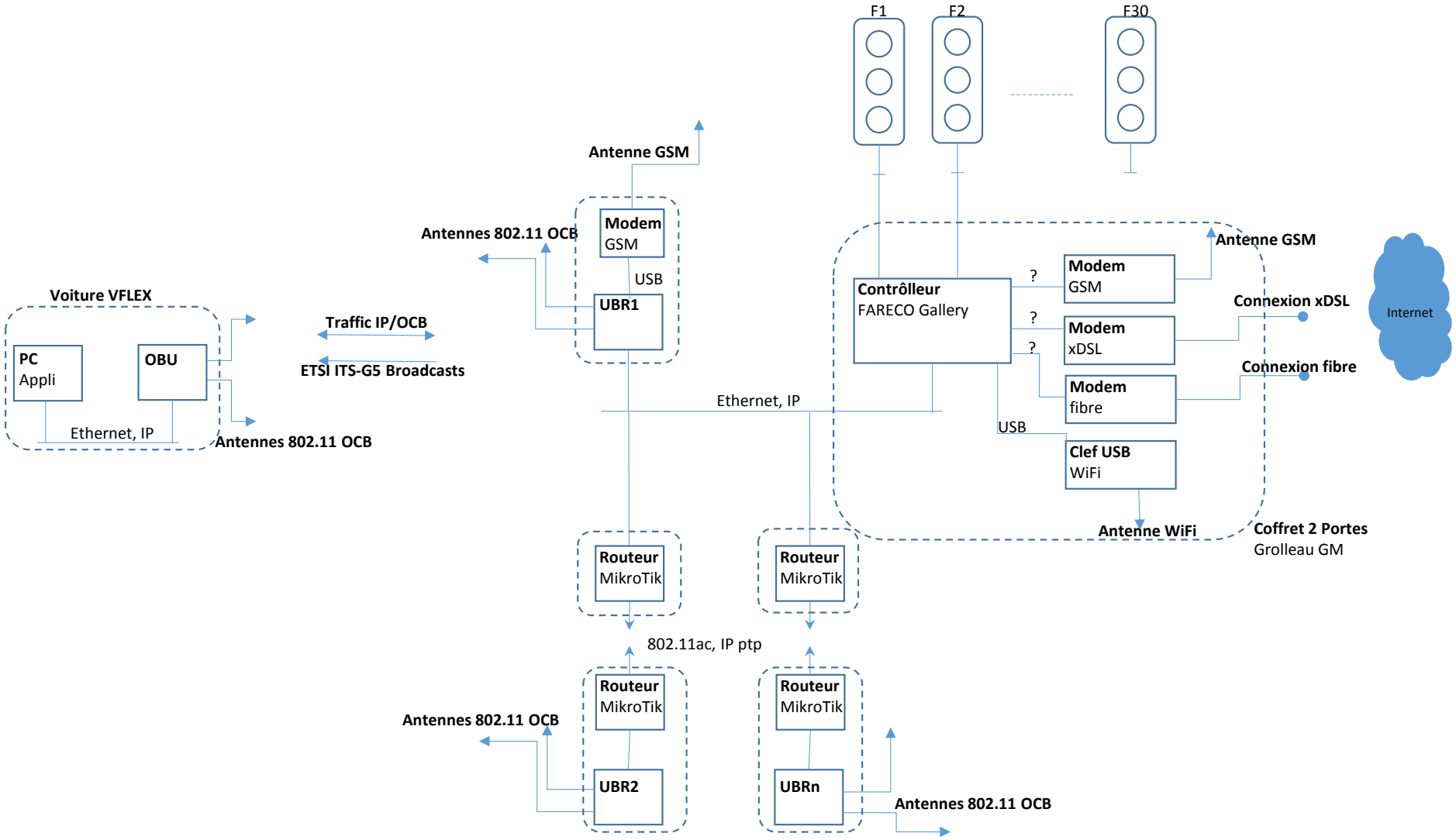


Figure 32: IP Communication System – Automated Car and Traffic Lights

In this figure the following communications links are illustrated:

- RSU to traffic light controller
- RSU to Internet, on cellular
- RSU to RSU, on point to point links

IP UBR to car communication: **mix of IP and MAC** communications (IPv6-over-80211-OCB and ETSI ITS-G5).

IP OBU to OBU

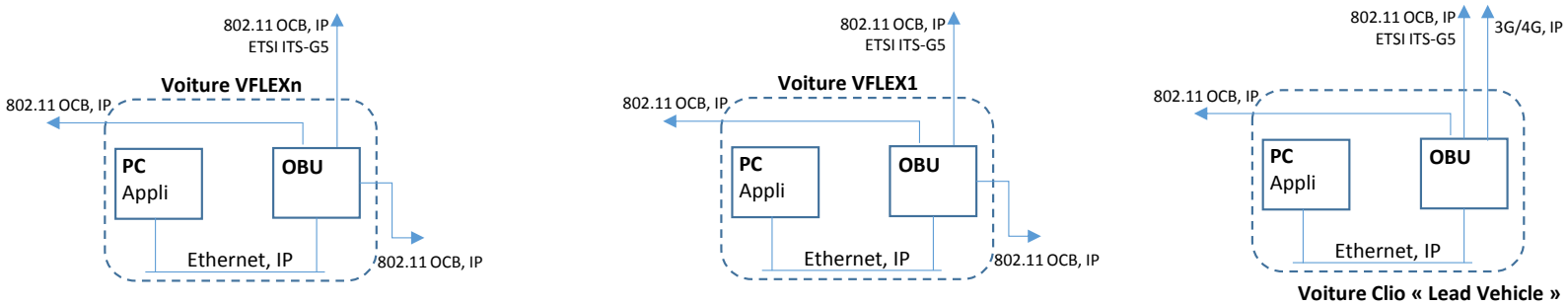


Figure 33: OBU to OBU communications

Communication among the vehicles will be obtained thanks to the OBU. Three antennas tuned in three different channels allowed by ETSI ITS-G5, will give connection respectively to the front vehicle, the rear vehicle and the infrastructure (Figure 33). Once established the 80211-OCB channels the communication between the car can be obtained using IP and up to it any transport layer protocol.

4 Autopilot Infrastructure Architecture

This section has the goal to identify the relevant communication interfaces for the AUTOPILOT ecosystem and their general description. In order to get this goal a general reference architecture scheme that can be in principle applied to all the pilot sites trials and a description of all the macro elements that are part of the reference architecture will be initially provided. The work for this chapter is based on the outputs of task 1.2 “IoT Architecture and Specification” and task 1.3 “Vehicle IoT platform specification”, with the focus to highlight mainly communications aspects involved by the project.

The communication technologies mentioned in this section are described in detail in Section 3.

4.1 Reference architecture scheme

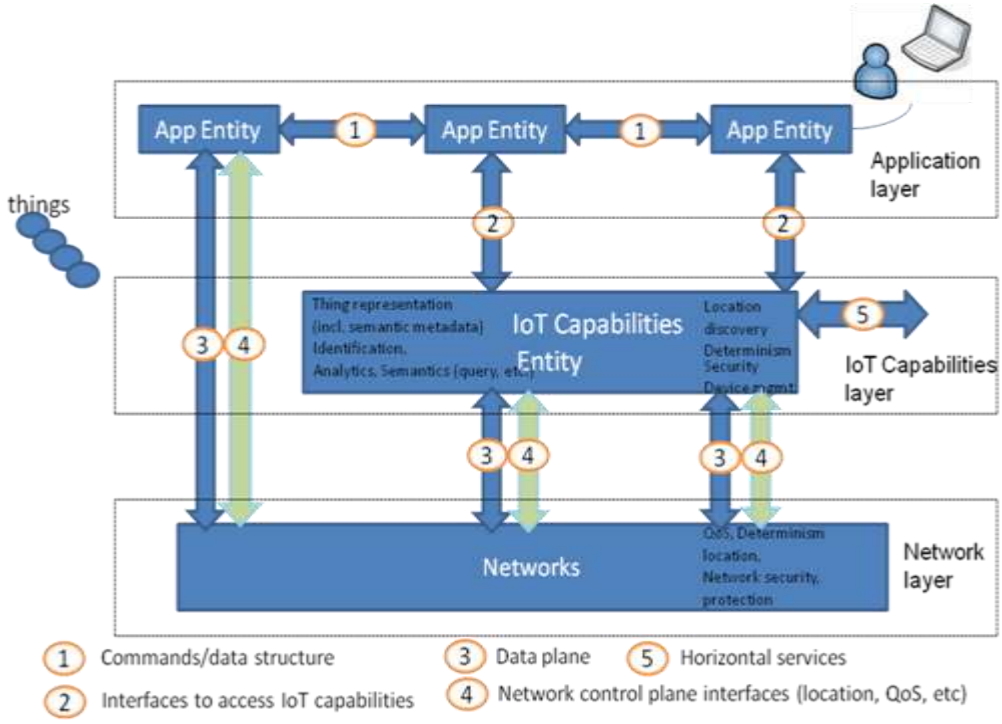


Figure 34 - AIOTI functional view as a reference model for AUTOPILOT architecture (from AIOTI_IoT_HLA [2])

Figure 34 shows the AIOTI functional view which serves as the reference model for AUTOPILOT architecture. The functional view is based on three main layers: Networks layer, IoT Capabilities layer and Application layer. Let us describe the three layers below.

The Networks layer: the services of the Network layer can be divided into two groups:

- data plane services, providing short and long range connectivity and data forwarding between entities
- control plane services such as location, device triggering, QoS.

Interfaces are the following:

1. Commands/data structure interface defines the structure of the data exchanged between App Entities (the connectivity for exchanged data on this interface is provided by the underlying Networks). Typical examples of the data exchanged across this interface are: authentication and authorization, commands, measurements, etc.
2. Interface to access IoT capabilities enables access to services exposed by an IoT Entity to e.g. register/subscribe for notifications, expose/consume data, etc.

3. Data Plane interface enables the sending/receiving of data across the Networks to other entities.
4. Network control plane interface enables the requesting of network control plane services such as: device triggering, location of a device, QoS bearers, etc.
5. Horizontal services interface enables the exposing/requesting services to/from other IoT Entities. Examples of the usage of this interface are to allow a gateway to upload data to a cloud server, retrieve software image of a gateway or a device, etc.
6.

The Application layer: contains the communications and interface methods used in process-to-process communications.

The IoT layer: groups IoT specific functions, such as data storage and sharing, and exposes them to the application layer via interfaces commonly referred to as Application Programming Interfaces (APIs).

4.2 Architecture layers

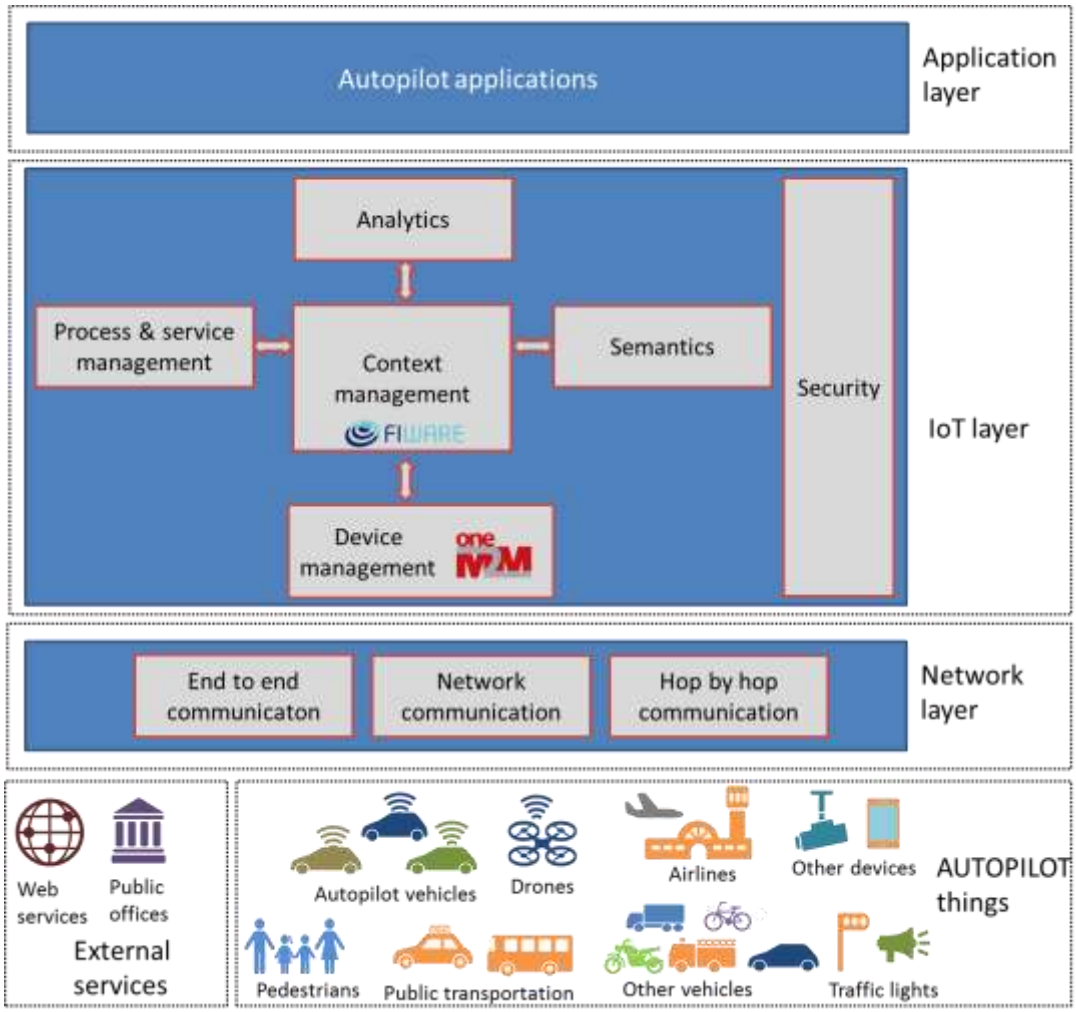


Figure 35 - AUTOPILOT IoT architecture functional view (from D1.3 [3])

In this section we describe the AUTOPILOT architecture and the layers (tiers) of the AUTOPILOT architecture. For more detailed descriptions about the architecture and the functional blocks, we refer the readers to D1.3 [3].

AUTOPILOT architecture is based on the aforementioned AIOTI reference model and the functional blocks are more specific to the elements of the AUTOPILOT infrastructure. Figure 35 shows the functional view of the architecture. This architecture view provides a high level view which can be applicable to all pilot sites and use cases. The decision of using such reference architecture is based on the discussions through different alternatives, existing technologies, the necessities of AUTOPILOT, as well as the differences and commonalities of the pilot sites. The high level functional view is composed of four layers: 1) AUTOPILOT things & external services layer, 2) network layer, 3) IoT layer, 4) AUTOPILOT applications layer. The first layer consists of various entities (south bound). The second and the third layers consist of different functional building blocks. The north bound is represented by the applications that will be developed for AUTOPILOT. This functional view does not provide restriction on the physical view where processing or communication units are deployed in different places dependent on the needs. For instance, processing units can be located either in Cloud or in Edge.

4.2.1 Things layer

4.2.1.1 Vehicular Platform

To communicate with the IoT platform, things need to access to the Internet network. Accessing to Internet will be enabled by the network layer which is, in practical terms, the telecommunications network infrastructure and related communications technologies (refer to sections 3.1 & 3.3).
Classic communications are end-to-end (Figure 36) where features such as control flow are located at end nodes (transmitter and final receiver). This network design pattern implies that end nodes contains enough “intelligence” and that intermediate nodes (in the network layer) do not realize features such as control flow.

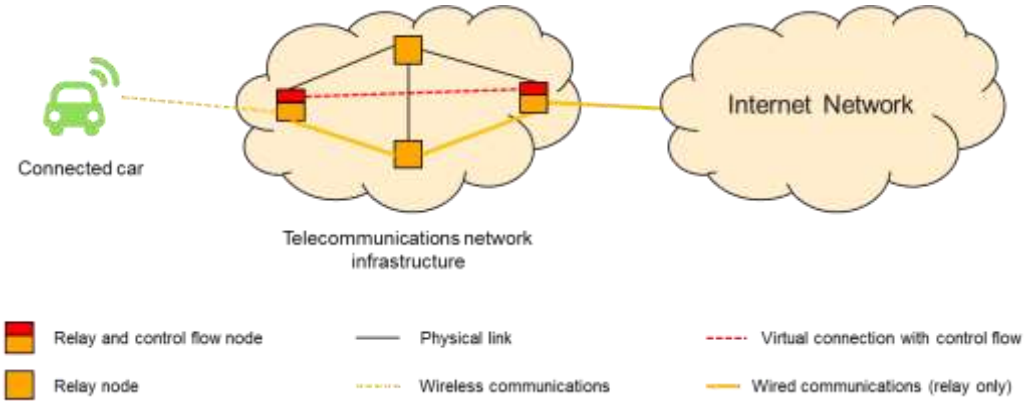


Figure 36 - End-end communications

Because future communications within an IoT context may involve high mobility, intermittent connectivity and low-power devices, “intelligence” may be shift to the network layer nodes. As result, feature like control flow will be realized in-between each intermediate nodes. This network design pattern is called hop-by-hop communications (Figure 37).

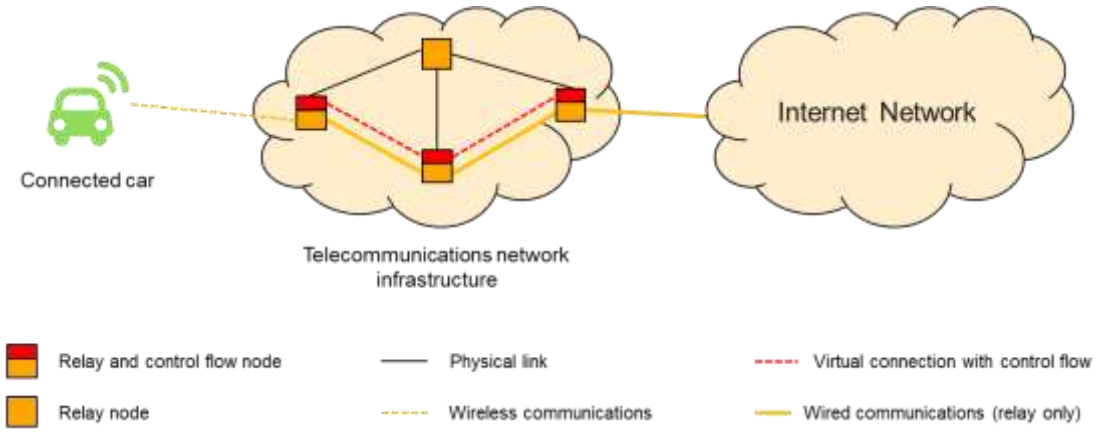


Figure 37 - Hop-by-hop communications

4.2.1.2 IoT eco-system

AUTOPILOT IoT eco-system include various "*things*" such as IoT devices or infrastructure elements. For instance, smartphones of pedestrians or passengers, static or on-board cameras, and drones can be seen as IoT devices. Traffic lights, transportation services, sensors deployed on or close to the roads (e.g., flooding sensors), can be seen as infrastructure elements. Moreover, transportation services can be seen as part of the IoT eco-system, where city-wide public transport services the people with non-autonomous vehicles or in the future with autonomous vehicles. Lastly, pedestrians are also the actors of the IoT eco-system.

In the AUTOPILOT IoT eco-system, things may be data providers, data consumers or neither of those (passive participation to the eco-system). For instance, some things can be simply observed by the sensors. An example for that may be the cameras which count the number of people in a certain area. In this scenario, the people are observed, while they do not provide or consume data.

Other than the aforementioned members of the IoT eco-system, there exist "*external services*" which can provide information through their APIs or request information from the IoT PFs. Some use cases need information such as weather measurements or information from government agencies or public departments such as the police department.

4.2.2 Network layer

The network elements can be inside the cars, in the road site, or through the Internet. Communication interfaces, communication technologies and the communication requirements will be discussed in detail (refer to sections 3.1 & 3.3). In the functional view (Figure 35), the network layer is listed with the functionalities of end to end communication, network communication, and hop by hop communication.

4.2.3 IoT layer

The IoT layer in Figure 35 includes the IoT platforms (PFs) which consist of a set of services. An IoT PF consists of a set of services that may have various capabilities including processing, communication, resource management, context management, and security.

IoT PFs can be considered as the middle layer between "things" and the "applications" and requires network layer functionalities in order to operate. As they offer a set of functionalities and various levels of abstractions, IoT PFs can make the life of application developers much easier compared to having traditional approaches. In the traditional deployments, developers need to connect and

manage devices along with other services, whereas IoT PFs provide abstractions and hides the complexity of the deployments from the application developers.

One of the key aspects of the AUTOPILOT project for leveraging IoT in autonomous cars is data collection in real and near-real time. In order to drive autonomously, a vehicle must collect data from its local surroundings. Data collection must be from other vehicles, others participants in traffic (e.g., pedestrians, cyclists), fixed infrastructure (roads, buildings, etc.), and dynamic elements (e.g., traffic lights).

The functional blocks are listed as device management, context management, semantics, process & service management, analytics, and security. These functional blocks are described in D1.3 in detail.
In AUTOPILOT project, it is not required for every pilot site to use only one IoT PF. On the other hand, it is expected to have a central IoT PF where other IoT PFs from pilot sites and 3rd party IoT PFs can access this IoT PF if necessary.

4.2.4 Applications layer

Applications layer consists of a set of AUTOPILOT applications which operate on top of IoT layer. For instance, the applications developed in AUTOPILOT can connect to the central IoT PF or a 3rd party IoT PF. In Figure 35, applications layer stay on top of the IoT layer in the north bound. The applications are necessary for the realization of use cases which are defined in [1].
In addition to those use cases which are listed above, there may be other external applications (applications of organizations other than the AUTOPILOT project partners) or services which connect to the AUTOPILOT IoT PFs for accessing IoT information from pilot sites. The connection of vehicles to the Internet offers new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. The mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications are created and the developments such as Internet of Vehicles (IoV) that converge with the autonomous vehicles implementations.
This support the deployment of safe and autonomous vehicles (SAE international level 5, full automation [62]) in different use case scenarios, using local and distributed information and intelligence based on real-time reliable IoT platforms managing mixed mission and safety critical vehicle services, advanced sensors/actuators, navigation and cognitive decision-making technology, interconnectivity between vehicles (V2V), vehicle to infrastructure (V2I), vehicle to devices (V2D), vehicle to pedestrians (V2P), vehicle to grid (V2G) communication.

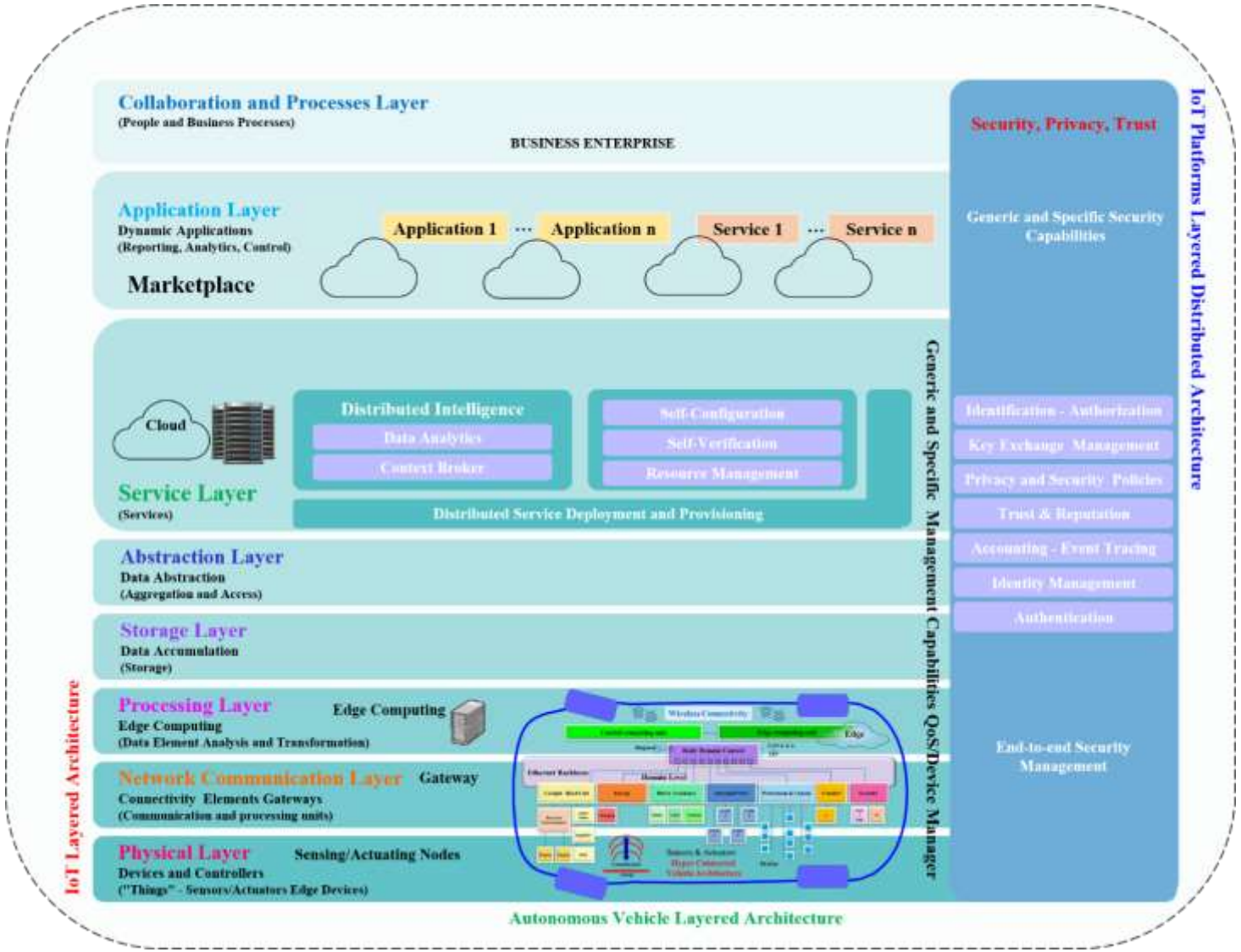


Figure 38 – IoT layered architecture (Source [3])

The layered IoT architecture (Figure 38) used in autonomous systems implementations integrate new components in the different IoT architecture layers to address the challenges for connectivity and intelligence, actuation and control features, linkage to modular and ad-hoc cloud services, data analytics and open APIs and semantic interoperability across use cases and conflict resolution by addressing object identity management, discovery services, virtualization of objects, devices and infrastructures and trusted IoT approaches. Figure 38 presents the IoT layered architecture that solution providers can use, share, reuse the data streams and perform analytics on shared data increasing the value added of IoT applications. The IoT applications using this approach integrate data and services among different IoT platforms and between different applications, using shared infrastructure and common standards and reducing the cost for deployment and maintenance.

4.3 Communication interfaces

In this paragraph are described all the communication interfaces related the AUTOPILOT architecture (Figure 35); so both aspects have been analysed: the IoT components (FIWARE, oneM2M, and Watson IoT PF - from section 4.3.1 to section 4.3.3) and the vehicle to vehicle/infrastructure subsystem (from section 4.3.4 to section 4.3.6).

The requirements for IoT platforms for autonomous vehicle applications need to ensure an inclusive IoT environment that is accessible to various applications across the functional context and interface with other autonomous systems. This requires a stable, secure, and trustworthy IoT environment that assure a globally connected, and interoperable IoT platforms and environments built upon industry-driven, standards-based that enable interoperability, infrastructure development and access by fostering the technological, physical and spectrum- related assets needed to support autonomous vehicle applications and deployments. In this context the safety, reliability, robustness, and security of heterogeneous communication interfaces are essential (please refer to sections: 3.2 & 3.3).

4.3.1 FIWARE

FIWARE [110] focuses on a common data model and powerful interfaces for searching and finding information in IoT. FIWARE is using the OMA Next Generation Service Interface (NGSI) data model as the common information model of IoT-based systems and the protocol for communication. NGSI-9 and NGSI-10 are HTTP-based protocols which support JSON and XML formats for data. Let us shortly describe these two interfaces.

NGSI9: it is used to manage the availability of context entity. A system component can register the availability of context information, and later on the other system component can issue either discover or subscribe messages to find out the registered new context information. Detailed specifications can be found in [53].

NGSI10: it is used to enable the context data transfer between data producers and data consumers. NGSI10 has query, update, subscribe and notify context operations for providing context values. A context broker is necessary for establishing data flow between different resources as well as consumers or providers. Detailed specifications can be found in [54].

4.3.2 Watson IoT Platform

Watson IoT Platform [111] is a pub/sub broker that supports the MQTT protocol [64] for publishing and subscribing to device data. This information is also included in the D1.3 document.

In Watson IoT Platform, devices publish data using events. The device controls the content of the

event and assigns a name for each event that is sent. When an event is received by the Watson IoT Platform from a device, the credentials of the connection on which the event was received are used to determine from which device the event was sent. This architecture prevents a device from impersonating another device.

Connecting Devices to Watson IoT Platform

Watson IoT Platform provides a HTTP API and an MQTT messaging interface. Typically, the HTTP API is used for registering and managing devices, publishing events and retrieving data. The MQTT interface allows devices to publish and subscribe to events.
A device must be registered with an organisation before it can connect to Watson IoT Platform. Registered devices identify themselves to the Watson IoT Platform with a unique device identifier, for example the MAC address, and an authentication token that is accepted for that device only.

MQTT Messaging Interface

This section is not intended to be a comprehensive documentation of the MQTT messaging interface of Watson IoT Platform. Rather it provides a brief overview of it. For further details, readers may refer to the official reference pages [63] .

MQTT is the primary protocol that devices and applications use to communicate with the IBM Watson IoT Platform.

4.3.3 oneM2M

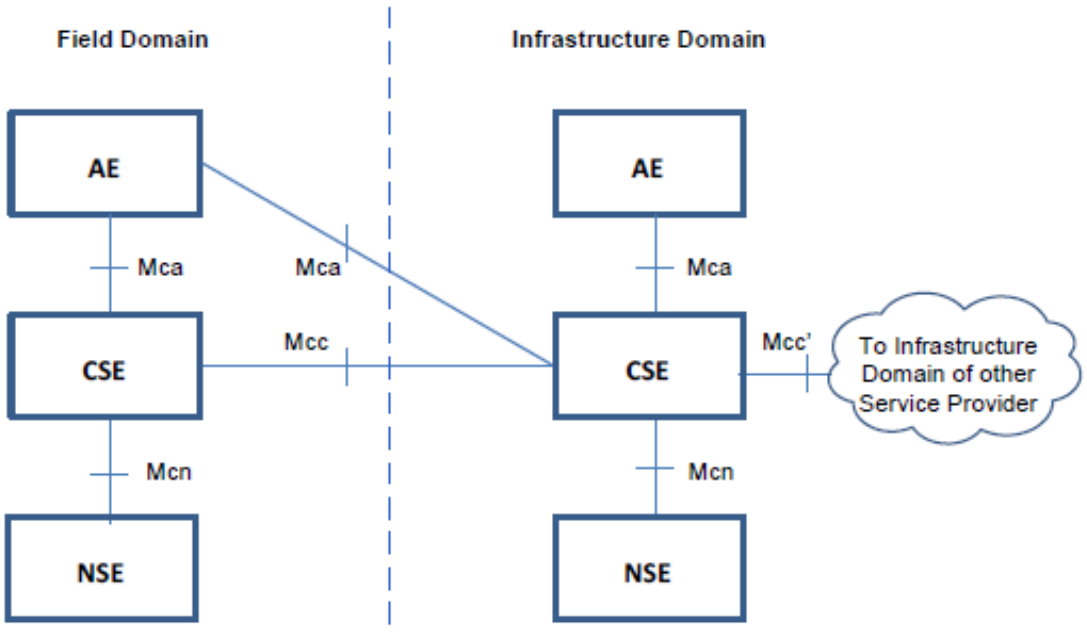


Figure 39: oneM2M functional architecture (from [120]).

The standard to develop technical specifications for Machine-to-Machine and Internet of Things services, is called oneM2M [108]. The oneM2M has a functional architecture which comprises the following functions (from the list in [55]):

- **Application Entity (AE):** Application Entity is an entity in the application layer that implements an M2M application service logic. Each application service logic can be resident in a number of M2M nodes and/or more than once on a single M2M node. Each execution instance of an application service logic is called an "Application Entity" (AE) and is identified with a unique AE-ID (AE-Identifier). Examples of the AEs include an instance of a fleet tracking application, a remote blood sugar monitoring application, a power metering application, or a controlling application.
- **Common Services Entity (CSE):** A Common Services Entity represents an instantiation of a set of "common service functions" of the M2M environments. Such service functions are exposed to other entities through the Mca and Mcc reference points. Reference point Mcn is used for accessing underlying Network Service Entities. Each CSE is identified with a unique CSE-ID (CSE-Identifier). Examples of service functions offered by CSE include: Data Management, Device Management, M2M Service Subscription Management, and Location Services. Such "sub-functions" offered by a CSE may be logically and informatively conceptualized as Common Services Functions (CSFs).
- **Network Services Entity (NSE):** A Network Services Entity provides services from the underlying network to the CSEs. Examples of such services include device management, location services and device triggering. No particular organization of the NSEs is assumed.

oneM2M [108] is defined hierarchically, thus it's not flat architecture, in which we can make a distinction between the node types as shown in Figure 39. Note that the figure is simplified since participating nodes do not contain a NSE (Network Service Entry) which every element must have in order to communicate.

In oneM2M, a reference point consists of one or more interfaces of any kind. The following reference points are supported by the Common Services Entity (CSE) (information included from oneM2M technical architecture document [55], [107]):

Mca Reference Point: Communication flows between an Application Entity (AE) and a Common Services Entity (CSE) cross the Mca reference point. These flows enable the AE to use the services supported by the CSE, and for the CSE to communicate with the AE.
Mcc Reference Point: Communication flows between two Common Services Entities (CSEs) cross the Mcc reference point. These flows enable a CSE to use the services supported by another CSE.
Mcn Reference Point: Communication flows between a Common Services Entity (CSE) and the Network Services Entity (NSE) cross the Mcn reference point. These flows enable a CSE to use the supported services (other than transport and connectivity services) provided by the NSE.
Mcc' Reference Point: Communication flows between two Common Services Entities (CSEs) in Infrastructure Nodes (IN) that are oneM2M compliant and that resides in different M2M SP domains cross the Mcc' reference point. These flows enable a CSE of an IN residing in the Infrastructure Domain of an M2M Service Provider to communicate with a CSE of another IN residing in the Infrastructure Domain of another M2M Service Provider to use its supported services, and vice versa. Mcc' extends the reachability of services offered over the Mcc reference point, or a subset thereof. The trigger for these communication flows may be initiated elsewhere in the oneM2M network.

4.3.4 Vehicle to Vehicle/Infrastructure (V2X) communication interfaces

The below section describes the physical and protocol interfaces of the vehicle to vehicle/infrastructure subsystem.

The Figure 40 below represents the different layers, block diagrams and the communication interfaces, inside a car and between cars, from a conceptual functional point-of-view.

We are re-using the terminology introduced in the specification ETSI EN 302 665 [65] (which provides a reference architectural split of the ITS stack) with the different layers labelled as “Access technology”, “Networking & Transport”, “Facilities” and “Applications.

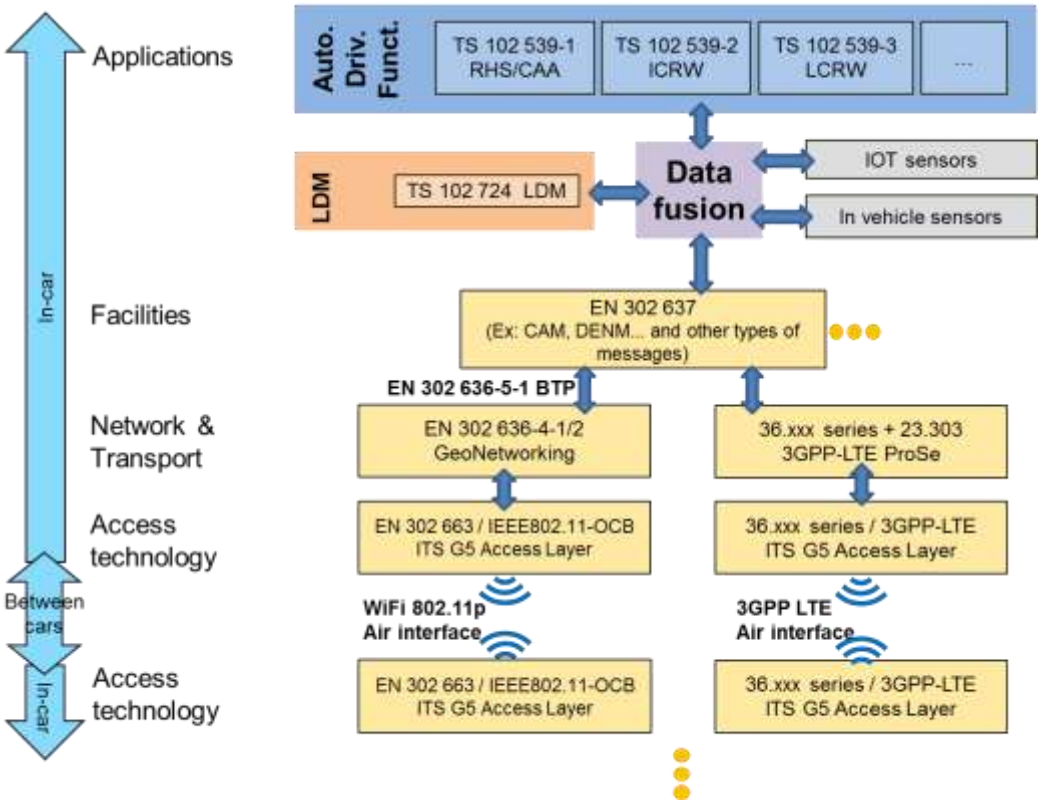


Figure 40 - V2X Communication interfaces block-diagram (conceptual functional architecture)

The “**Access technology**” is the wireless physical connection method that allows vehicles to exchange waveforms between each other (see section 3.2.4.1.2). This layer can be based on IEEE 802.11-OCB [66] or 3GPP LTE 36 series (Rel-14) [67]. The “Access technology” conveys the messages formed at the “Facilities” layer and which dissemination is controlled by “Networking & Transport” layer.

The “**Networking & Transport**” layer controls the dissemination of the messages, over time and geographical range (see section 3.2.4.1.3). The hopping or relaying of important messages to surrounding users aims to provide wider geographical & time range of the message, although at the expense of extra usage of the physical interface.

The “**Facilities**” layer is in principle agnostic to the technology used for the “Access” and “Networking & Transport”, which can be WiFi or LTE based (see section 3.2.4.1.4). The “Facilities” layer specifies the ITS messages formatting, such as the CAM & DEMN messages (EN 302 637 [69], [70]).

The “**Applications**” layer (see section 3.2.4.1.5) provides a set of features which are used for autonomous driving functionality. Amongst others, we can note Road Hazard Signaling (RHS), Co-operative Awareness Application (CAA), Intersection Collision Risk Warning (ICRW), Longitudinal Collision Risk Warning (LCRW).

Figure 41 shows an example of how the block diagrams of Figure 40 can be grouped together in a real-life implementation. This grouping can form a IEEE802.11-OCB stack, a LTE-based stack, and an above layer called “World Model”.

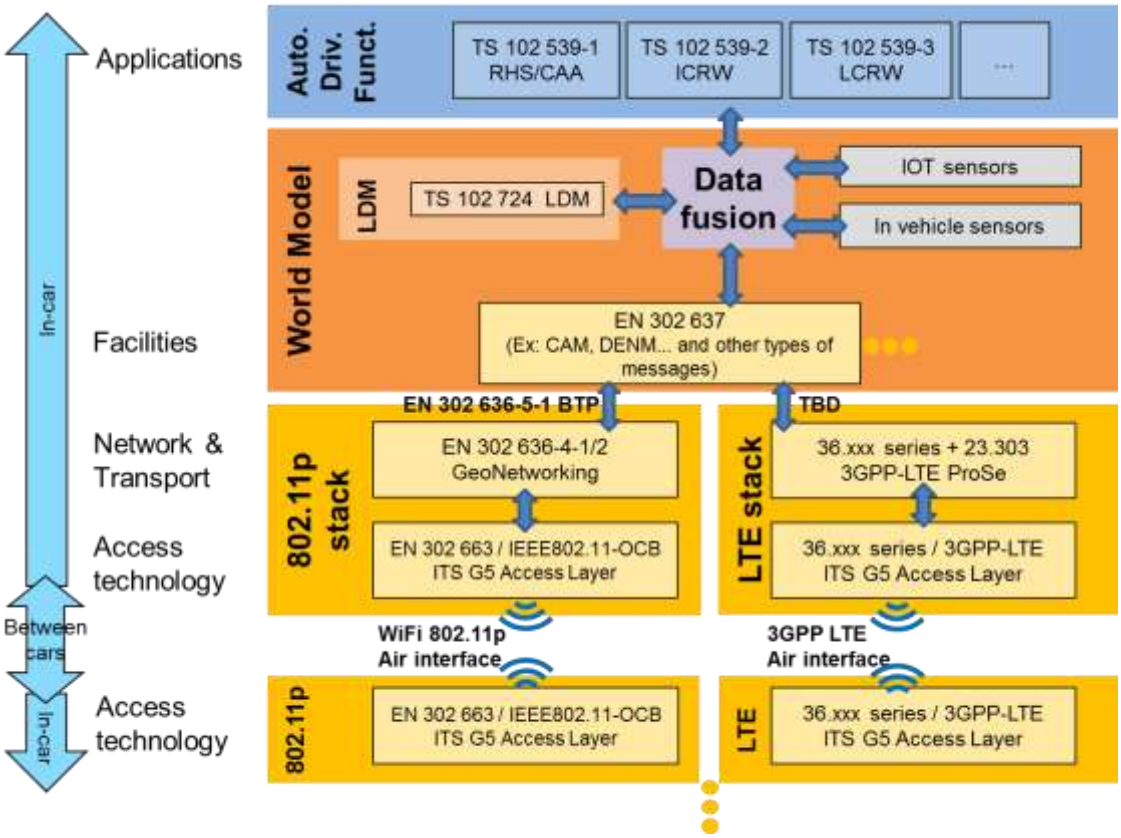


Figure 41 - V2X Communication interfaces block-diagram (mapping example)

In this example mapping, the IEEE802.11-OCB stack and LTE-based stacks have their own track for the “Network & Transport” and “Access technology” layers. They could for instance be running on two different separate devices.

The central “Facilities” layer can be seen as the place to switch or merge the stacks events & messages. Each of the stack is communicating with the “Facilities” layer (for example the 802.11-OCB stack is using EN 302 636-5-1 BTP). This central “Facilities” entity provides one level of abstraction to the “Data Fusion” so that the Data Fusion can be designed agnostically of the Access technologie(s) that are used over the air (it could be IEEE802.11-OCB, LTE, or both).

The central “Facilities”, together with the LDM and Data Fusion can be grouped into the “**World Model**” domain. This “World Model’ functionality may be run on a centralized processor where the most of data processing is carried out.

4.3.5 Communication interfaces internal to the car (in-car application platform)

Internal to the car, communication is required between the blocks and layers depicted in Figure 41. Relating the Interface between the Facilities layer and the Data Fusion block:

- The upper layer of the Communication block are the messages specified in EN 302 637 (such as CAM, DENM – See section 3.2.4.1.4)
- Therefore, it is proposed to follow the CAM & DENM PDU (Packet Data Unit) description of the EN 302 637 for these messages

4.3.6 Communication interfaces external to the car (between two 802.11-OCB systems, either car-to-car, car-to-RSU, car-to-personal devices)

For two (or more) vehicles to communicate, they need to use the same access technology and the same set of features and functionalities. The WiFi IEEE802.11-OCB can be used to serve the transfer of CAM & DEMN messages, which formatting is fully described in ETSI EN 302 637[69][70] (see section 3.2.4).

- Interface between cars (at Physical level)
  - EN 302 663 [71] / IEEE802.11-OCB
- Interface between cars (at Facilities messages level)
  - ETSI EN 302 637
  - SPAT and MAP type of messages from intersections (RSU combined with Traffic Light Controllers)
- Support of non-standard messages for applications using V2X:
  - CACC, Platooning
  - GPS RTK correction messages over ITS-G5

5 Communication requirements identification

5.1 Communication interfaces requirements definition

Task 1.4 is devoted to the identification and analysis of the communications-related requirement relevant for the use cases selected in Task 1.1. For this reason basing on both, the requirements collection format prepared within Task 1.2 [98] and the guidelines available on document "5G Automotive Vision" [99], a framework to collect communication requirements has been worked out. The format has been included in an excel file in order to facilitate the operation effectiveness (see section 7.2, [100]). The xls file consists of 2 different sheets; the first one presents communications KPIs to consider, while the second one allows communication requirements collection by use case/pilot site. This file has been distributed to task members and to pilots site leaders in order to receive their contribution.

In the next two sections a presentation of the identified communication requirements is carried out: Section 5.1.1 presents an overview of them while section 5.1.2 presents Communications KPIs definition and KPIs requirements analysis.

5.1.1 Requirements by use cases

All the communication requirements collected during the survey are listed in a specific xls file (see section 7.2, [100]).

After the requirements identification and collection phase, a harmonization activity has been performed in order to homogenize the requirements definition. At the end of this phase 43 communication requirements have been identified; 38 requirements have been deduced by use cases analysis and main topics (Table 7), while the other ones arose from transversal subjects (V2X and IoT services):

Use Case	Communication requirements (#CR)
Automated Valet Parking	19, 24, 25, 26, 27, 36, 38, 39, 40
Highway Pilot	29, 30
Platooning	30, 31, 32, 33, 34
Urban Driving	18, 20, 21, 22, 23, 41, 42, 43
Car sharing	28, 35
Hazard on the roadway	1, 2, 3, 4, 5, 6, 7, 8, 44
Traffic Services	8, 12, 41, 42, 43
Traffic Light	11, 17, 18, 42
Connected bicycle	9
General requirements	10, 13, 14, 15, 16

Table 7: Communications requirements by use cases

For each requirement the priority (MUST, SHOULD, MAY) and the performance levels required for the 7 KPIs have been evaluated.

In the following section are presented the communication requirements grouped by use cases/main topics with the Pilot site priority. The complete requirements description could be found into Annex 7.3.

5.1.1.1 Automated Valet Parking

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR19	Communication between vehicle and cloud/camera management centre	NA	NA	NA	MUST	MAY
CR24	Communication between Vehicle and AVP application	NA	NA	NA	NA	MUST
CR25	Communication between AVP application and cloud	NA	NA	NA	NA	MUST
CR26	Communication between Drone and cloud	NA	NA	NA	NA	MUST
CR27	Communication static camera and cloud	NA	NA	NA	NA	MUST
CR36	Communication between the application hosted on the user device and the cloud-based parking control system	MUST	NA	NA	NA	NA
CR38	The vehicle must receive exchange information (e.g. a detailed layout of the parking place, the location of dynamic objects, pedestrian location, vehicle position) with the parking control system	MUST	NA	NA	NA	NA
CR39	The vehicle must be able to provide its identification to be authorized at the parking place	MUST	NA	NA	NA	NA
CR40	Communication between parking infrastructure and cloud	MUST	NA	NA	NA	NA

5.1.1.2 Highway Pilot

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR29	V2X Communication between vehicles and infrastructure	NA	NA	NA	NA	MUST
CR30	The vehicle may send and receive information to/from the cloud	NA	NA	NA	NA	MAY

5.1.1.3 Platooning

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR30	The vehicle may send and receive information to/from the cloud	NA	NA	NA	NA	MAY
CR31	V2X Communication between Vehicle and RSU	NA	NA	NA	NA	MUST
CR32	Communication between vehicles and cloud	NA	NA	NA	NA	MUST
CR33	V2V Communication between Vehicles	NA	NA	NA	NA	MUST
CR34	Cellular Communication between Vehicles	NA	NA	NA	NA	MUST

5.1.1.4 Urban Driving

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR18	Communication between vehicle and cloud/traffic light control system	NA	NA	NA	MUST	NA
CR20	The vehicle must receive information about VRU presence and localization by a smartphone application	NA	NA	NA	NA	MUST
CR21	Communication between lecture schedule webserver of TU/e and AD vehicle	NA	NA	NA	NA	MUST
CR22	The vehicle must receive wheather information by a cloud-based web server	NA	NA	NA	NA	MUST
CR23	The vehicle and the service center must communicate each other information for managing relocation requests of vehicles	NA	NA	NA	NA	MUST
CR41	Communication between vehicle and cloud/traffic control system	MUST	NA	NA	NA	NA
CR42	Communication between infrastructure (traffic lights) and cloud/traffic control system	MUST	NA	NA	NA	NA
CR43	Communication between traffic alert system and cloud/traffic control system	MUST	NA	NA	NA	NA

5.1.1.5 Car sharing service

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR28	Communication between the application hosted on the user device and the service center cloud	NA	NA	NA	NA	MUST
CR35	Communication between vehicle and Service center cloud	NA	NA	NA	NA	MUST

5.1.1.6 Hazard on the roadway

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR1	The vehicle must receive the geocasted notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from RSU	MUST	MUST	NA	NA	MUST
CR2	The WSN on the road must notify the presence of puddles on the road whenever they are detected	NA	MUST	NA	NA	NA
CR3	The traffic control system must receive geolocalized notifications of hazard events from RSU (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.)	NA	MUST	NA	NA	NA
CR4	Geolocalized notifications of hazard events (e.g. potholes, roadway works, puddles, etc.) from RSU may be stored by the data management service of the IoT platform	NA	MAY	NA	NA	NA
CR5	The detection event of pedestrians on the roadway must be notified to the RSU from the camera	NA	MUST	NA	NA	NA
CR6	The number of detected pedestrians on the roadway detected by the camera may be stored by the data management service of the IoT platform	NA	MAY	NA	NA	NA
CR7	Every time the vehicle detects an hazard, it must be geocasted to other vehicles	NA	MUST	NA	NA	NA
CR8	The traffic control system must receive geolocalized notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from vehicles	NA	MUST	NA	NA	NA

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR44	The In-vehicle PF can be able to receive information related with VRU presence, generated by IoT infrastructure PF (alternative to CAM/DENM from ITS-G5 channel, for long range).	MUST	MUST	NA	NA	NA

5.1.1.7 Traffic services

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR8	The traffic control system must receive geolocalized notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from vehicles	NA	MUST	NA	NA	NA
CR12	The traffic control system must receive information about traffic conditions	MUST	MUST	NA	NA	NA
CR41	Communication between vehicle and cloud/traffic control system	MUST	NA	NA	NA	NA
CR42	Communication between infrastructure (traffic lights) and cloud/traffic control system	MUST	NA	NA	NA	NA
CR43	Communication between traffic alert system and cloud/traffic control system	MUST	NA	NA	NA	NA

5.1.1.8 Traffic Light

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR11	Traffic light must continuously geocast its light phase and the topology of the crossroad to vehicles on the road	MUST	MUST	NA	NA	MUST
CR17	The vehicle should be able to receive Signal Phase information, coming from IoT infrastructure platform (alternative to SPAT/MAP from ITS-G5 channel, for long range)	SHOULD	SHOULD	NA	SHOULD	MAY

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR18	Communication between vehicle and cloud/traffic light control system	NA	NA	NA	MUST	NA
CR42	Communication between infrastructure (traffic lights) and cloud/traffic control system	MUST	NA	NA	NA	NA

5.1.1.9 Connected bicycle

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR9	Bicycles must geocast their position, speed, orientation to other vehicles on the road	NA	MUST	NA	NA	NA

5.1.1.10 General requirements

ID	Requirement description	Spain Priority Must/Should/May	Italy Priority Must/Should/May	France Priority Must/Should/May	Finland Priority Must/Should/May	Nederland Priority Must/Should/May
CR10	Vehicles must geocast their position, speed, orientation to other vehicles on the road	MUST	MUST	NA	NA	MAY
CR13	Vehicles must be able to receive CAM/DENM contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST
CR14	Vehicles must be able to receive SPAT/MAP contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST
CR15	Vehicle must be able to receive data from communication system, related with contents received from IoT external services.	MUST	MUST	MUST	MUST	MUST
CR16	Vehicles must be enabled to provide /communicate elaborated data to IoT external services, through communication system.	MUST	MUST	MUST	MUST	MUST

5.1.2 Communications KPIs

Regarding communications KPIs the definitions and parameters listed in Table 8 have been considered and evaluated. For each KPI a quantitative evaluation mechanism based on performances ranges has been worked out in order to allow performance measurements during

Task 2.5 “Pilot Readiness verification”.

KPI Name	KPI Description	Possible Values
End-to-end latency (L)	Maximum tolerable elapsed time from the instant a data packet is generated at the source application to the instant it is received by the destination application. If direct mode is used, this is essentially the maximum tolerable air interface latency. If infrastructure mode is used, this includes the time needed for uplink, any necessary routing in the infrastructure, and downlink.	High: L > 100 ms Medium: 10ms < L < 100ms Low: L < 10ms
Reliability (R)	Maximum tolerable packet loss rate at the application layer (i.e., after HARQ, ARQ, etc.). A packet is considered lost if it is not received by the destination application within the maximum tolerable end-to-end latency for that application. For example, 10^{-5} means the application tolerates at most 1 in 100,000 packets not being successfully received within the maximum tolerable latency. This is sometimes expressed as a percentage (e.g., 99.999%) elsewhere.	High: R > 10^{-4} Med.: 10^{-4} < R <10^{-6} Low: R < 10^{-6}
Bandwidth (B)	Minimum required bit rate for the application to function correctly.	High: B > 100 Mb/s Medium: 100 Mb/s > B > 1 Mb/s Low: B < 1 Mb/s
Communication range (CR)	Maximum distance between source and destination(s) of a radio transmission within which the application should achieve the specified reliability.	Long Range Communication V2X communication (URBAN: 50-100 m, SUBURBAN: 100-200 m, HIGHWAY: 200-1000 m)
Node mobility (N)	Maximum relative speed under which the specified reliability should be achieved	Pedestrian: 0-10 km/h Vehicular (URBAN: 0-70 km/h, SUBURBAN: 0-100 km/h, HIGHWAY: 0-160 km/h)
Network density (D)	Maximum number of vehicles per unit area under which the specified reliability should be achieved.	URBAN: 1000-3000 v/km^2 SUBURBAN: 500-1000 v/km^2 HIGHWAY: 100-500 v/km^2
Security (S)	Specific security features required by the application. These include user authentication, authenticity of data, integrity of data, confidentiality, and user privacy.	Specify Requirements

Table 8: Communications KPI based on [99]

In the following section the KPIs analysis for the collected requirements is presented.

5.1.2.1 End-to-End Latency (L)

Table 9 and Figure 42 present the distribution of the End-to-End latency requirement.

The 13 cases that require *Low/Low-medium latency* are related mainly to notification to vehicles of hazard events on the road or to V2V communications.

The 22 cases that require *High /Medium-High latency* are related to the notification of hazard events (e.g. potholes, roadway works) to control systems or in general to communication with the cloud service centers .

End-to-End Latency (L)	
High	20
Medium / High	2
Medium	8
Low / Medium	2
Low	11

Table 9: End-to-End Latency requirements distribution

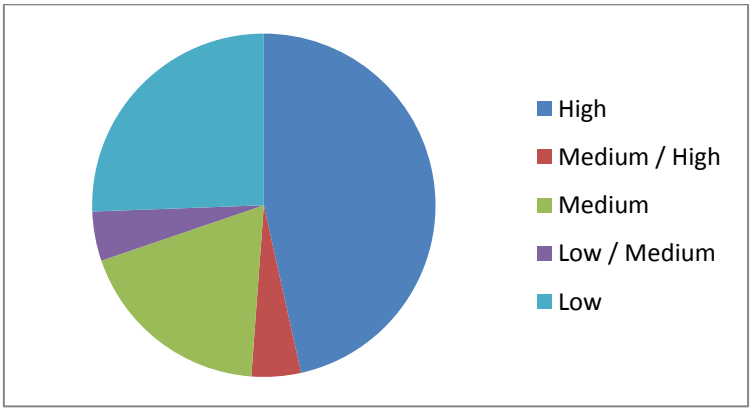


Figure 42 - End-to-End Latency requirements distribution

5.1.2.2 Reliability (R)

Table 10 and Figure 43 present the distribution of the Reliability requirement.

The majority of the communication requirements require an High (27) or Medium (13) level of Reliability, only few case (3) have less stringent requirements (e.g. communication between static camera and cloud or between drone and cloud).

Reliability (R)	
High	27
Medium	13
Low	3

Table 10: Reliability requirements distribution

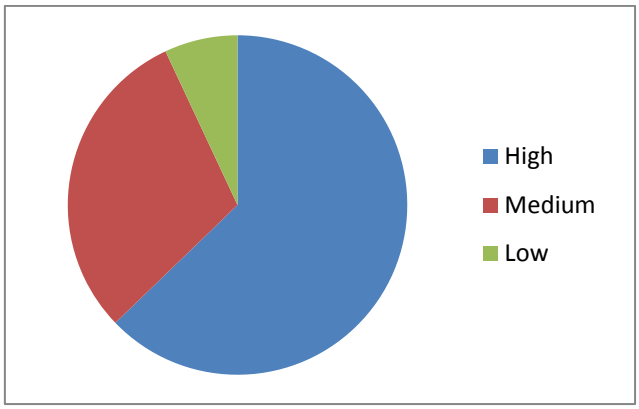


Figure 43 - Reliability requirements distribution

5.1.2.3 Bandwidth (B)

Table 11 and Figure 43 present the distribution of the Bandwidth requirement.
The majority of the communication requirements require a Low (31) or Medium (9) Bandwidth, only few case (3) require high bandwidth requirements (e.g. communication between static camera and cloud or between drone and cloud). The requirements that need High level of bandwidth are the ones that require low level of reliability.

Bandwidth (B)	
Medium / High	3
Medium	9
Low	31

Table 11: Bandwidth requirements distribution

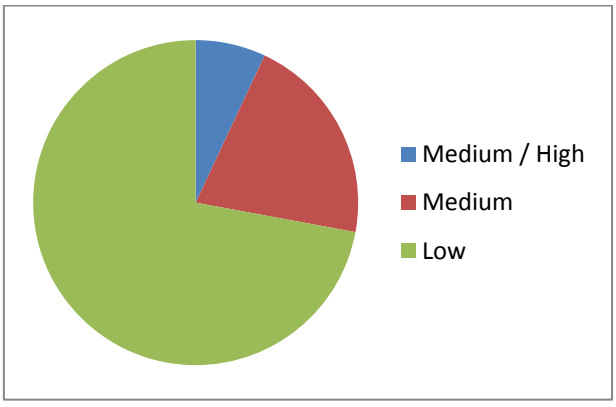


Figure 44 - Bandwidth requirements distribution

5.1.2.4 Communication range (CR)
Table 12 and Figure 45 present the distribution of the Communication range requirement.
It should be noted that many communication requirements need different Communication ranges, so the total of the distribution below is greater than the total of number of requirements.
Long range communication requirements refer to communication with cloud platforms.
Concerning V2X communication only two requirements (req. 7 on detection of hazard and req. 33 on

platooning V2V communication) foresee communication ranges in all the ranges: URBAN, SUBURBAN and HIGHWAY the other V2X communication requirements are distributed in the three ranges: URBAN (5) , SUBURBAN (3) and HIGHWAY (5).

Communication range (CR)	
Long Range	25
Short Range	6
V2X URBAN (50-100 m)	7
V2X SUBURBAN (100-200 m)	5
V2X HIGHWAY (200-1000 m)	7

Table 12: Communication range requirements distribution

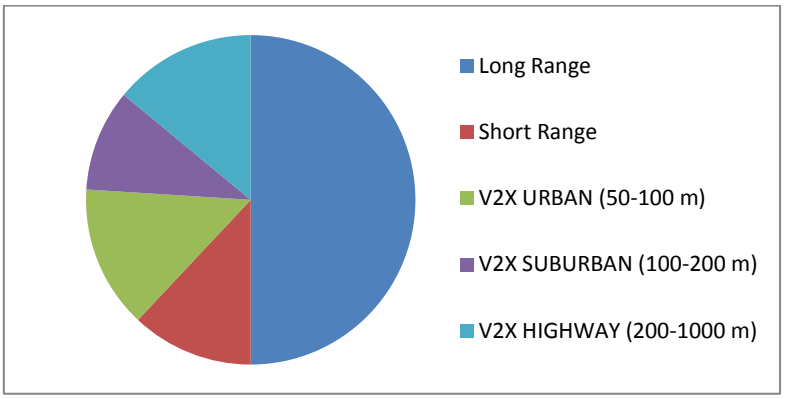


Figure 45 - Communication range requirements distribution

5.1.2.5 Node mobility (N)

Table 13 and Figure 45 present the distribution of the Node mobility requirement.

Unless the six requirements where mobility is not foreseen, there are six requirements with low speed requirement (Pedestrian) in which are involved the communication with a user device or a communication with a vehicle into a parking area; the other requirements foresee more high speed (Vehicular) as refer to communication from / vehicle in the different areas: Urban, Suburban and Highway.

It should be noticed that many communication requirements apply to multiple relative speed ranges so the total of the distribution below is greater than the total of number of requirements, for example there are 11 communication requirements that foresee a node mobility Vehicular for all the URBAN, SUBURBAN and HIGHWAY speed.

Node mobility (N)	
Pedestrian	6
Vehicular URBAN	22
Vehicular SUBURBAN	16
Vehicular HIGHWAY	15
No mobility	6

Table 13: Node mobility requirements distribution

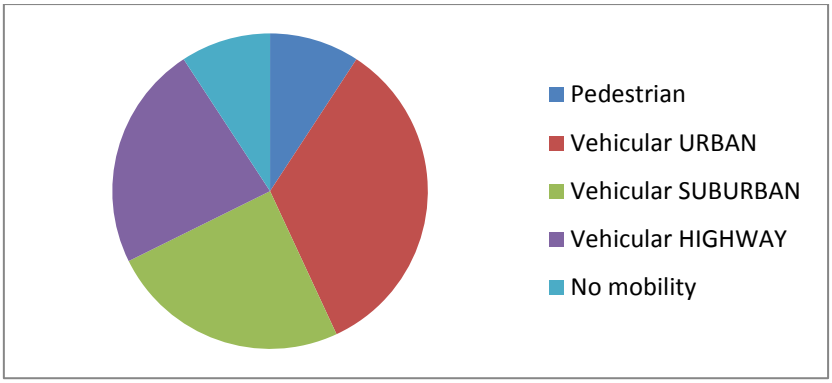


Figure 46 - Node mobility requirements distribution

5.1.2.6 Network density (D)

Table 14, Table 13 and Figure 47 present the distribution of the Network density requirement. There are six requirements for which the parameter is not meaningful as mobility is not foreseen. The majority (31) of communication requirements can require High density of vehicles per unit area (URBAN) while the other can require more low density (SUBURBAN, HIGHWAY).

It should be noted that communication requirements can be used in multiple context, so for example there are ten communication requirements that foresee the three density: URBAN, SUBURBAN, HIGHWAY. Also in this case the total of the distribution below is greater than the total of number of requirements.

Network density (D)	
URBAN	31
SUBURBAN	13
HIGHWAY	15
NA	6

Table 14: Network density requirements distribution

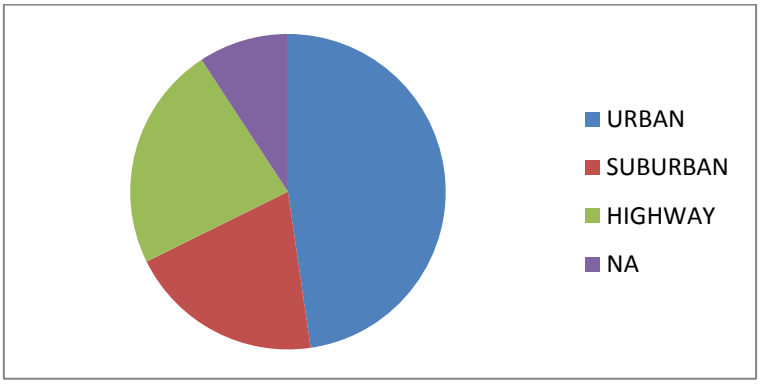


Figure 47 - Network density requirements distribution

5.1.2.7 Security (S)

Table 15, Table 13 and Figure 48 present the distribution of the Security requirement.
All communication requirements foresee multiple security aspects to be covered. Almost all requirements (42 of 43) require data integrity and most of them (35) require authentication (vehicular, user, application). Confidentiality and Privacy are the other two aspects that are foresee for a large number of communication requirements (respectively 31 and 27 cases).

Security (S)	
Authentication	35
Integrity of data	42
Authenticity of data	14
Confidentiality	31
Privacy	27

Table 15: Security requirements distribution

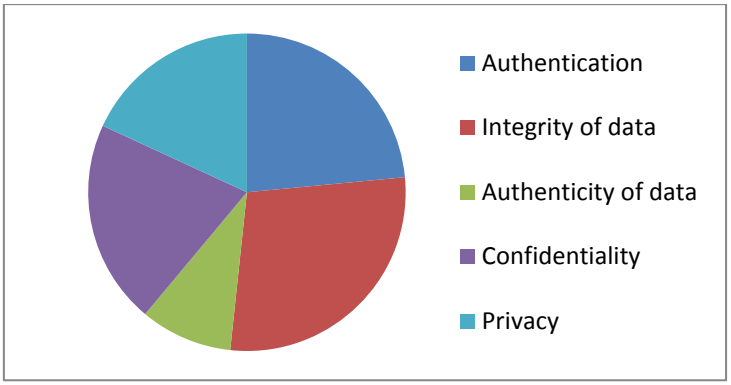


Figure 48 - Security requirements distribution

5.2 Mapping with existing communication standards and gap analysis

The requirements were analysed in order to identify the presence of gaps. For this reason these 3 topics were highlighted (see Table 20 in section 7.3): the standard covering the corresponding requirement, the presence or not of a gap between the standardized condition and the requirement condition, and a short note/description of possible gaps. Here below a summary of all requirements that contained gaps, with a short subset of the requirements describing them. The gaps identified are mainly related with communication/connectivity knowledge area (KA), given the absence of existing standard protocols covering the requirement conditions (see Table 16).

ID	**CR12**
Use case	Traffic conditions
Requirement description	The traffic control system must receive information about traffic conditions
Comm. range (CR)	V2X URBAN
Node mobility (N)	Vehicular SUBURBAN Vehicular HIGHWAY
Network density (D)	SUBURBAN HIGHWAY
Security (S)	authentication, integrity of data, confidentiality, privacy
standards/protocols covering CR	LTE
Gap	yes
notes/Gap description	GAP: requires to define the protocol that will be used to communicate to exchange traffic information. It is not defined who sends the traffic information to TCC (if vehicles directly or aggregated information through RSUs) KA: Communications and Interoperability

ID	**CR21**
Use case	Urban Driving (relocation TU/e)
Requirement description	Communication between lecture schedule webserver of TU/e and AD vehicle
Comm. range (CR)	SUBURBAN
Node mobility (N)	Vehicular URBAN
Network density (D)	URBAN
Security (S)	integrity of data, confidentiality, authenticity of data
standards/protocols covering CR	HTTP
Gap	yes

notes/Gap description	GAP: There seems not to be a standard to cover this communication over HTTP, application level must implement the protocol. KA: Communication/connectivity

ID	**CR24**
Use case	Automated Valet Parking
Requirement description	Communication between Vehicle and AVP application
Comm. range (CR)	Short range and long range
Node mobility (N)	URBAN
Network density (D)	URBAN
Security (S)	integrity of data, authenticity of data, confidentiality, privacy
standards/protocols covering CR	LTE
Gap	yes
notes/Gap description	GAP: At the time of the writing of this document, no standard protocol was specified for this communication and no access technology, since it specifies long and short range. KA: communication/connectivity

ID	**CR26**
Use case	Automated Valet Parking
Requirement description	Communication between Drone and cloud
Comm. range (CR)	Short range and long range
Node mobility (N)	URBAN
Network density (D)	URBAN
Security (S)	integrity of data, authenticity of data
standards/protocols covering CR	LTE,TCP/IP
Gap	yes
notes/Gap description	GAP: not specified which higher layer protocol will be used, standard application-layer protocols does not seem to be available. KA: Communications/connectivity

ID	CR27
Use case	Automated Valet Parking
Requirement description	Communication static camera and cloud
Comm. range (CR)	Short range and long range
Node mobility (N)	URBAN
Network density (D)	URBAN
Security (S)	integrity of data, authenticity of data
standards/protocols covering CR	TCP/IP
Gap	yes
notes/Gap description	GAP: not specified which standard higher-layer protocols will be used. KA: Communications/Connectivity

ID	CR35
Use case	Car sharing service
Requirement description	Communication between vehicle and Service center cloud
Comm. range (CR)	Long Range
Node mobility (N)	Vehicular SUBURBAN
Network density (D)	SUBURBAN
Security (S)	user authentication, integrity of data, confidentiality, privacy
standards/protocols covering CR	LTE
Gap	yes
notes/Gap description	GAP: standard application protocols are undefined for this communication, the LTE was assumed due to the range of communication. KA: Communication/connectivity

Table 16: Gaps identified in communication requirements

6 Conclusion

This document, D1.7, identifies the requirements concerning communication aspects and in particular the capabilities necessary for Internet of Things (IoT) and Automated Driving (AD) use cases. It must be delivered in M09 and it has been produced basing on: T1.4 activities, use case definitions by T1.1, IoT Architecture and Specification by T1.2 as well as pilot sites infrastructure information.

The document starts from a general overview of the AUTOPILOT scenario summarising: reference use cases, a description of the communication infrastructure currently present in the various AUTOPILOT sites and a general reference architecture scheme applicable in principle to all the pilots.
An overview about the various communications technologies that can be used within the project has been performed in order to identify their applicability area and to provide the main features/functionalities description and the indicators evaluating key performances.

Finally a preliminary identification and collection of communication requirements has been performed amongst all the pilot sites focusing 7 different KPIs: End-to-end latency (L), Reliability (R), Bandwidth (B), Communication range (CR), Node mobility (N), Network density (D) and Security (S). For each KPI a quantitative evaluation mechanism based on performances ranges has been worked out in order to allow performance measurements during Task 2.5 “Pilot Readiness verification”.
An harmonization activity has been performed in order to homogenize the requirements definition. At the end of this phase 44 communication requirements have been described and linked to the several use cases. For each requirement the priority (MUST, SHOULD, MAY) and the performance levels required for the 7 KPIs have been evaluated.

In particular, this document focused on:

- General Autopilot Infrastructure Architecture.
- Collection of communication requirements and capabilities associated with the AUTOPILOT use cases supported by AUTOPILOT pilot sites focusing on seven different KPIs: End-to-end latency (L), Reliability (R), Bandwidth (B), Communication range (CR), Node mobility (N), Network density (D) and Security (S).
- Identification of gaps in standardization associated with the fulfilment of the communication requirements.

The work related the specification of requirements concerning communication will be used within AUTOPILOT Task 2.4 “Development and integration of IoT devices” and Task 2.5 “Pilot Readiness verification”; it will be finalized in D1.8 “Final specification of Communication System for IoT-enhanced AD” when a more detailed requirements analysis will be carried out in order to compare the preliminary set of information presented in this deliverables with the ones arising from AD use cases technical implementation.

7 Annexes

7.1 Annex 1 – Standardization of 5G

All the information presented in this section are based on the work carried out within 3GPP [4] and ITU-R [5].

7.1.1 The main standardization bodies

Behind the success of a technology there is not a single standardization body, but a number of entities strictly collaborating among them. If we look to a success story of the recent past, LTE, we can see that there are a number of players contributing to the final availability of a simple smartphone.

A first aspect that is required to ensure the success of a technology is the spectrum availability. Spectrum is the very scarce resource which is required to provide wireless communications. Without spectrum, there is no wireless. And spectrum fragmentation (i.e. different frequency bands allocated in different countries or continents) is also a major hindering factor when developing products, since multiple radio frequency (RF) components are required to allow a smartphone to operate both in Europe and in USA. The main entities, which identify the spectrum needs for mobile communications and the rules for its use, are: ITU-R (during the World Radiocommunication Conferences, WRCs [11]) and Regional bodies such as CEPT in Europe [13], APT [14] in Asia and Citel [15] for the Americas. Note that the ultimate owner of the spectrum is however the national regulator, and so it will be e.g. FCC in the USA (and corresponding entities elsewhere) that will allocate and license the spectrum.
The spectrum alone is however not sufficient to develop a successful system. We need common requirements and goals to be achieved by the system and then we need to develop the components of the technology. 3GPP was the main standardization body delivering technical specifications of LTE, but the work was built upon collaboration with a number of other standards organizations in order to reuse as far as possible best-in-class standardized technologies like, e.g. IETF [16] for the IP protocol suite developed for the Internet, IEEE [17] for interworking with WiFi, OMA [18] for device management, ETSI [19] for the specifications of the smart card which hosts USIM applications, and so on.

A device before being commercialized needs to be tested in order to be sure it works as expected. Therefore 3GPP specifies testing procedures which allow certification bodies such as GCF [20] to provide the rules for certification of conformity.

GSMA [21] finally provides the business rules to ensure, for example, the roaming and interconnection procedures, fraud management and security best practices.

In case of 5G we can expect also new standardization bodies to enter the ecosystem, as new technologies (such as virtualization and software-define networking) will enter the landscape. Also new stakeholders will enter the 5G ecosystem as new requirements for the verticals (such as car communications, public safety, and smart cities) need to be developed by the relevant industry associations.

7.1.2 5G standardization process

Figure 49 provides an overview of the standardization process for 5G. The process can be subdivided in three phases:

- pre-standard phase, focused on industry vision building
- Technical specifications

- Policy and profiling

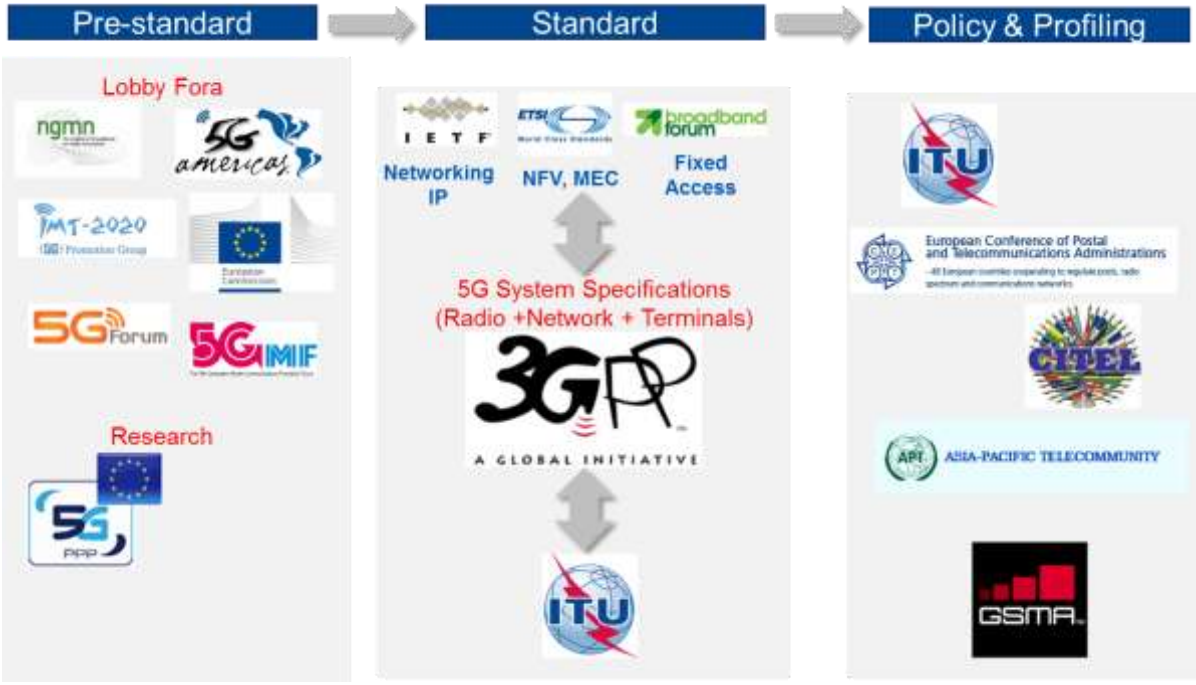


Figure 49 - 5G standardization landscape

The setting of requirements is usually elaborated in the pre-standardization phase, often by means of White Papers providing the vision of the industry and associations. Several White Papers have been published by many organizations, e.g. 5G Americas [22], European Union [23], 5G Forum [24], 5GMF [25], NGMN [26] and by many vendors as well. In Europe the research program under the 5G Infrastructure Association [27] umbrella also set the basis for the vision towards 5G.

In particular, the NGMN White Paper elaborates on the new business opportunities brought by 5G, by identifying new industrial vertical segments interested in exploiting the new technology. As already explained above, "vertical" is a generic name to indicate industries committed to deliver specific applications to the users, which typically falls out of the traditional Telco business. A non-exhaustive list of such verticals comprises automotive (connected cars and self-driving cars), public safety (mission critical services to police, fire brigades), e-Health (remote diagnosis and treatments, remote surgery), smart cities (street lighting optimal usage, waste management, smart parking, etc.), railway companies (communication between trains and infrastructure) and many others.
Taking into account 5G use cases analyses from the cited above organizations, it is generally recognized that they can be categorized in three main classes (see Figure 50):

- Extreme Mobile Broadband (eMBB) - encompassing all the services deriving from the evolution of traditional Telco Services towards an enhanced user experience (e.g. 3D video, augmented reality, 50Mbps everywhere,…);
- Massive Machine Type Communications (mMTC) – encompassing all the communications established between billions of devices and a cloud, which will create the new Internet of Everything (e.g. ultra low power, low complexity sensors like wearables, utility meters…);
- Ultra Reliable and Low Latency Communications (URLLC) – encompassing the capabilities to communicate and manage the status of remote objects (e.g. robots, actuators) in a very reliable way and with very low latency (e.g. for remote surgery, remotely controlled vehicles, drone delivery, robot control in factory automation, …). This new communication paradigm which enables not only inter-networking among objects but also remote control over such

objects, as if they were physically located nearby the controller, is often referred to as "Tactile Internet".

These three use cases are often represented at the extreme corners of a triangle which should encompass all the different 5G services, some of them even yet unknown today.

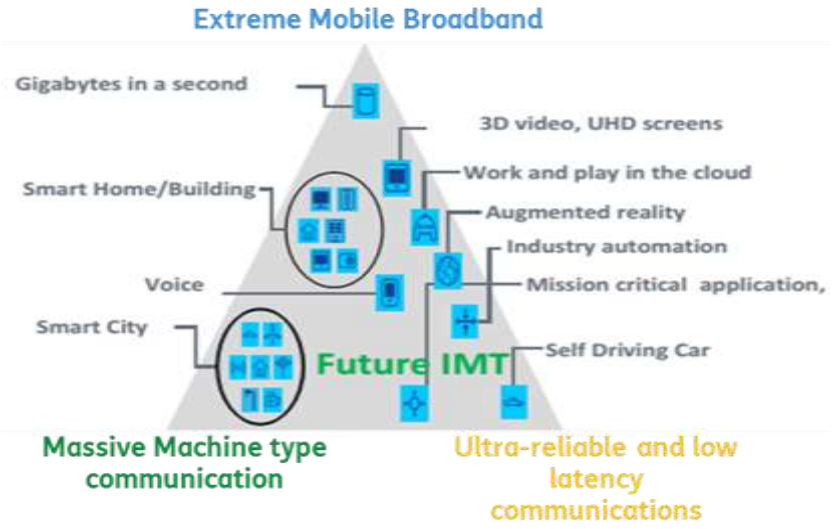


Figure 50 - 5G use cases based on [28]

Each use case is characterized by Key Performance Indicators (KPIs) representing the target behavior the system must exhibit to satisfy the use cases. As it is shown in Figure 51, each main category gives value to distinct extreme KPI values. In the case of mMTC, connection density will be the critic factor to achieve a scalable network as throughput is foreseen to be quite limited for such services. On the contrary, eMBB is expected to adhere to challenging KPIs in areas including at least user experienced data rate and mobility. Finally, URLLC applications will need challenging KPIs in the latency and mobility dimensions, more than in other ones.

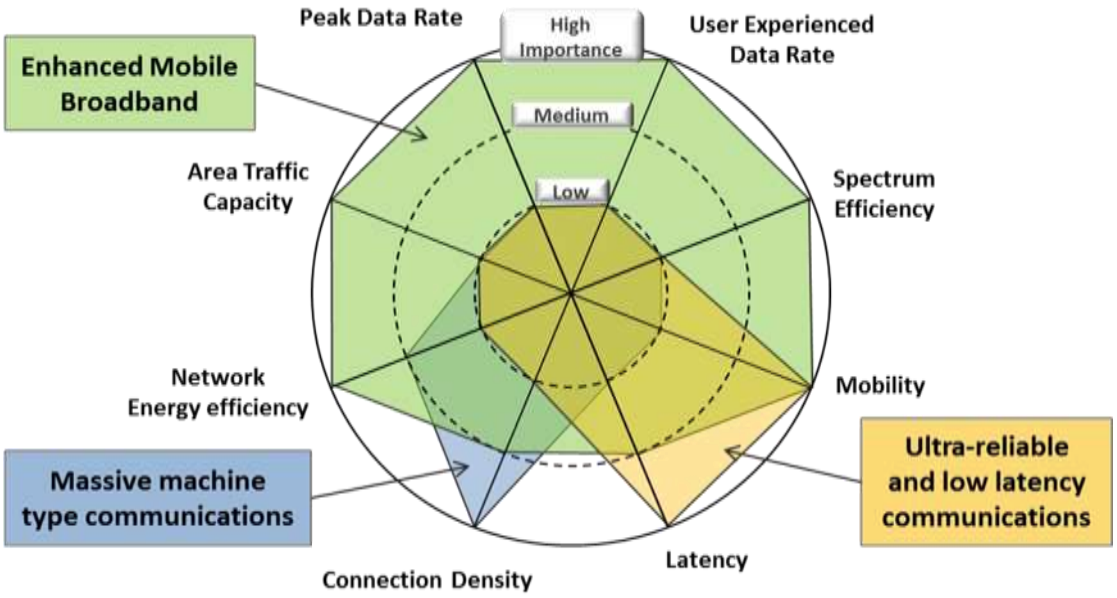


Figure 51 - KPIs for 5G use cases based on [28]

Finally most White Papers address the spectrum and Intellectual Property Rights (IPRs) aspects, to

ensure a complete ecosystem is made available to the new system. Spectrum is the fuel to radio communications, and it must be allocated in a suitable way with sufficient resources to satisfy the capacity needs. A clear policy for IPRs is on the other hand a must to ensure that nobody is discriminated and new companies are attracted by the 5G ecosystem, contributing to innovation with their R&D efforts and with their products.

The following phase, as depicted in Figure 49, is the definition of technical standards. This is not a job for a single organization, as illustrated above, but most likely the result of the collaboration between different SDOs (Standard Development Organizations), each providing a subset of the full system. The expectation is that ITU-R will define the requirements that the new IMT-2020 radio family will have to meet and 3GPP will be the SDO playing the master role in the definition of the whole 5G system and radio aspects, complying with ITU-R requirements. Similarly to the LTE story case, some features need to be developed by other entities, such as IETF (e.g. for IP protocols), ETSI (e.g. for NFV and management and orchestration solutions, Smart Card Platform), BBF (e.g. for integration with fixed access), IEEE (for WiFi evolution), ITU-T (e.g. for transport capabilities). The next Section will focus on the work of ITU-R and 3GPP to provide an insight on what are their plans and milestones.

The final leg of the standardization process is represented by policy and profiling activities. Some examples of these activities are the identification of the spectrum to be used for 5G applications and the definition of the rules on how to use such spectrum. This activity is mainly carried out by National Regulators and ITU-R (in the World Radiocommunication Conferences, WRC). In particular, WRCs try to harmonize the spectrum worldwide, therefore minimizing the market fragmentation. Once 3GPP 5G system specifications will be finalized, other bodies like the GSMA are expected to define on top of those the minimum set of features (profiles) to increase interoperability among UEs and networks (e.g. like it was for the IMS-based VoLTE, Voice over LTE), and to define proper business references to Operators and international carriers for the cooperative delivery of 5G services to their subscribers (e.g. international roaming models, inter-operator accounting, interconnection models, etc.).

7.1.3 ITU-R

As done for the previous generations of mobile systems, ITU-R is defining the process for the definition of IMT-2020. The key group is Working Party 5D “IMT Systems” and the final result will be a set of Recommendations containing the technical specifications of IMT-2020 (e.g. technical characteristics, out of band emissions, etc.). The process is not different from the one used for the definition of IMT-Advanced, which led to the creation of Recommendations M.2012 (Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced) [29]), M.2070 (Generic unwanted emission characteristics of base stations using the terrestrial radio interfaces of IMT-Advanced [30]) and M.2071 (Generic unwanted emission characteristics of mobile stations using the terrestrial radio interfaces of IMT-Advanced [31]).

The overall process (see Figure 52) can be subdivided in several phases: a preparation phase, aimed to define the vision of IMT beyond 2020 and therefore start the discussion on the identification of suitable spectrum during WRC 2015; the definition of Key Performance Indicators and evaluation criteria (in 2016-2017); and finally a call for proposals, their evaluation and decision on which radio access technologies can be labelled as IMT-2020. Another important milestone will be WRC 2019 which plans to identify spectrum for IMT applications beyond 6 GHz.

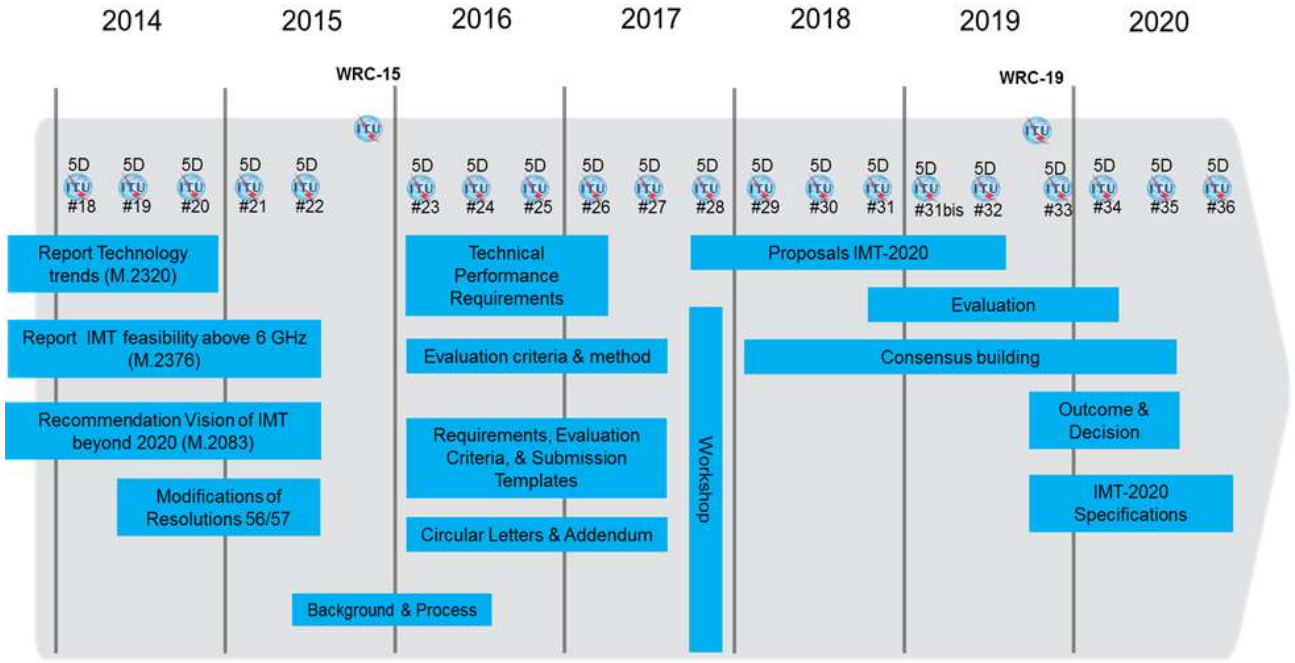


Figure 52 – Detailed Timeline and Process for IMT-2020 in ITU-R (from [32])

The main outcome of the first phase is Recommendation M.2083 (IMT Vision – "Framework and overall objectives of the future development of IMT for 2020 and beyond" [28]) which poses the basis for the definition of what should be expected in terms of new services by IMT-2020. The document identifies the three usage scenarios (eMBB, mMTC, URLLC), similarly to those identified by NGMN, and the capabilities of IMT-2020.

The second phase started with the publication of the Circular Letter 5/LCCE/59 [33] which invites the submission of Radio Interface Technologies (RIT) or Set of Radio Interface Technologies (SRIT) to be recognized as IMT-2020. The Circular Letter addresses only the terrestrial component of IMT-2020 (in scope of WP5D), while the satellite component is in the scope of other Working Groups. In particular, a RIT is a single technology which satisfies the performance criteria, while a SRIT may be composed by different RITs, each addressing different performance criteria (e.g. a radio interface optimized for machine type communications and a solution optimized for mobile broadband, interworking with each other). The Radio Interfaces are developed outside ITU and should be submitted to ITU-R according to a submission template to demonstrate that the proposal is able to fulfil the minimum technical performance requirements and evaluation criteria. The submission template must contain a self-evaluation and may be integrated by any relevant information the proponent may consider useful to better evaluate the proposal. Finally the proponents must indicate their compliance with the ITU policy on intellectual property rights [34].

After the submission, candidate RITs or SRITs will be assessed by organizations registered as evaluators in the IMT-2020 web page [35]. An independent evaluation may be done by ITU-R members, standards organizations and other organizations, such as universities and research projects. The first evaluator to register was the 5G Infrastructure Association [27]. The evaluation report, based on agreed methodologies in ITU-R WP5D will be made available in the same web page [35].

Based on the different evaluations, WP5D will assess if the proposal(s) meet the minimum technical performance requirements and evaluation criteria of the IMT-2020. Based on the evaluation results, modifications to the proposals may be required, and in case of multiple candidates a phase of

consensus building will start to harmonize as much as possible the different solutions.

Finally, a number of Recommendations will be developed within ITU-R, sufficiently detailed to enable worldwide compatibility of operation and equipment, including roaming.

7.1.4 3GPP

The work in 3GPP is not organized directly according to the OSI layers, but it somehow reflects such classification. 3GPP is subdivided in three main areas: System Aspects (SA), Core Network and Terminals (CT) and Radio Access Network (RAN). Each area is governed by a Technical Specification Group (TSG) Plenary, which defines the workplan and approves the technical specifications developed by the respective Working Groups. RAN focuses on the Media Layers (1-3); RAN3 defines the radio architecture and interfaces between radio nodes and the Core Network. RAN4 defines the performance of the radio access technologies and RAN5 defines the test procedures to ensure a device is compliant to 3GPP specifications. SA defines the services and the system aspects. SA1 specifies the requirements for the new services both from a user perspective and from a network perspective; SA2 defines the network architecture while the security aspects are defined by SA3. SA4 focuses on codecs and SA5 on telecom management. SA6 deals with mission critical applications. Finally, CT implements the protocols (layers 3-5) to ensure communications inside the mobile network and the interconnectivity with external network. The specific contribute of each Working Group to the 5G work plan will be detailed later on in this chapter.

Following the ITU-R procedure, 3GPP decided that its solutions will be submitted to ITU-R to become part of IMT-2020. In particular, one key requirement is that LTE and the new radio (NR) must be tightly integrated, part of the 3GPP system. The new radio access technology will have ultimately the goal to satisfy all the requirements set by ITU-R, but 3GPP will submit both LTE and the new radio for inclusion in IMT-2020.

Figure 53 represents the 3GPP workplan as defined in September 2016. This picture may be not definitive, since 3GPP is always striving to satisfy the different market requirements. As a consequence, the roadmap has been already modified twice in 2016 to ensure that at least a subset of the expected full-blown 5G technical specifications is available already at the end of 2017 for Operators planning commercial launches in 2018.

Figure 53 – 3GPP workplan

In general, the workplan is based on a phased approach. In Release 14, 3GPP studied the feasibility

of 5G solutions (SA1 identified the service requirements, SA2 the system architecture and RAN the radio access technology). Based on the study phase, technical specifications are derived in two phases. Phase 1 will be delivered within the Release 15 timeframe (with completion date June 2018). This phase will mainly focus on the eMBB use case, and will provide technical specifications for the new radio access technology and the foundations of the next generation Core Network. However, the work must be done by taking into account that a following phase will arrive with Release 16, planned for December 2019. Therefore, the solutions specified in Release 15 must allow Release 16 to be built on such foundations set in 2018 (this is indicated within 3GPP as forward compatibility). The Release 16 specifications must fulfill all the requirements and be ready for incorporation in the ITU-R technical description of IMT-2020.

Finally a number of operators indicated the willingness to anticipate in 2018 the commercial launch of 5G services. As a consequence, it was decided to anticipate around the end of 2017 a preliminary set of specifications based on a LTE-assisted approach (see Figure 54). The new radio access technology will be mainly used for capacity enhancements of current LTE networks (with the possibility to operate the new radio on new bands, e.g. 28 GHz). No modifications are required in the LTE Core Network (EPC), apart from the capability to handle grater throughputs than today. In fact, the EPC will be connected to an LTE base station (eNB) via the current S1 interface. The new radio base station will be connected to the LTE eNB by exploiting the "dual connectivity" feature [36], and the 5G device will have to connect to both base stations: the LTE one will ensure the signaling flow with the core network (e.g. mobility management, paging – dotted line in Figure 54), while the user data will be carried both by the new radio base station and by the LTE base station (continuous line in Figure 54). This approach requires "only" the definition of the low layers of the new radio, with no functional change to EPC and therefore it is quicker to specify and commercialize. Note that 3GPP ruled out the possibility for a new radio base station alone to attach to the LTE CN: a new radio base station in stand-alone deployment (i.e. not used in "dual connectivity" with LTE eNB) will connect only to the next generation core.

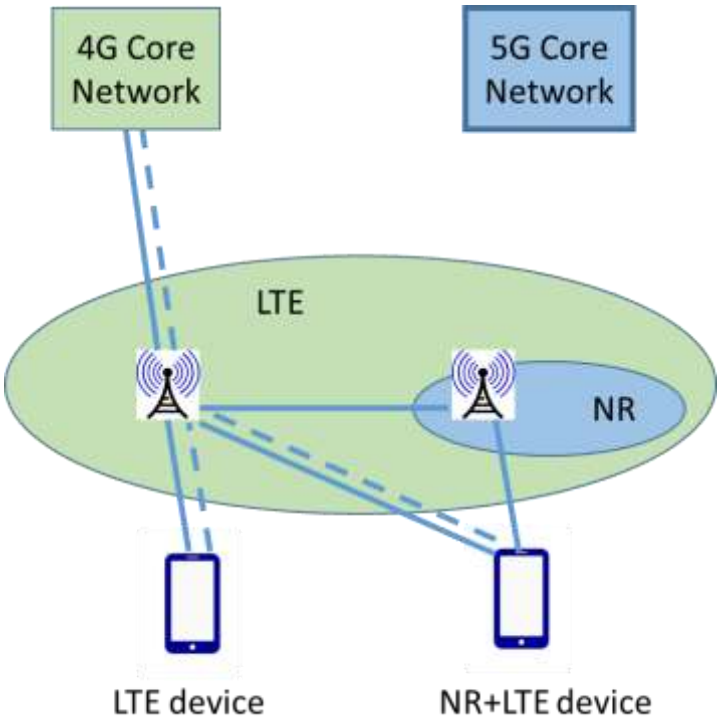


Figure 54 – LTE-assisted approach

SMARTER (New Services and Markets Technology Enablers) was the name of the SA WG1 project

which developed high-level use cases and identified the related high-level potential requirements to enable 5G.

The study aimed at identifying the market segments and verticals whose needs 3GPP should focus on and that could not be met with LTE/EPS state of the technology.

The Release 14 Study Item SMARTER followed a phased approach at the conclusions of which a number of Technical Reports were finalized for each of the following macro areas:

- TR 22.861 [37] Feasibility study on massive Internet of Things – which collects requirements for the Internet of Things characterized by a large numbers of devices which may experience long battery life, high reliability (e.g. Smart wearables), and low complexity (sensors). In this context, also a new approach to SIM remote management is studied, like for example the provisioning of 'blank' IoT devices with 3GPP subscription where change subscription/credentials can happen over the air
- TR 22.862 [38] Feasibility study on new services and markets technology enablers for critical communications – which collects requirements including high reliability and ultra-low latency derived from Tactile internet and other use cases like factory automation (closed-loop control applications running over 5G short range radio), UAV remote control (unmanned aerial vehicles, drones), cars collision avoidance and mission critical services.
- TR 22.863 [39] Feasibility study on new services and markets technology enablers for enhanced mobile broadband – collecting requirements from office and dense urban scenarios (e.g. real-time video meeting with very high data rates) and fast moving devices (car and trains)
- TR 22.864 [40] Feasibility study on new services and markets technology enablers for network operation – which describes the required system capabilities in terms of flexibility (e.g. network slicing, efficient user plane allocation, exposure to 3rd parties …), scalability, mobility support, efficient content delivery, non-3GPP and 3GPP access integration, migration, security, …

Together with the above listed SMARTER studies, SA1 has developed also a study on the enhancement of 3GPP support for 5G V2X services (TR 22.886 [41]), which has been conceived as the natural evolution of Release 14 support for LTE based V2X.

At the end of the Release 14 5G study phase, the result of all such TRs has built the basis for the corresponding normative activity for the phase 1 (Release 15), which is documented in the Technical Specification TS 22.261 "Service requirements for next generation new services and markets" [42] (completed by March 2017).

In December 2015, SA approved the SA2 study item for the next generation 3GPP system architecture to achieve a simple, flexible, scalable and extensible architecture (NextGen) with two distinct characteristics with respect to previous ones:

- A high overall efficiency for all types of communication services of significantly differing traffic characteristics
- A high flexibility for deploying networks and network slices of different characteristics for serving various user and service needs adequately and efficiently.

It is worth underlying again that the overall NextGen system work is split into two phases:

- Phase 1 (Release 15) Developing a baseline NextGen system including the NextGen core network that can be built upon in subsequent releases.

- Phase 2 (Release 16) Building a complete and feature rich NextGen system that builds on top of Phase-1.

The corresponding Release 15 TR 23.977 “Study on Architecture for Next Generation System” [43] (also referred to as NextGen) contains the agreed high level principles and documents solutions to a number of key issues in which the architectural work has been decomposed such as: network slicing, QoS framework, mobility framework, session management, support for session and service continuity and efficient user plane paths, policy framework, support for IMS, … just to mention some. The target is to reach an agreement for each key issue and, from this solutions set, building up the foundations of the NextGen architecture.

The architecture has been developed with the following non-exhaustive list of operational efficiency and optimization characteristics:

- Ability to handle the rapid growth in mobile data traffic/device numbers resulting from existing and new communication services in a scalable manner.
- Allow independent evolution of core and radio networks.
- Support techniques (e.g. Network Function Virtualization and Software Defined Networking) to reduce total cost of ownership, improve operational efficiency, energy efficiency, and simplicity in and flexibility for offering new services.

From the conclusions of the TR 23.977 (December 2016), the normative work item for phase 1 of the NextGen architecture has started, with the aim to be finalized by the end of 2017.

In March 2016 SA3 has started to study preliminary threats, requirements and solutions for the security of next generation mobile networks. TR 33.899 [44] captures the output of this study.

Finally, also SA5 started some NextGen related work to understand how the network management should evolve e.g. how to satisfy the operational and management requirements and the role and location of the management functionalities, to investigate use cases and requirements for management and orchestration of network slicing, to define management and orchestration architecture to support network operational features such as real-time, on demand, automation etc. as well as vertical applications (e.g. eV2X).

At this purpose SA5 is developing for the Release 15 the following studies

- TR 28.802, Study on Management Aspects of Next Generation Network architecture and features [45]
- TR 28.800, Study on Management and Orchestration Architecture of Next Generation Network and Service [46]
- TR 28.801, Study on management and orchestration of network slicing for next generation network [47]

The studies will define also the relationship between network slice management and orchestration concepts developed in SA5 and the management and orchestration concepts defined by ETSI NFV.
In September 2016 RAN approved the radio requirements for the new radio [48]. This document provides the KPIs for the radio interface (see Figure 55) and the deployment scenarios to be used to verify the KPIs are met. The document also provides a number of requirements on architecture, supplementary services (MBMS [49], positioning, critical communications), and operational requirements.

From the architecture perspective, some new aspects have been introduced, such as splitting the RAN architecture (Cloud RAN), network function virtualization and SDN, and network slicing.

One of the big novelties for the radio is the approach to spectrum: in order to achieve very high throughput it is necessary to explore new spectrum. Therefore, 3GPP decided to develop solutions able to operate up to 100 GHz. The challenge to provide cellular service at these frequency ranges is very high, but trials and literature indicate it as feasible [50].

KPI	value
Peak data rate	20Gbps DL 10Gbps UL
Peak Spectral efficiency	30bps/Hz - 15bps/Hz
Control plane latency	10ms from idle to active mode
User plane latency	URLLC: 0.5ms UL&DL eMBB: 4 ms UL&DL
Latency for infrequent small packets	UL: 10 s for a 20 byte application packet @ e maximum coupling loss of 164dB
Mobility interruption time	0 ms
Inter-system mobility	With other IMT systems
Reliability	URLLC: P=10-5 in 1ms
Coverage	mMTC 164dB @ 160bps

KPI	value
Extreme Coverage	100-400 km voice/low data
UE battery life	mMTC > 10 years (target 15 years)
Cell/Transmission Point/ TRP spectral efficiency	3x IMT-A
Area traffic capacity	To be derived area capacity (bps/m2) = site density (site/m2) × bandwidth (Hz) × spectrum efficiency (bps/Hz/site)
User experienced data rate	TBD - NGMN: 50 Mbps everywhere (2Gbps indoor hotspot)
5th percentile user spectrum efficiency	3x IMT-A
Connection density	mMTC 1M device/km2
mobility	500 km/h

Figure 55: 3GPP radio KPIs for New Radio

7.1.4.1 New Radio main features

The main features of the "New Radio" under study and standardization in 3GPP are:

- adoption of centimeter / millimeter waves / technologies that in turn imply:
  - densification of radiating points (UDN: Ultra Dense Network);
  - new waveform design and "ultra-lean signaling";
- massive / Full Dimensional MIMO and Beamforming

The potential benefits of using cm / mm waves may be summarized in:

- availability of large spectrum portions of the order of hundreds of MHz;
- extremely high data rates, (for example, the 20 Gbps peak downlink indoor environment);
- very high spatial reuse thanks to beamforming techniques;
- "Flexible deployment": it is possible to use the radio interface for both user terminals and backhauling / fronthauling access.

The main challenges, however, can be summarized in:

- High link attenuation (partly attenuated by beamforming gains) and high sensitivity to "blocking" and absorption phenomena, in addition to the difficulties associated with indoor penetration
- need for robust and efficient algorithms for track / search of the beams and complex system management with numerous "directional" connections.

Under these assumptions, the main features of the new waveform design currently being discussed in 3GPP RAN groups are summarized in:

- Use of OFDM as in LTE, but increasing efficiency in the use of available bandwidth (90% LTE

at 95% -98%)

- Different pilot symbols (RS) with respect to LTE, in order to manage the effects of the radio channel above 6GHz, also trying to reduce overhead (OH) and interference generated
- Adoption of different carrier spacing values (30, 60, 120, 240, 480 KHz and not just 15 kHz as in LTE) to handle different bandwidths and different use cases, even dynamically and possibly simultaneously
- Adoption of several Cyclix Prefix values to manage different coverage ranges as the frequency range varies
- "Ultra Lean Signaling": attempts to reduce overhead control channels, both common and dedicated, adoption of "grant free operation" for low latency use and "self contained signaling".

The fundamental principles of the Full Dimensional (FD) / Massive MIMO adopted in the 5G are summarized in Figure 56:

- High number of antenna elements (increasing with frequency) at the Base Station;
- tens of users simultaneously served on the same radio resources thanks to the Multi User MIMO (MU-MIMO) realized using beamforming techniques, both horizontally and vertically.

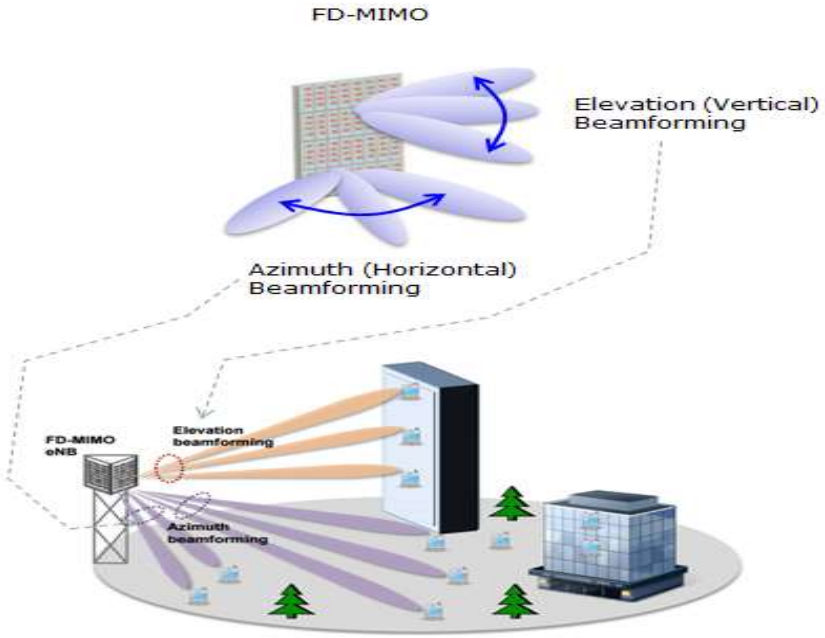


Figure 56 - Main principles of FD/Massive MIMO

7.2 Annex 2 – 170503_Autopilot_T1.4_CommunicationRequirements.xlsx

KPI Name	KPI Description	Possible Values
End-to-end latency (L)	Maximum tolerable elapsed time from the instant a data packet is generated at the source application to the instant it is received by the destination application. If direct mode is used, this is essentially the maximum tolerable air interface latency. If infrastructure mode is used, this includes the time needed for uplink, any necessary routing in the infrastructure, and downlink.	High: L > 100 ms Medium: 10ms < L < 100ms Low: L < 10ms
Reliability (R)	Maximum tolerable packet loss rate at the application layer (i.e., after HARQ, ARQ, etc.). A packet is considered lost if it is not received by the destination application within the maximum tolerable end-to-end latency for that application. For example, 10-5 means the application tolerates at most 1 in 100,000 packets not being successfully received within the maximum tolerable latency. This is sometimes expressed as a percentage (e.g., 99.999%) elsewhere.	High: R > 10-4 Medium: 10-4 < R <10-6 Low: R < 10-6
Bandwidth (B)	Minimum required bit rate for the application to function correctly.	High: B > 100 Mb/s Medium: 100 Mb/s < B < 1 Mb/s Low: B < 1Mb/s
Communication range (CR)	Maximum distance between source and destination(s) of a radio transmission within which the application should achieve the specified reliability.	Wired communication Wireless PAN Range communication: 0-100 m Wireless LAN Range communication: 100-1000 m Wireless WAN Range Communication: 1000-10000 m Wireless Long Range communication: CR > 1000 m V2X communication URBAN: 50-100 m V2X communication SUBURBAN: 100-200 m V2X communication HIGHWAY: 200-1000 m

Node mobility (N)	Maximum relative speed under which the specified reliability should be achieved	No mobility: 0 km/h Pedestrian: 0-10 km/h Vehicular URBAN: 0-70 km/h Vehicular SUBURBAN: 0-100 km/h Vehicular HIGHWAY: 0-160 km/h
Network density (D)	Maximum number of vehicles per unit area under which the specified reliability should be achieved.	URBAN: 1000-3000 v/km2 SUBURBAN: 500-1000 v/km2 HIGHWAY: 100-500 v/km2
Security (S)	Specific security features required by the application. These include user authentication, authenticity of data, integrity of data, confidentiality, and user privacy.	Specify Requirements

Table 17: Communication KPI sheet

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
1	Hazard on the roadway	Livorno	Communication between sensors, Traffic Control Center, cloud and vehicles	MUST				V2X HIGHWAY	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM
2	Roadway works with TCC in the loop	Livorno	Communication between sensors, Traffic Control Center, cloud and vehicles	MUST				V2X HIGHWAY	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM
3	Surface road condition	Livorno	Communication between sensors, Traffic Control Center, cloud and vehicles	MUST				V2X HIGHWAY	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM
4	Pedestrian detection with camera	Livorno	Communication between sensors, Traffic Control Center, cloud and vehicles	MUST				V2X URBAN	Pedestrian Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	CNIT, TIM
5	Connected bicycle	Livorno	Communication between sensors, Traffic Control Center, cloud and vehicles	MUST				V2X URBAN	Pedestrian Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	CNIT, TIM
6	Urban Driving/Intersection support	Tampere	Communication between vehicle and cloud/traffic light control	MUST	high	high	medium	Long Range Communication	Vehicular Suburban	URBAN/SUBURBAN	low	VTT/Johan Scholliers

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
			system									
7	Automated Valet Parking	Tampere	Communication between vehicle and cloud/camera management centre	MUST	High	High	medium	short range/cellular	Pedestrian	urban	vehicle authentication, integrity of data, confidentiality, privacy	VTT/Johan Scholliers
8	Highway Pilot	Brainport	Communication between V2X	MUST	High	High	Low	V2X Highway	Vehicular Highway	Highway	user authentication,	TECH/Jan Bosma
9											authenticity of data,	
10											integrity of data	
11	Urban Driving (relocation TU/e)	Brainport (TU/e)	VRU detection & localization: direct communication between smartphone application of VRU (vulnerable road user) and AD (automated driving) vehicle	MUST	High	High	Medium	URBAN + SUBURBAN (0-200m)	Vehicular URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	TU/e (Jos den Ouden)
12	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between lecture schedule webserver of TU/e and AD vehicle	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, confidentiality, authenticity of data	TU/e (Jos den Ouden)

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
13	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between weather information webserver and AD vehicle	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, authenticity of data	TU/e (Jos den Ouden)
14	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between AD vehicle and Service center for managing relocation requests of AD vehicles over TU/e Campus	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	vehicle authentication, authenticity of data, integrity of data, confidentiality	TU/e (Jos den Ouden)
15	Highway Pilot	Brainport	Communication between vehicles and infra (V2X)	MUST	High	High	Low	V2X Highway	Vehicular Highway	Highway	user authentication, authenticity of data, integrity of data	TECH/Jan Bosma
16	Highway Pilot	Brainport	Communication cloud and Vehicle	MAY	High	High	Medium	Long Range Communication	Vehicular Highway	Highway	integrity of data, authenticity of data	TECH/Jan Bosma
17	Urban Driving (relocation TU/e)	Brainport (TU/e)	VRU detection & localization: direct communication between smartphone application of VRU (vulnerable road user) and AD (automated driving) vehicle	MUST	High	High	Medium	URBAN + SUBURBAN (0-200m)	Vehicular URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	TU/e (Jos den Ouden)

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
18	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between lecture schedule webserver of TU/e and AD vehicle	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, confidentiality, authenticity of data	TU/e (Jos den Ouden)
19	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between weather information webserver and AD vehicle	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, authenticity of data	TU/e (Jos den Ouden)
20	Urban Driving (relocation TU/e)	Brainport (TU/e)	Communication between AD vehicle and Service center for managing relocation requests of AD vehicles over TU/e Campus	MUST	Low	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	vehicle authentication, authenticity of data, integrity of data, confidentiality	TU/e (Jos den Ouden)
21	Urban Driving (relocation TU/e)											
22	Platooning	Brainport	Communication between Vehicle and RSU V2X	MUST	Low / Medium	Low	Low	Short <300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO
23	Platooning	Brainport	Communication between vehicles and cloud	MUST	Medium / High	Medium	Low	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
24	Platooning	Brainport	Communication between Vehicles V2V	MUST	Low / Medium	Low	Low	Short <300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO
25	Platooning	Brainport	Communication between Vehicles cellular	MUST	Medium / High	Medium	Medium / High	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO
26	Platooning	Brainport										
27	Automated Valet Parking	Brainport	Communication between Vehicle and AVP app	MUST	High	Medium	Low	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR
28	Automated Valet Parking	Brainport	Communication between AVP app and cloud	MUST	High	Medium	Low	Long Range Communication	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR
	Automated Valet Parking	Brainport	Communication between Vehcile and cloud	MUST	High	Medium	Low	Long Range Communication	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
29	Automated Valet Parking	Brainport	Communication between Drone and cloud	MUST	Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR
30	Automated Valet Parking	Brainport	Communication static camera and cloud	MUST	Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR
31	Car sharing service	Brainport	Communication between app (user device) and Service center cloud	MUST	High	High	Medium	Long Range Communication	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	IBME
32	Car sharing service	Brainport	Communication between vehicle and Service center cloud	MUST	High	High	Medium	Long Range Communication	Vehicular Suburban	SUBURBAN	user authentication, integrity of data, confidentiality privacy	IBME
33	Automated Valet Parking	Vigo	Communication between app (user device) and cloud/parking control system	MUST	High	High	Low	Long Range Communication	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	CTAG/Silvia Alén

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
34	Automated Valet Parking	Vigo	Communication between vehicle and valet parking control system	MUST	medium	high	medium/high	short range	Pedestrian	urban	vehicle authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén
35	Automated Valet Parking	Vigo	Communication between vehicle and parking infraestructure	MUST	low	High	low	short range	Pedestrian	urban	vehicle authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén
36	Automated Valet Parking	Vigo	Communication between parking infraestructure and cloud	MUST	medium	High	medium	Long Range Communication			authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén
37	Urban Driving	Vigo	Communication between vehicle and cloud/traffic control system	MUST	medium	High	Medium	Long Range Communication	Vehicular Suburban	urban	vehicle authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén

Index	Use case name	Pilot site name (if applicable)	Requirement description	Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator/Modifiers Name & Organization
38	Urban Driving	Vigo	Communication between infraestructure (traffic lights) and cloud/traffic control system	MUST	medium	High	low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén
39	Urban Driving	Vigo	Communication between traffic alert system and cloud/traffic control system	MUST	High	High	low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén
40	Urban Driving	Vigo	V2X Communication	MUST	low	high	Low	Short Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén

Table 18: Requirement per UC sheet

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR1	Hazard on the roadway	The vehicle must receive the geocasted notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from RSU	MUST	MUST			MUST		low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB
CR2	Hazard on the roadway	The WSN on the road must notify the presence of puddles on the road whenever they are detected		MUST					high	High	low	Wireless PAN Wireless LAN Wireless WAN	No mobility	NA	user authentication, integrity of data	ISMB
CR3	Hazard on the roadway	The traffic control system must receive geolocalized notifications of hazard events from RSU (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.)		MUST					high	High	Low	Wired Long Range	No mobility	NA	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB
CR4	Hazard on the roadway	Geolocalized notifications of hazard events (e.g. potholes, roadway works, puddles, etc.) from RSU may be stored by the data		MAY					high	Medium	Low	Long Range	No mobility	NA	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
		management service of the IoT platform														
CR5	Pedestrian detection	The detection event of pedestrians on the roadway must be notified to the RSU from the camera		MUST					low	high	low	Wired Wireless LAN	No mobility	NA	user authentication, integrity of data	ISMB
CR6	Pedestrian detection	The number of detected pedestrians on the roadway detected by the camera may be stored by the data management service of the IoT platform		MAY					high	Medium	Low	Wired Long Range	No mobility	NA	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB
CR7	Hazard on the roadway	Every time the vehicle detects an hazard, it must be geocasted to other vehicles		MUST					low	high	Low	V2X URBAN V2X SUBURBAN V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB
CR8	Hazard on the roadway with TCC in the loop	The traffic control system must receive geolocalized notifications of hazard events (e.g. potholes,		MUST					high	Medium	Low	Long Range	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
		roadway works, pedestrians, VRUs, puddles, etc.) from vehicles														
CR9	Connected bicycle	Bicycles must geocast their position, speed, orientation to other vehicles on the road		MUST					low	High	Low	V2X URBAN	Pedestrian Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB
CR10	V2V communication	Vehicles must geocast their position, speed, orientation to other vehicles on the road	MUST	MUST			MAY		low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB, CTAG
CR11	V2X communication	Traffic light must continuously geocast its light phase and the topology of the croassroad to vehicles on the road	MUST	MUST			MUST		low	High	Low	V2X URBAN	Vehicular URBAN	URBAN	authentication, integrity of data, confidentiality, privacy	CNIT, TIM, ISMB, CTAG
CR12	Traffic conditions	The traffic control system must receive information about traffic conditions	MUST	MUST					High	High	low	V2X URBAN	Vehicular SUBURBAN Vehicular HIGHWAY	SUBURBAN HIGHWAY	authentication, integrity of data, confidentiality, privacy	CTAG/Silvia Alén, ISMB

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR13	V2X communication	Vehicles must be able to receive CAM/DENM contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST	MUST	low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB, TECH, CTAG
CR14	V2X communication	Vehicles must be able to receive SPaT/MAP contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST	MUST	low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB, TECH, CTAG
CR15	IoT services	Vehicle must be able to receive data from communication system, related with contents received from IoT external services.	MUST	MUST	MUST	MUST	MUST	MUST	high	medium	low	Long Range Communication	Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	ISMB
CR16	IoT services	Vehicles must be enabled to provide /communicate elaborated data to IoT external services, through communication system.	MUST	MUST	MUST	MUST	MUST	MUST	high	medium	low	Long Range Communication	Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	ISMB

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR17	Traffic Light handling	The vehicle should be able to receive Signal Phase information, coming from IoT infrastructure platform (alternative to SPaT/MAP from ITS-G5 channel, for long range)	SHOULD	SHOULD		SHOULD	MAY		high	high	low	Long Range Communication	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB
CR18	Urban Driving Intersection support	Communication between vehicle and cloud/traffic light control system				MUST			high	high	medium	Long Range	Vehicular Suburban	URBAN SUBURBAN	low	VTT
CR19	Automated Valet Parking	Communication between vehicle and cloud/camera management centre				MUST	MAY		High	High	medium	Wireless LAN Long Range	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	VTT
CR20	Urban Driving (relocation TU/e)	The vehicle must receive information about VRU presence and localization by a smartphone application					MUST		Low	High	Medium	Wireless LAN Long Range	Vehicular URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	TU/e
CR21	Urban Driving (relocation TU/e)	Communication between lecture schedule webserver of TU/e and AD					MUST		Mdium	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, confidentiality, authenticity of data	TU/e

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
		vehicle														
CR22	Urban Driving (relocation TU/e)	The vehicle must receive wheather information by a cloud-based web server					MUST		High	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, authenticity of data	TU/e
CR23	Urban Driving (relocation TU/e)	The vehicle and the service center must communicate each other information for managing relocation requests of vehicles					MUST		High	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	vehicle authentication, authenticity of data, integrity of data, confidentiality	TU/e
CR24	Automated Valet Parking	Communication between Vehicle and AVP application					MUST		Medium	Medium	Low	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR
CR25	Automated Valet Parking	Communication between AVP application and cloud					MUST		High	Medium	Low	Long Range Communication	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR26	Automated Valet Parking	Communication between Drone and cloud					MUST		Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR
CR27	Automated Valet Parking	Communication static camera and cloud					MUST		Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR
CR28	Car sharing service	Communication between the application hosted on the user device and the service center cloud					MUST		High	High	Medium	Long Range	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	IBME
CR29	Highway Pilot	V2X Communication between vehicles and infrastructure					MUST		Low/Medium	High	Low	V2X Highway	Vehicular Highway	Highway	user authentication, authenticity of data, integrity of data	TECH/Jan Bosma
CR30	Highway Pilot, Platooning	The vehicle may send and receive information to/from the cloud					MAY		High	High	Medium	Long Range	Vehicular Highway	Highway	user/vehicle authentication, integrity of data, authenticity of data	TECH, TNO
CR31	Platooning	V2X Communication between Vehicle and RSU					MUST		Low / Medium	Low	Low	Short <300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR32	Platooning	Communication between vehicles and cloud					MUST		Medium / High	Medium	Low	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO, DLR
CR33	Platooning	V2V Communication between Vehicles					MUST		Low	Medium	Low	V2X URBAN V2X SUBURBAN V2X HIGHWAY	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO
CR34	Platooning	Cellular Communication between Vehicles					MUST		Medium / High	Medium	Medium / High	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO
CR35	Car sharing service	Communication between vehicle and Service center cloud					MUST		High	High	Medium	Long Range	Vehicular SUBURBAN	SUBURBAN	user authentication, integrity of data, confidentiality privacy	IBME
CR36	Automated Valet Parking	Communication between the application hosted on the user device and the cloud-based parking control system	MUST						High	High	Low	Long Range	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	CTAG

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR38	Automated Valet Parking	The vehicle must receive exchange information (e.g. a detailed layout of the parking place, the location of dynamic objects, pedestrian location, vehicle position) with the parking control system	MUST						medium	high	medium	Short Range Communication	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	CTAG
CR39	Automated Valet Parking	The vehicle must be able to provide its identification to be authorized at the parking place	MUST						low	High	low	Short Range Communication	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	CTAG
CR40	Automated Valet Parking	Communication between parking infraestructure and cloud	MUST						medium	High	medium	Long Range Communication	No mobility	NA	authentication, integrity of data, confidentiality, privacy	CTAG
CR41	Urban Driving	Communication between vehicle and cloud/traffic control system	MUST						medium	High	Medium	Long Range Communication	Vehicular Suburban	urban	vehicle authentication, integrity of data, confidentiality, privacy	CTAG

ID	Use case name / keyword	Requirement description	Spain Priority (Must/Should/May)	Italy Priority (Must/Should/May)	France Priority (Must/Should/May)	Finland Priority (Must/Should/May)	Nederland Priority (Must/Should/May)	Korea Priority (Must/Should/May)	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization
CR42	Urban Driving	Communication between infraestructure (traffic lights) and cloud/traffic control system	MUST						medium	High	low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG
CR43	Urban Driving	Communication between traffic alert system and cloud/traffic control system	MUST						High	High	low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG
CR44	Obstacle or VRU detection	The In-vehicle PF can be able to receive information related with VRU presence, generated by IoT infrastructure PF (alternative to CAM/DENM from ITS-G5 channel, for long range).	MUST	MUST					high	high	low	Long Range Communication	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentialityprivacy	ISMB

Table 19: Revised Requirement sheet

7.3 Annex 3 – Communication requirements

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 1	Hazard on the roadway	The vehicle must receive the geocasted notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from RSU	MUST	MUST	NA	NA	MUST	NA	Low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authenticat ion, integrity of data, confidentia lity privacy	CNIT, TIM, ISMB	covered by ITSG5 DENBS, RSUs must support GeoBroadcast forwarding	no	-
CR 2	Hazard on the roadway	The WSN on the road must notify the presence of puddles on the road whenever they are detected	NA	MUST	NA	NA	NA	NA	high	High	Low	Wireless PAN Wireless LAN Wireless WAN	No mobility	NA	user authenticat ion, integrity of data	ISMB	NB-IoT OneM2M	no	-
CR 3	Hazard on the roadway	The traffic control system must receive geolocalized notifications of hazard events from RSU (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.)	NA	MUST	NA	NA	NA	NA	High	High	Low	Wired Long Range	No mobility	NA	user authenticat ion, integrity of data, confidentia lity privacy	CNIT, TIM, ISMB	DATEX, DENM XER	no	-
CR 4	Hazard on the roadway	Geolocalized notifications of hazard events (e.g. potholes, roadway works, puddles, etc.) from RSU may be stored by the data management service of the IoT platform	NA	MAY	NA	NA	NA	NA	High	Medium	Low	Long Range	No mobility	NA	user authenticat ion, integrity of data, confidentia lity privacy	CNIT, TIM, ISMB	OneM2M	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 5	Pedestrian detection	The detection event of pedestrians on the roadway must be notified to the RSU from the camera	NA	MUST	NA	NA	NA	NA	Low	High	Low	Wired Wireless LAN	No mobility	NA	user authentication, integrity of data	ISMB	ITSG5 through RSU gateway	no	-
CR 6	Pedestrian detection	The number of detected pedestrians on the roadway detected by the camera may be stored by the data management service of the IoT platform	NA	MAY	NA	NA	NA	NA	High	Medium	Low	Wired Long Range	No mobility	NA	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB	OneM2M	no	-
CR 7	Hazard on the roadway	Every time the vehicle detects an hazard, it must be geocasted to other vehicles	NA	MUST	NA	NA	NA	NA	Low	High	Low	V2X URBAN V2X SUBURBAN V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB	ITSG5 - DENM	no	Vehicles must be able to geobroadcast forwarding.
CR 8	Hazard on the roadway with TCC in the loop	The traffic control system must receive geolocalized notifications of hazard events (e.g. potholes, roadway works, pedestrians, VRUs, puddles, etc.) from vehicles	NA	MUST	NA	NA	NA	NA	High	Medium	Low	Long Range	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB	ITSG5, DATEX, DENM XER	no	through a RSU gateway to TCC In addition to DATEX (used for RSU<->DATEX Node communications) also DENM XER is employed (for RSU<-> DATEX 2 C-ITS Adapter communications)

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 9	Connected bicycle	Bicycles must geocast their position, speed, orientation to other vehicles on the road	NA	MUST	NA	NA	NA	NA	Low	High	Low	V2X URBAN	Pedestrian Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB	ITSG5	no	-
CR 10	V2V communication	Vehicles must geocast their position, speed, orientation to other vehicles on the road	MUST	MUST	NA	NA	MAY	NA	Low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	CNIT, TIM, ISMB, CTAG	ITSG5	no	-
CR 11	V2X communication	Traffic light must continuously geocast its light phase and the topology of the croassroad to vehicles on the road	MUST	MUST	NA	NA	MUST	NA	Low	High	Low	V2X URBAN	Vehicular URBAN	URBAN	authentication, integrity of data, confidentiality, privacy	CNIT, TIM, ISMB, CTAG	ITSG5 through SPAT and MAP messages, and proprietary protocol over 802.11	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 12	Traffic conditions	The traffic control system must receive information about traffic conditions	MUST	MUST	NA	NA	NA	NA	High	High	Low	V2X URBAN	Vehicular SUBURBAN Vehicular HIGHWAY	SUBURBAN HIGHWAY	authentication, integrity of data, confidentiality, privacy	CTAG /Silvia Alén, ISMB		yes	GAP: requires to define the protocol that will be used to communicate to exchange traffic information. It is not defined who sends the traffic information to TCC (if vehicles directly or aggregated information through RSUs) KA: Communications and Interoperability
CR 13	V2X communication	Vehicles must be able to receive CAM/DENM contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST	MUST	Low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB, TECH, CTAG	ITSG5	no	-
CR 14	V2X communication	Vehicles must be able to receive SPaT/MAP contents from received ITS-G5 messages	MUST	MUST	MUST	MUST	MUST	MUST	Low	High	Low	V2X HIGHWAY	Vehicular URBAN Vehicular SUBURBAN Vehicular HIGHWAY	URBAN SUBURBAN HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB, TECH, CTAG	ITSG5	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 15	IoT services	Vehicle must be able to receive data from communication system, related with contents received from IoT external services.	MUST	MUST	MUST	MUST	MUST	MUST	High	Medium	Low	Long Range Communication	Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	ISMB	LTE,OneM2M	no	-
CR 16	IoT services	Vehicles must be enabled to provide /communicate elaborated data to IoT external services, through communication system.	MUST	MUST	MUST	MUST	MUST	MUST	High	Medium	Low	Long Range Communication	Vehicular URBAN	URBAN	user authentication, integrity of data, confidentiality privacy	ISMB	LTE,OneM2M	no	-
CR 17	Traffic Light handling	The vehicle should be able to receive Signal Phase information, coming from IoT infrastructure platform (alternative to SPaT/MAP from ITS-G5 channel, for long range)	SHOULD	SHOULD	NA	SHOULD	MAY	NA	High	High	Low	Long Range Communication	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB	oneM2M	no	-
CR 18	Urban Driving Intersection support	Communication between vehicle and cloud/traffic light control system	NA	NA	NA	MUST	NA	NA	High	High	Medium	Long Range	Vehicular Suburban	URBAN SUBURBAN	low	VTT	TCP/IP	no	-
CR 19	Automated Valet Parking	Communication between vehicle and cloud/camera management centre	NA	NA	NA	MUST	MAY	NA	High	High	Medium	Wireless LAN Long Range	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	VTT	TCP/IP	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 20	Urban Driving (relocation TU/e)	The vehicle must receive information about VRU presence and localization by a smartphone application	NA	NA	NA	NA	MUST	NA	Low	High	Medium	Wireless LAN Long Range	Vehicular URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	TU/e	ITSG5	no	-
CR 21	Urban Driving (relocation TU/e)	Communication between lecture schedule webserver of TU/e and AD vehicle	NA	NA	NA	NA	MUST	NA	Mdium	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, confidentiality, authenticity of data	TU/e	HTTP	yes	GAP: There seems not to be a standard to cover this communication over HTTP, application level must implement the protocol. KA: Communication/connectivity
CR 22	Urban Driving (relocation TU/e)	The vehicle must receive wheather information by a cloud-based web server	NA	NA	NA	NA	MUST	NA	High	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	integrity of data, authenticity of data	TU/e	HTTP	no	-
CR 23	Urban Driving (relocation TU/e)	The vehicle and the service center must communicate each other information for managing relocation requests of vehicles	NA	NA	NA	NA	MUST	NA	High	Medium	Low	SUBURBAN	Vehicular URBAN	URBAN	vehicle authentication, authenticity of data, integrity of data, confidentiality	TU/e	HTTP	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 24	Automated Valet Parking	Communication between Vehicle and AVP application	NA	NA	NA	NA	MUST	NA	Medium	Medium	Low	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR	-	yes	GAP: At the time of the writing of this document, no standard protocol was specified for this communication and no access technology, since it specifies long and short range. KA: communication/connectivity
CR 25	Automated Valet Parking	Communication between AVP application and cloud	NA	NA	NA	NA	MUST	NA	High	Medium	Low	Long Range Communication	URBAN	URBAN	integrity of data, authenticity of data, confidentiality, privacy	DLR	TCP/IP	no	-
CR 26	Automated Valet Parking	Communication between Drone and cloud	NA	NA	NA	NA	MUST	NA	Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR	TCP/IP.	yes	GAP: not specified which Higher layer protocol will be used, standard application-layer protocols does not seem to be available. KA: Communications/connectivity

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 27	Automated Valet Parking	Communication static camera and cloud	NA	NA	NA	NA	MUST	NA	Medium	Low	Medium / High	Short range and long range	URBAN	URBAN	integrity of data, authenticity of data	DLR	TCP/IP	-	GAP: not specified which standard Higher-layer protocols will be used. KA: Communications/Connectivity
CR 28	Car sharing service	Communication between the application hosted on the user device and the service center cloud	NA	NA	NA	NA	MUST	NA	High	High	Medium	Long Range	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	IBME	TCP/IP/HTTP	no	-
CR 29	Highway Pilot	V2X Communication between vehicles and infrastructure	NA	NA	NA	NA	MUST	NA	Low/Medium	High	Low	V2X Highway	Vehicular Highway	Highway	user authentication, authenticity of data, integrity of data	TECH /Jan Bosma	ITSG5, LTE	no	same as CR31 but with Higher reliability and distance
CR 30	Highway Pilot, Platooning	The vehicle may send and receive information to/from the cloud	NA	NA	NA	NA	MAY	NA	High	High	Medium	Long Range	Vehicular Highway	Highway	user/vehicle authentication, integrity of data, authenticity of data	TECH, TNO	LTE	no	GAP: it depends from the type of information

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 31	Platooning	V2X Communication between Vehicle and RSU	NA	NA	NA	NA	MUST		Low / Medium	Low	Low	Short <300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO	ITSG5, LTE	no	-
CR 32	Platooning	Communication between vehicles and cloud	NA	NA	NA	NA	MUST		Medium / High	Medium	Low	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO, DLR	same as CR30	yes	-
CR 33	Platooning	V2V Communication between Vehicles	NA	NA	NA	NA	MUST		Low	Medium	Low	V2X URBAN V2X SUBURBAN V2X HIGHWAY	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO	3GPP LTE	no	should'nt it be High reliability?
CR 34	Platooning	Cellular Communication between Vehicles	NA	NA	NA	NA	MUST	NA	Medium / High	Medium	Medium / High	Long > 300m	URBAN SUBURBAN HIGHWAY	URBAN SUBURBAN HIGHWAY	user/vehicle authentication, integrity of data, authenticity of data	TNO	LTE	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 35	Car sharing service	Communication between vehicle and Service center cloud	NA	NA	NA	NA	MUST	NA	High	High	Medium	Long Range	Vehicular SUBURBAN	SUBURBAN	user authentication, integrity of data, confidentiality privacy	IBME	LTE?	yes	GAP: standard application protocols are undefined for this communication, the LTE was assumed due to the range of communication. KA: Communication/connectivity
CR 36	Automated Valet Parking	Communication between the application hosted on the user device and the cloud-based parking control system	MUST	NA	NA	NA	NA	NA	High	High	Low	Long Range	Pedestrian	URBAN	user authentication, integrity of data, confidentiality	CTAG	LTE, HTTP	no	-
CR 38	Automated Valet Parking	The vehicle must receive exchange information (e.g. a detailed layout of the parking place, the location of dynamic objects, pedestrian location, vehicle position) with the parking control system	MUST	NA	NA	NA	NA	NA	Medium	High	Medium	Short Range Communication	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	CTAG	ITSG5 MAP	no	-
CR 39	Automated Valet Parking	The vehicle must be able to provide its identification to be authorized at the parking place	MUST	NA	NA	NA	NA	NA	Low	High	Low	Short Range Communication	Pedestrian	URBAN	vehicle authentication, integrity of data, confidentiality, privacy	CTAG	ITSG5 TS 102 731 (security)	no	-

ID	Use case name / keyword	Requirement description	Spain Priority	Italy Priority	France Priority	Finland Priority	Nederland Priority	S. Korea Priority	End-to-end latency (L)	Reliability (R)	Bandwidth (B)	Communication range (CR)	Node mobility (N)	Network density (D)	Security (S)	Creator Organization	Standards/ protocols covering CR	Gap	Notes/Gap description
CR 40	Automated Valet Parking	Communication between parking infrastructure and cloud	MUST	NA	NA	NA	NA	NA	Medium	High	Medium	Long Range Communication	No mobility	NA	authentication, integrity of data, confidentiality, privacy	CTAG	TCP/IP/HTTP?	no	-
CR 41	Urban Driving	Communication between vehicle and cloud/traffic control system	MUST	NA	NA	NA	NA	NA	Medium	High	Medium	Long Range Communication	Vehicular Suburban	urban	vehicle authentication, integrity of data, confidentiality, privacy	CTAG	LTE, TCP/IP ?	no	-
CR 42	Urban Driving	Communication between infrastructure (traffic lights) and cloud/traffic control system	MUST	NA	NA	NA	NA	NA	Medium	High	Low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG	TCP/IP, DATEX?	no	-
CR 43	Urban Driving	Communication between traffic alert system and cloud/traffic control system	MUST	NA	NA	NA	NA	NA	High	High	Low	Long Range Communication	Vehicular Suburban	urban	authentication, integrity of data, confidentiality, privacy	CTAG	TCP/IP/DATEX?	no	-
CR 44	Obstacle or VRU detection	The In-vehicle PF can be able to receive information related with VRU presence, generated by IoT infrastructure PF (alternative to CAM/DENM from ITS-G5 channel, for long range).	MUST	MUST	NA	NA	NA	NA	High	High	Low	Long Range Communication	Vehicular HIGHWAY	HIGHWAY	user authentication, integrity of data, confidentiality privacy	ISMB	OneM2M	no	-

Table 20: Communication Requirements List

7.4 Annex 4 - LTE Technical Features

To comply with the IMT-Advanced requirements, such as 100Mbps peak data rates to high-mobility users, and 1Gbps peak data rates for low-mobility ones, defined by ITU-R, 3GPP has developed enhancements since the initial LTE Rel-8 standard published in 2008. 3GPP Rel-10 introduced LTE-Advanced to meet or even exceed the IMT-Advanced requirements. Figure 57 illustrates LTE development timelines with main features up to Rel-12.

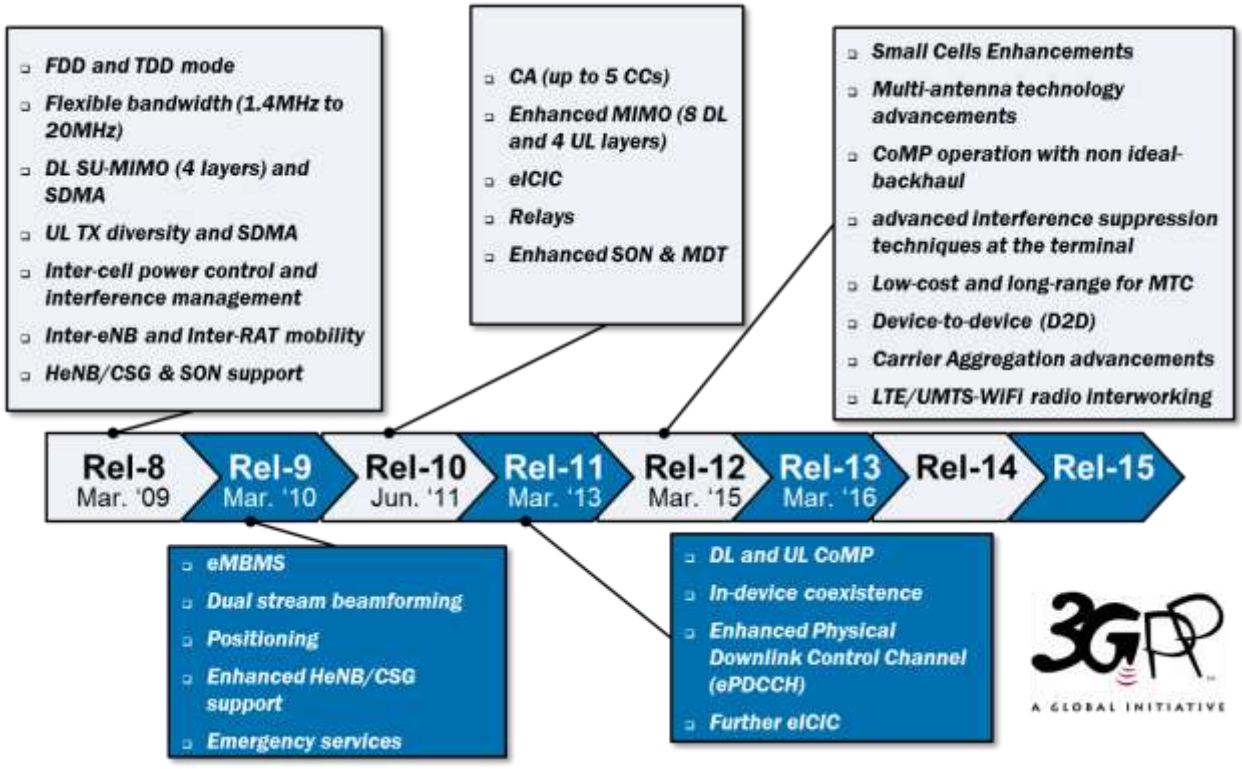


Figure 57 – LTE release timeline showing main enhancements on radio side (Source 3GPP [4])

Some of the main features already adopted in current LTE and LTE ADV operated networks**, such as Carrier Aggregation and MIMO are briefly described hereafter.**

<u>Carrier Aggregation</u>

Carrier Aggregation (CA) groups individual component carriers (CC) together to effectively increase the transmission bandwidth available. Component carriers can be located across the spectrum of LTE bands. CA allows to better utilize fragmented spectrum e.g. from 800MHz to 2.6GHz, delivering higher user peak data rates. Rel-10 specifies 100MHz of maximum aggregated bandwidth per user, comprising up to five 20MHz component carriers. Carrier aggregation can be used in FDD or TDD modes, and supports bandwidths of 1.4, 3, 5, 10, 15, and 20MHz. Different CA combinations are specified in Rel-10, Rel-11, and Rel-12 for both uplink and downlink.
There are three types of CA (Figure 58): intra-band contiguous, intra-band noncontiguous, inter-band noncontiguous, as explained and shown in Figure D. It should be noted that the RF-implementation complexity is vastly different with the first case being the least complex.

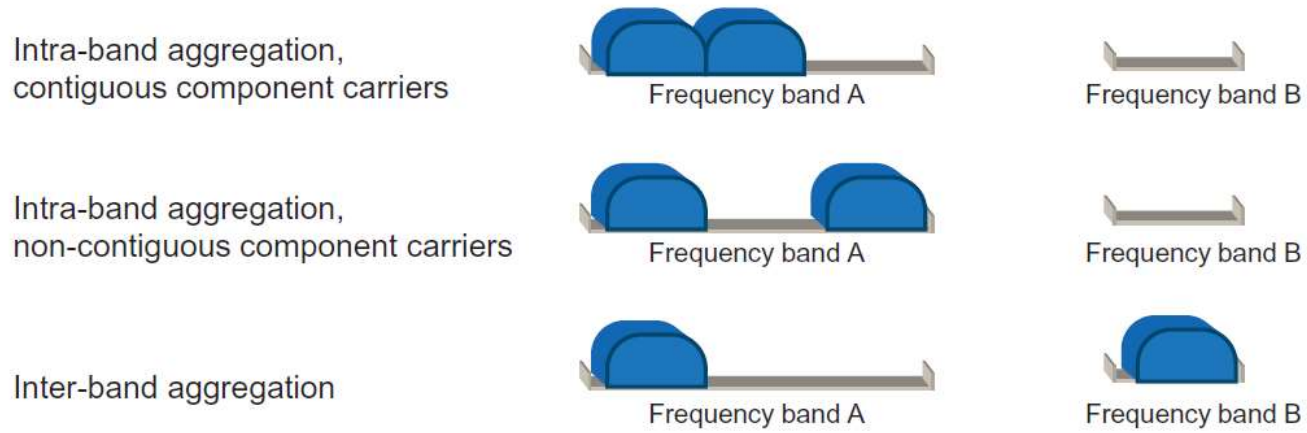


Figure 58 – Different types of Carrier Aggregation (Source 3GPP [4])

MIMO

As wireless communication links approach the limits of Shannon's capacity theorem, the spatial dimension must be exploited and, hence, spatial multiplexing with multiple antenna configurations must be adopted. Adopting spatial multiplexing with YxY MIMO can deliver a maximum theoretical Y increase in throughput without additional spectrum bandwidth. In situations where communication link reliability is important or poor signal conditions exist, then spatial diversity (transmit diversity) might be employed to obtain diversity gain and improve signal-to-interference-plus-noise-ratio (SINR).

LTE Rel-8 specified 2X2 and 4X4 MIMO with 4-layer transmission. Rel-10 extended this to 8X8 downlink MIMO, also called transmission mode 9 (TM9). Rel-12 and onwards explore ways to optimize 8X8 DL MIMO and include full-dimension MIMO (FD-MIMO), complemented by AAS (Adaptive Antenna Systems). It should be noted that these advanced techniques require multiple antennas at both the eNodeB and the mobile user equipment (UE). For example, deploying 8x8 MIMO requires eight antennas at the eNodeB and UE, as shown in Figure E. Because antenna spatial separation is needed, it may be difficult to integrate eight antennas in a small-form-factor mobile device like a smartphone. However, 4X4 MIMO is under deployment by several operators. Larger-form-factor devices like tablets and notebook PCs will have an easier time integrating eight antennas (Figure 59).

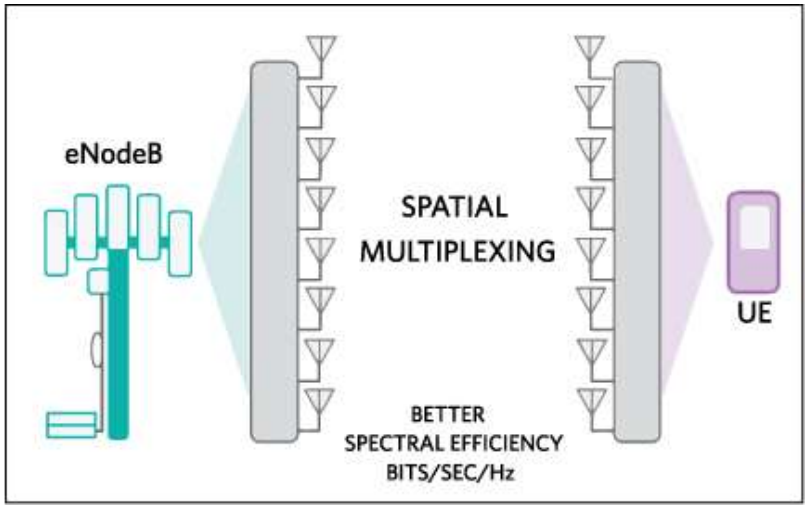


Figure 59 – Spatial multiplexing with 8X8 MIMO (Source 3GPP [4])

Much of MIMO features were completed in Rel-8 thru Rel-11. This included the development of Transmission Modes 1-9, code book structure, channel state information (CSI) feedback, demodulation reference signal (DM RS), downlink control information (DCI) format, and dynamic switching between SU-MIMO and MU-MIMO. Nine MIMO Transmission Modes (TM) are defined for LTE downlink (3GPP TS 36.211 and TS 36.213).

The TM for each UE is **configured semi-statically** via higher layer RRC signaling. The TM, summarized in Table 21, can be classified in two main categories:

- **modes that are used for diversity** in order to improve reliability and coverage (TM 2, 6 and 7) – orange color in table
- **modes** used **to improve the peak data rate** through the transmission of multiple parallel data layers (TM 3, 4, 5, 8 and 9) – green color in the table

DL TX mode	Reference TX scheme	3GPP Release
Mode 1	Single antenna transmission	LTE Rel.8
Mode 2	Transmit diversity	LTE Rel.8
Mode 3	Open loop spatial multiplexing	LTE Rel.8
Mode 4	Closed loop spatial multiplexing	LTE Rel.8
Mode 5	Multi-user MIMO	LTE Rel.8
Mode 6	Single Layer Closed loop precoding	LTE Rel.8
Mode 7	Single Layer beamforming	LTE Rel.8
Mode 8	Dual Layer beamforming	LTE Rel.9
Mode 9	Up to 8 layer transmission	LTE-A Rel.10

Table 21: MIMO TM (Source 3GPPP [4])

To improve spectral efficiency Rel-12 focuses on two CSI enhancements: (1) 4TX Precoding Matrix Index feedback, and (2) aperiodic feedback Physical Uplink Shared-Channel mode3-2. Rel-12 also begins introduction of FD-MIMO that unites AAS, 3D beamforming, and spatial multiplexing to deliver efficient spectrum utilization while increasing network capacity. The main features of FD-MIMO are shown in Figure 60, where antenna beams can be precisely and independently focused on different mobile users at different azimuth and elevation planes. In Rel-10 and Rel-11 the MIMO features specifically addressed eNodeB antenna directivity in the azimuth. Rel-12 explores ways to fully utilize the spatial domain.

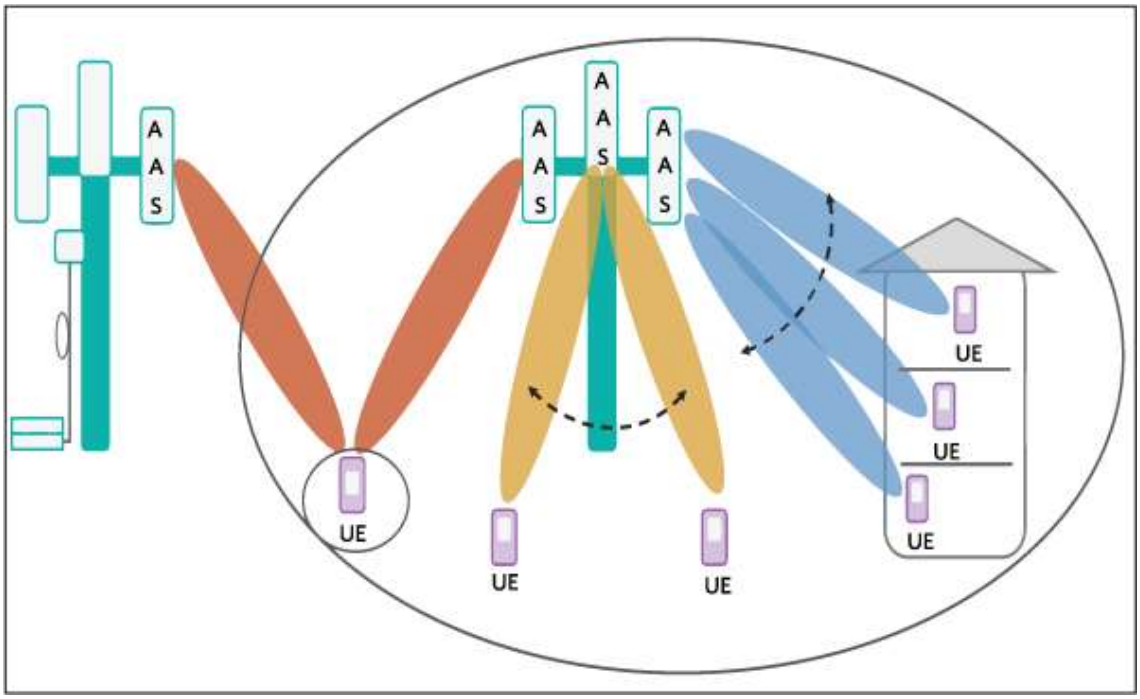


Figure 60 – Full-dimension MIMO (FD-MIMO) with 3D beamforming (Source 3GPP [4])

8 References

[1] AUTOPILOT, “D1.1 Initial Specification of IoT-enabledAutonomous Driving use cases“, 2017

[2] https://aioti-space.org/wp-content/uploads/2017/06/AIOTI-HLA-R3-June-2017.pdf

[3] AUTOPILOT, “D1.3 Initial IoT Self-organizing platform for self-driving vehicles “, 2017

[4] 3rd Generation Partnership Project (3GPP). [Online]. Available: http://www.3gpp.org/about-3gpp

[5] ITU Radiocommunication Sector. [Online]. Available: http://www.itu.int/en/ITU-R/Pages/default.aspx

[6] Afif Osseiran, Jose F. Monserrat, Patrick Marsch “5G Mobile and Wireless Communications Technology”, Cambridge University Press, June 2016

[7] A. Noll Barreto et al., "5G – Wireless Communications for 2020”, Journal of Communication and Information Systems, Vol 31, No 1 (2016)

[8] H. Tullberg et al., “METIS research and standardization: A path towards a 5G system”, 2014 IEEE Globecom Workshops (GC Wkshps)

[9] V. Frascolla et al., “MmWave use cases and prototyping: A way towards 5G standardization”, 2015 European Conference on Networks and Communications (EuCNC)

[10] V. Frascolla et al., “Challenges and opportunities for millimeter-wave mobile access standardisation”, 2014 IEEE Globecom Workshops (GC Wkshps)

[11] World Radiocommunication Conferences (WRC). [Online]. Available: http://www.itu.int/en/ITU-R/conferences/wrc/Pages/default.aspx

[12] Erik Dahlman et al., “4G, LTE-Advanced Pro and The Road to 5G, Third Edition”, Academic Press ©2016, ISBN:0128045752 9780128045756

[13] European Conference of Postal and Telecommunications Administrations. [Online]. Available: http://www.cept.org/

[14] Asia-Pacific Telecommunity (APT). [Online]. Available: http://www.aptsec.org/

[15] Inter-American Telecommunication Commission (CITEL). [Online]. Available: mission (CITEL). [Online]. Available: https://www.citel.oas.org/en/Pages/default.aspx

[16] The Internet Engineering Task Force (IETF®). [Online]. Available: https://www.ietf.org/

[17] Institute of Electrical and Electronic Engineers. [Online]. Available: https://www.ieee.org/standards/index.html

[18] Open Mobile Alliance. [Online]. Available: http://openmobilealliance.org/

[19] European Telecommunications Standards Institute. [Online]. Available: http://www.etsi.org/

[20] Global Certification Forum (GCF). [Online]. Available: http://www.globalcertificationforum.org/

[21] GSM Association. [Online]. Available: http://www.gsma.com/

[22] White Paper “4G Americas' Recommendations on 5G Requirements and Solutions”. [Online]. Available: http://www.5gamericas.org/en/resources/white-papers/

[23] “Towards 5G”. [Online]. Available: https://ec.europa.eu/digital-single-market/en/towards-5g

[24] 5G Forum (Korea) [Online]. Available: https://www.5gforum.org/eng

[25] Fifth Generation Mobile Communication Promotion Forum (5GMF) (Japan). [Online]. Available: http://5gmf.jp/en/

[26] “NGMN 5G White Paper”. [Online]. Available: http://ngmn.org/5g-white-paper/5g-white-paper.html

[27] 5G Infrastructure Association. [Online]. Available: https://5g-ppp.eu/

[28] Recommendation M.2083-0 (09/2015) IMT Vision - "Framework and overall objectives of the future development of IMT for 2020 and beyond". [Online]. Available: https://www.itu.int/rec/R-REC-M.2083

[29] Recommendation M.2012-2 (09/2015) “Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced)”. [Online]. Available: https://www.itu.int/rec/R-REC-M.2012

[30] Recommendation M.2070-1 (02/2017) "Generic unwanted emission characteristics of base stations using the terrestrial radio interfaces of IMT-Advanced". [Online]. Available: https://www.itu.int/rec/R-REC-M.2070/en
[31] Recommendation M.2071-1 (02/2017) "Generic unwanted emission characteristics of mobile stations using the terrestrial radio interfaces of IMT-Advanced". [Online]. Available: https://www.itu.int/rec/R-REC-M.2071/en
[32] ITU towards "IMT for 2020 and beyond". [Online]. Available: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx
[33] Radiocommunication Bureau, Circular Letter 5/LCCE/59 "Invitation for submission of proposals for candidate radio interface technologies for the terrestrial components of the radio interface(s) for IMT-2020 and invitation to participate in their subsequent evaluation". [Online]. Available: http://www.itu.int/md/R00-SG05-CIR-0059
[34] Common Patent Policy for ITU-T/ITU-R/ISO/IEC. [Online]. Available: http://www.itu.int/en/ITU-T/ipr/Pages/policy.aspx
[35] IMT-2020 submission and evaluation process. [Online]. Available: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/submission-eval.aspx
[36] NTT DOCOMO, INC., NEC Corporation, "Revised Work Item Description: Dual Connectivity for LTE", RP-141266. [Online]. Available: http://www.3gpp.org/ftp/tsg_ran/tsg_ran/TSGR_65/Docs/
[37] 3GPP TR 22.861 "FS_SMARTER - massive Internet of Things". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[38] 3GPP TR 22.862 "Feasibility study on new services and markets technology enablers for critical communications". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[39] 3GPP TR 22.863 "Feasibility study on new services and markets technology enablers for enhanced mobile broadband". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[40] 3GPP TR 22.864 "Feasibility study on new services and markets technology enablers for network operation". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[41] 3GPP "TR 22.886 Study on enhancement of 3GPP support for 5G V2X services". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[42] 3GPP TS 22.261 "Service requirements for next generation new services and markets". [Online]. Available: http://www.3gpp.org/DynaReport/22-series.htm
[43] 3GPP TR 23.977 "Study on Architecture for Next Generation System". [Online]. Available: http://www.3gpp.org/DynaReport/23-series.htm
[44] 3GPP TR 33.899 "Study on the security aspects of the next generation system". [Online]. Available: http://www.3gpp.org/DynaReport/33-series.htm
[45] 3GPP TR 28.802 "Study on Management Aspects of Next Generation Network architecture and features. [Online]". Available: http://www.3gpp.org/DynaReport/28-series.htm
[46] 3GPP TR 28.800 "Study on Management and Orchestration Architecture of Next Generation Network and Service". [Online]. Available: http://www.3gpp.org/DynaReport/28-series.htm
[47] 3GPP TR 28.801 "Study on management and orchestration of network slicing for next generation network". [Online]. Available: http://www.3gpp.org/DynaReport/28-series.htm
[48] 3GPP TR 38.913 "Study on Scenarios and Requirements for Next Generation Access Technologies". [Online]. Available: http://www.3gpp.org/DynaReport/38-series.htm
[49] Jordi Calabuig et al., "5th generation mobile networks: A new opportunity for the convergence of mobile broadband and broadcast services", IEEE Communications Magazine (Volume: 53, Issue: 2, Feb. 2015)
[50] Theodore S. Rappaport et al., "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!", IEEE Access (Volume: 1), 10 May 2013
[51] ZigBee Alliance. Available Online: http://www.zigbee.org/
[52] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 packets over IEEE

802.15.4 networks, IETF RFC 494
[53] A. Dunkels, J. Vasseur, IP for Smart Objects, IPSO Alliance White Paper 1
[54] Bluetooth Low Energy. http://www.bluetooth.com/Pages/Low-Energy.aspx/
[55] Rohde&Schwarz, "Narrowband Internet of Things Wgitepaper". Available online: https://cdn.rohde-schwarz.com
[56] "FI-WARE NGSI-9 Open RESTful API Specification", FIWARE Forge, 2017, to be retrieved via, https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-9_Open_RESTful_API_Specification
[57] "FI-WARE NGSI-10 Open RESTful API Specification", FIWARE Forge, 2017, to be retrieved via, https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-10_Open_RESTful_API_Specification
[58] "Functional Architecture", OneM2M, TS-0001-V2.10.0, August 2016, to be retrieved via: http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf.
[59] "FI-WARE NGSI-9 Open RESTful API Specification", FIWARE Forge, 2017, to be retrieved via, https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-9_Open_RESTful_API_Specification
[60] "FI-WARE NGSI-10 Open RESTful API Specification", FIWARE Forge, 2017, to be retrieved via, https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-10_Open_RESTful_API_Specification
[61] "Functional Architecture", OneM2M, TS-0001-V2.10.0, August 2016, to be retrieved via: http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf.
[62] SAE Information Report: (J3016) "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems", 2014
[63] Watson IoT Reference Pages: https://console.ng.bluemix.net/docs/services/IoT/iotplatform_overview.html#about_iotplatform
[64] MQTT: http://mqtt.org
[65] ETSI EN 302 665 V1.1.1 "Intelligent Transport Systems – Communications Architecture" (2010-09)
[66] 802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[67] http://www.3gpp.org/release-14
[68] ETSI EN 302 636-4-1 V1.2.0, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality , 2014
[69] ETSI EN 302 637-2 V1.3.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, 2014
[70] ETSI EN 302 637-3 V1.2.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, 2014
[71] ETSI EN 302 663 V1.2.1 Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band, 2013
[72] ISO 11898 CAN Road vehicles -- Controller area network (CAN) Part 1: Data link layer and physical signalling, 2015
[73] IETF RFC 1122, Requirements for Internet Hosts -- Communication Layers, 1989
[74] IETF RFC 793, Transmission Control Protocol, 1981
[75] IETF RFC 768, User Datagram Protocol, 1980

[76] https://www.qualcomm.com/invention/technologies/lte/advanced-pro/cellular-v2x
[77] http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/?Itemid=277
[78] http://www.3gpp.org/images/PDF/R13_IOT_rev3.pdf
[79] http://www.3gpp.org/release-13
[80] https://www.qualcomm.com/invention/technologies/lte/advanced-pro/lte-iot
[81] IEEE 802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks
[82] Specification of the Bluetooth System, Core Version 4.2, 2014, available on: https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439
[83] ETSI EN 302 665 ITS Communication Architecture, v1.1.1 (2010-09)
[84] ISO TS 19091:2017 "Intelligent transport systems -- Cooperative ITS -- Using V2I and I2V communications for applications related to signalized intersections"
[85] ETSI - EN 302 895 - INTELLIGENT TRANSPORT SYSTEMS (ITS); VEHICULAR COMMUNICATIONS; BASIC SET OF APPLICATIONS; LOCAL DYNAMIC MAP (LDM), 2014
[86] ETSI TR 102 638 V1.1.1 (2009-06) Technical Report Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions
[87] ETSI TR 103 299 Intelligent Transport System (ITS); Cooperative Adaptive Cruise Control (C-ACC); Pre-standardization study
[88] ETSI TR 103 298 Intelligent Transport Systems (ITS); Platooning; Pre-standardization study
[89] ETSI TS 103 324 Intelligent Transport Systems (ITS); Cooperative Observation Service -
[90] ETSI TS 103 301 V1.1.1 (2016-11), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
[91] https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf
[92] http://www.3gpp.org/release-14
[93] http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/
[94] http://the-mobile-network.com/2016/03/3gpp-announces-ran-work-programme-for-r14/
[95] http://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14
[96] ftp://ftp.3gpp.org/TSG_RAN/TSG_RAN/TSGR_73/Docs/RP-161894.zip
[97] http://www.3gpp.org/specifications/releases/68-release-12
[98] AUTOPILOT Task 1.2, "Autopilot_T1.2_FunctionalRequirements.xlsx"available on: https://service.projectplace.com/pp/pp.cgi/r1512593890
[99] "5G Automotive Vision"edited by ERTICO, European Commission and 5GPP", available on: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf
[100] AUTOPILOT Task 1.4 "170503_Autopilot_T1.4_CommunicationRequirements.xlsx", available at URL: https://service.projectplace.com/pp/pp.cgi/r1339416605
[101] 3GPP TS 23.502 V0.6.0 (2017-08) System Architecture for the 5G System; Stage 2, http://www.3gpp.org/ftp/specs/archive/23_series/23.501/
[102] 3GPP TS 23.502 V0.6.0 (2017-08) Procedures for the 5G System; Stage 2 (Release 15), http://www.3gpp.org/ftp/specs/archive/23_series/23.502/
[103] 5GAA white paper on comparison between LTE-V2X and IEEE 802.11p, please see: http://5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf
[104] ETSI ES 202 663 "ITS European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band"
[105] EN 302 663 "ITS Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band"
[106] Source: http://www.4gdekking.nl/, September 2016
[107] http://onem2m.org/application-developer-guide/architecture
[108] oneM2M: http://www.onem2m.org/about-onem2m/why-onem2m
[109] ETSI EN 302 636-5-1 v1.2.1: Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol

[110] https://www.fiware.org/ - FIWARE is platform specification maintaned by the FIWARE community
[111] https://www.ibm.com/watson/ Watson IoT platform is a product from IBM
[112] The European Research Cluster on the Internet of Things (IERC) (http://www.internet-of-things-research.eu).
[113] O. Vermesan, P. Friess, et. al. Digitizing the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds. River Publisher vol. 49, 2016.
[114] Report on Internet of Things Applications, AIOTI WG01, AIOTI/IERC, October 2015.
[115] Report on Smart mobility, AIOTI WG09, October 2015. (https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020).
[116] IETF, RFC 791 Internet Protocol Specification, September 1981
[117] IETF, RFC 2460 IPv6 Specification, published in December 1998
[118] ETSI EN 302 208 Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W and in the band 915 MHz to 921 MHz with power levels up to 4 W, 2012
[119] Choi, Hong et al, Transmission of IPv6 Packets over Near Field Communication draft-ietf-6lo-nfc-07, 2017 available at: https://tools.ietf.org/html/draft-ietf-6lo-nfc-07
[120] OneM2M, TS-0001-V2.10.0 "Functional Architecture" , August 2016, to be retrieved via: http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf)
[121] 3GPP TR 25.913 Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN), 2009