5G PPP H2020 ICT-18-2018 Projects

White Paper

5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors

- Challenges and Opportunities

Version 1.0, October 2020

Executive Summary

The European Commission's (EC) vision to launch initial 5G services by 2020 and to cover major urban areas and main transport paths by 2025 [1] is starting to take shape. This EC action plan has set forth a clear roadmap for public and private investment into 5G infrastructure along the main EU transport paths, to enable a series of advanced Cooperative, Connected and Automated Mobility (CCAM) use cases and services across Europe. Nowadays, only basic safety features are supported by mass production vehicles (e.g. traffic information, local hazard warnings). The 5G Automotive Association (5GAA), representing the leaders of both the automotive and telecommunication industries, projects that advanced Autonomous Driving (AD) use cases, such as Highway Pilot and Cooperative Manoeuvres, will be introduced to mass production vehicles, equipped with 5G / 5G-V2X (Vehicle to Everything) capabilities, starting from 2026 onwards [2].

The provision of CCAM functionality over 5G connectivity poses a number of technical, organizational, business and administrative challenges in highway and national border (corridors) environments. The 5G Public Private Partnership (5G PPP) has commissioned three international innovation projects under the European research programme H2020[1] to investigate exactly these points. The three projects funded under the H2020-ICT-18-2018 action, namely 5GCroCo, 5G-CARMEN and 5G-MOBIX, are tasked with performing 5G-enabled AD trials at national border conditions and draw useful insights regarding the challenges and opportunities of provisioning 5G-enabled CCAM services in cross-border conditions. This white paper is a joint effort of the three projects and presents preliminary results, based on currently available technological enablers with the capacity to mitigate and/or resolve the abovementioned challenges.

The white paper introduces the scope, use cases, trial sites and particularities of each of the three corridor projects. It also identifies and elaborates on the main concerns and challenges arising from deploying advanced CCAM use cases at regional borders. This analysis takes into consideration technological, administrative, security and legislatorial aspects. From a networking point of view, it is highlighted that ***Service and Session continuity*** as well as ***Data routing (Home routing (HR), Local break-out (LBO))*** solutions**,** when moving across neighbouring networks, play a critical role in meeting the specified requirements of advanced CCAM use cases. This entails significant -currently unresolved- challenges, as the ***inter-PLMN Network Handover*** due to cross-border mobility, introduces complex connectivity, configuration and routing aspects. Consequently, the network management including ***radio planning/optimization***, ***frequency spectrum allocation, roaming configuration***, etc. must be considered, as it plays an increasingly important role in CCAM service provisioning at the borders.

The three corridor projects have investigated a multitude of potentially viable solutions to address the above identified challenges and will progress with the testing of the most prominent ones in the field during their scheduled trials. The proper deployment, configuration and use of ***edge computing***, depending on the specific geographical and morphological cross-border conditions as well as on the type of CCAM use case supported, has emerged as one of the key enabling factors to reduce end-to-end latency and to provide the necessary computational resources where and when needed. Special attention has to be given to the edge computing system interconnection and integration into an automated ***service management and orchestration architecture*** coupled with the 5G systems. Careful, per case ***data routing (e.g. LBO)*** and specialized ***5G features available in latest 3GPP releases*** help mitigate the effects on mobility interruption and contribute towards service and session continuity, while the use of ***direct Vehicle to Vehicle (V2V) communications (sidelink)*** offers an alternative connectivity option to ease the effects of network-based communication interruption.

Moreover, the use of ***Quality of Service (QoS) prediction*** mechanisms can have significant benefits in mitigating the mobility interruption effects by allowing pre-emptive actions on behalf of the service provider (e.g. pre-allocation of resources). The enabler with potentially the strongest effect on connectivity would be the creation of a thorough (***network management) collaboration framework*** allowing synchronized approaches and a more efficient network governance all over Europe, thus mitigating several challenges

---

[1] https://ec.europa.eu/programmes/horizon2020/en

originating from a nationally-oriented telecommunication landscape. Nonetheless, the collaboration of all CCAM stakeholders across borders is essential for a ***consistent ecosystem*** and to overcome the obstacles behind topics such as ***protocol interoperability, security, spectrum harmonization and data management***.

Finally, the development and fostering of viable and appealing ***5G-CCAM business models*** extends the CCAM ecosystem and drives the faster adoption and acceptance of cross-country CCAM solutions. All three projects emphasize the fact that besides the technical challenges, there is a strong need for further EU steering in terms of ***aligned and applied regulation, security and privacy, as well as stakeholder integration.*** Currently private and public projects face uncertainty and/or considerable non-technical issues when attempting to deploy such services across regional borders. This in turn has adverse effects on potential business motives, further rollouts of 5G and advanced CCAM solutions, and thus the European economy.

Table of Contents

1 Introduction....8
2 Overview of 5G PPP ICT-18 corridor projects 10
2.1 5GCroCo....10
2.1.1 Use cases....10
2.1.2 Corridors and trials 11
2.2 5G-CARMEN 13
2.2.1 Use cases....13
2.2.2 Corridors and trials 14
2.3 5G-MOBIX....15
2.3.1 Use cases....15
2.3.2 Corridors and trials 17
2.4 ICT-18 Roadmap 18
3 Cross-border Challenges & Considerations....20
3.1 Cellular coverage and radio access aspects (Ch.1) 22
3.1.1 Radio Planning and Cellular Network coverage at the borders 22
3.1.2 Inter-PLMN Handover....23
3.1.3 Network Reselection....24
3.2 Service and Session continuity aspects (Ch.2) 24
3.2.1 Service Continuity and End-to-End QoS Across Borders 24
3.2.2 Keeping Short End-to-End Routes as the Vehicle Moves 25
3.3 MNO collaboration & Data Plane routing (Ch.3)....26
3.3.1 Roaming Impact to Service and Session Continuity....26
3.3.2 Need for Local Breakout support across MNO domains....27
3.4 Data Management & Protection (Ch.4)....27
3.4.1 Data Management 27
3.4.2 Security/Privacy and Regulatory compliance....28
3.5 Non-functional Aspects & Business Enablers (Ch.5)....29
3.5.1 Protocol Interoperability 29
3.5.2 Spectrum Harmonization 29
3.5.3 Road and Traffic related regulation....30
3.5.4 Business models for cross-border environments 30
4 Technological Enablers for Cross Border Solutions 32
4.1 Edge Computing 32
4.1.1 Session/service continuity....32
4.1.2 Connecting MEC to the 3GPP network....33
4.1.3 Collaborating Systems: MEC – 5G – NFV Management and Orchestration....34
4.2 QoS Prediction....36
4.3 V2X Message routing 36
4.3.1 Sidelink....36
4.3.2 Cross-border Message Broker 37
4.4 MNO Collaboration Framework 38
4.5 Business & Deployment Enablers....39
4.5.1 Developing and fostering 5G-CCAM business models....39
4.5.2 Strategic Deployment Agenda (SDA) for CCAM in Europe....39
4.6 Standardization, security and regulation alignment....40
4.6.1 Cross-Border Regulatory Framework 40
4.6.2 Data Ownership and Data Exchange....40
4.6.3 Cyber-Security Measures....41
4.7 Challenges / Solutions Overview 41
5 Conclusions....43
References....45
List of Contributors 47
Contributing 5G PPP Projects 48
Acknowledgements....48

List of Figures

Figure 1: 5GCroCo Use cases: a) Tele-operated Driving, b) HD mapping and c) ACCA 11

Figure 2: Map of the 5GCroCo Corridor 12

Figure 3: 5G-CARMEN use cases: a) Cooperative Lane Merging, b) situation awareness and c) green driving 14

Figure 4: 5G-CARMEN trial locations 15

Figure 5: 5G-MOBIX Cross Border Corridors in a) Spain - Portugal (ES-PT) and b) Greece - Turkey (GR-TR) 18

Figure 6: High-level roadmap of the ICT-18 projects' phases 19

Figure 7: End-to-end data plane between vehicle and MEC service instance 20

Figure 8: A vehicle communicating with an Edge Server that is accessed via a far away gateway (HR concept) 25

Figure 9: Mapping of 5G Core to 4G Evolved Packet Core (EPC) terms 33

Figure 10: Abstract view of integrated 5G, MEC and NFV MANO systems [20] 35

List of Tables

Table 1: 5G-MOBIX User Story classification 16

Table 2: Key Challenges for CCAM service provisioning in cross-border environments 21

Table 3: Overview of challenges and potential solutions for effective cross-border CCAM service provisioning over 5G networks 42

List of Acronyms and Abbreviations

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5GC	5G Core
5G PPP	5G Private Public Partnership
5GAA	5G Automotive Association
5GS	5G System
ACCA	Anticipated Cooperative Collision Avoidance
AD	Automated Driving
ADAS	Advanced Driver Assistance System
AF	Application Function
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
AS	Application Server
BSA	Back situation awareness
BW	Bandwidth
C-ITS	Cooperative ITS
C-V2X	Cellular-V2X
CAM	Cooperative Awareness Message
CAPEX	Capital Expenditure
CBC	Cross-Border Corridor
CCAM	Cooperative Connected Automated Mobility
CCMS	C-ITS security Credential Management System
CEF	Connecting Europe Facilities
CLM	Cooperative Lane Merging
CPM	Cooperative Perception Message
CUPS	Control User Plane Separation
D2D	Device to Device
DENM	Decentralized Environmental Notification Message
DSM	Digital Single Market
EC	European Commission
ECC	Electronic Communications Committee
ECU	Electronic Control Unit
EDM	Edge Dynamic Map
eMBB	Enhanced mobile broadband

eNB	Evolved Node B
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
gNB	Next generation NodeB
HCM	Harmonized Coordination Model
HD	High Definition
HO	Handover
HR	Home Routing
HSS	Home Subscriber Server
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMT	International Mobile Telecommunication
IP	Internet Protocol
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LBO	Local Break Out
LIDAR	Light Detection And Ranging
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	(Multi-Access/Mobile) Edge Computing/Cloud
MEC PF	MEC Platform
MEC PF Mgr	MEC Platform Manager
MM	Mobility Management
MME	Mobility Management Entity
mmW	millimeter Wave
MNO	Mobile Network Operator
MQTT	MQ Telemetry Transport
MU-MIMO	Multi-User- Multiple Input Multiple Output
NAT	Network Address Translation
NFV	Network Functions Virtualization

NR	New Radio
NSA	Non Standalone
NWDAF	Network Data Analytics Function
OBU	On Board Unit
OEM	Original Equipment Manufacturers
OPEX	Operational Expenditure
PC5	Proximity Services (ProSe) direct Communication interface 5
PLMN	Public Land Mobile Network
PDN	Packet Data Network
PDU	Protocol Data Unit
PGW	Packet Gateway
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RSI	Roadside Infrastructure
RSPG	Radio Spectrum Policy Group
RSU	Roadside Unit
SA	Standalone
SAE	Society of Automotive Engineers
SBA	Service-Based Architecture
SDA	Strategic Deployment Agenda
SDN	Software Defined Networking
SGW	Serving Gateway
SINR	Signal to interference and Noise Ratio
SIPTO	Selective IP Traffic Offload
SLA	Service Level Agreement
SMF	Session Management Function
SSC	Session and Service Continuity
SW	Software
TCP/IP	Transmission Control Protocol / Internet Protocol
ToD	Tele-operated Driving
TS	Trial Site
UDP	User Datagram Protocol
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communication
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VRU	Vulnerable Road User
VSSS	Vehicle sensors and state sharing
WG	Working Group

1 Introduction

Even if a clear date for a global commercial launch of SAE[2] Level 4 and above autonomous driving services has not been established yet [3], various tests are already ongoing in different parts of the world. In this context, the external wireless connectivity represents a powerful extension to the embedded sensors already used by cars. In fact, all Original Equipment Manufacturers (OEMs) agree to consider the connectivity as a must for autonomous driving levels 4 or 5. Interestingly enough, the role of connectivity as a further Advanced Driving Assistance System (ADAS) functionality has been found to be valuable already from autonomous driving SAE level 1. As in the case of previous enabling technologies (e.g. such as the radar), connectivity can provide an added value to increase safety and comfort not only for autonomous driving vehicles, but also for humans (drivers and Vulnerable Road Users (VRUs)). In particular, the role of the *cellular* connectivity for the automotive sector is forcefully emerging, as analysed in e.g. [4].

Meeting some of the automotive industry’s requirements was possible since the fourth-generation (4G) cellular systems [5], that relied on the Long-Term Evolution (LTE) standard. However, it is important to point out the added-value of the fifth-generation (5G) cellular connectivity for the automotive sector. Besides the huge advantages in terms of additional bandwidth, extreme reliability and extremely low end-to-end latency, 5G offers advanced features which will revolutionize customers’ mobility and experience.

The enhanced features of 5G New Radio (NR) [6] already help in this direction as the automotive’ s vertical sector requirements have been taken into account since the design phase of NR and led to a more flexible radio framework capable of supporting a multitude of diverse users while providing a number of significant advantages compared to 4G radio. 5G NR’s significant enhancements in areas like flexibility, scalability, latency and efficiency [6] contribute significantly to the effective service provisioning of stringent CCAM applications. The enhanced physical layer, supporting scalable numerology in combination with the new spectrum used for NR, allows for a much more flexible use of the spectrum, with scalable frames and variable transmission slots that significantly reduce the radio latency. Moreover, the possibility to utilize both traditional cellular communication bands (< 6 GHz) as well as the mmW bands (> 20 GHz) provides extreme capacity capabilities, enabling new automotive services (see Section 2 use cases). On top of that Advanced Beamforming and Multi-User- Multiple Input Multiple Output (MU-MIMO) techniques enable extreme beam directivity contributing to increased Signal to Interference and Noise Ratio (SINR) and the capability for increased bitrates through multiple, simultaneous beams (spatial reuse), addressing multiple users in specific areas.

Another key feature for 5G networks is the support of network slicing i.e., the support of multiple logical networks over the same physical infrastructure. This allows 5G networks concurrently serve the needs of different services that may have different network requirements, in terms of reliability, delay, throughput, security etc.

Using network slicing, the scalable numerology and the available bandwidth in different bands, various types of CCAM applications may be supported at the same time, (e.g. supporting a reliable and low latency remote driving application at sub-6 GHz BW, while at the same time supporting platooning with video streaming over multiple trucks with mmW and beam steering). This notion of service differentiation and customizable *Quality of Service* (QoS) via dedicated network slices in combination with additional novel technological enablers such as edge computing, precise positioning and Cellular V2X (C-V2X) communications enable the desired level for service provisioning even for the most extremely demanding CCAM applications and services that will operate under demanding environments such as geographical cross-border areas.

---

[2] Society of Automotive Engineers (SAE): Levels of Autonomous driving, https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

This enhanced performance delivered by 5G connectivity has the potential to significantly impact several key aspects of mobility and the automotive industry in general, such as the capabilities of *autonomous driving, infotainment/entertainment aspects* as well as *drivers' and VRUs' safety* (such as pedestrians, motorcyclists, cyclists). The extreme low latencies and high reliabilities offered by 5G networks along with the availability of huge computational resources at the edge network and the assistance of intelligent Road Side Infrastructure / Units (RSI/RSU), immediately accessible over direct communication protocols (e.g. C-V2X), will transform the autonomous driving landscape. These will enable the realization of stringent use cases such as remote driving, autonomous lane merging & overtaking, obstacle avoidance and platooning, to name a few.

Moreover, the extreme bandwidth, ultra-low latency and high reliability of 5G are also key enablers for the increased Quality of Experience (QoE) of the passengers when streaming high-quality infotainment/entertainment services. Passengers' increased expectations will include full-blown multimedia entertainment (e.g. a 4k movie) during their daily commute, as well as a connection with minimal interruptions, which delivers the level of speed and latency needed for high-quality video streaming, no matter their location or velocity. A 5G-guaranteed high throughput and low latency service instantiated via dedicated network slices, combined with enhanced content caching at the edge of the radio access network, will be capable of meeting such requirements.

Thanks to the assistance of 5G cellular networks and edge computing infrastructures, the drivers' awareness about upcoming unexpected hazardous situations can be improved by increasing the dispatching area of vehicular information, thus enhancing the drivers' safety. Finally, the increased collaborative environmental awareness achieved through the ultra-fast exchange of information among the various vehicles and VRUs will identify every single road user, even in "blind-spots" and will update accordingly all connected maps applications and user interfaces while also providing valuable information to the autonomous driving mechanisms, hence improving the safety of all VRUs.

As it is the vision of the European Commission to provide such advanced CCAM services along the major European transport paths/corridors by 2025 [1] mainly enabled by 5G networks, smooth and uninterrupted CCAM service provisioning must be guaranteed across the entire corridors irrespective of the network provider, vehicle and equipment manufacturers, cloud/edge and application providers and On Board Units (OBU)/RSI developers. As it can be understood, the most challenging environment in this case become the national borders between countries where interoperability and smooth service migration between the neighbouring networks, infrastructures and applications need to be guaranteed. Addressing advanced CCAM scenarios at the borders is particularly important because they feature significant technological barriers related to cellular network coverage and service continuity, thus representing a challenge for the widespread adoption of 5G-enabled CCAM services.

This white paper provides a comprehensive overview about the ongoing activities in the scope of the three EU-funded projects supporting 5G-enabled CCAM in ***cross-border scenarios***, namely 5G-CARMEN[3], 5GCroCo[4] and 5G-MOBIX[5]. The whitepaper is structured as follows: in Section 2, we provide an overview of the ongoing 5G PPP Phase III corridor projects dealing with cross-border CCAM applications. In Section 3, we detail the specific challenges of cross-border environments, which will be mapped against the envisioned solutions/enablers provided by 5G systems in Section 4. Finally, in Section 5 we draw our conclusions.

---

[3] https://5gcarmen.eu/

[4] https://5gcroco.eu/

[5] https://www.5g-mobix.com/

2 Overview of 5G PPP ICT-18 corridor projects

In this section, we provide an overview of the three ongoing cross-border projects of the 5G PPP Phase III (namely, 5GCroCo, 5G-CARMEN and 5G-MOBIX), highlighting the use cases under study and the status of the project activities, focusing specifically on the planned tests.

2.1 5GCroCo

2.1.1 Use cases

5GCroCo aims at validating three CCAM use cases in cross-border situations. The use cases have been selected to ensure that they allow testing the need for high performance 5G features and the need for cross-border operation. The use cases of 5GCroCo are complementary of each other, focusing on different 5G features.

A. Tele-operated Driving (ToD)

ToD is defined as the remote control or support of automated vehicles by a human over a mobile radio network, as illustrated in Figure 1a. ToD in the context of Automated Driving (AD) can be deployed in different traffic situations, such as

- **Non-responding driver:** even though Level 4 automated driving vehicles are not able to handle every situation, the driver is neither required to be always ready to regain control as with Level 3 autonomous driving. In the case that the driver does not respond to the request of taking over control, an operator in a ToD command centre can take over control.
- **Handling in special areas:** a vehicle could be remotely operated in special situations or areas. For example, at freight centres, a Level 3 truck could be remotely handled by a tele-operator in order to allow the driver to take his recreation time during the period of loading or unloading freight.
- **Undefined traffic situations**: in the event of a highly automated driving enabled vehicle (Level 4) not capable to handle a certain traffic situation, ToD can remotely involve a human operator to handle the situation. This could include temporarily taking over control to resolve the situation or proposition of a new route.

Camera information, together with data from other sensors should be provided to the tele-operator with low latency, high reliability and high data rates to allow safe tele-operation. Cross-border operations impose additional challenges for lag-free data transmission when handing over between Mobile Network Operators (MNOs). Also, service continuity can be supported by a method to predict expected changes in the QoS. 5GCroCo is testing and trialling 5G solutions to address the abovementioned challenges.

B. High definition (HD) map generation and distribution for automated driving

Intelligent and dynamic HD maps, exemplified in Figure 1b, provide highly accurate position of dynamic and static objects which enable tactical and operational planning by an autonomously or semi-autonomously driven vehicle. Such maps could be constructed by smartly fusing all the available data from different sources at and along the roads, e.g. the sensor data shared by the vehicles, data shared by the road infrastructure, or by map content providers, among others.

The main challenge for HD mapping is the on-time availability of up-to-date HD map information before entering a specific area. This corresponds to the minimum throughput requirements for the communication network. Again, here the combination of data rate, data quality, seamless coverage and latency is where 5G gives the desired solution. Information must not be too old and, therefore, cannot be uploaded too much in advance. On the other hand, information exchange needs to start early enough to be finalized with no remaining errors before entering the area of interest.

5GCroCo is testing 5G technology for exchanging the data required to generate the HD maps between the vehicles, data servers, and map providers. The focus is on using sensor information, harvested in real time from cars, to update a cloud-based HD map.

C. Anticipated Cooperative Collision Avoidance (ACCA)

At high speed, a typical stand-alone sensing system (e.g., radars, cameras, lidars) will not have sufficient and safe means to detect and localize dangerous events on the road in all situations and with sufficient level of anticipation. For instance,

- Temporarily static events like traffic jams.
- High deceleration, emergency braking, or unexpected manoeuvre of vehicles ahead (with or without visibility for the ego vehicle).
- Cut-in anticipation, e.g., when a vehicle suddenly comes in from another lane.

In such situations, a late detection of a dangerous event will trigger a hard braking and, possibly, a collision, depending on friction conditions (among other things). ACCA techniques (depicted in Figure 1c) can solve this kind of situations by allowing cooperation among vehicles. The cooperative vehicles (or the road side infrastructure, for example) will upload a set of information such as status (e.g., position, speed, acceleration), detected events, and some sensor data (camera/radar streams, or any other information based on a standardized format) to create an off-board dynamic map which handles and consolidates all collected information based on a known road topology. Again, this use case requires recently updated information and very high reliability that corresponds to low delay and very low packet loss ratio to be provided by the communications network.

In particular, 5GCroCo is defining, test and trial cooperative solutions to anticipate the detection and localization of dangerous events and to facilitate smoother and more homogeneous vehicle reaction.

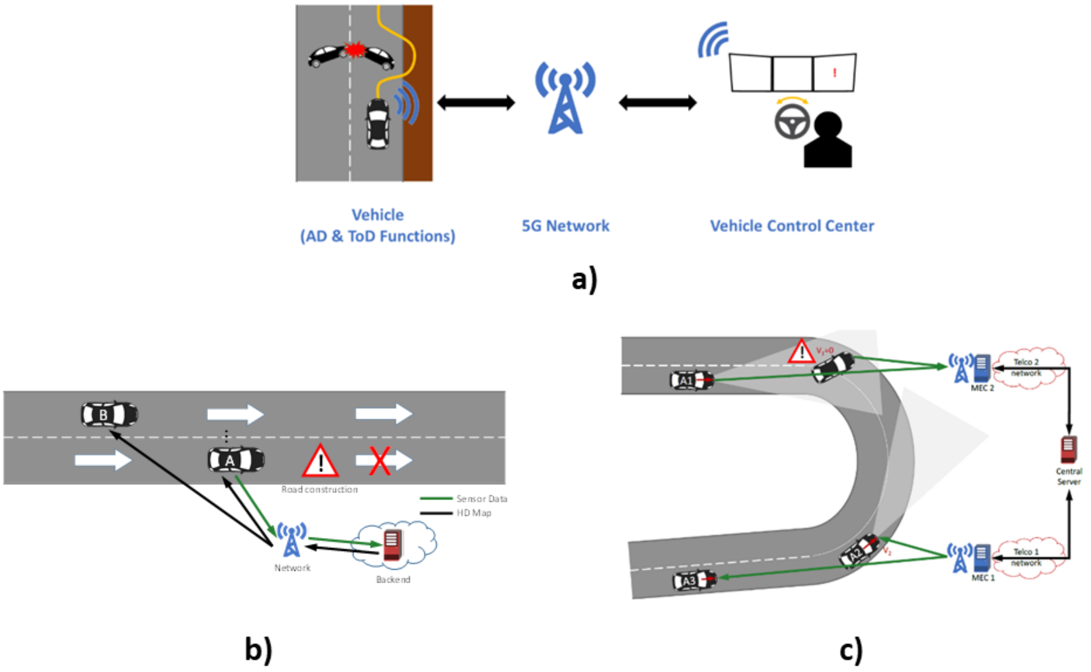


Figure 1: 5GCroCo Use cases: a) Tele-operated Driving, b) HD mapping and c) ACCA

2.1.2 Corridors and trials

Trials at both large and small scale will be conducted in 5GCroCo to validate the 5G technologies for the three use cases described.

Large-Scale Cross-Border Corridor

5GCroCo has the overall aim to trial all the use cases at the European cross-border corridor which connects cities in France, Germany, and Luxembourg, and is part of the pan-European network of 5G corridors facilitated through several regional agreements[6] . An overview of the location and use cases addressed is depicted in Figure 2.

These agreements allow Europe to count with hundreds of kilometres of motorways where tests can be conducted up to the stage where a car can drive autonomously with a driver present (Automated Driving Level 3 [8]). These corridors receive the support of the European Commission as part of its 5G Action Plan, which aims at ensuring commercial deployment of 5G technologies by the end of this decade [1].

5GCroCo aims at trialling all use cases on a cross-border road, on the France/Germany and Germany/Luxembourg border in summer 2020 and fall 2021. The large trials are planned to take place in two rounds. The first round is planned in Q4 2020. The final trail round is planned in summer 2021.

Small Scale Tests and Trials

As rolling out such trials is very complex, a good step-by-step preparation is necessary. 5GCroCo has several trial sites called “small scale” trial sites (as shown in Figure 2). Indeed, these sites aim at preparing all use cases and user stories as a first step to check that everything is validated and working before continuing at large scale. This allows also dealing with all potential problems and issues we could be facing and allows to collect best practice. 5GCroCo has small scale site in Germany, France, Spain and Sweden. The trials on the small-scale site were initially planned for summer 2020 (Q2/Q3).

These trials are deployed in a test track in Montlhéry-UTAC (South of Paris, France), two in Germany (in a section of Motorway A9 5G-ConnectedMobility test site and a test-site in the city centre of Munich), one in the city of Barcelona (Spain) where a cross-border city setting will be emulated and one in Sandhult near Göteborg (Sweden) on the AstaZero test track, where also virtual border-crossing is implemented.

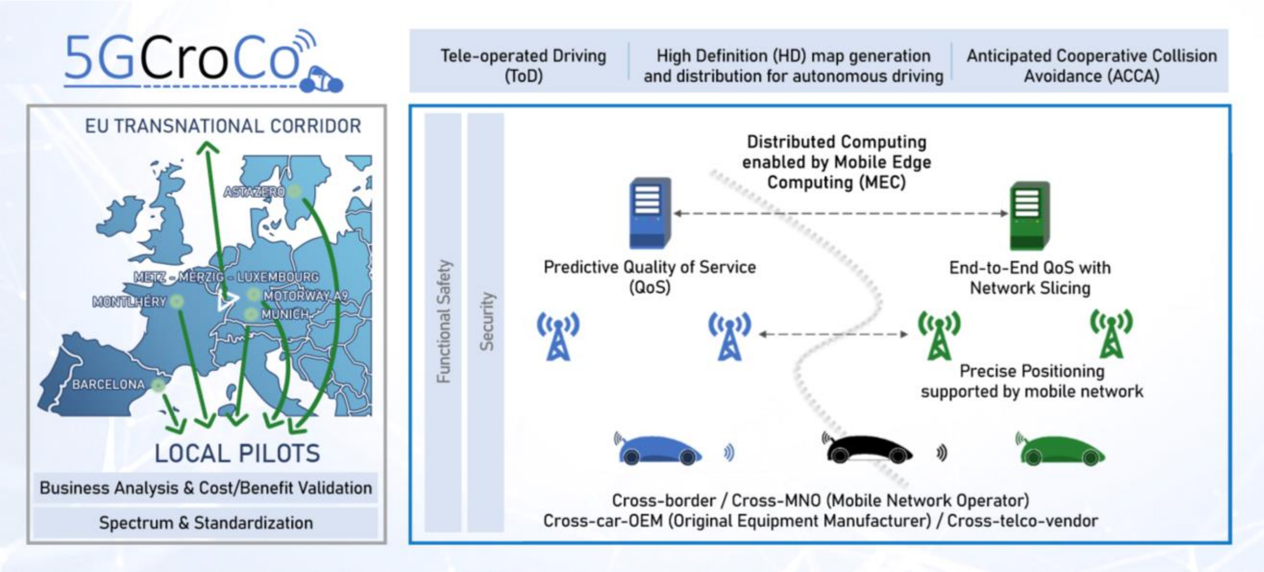


Figure 2: 5GCroCo Use case overview

The trials will allow testing 5G functionalities locally (often geographically close to the different involved project partners), and possibly in restricted closed areas, so that the complexity of doing the trials in the

---

[6] https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automated-mobility-cam

large-scale corridor can be managed. In addition, these small-scale tests will allow fine-tuning the 5G capabilities for the large-scale trials, thus reducing the uncertainties associated to their deployment and trial.

2.2 5G-CARMEN

2.2.1 Use cases

Focusing on the Bologna-Munich corridor (a 600-km-long highway crossing three EU countries – Italy, Austria, and Germany), the objective of the 5G-CARMEN project is to leverage the most recent 5G advances to provide a multi-tenant platform that can support the automotive sector delivering safer, greener, and more intelligent transportation, with the ultimate goal of enabling self-driving cars. To this end, 5G-CARMEN employs different enabling technologies such as 5G NR, C-V2X, Multi Access/Mobile Edge Computing (MEC), and a secure, multi-domain, cross-border service orchestration system to provide end-to-end, 5G-enabled CCAM services. In particular, the 5G-CARMEN project aims at investigating the following four cross-border use cases targeting automation levels ranging from SAE Level 0 to Level 4.

A. Cooperative Manoeuvring

5G-CARMEN addresses the implementation of cooperative manoeuvres that coordinate the trajectories of a group of vehicles in close proximity by i) sharing information produced locally by a vehicle, e.g., from radar, lidar, and on-board cameras, in a privacy-aware and secure fashion with other vehicles, and ii) combining vehicles' information with precise positioning and traffic information. The target is to provide the driver (or the autonomous driving system) with a more comprehensive view of the surrounding environment.

Specifically, 5G-CARMEN will implement a **Cooperative Lane Merging (CLM***)*, as illustrated in Figure 3a. CLM consists in managing the gaps between neighbouring vehicles, such that the vehicle #1 in Figure 3a that intends to merge into a lane occupied by the vehicles #2 and #3 can complete the manoeuvre safely and efficiently. The objective is achieved thanks to a *manoeuvring management entity* instantiated at the edge of the access network, which supervises the local CLM execution over PC5 by monitoring the current state of the traffic along a road stretch and the intentions of vehicles. If the traffic conditions are considered safe, the manoeuvre management entity allows the involved cars to exploit sidelink communication to negotiate the necessary actions, thus executing the CLM in a decentralized fashion. In case of autonomous driving cars, the necessary manoeuvres are automatically executed by the vehicle. On the other hand, in the manual driving mode, the Electronic Control Unit (ECU) sends recommendations to the driver through the human-machine interface (e.g., 'please slow down to create a gap').

B. Situation Awareness

The 5G-CARMEN project addresses the prevention of potential dangers for car drivers by increasing their awareness about the surrounding environment thanks to the 5G infrastructure. In this regard, the following two situational sub-use cases have been identified.

- Back situation awareness (BSA) facilitates emergency vehicles public service. Thanks to 5G wireless links, a MEC server informs the vehicles along a given road stretch that, e.g., an ambulance is coming (even before it is visible or audible), so that the drivers can create a safety corridor earlier and limit their obstruction, thus saving critical time for the emergency service – see Figure 3b. In the range of direct communication, the advanced notification is complemented by precise kinematics updates.

- Vehicle sensors and state sharing (VSSS) creates in-advance awareness about adverse weather conditions or other detected hazards. Such awareness is achieved exploiting the vehicle's own sensors, which will receive either direct (sidelink) communications from other vehicles or indirect communications generated by a cloud service (possibly running on a MEC platform) which merges information originating from different sources in the relevant area.

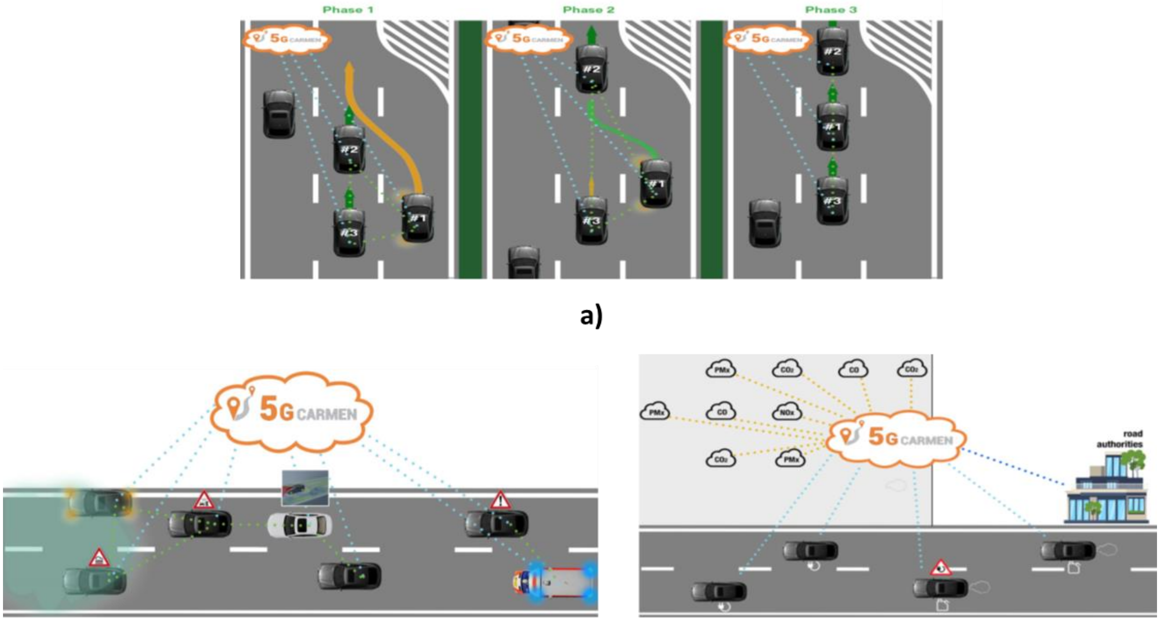
C. Green Driving

The target of the 5G-CARMEN green driving use case depicted in Figure 3c is to minimize the environmental impact of cars and, therefore, to improve the air quality in environmentally sensitive areas. A prominent example is that of Alpine valleys, which are strongly affected by air pollution due to the heavy road traffic conditions with additional peaks during holiday seasons. With the introduction of “Green Driving” modes, these sensitive areas will be relieved due to responsible and environment-friendly driving, resulting in an improved quality of air and life. In 5G-CARMEN, the green driving use case involves two sub use cases.

- Electric Vehicle Zones addresses the capability of 5G-CARMEN to inform the vehicles on alerts to switch to electric driving mode (applicable to hybrid vehicles only) for a specific stretch along the route (i.e. environmentally sensitive areas specified as electric zones), or to select an alternative route with less environment-related restrictions when respecting the alerts is not possible.
- Dynamic Speed Limit is meant to provide driving behaviour suggestions by collecting vehicle information and optimizing the speed profile to target pollution savings.

D. Video Streaming

5G-CARMEN will explore different network architectures and configurations aiming to satisfy the users’ QoE for video streaming (not shown in Figure 3). The key features in this regard are i) the prediction of the expected network QoS and ii) the proactive adaptation of video streaming applications, in order to avoid service interruptions as far as possible. In fact, a high-quality service should always be available, even in cross-border situations and inter-operator scenarios. In this regard, the 5G technologies will guarantee not only the data rate requirements but also the needed coverage to maximize service continuity.



a)

b)

c)

Figure 3: 5G-CARMEN use cases: a) Cooperative Lane Merging, b) situation awareness and c) green driving

2.2.2 Corridors and trials

5G-CARMEN aims at achieving worldwide impact on future CCAM services by conducting extensive trials to validate the above-mentioned use cases across a 5G-enabled corridor from Bologna to Munich.

Prototypes of connected and automated vehicles will be tested exhaustively in the local trials as well as in cross-border locations, with the aim of addressing service continuity and proving the effectiveness of a 5G European corridor serving road users across multiple member states.

In particular, 5G-CARMEN has identified five locations along the Munich-Bologna corridor for running these tests –(c.f., Figure 4). The two cross-border trials are located near Kufstein (Germany-Austria border) and at Brennero (Italy-Austria border). These trials are the main focus of 5G-CARMEN, as they will show continuous service provisioning when traveling from one country to another. In addition, three in-country "integration sites" will host integration work and collect data supporting the 5G-CARMEN evaluation: 1) the Munich trial, near the BMW premises; 2) the Trento trial, motivated by the presence of CRF-FCA, FBK, and the A22 traffic management centre; 3) the Modena trial due to the peculiar weather characteristics and the presence of CNIT.

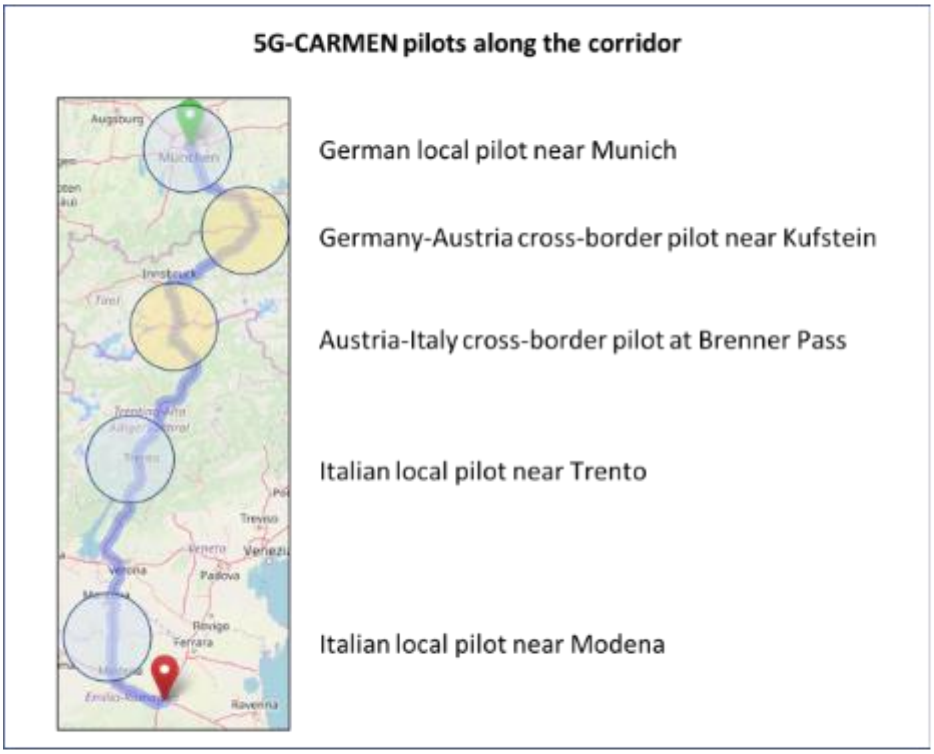


Figure 4: 5G-CARMEN trial locations

In the 5G-CARMEN trials, cars will demonstrate driving use cases up to SAE Level 3 automation, supported by 5G connectivity. The impact of 5G towards higher levels of automation (i.e., SAE Level 4 and beyond) will be derived from experimental data gathered during field trials and complemented by simulations.

2.3 5G-MOBIX

2.3.1 Use cases

In 5G-MOBIX five use cases are defined building on the work of 3GPP [9]. The descriptions given by 3GPP are high-level enough to accommodate very different implementations for each use case. In 5G-MOBIX the 3GPP use case derivatives are called user stories. Therefore, the user stories are defined in 5G-MOBIX under the umbrella of a standard 3GPP classification. In some cases, the user stories have more than one possible event flow, denoted as scenarios. The description of each use case is given below. Then the classification of user stories in use cases and their distribution among cross-border corridors and trial sites is briefly presented. A more comprehensive description of user stories can be found in 5G-MOBIX's deliverable D2.1 [9].

A. Advanced Driving Use Case

Advanced Driving enables semi-automated or fully-automated driving. Each vehicle and/or RSU shares data obtained from its local sensors with vehicles in proximity, thus allowing vehicles to coordinate their trajectories or manoeuvres. In addition, each vehicle shares its driving intention with vehicles in proximity. The benefits of this use case group are safer traveling, collision avoidance, and improved traffic efficiency.

B. Platooning Use Case

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

C. Extended Sensors Use Case

Extended Sensors enable the exchange of raw or processed data gathered through local sensors or live video data among vehicles, RSUs, devices of pedestrians and V2X application servers. The vehicles can enhance the perception of their environment beyond what their own sensors can detect and have a more holistic view of the local situation.

D. Remote Driving Use Case

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

E. Vehicle Quality of Service Support Use Case

Vehicle quality of service support enables a V2X application to be timely notified of expected or estimated change of quality of service before actual change occurs and to enable the system to modify the quality of service in line with V2X application's quality of service needs. Based on the quality of service information, the V2X application can adapt its behaviour to system's conditions. The benefits of this use case group are offerings of smoother user experience of service.

5G-MOBIX User Stories

In Table 1, the 5G-MOBIX user stories are listed. Each user story is classified in at least one use case and is implemented in a trial site. All of them are designed to be meaningful in a cross-border corridor context. The user stories planned at cross-border corridors (Spain-Portugal (ES-PT) and Greece-Turkey (GR-TR)) cover all use cases (indicated in the two top rows of Table 1). The user stories planned at local trial sites are quite evenly distributed and are meant to enable and facilitate the trials at the two cross-border corridors.

Table 1: 5G-MOBIX User Story classification

Trial site	Advanced Driving	Vehicles Platooning	Extended Sensors	Remote Driving	Vehicle QoS Support
ES-PT	Complex manoeuvres in cross-border settings *(Lane merging, Automated Overtaking)*		Complex manoeuvres in cross-border settings *(supporting HD maps)*	Automated shuttle remote driving across borders *(Remote Control)*	Public transport with HD media services and video surveillance

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

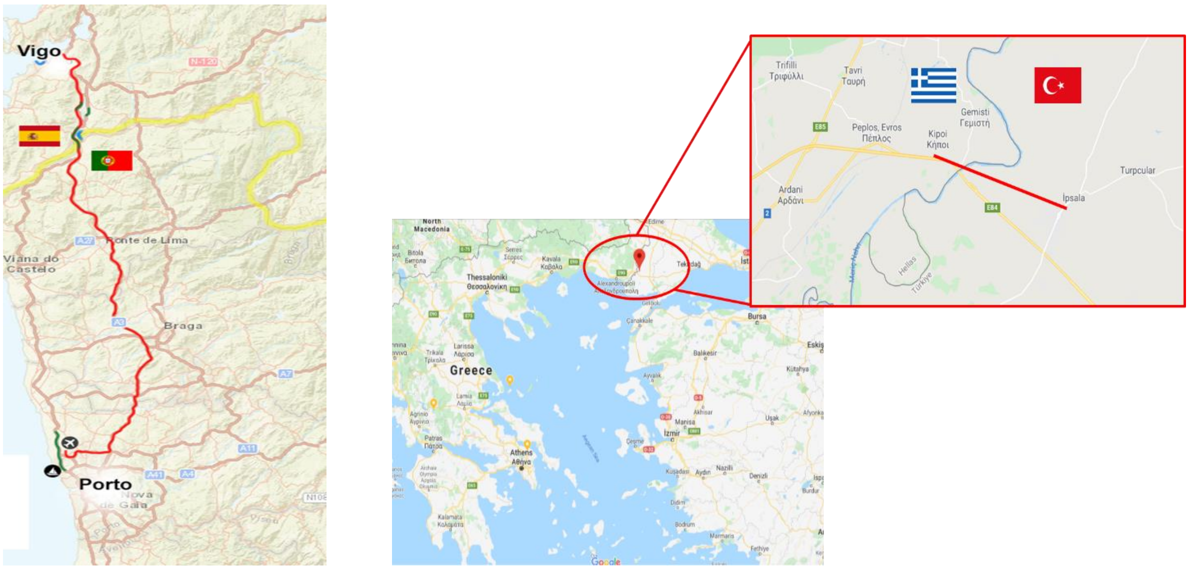
The work planned at the local sites (Germany, Finland, France, Netherlands, China and Korea) contribute to the 5G cross-border corridor roadmap in diverse aspects and complement the set of user stories to be deployed in 5G-MOBIX cross-border corridors, by e.g. applying different set-up, examining different Handover (HO) issues, preparing Hardware (HW) and Software (SW) for the cross-border corridors and more. Sometimes, the implementation of a user story variant is simply not feasible in a real cross-border corridor and needs to be implemented in a more controlled environment present at a local site.

2.3.2 Corridors and trials

5G-MOBIX is comprised of two Cross-Border Corridors (CBCs), as shown in Figure 5, which are the focus of the project in the borders of **Spain and Portugal (ES-PT)** and the borders of **Greece and Turkey (GR-TR)**. The two CBCs are enabled and assisted by four European Trial Sites (TS) in Germany (DE), Finland (FI), France (FR) and the Netherlands (NL) and their results and insights will be shared and benchmarked with two Asian Trial Sites in China (CH) and Korea (KR). Trial Sites will be used for early trialling, pretesting, configuration insights and extended evaluations of use cases in order for 5G-MOBIX to offer a well-rounded evaluation of the potential cross-border issues. More importantly the TSs will develop HW and SW solutions which will be integrated in the two CBCs, thus accelerating the project's time-schedule and contributing to the end-to-end cross border solution.

The **ES-PT** cross-border corridor is in the border of the north of Portugal with Spain. This border is established by the Minho/ Miño river, disposing of several bridges providing the road infrastructure serving trucks, cars and pedestrians. International trade as well as large passenger commuting flows are of great importance and provide ideal conditions for the execution of diversified trials to showcase the advantages offered by the 5G connectivity to CCAM use cases. The Spanish-Portuguese corridor connects the cities of Vigo and Porto, with a distance of around 250 Km. A multitude of advanced CCAM use cases will be trialled at the ES-PT border such as advanced driving manoeuvres (autonomous overtaking, lane merging, etc.), remote driving, HD map support with QoS guarantees and more.

The **GR-TR** cross-border corridor constitutes the south-eastern border of the European Union providing a challenging geo-political environment due to the existence of actual, physical borders, where customs agents perform rigorous border checks. The heterogeneity of traffic going through these borders, i.e. trucks with commercial goods, tourists, as well as the co-existence of multiple differentiated vehicles with pedestrians (security personnel, customs agents, etc.) provide ideal conditions for the execution of diversified trials to showcase the advantages offered by the 5G connectivity to CCAM use cases. Two main CCAM use cases will be developed and trialled at the GR-TR border, namely truck Platooning with “see-what-I-see” functionality and Assisted truck border-crossing & increased driver awareness.



a) **b)**

Figure 5: 5G-MOBIX Cross Border Corridors in a) Spain - Portugal (ES-PT) and b) Greece - Turkey (GR-TR)

All the 5G-MOBIX CBCs and TSs have performed an exhaustive scenario requirements analysis and have defined in detail the use cases to be executed in each corridor/site [9], the 5G network architecture and components specifications [11], the road side infrastructure and MEC specifications [12] and the specifications of the vehicles and OBUs [13] to be used in the trials.

2.4 ICT-18 Roadmap

All three corridor projects have just exceeded the first half of their duration and are eagerly preparing the start of their trialling activities. The first half of the projects’ lifetime has been devoted to scenario requirement analysis, use case specifications, network and infrastructure architecture definition, definition of integration and verification methodologies as well as deployment and trialling methodology. Development and implementation of SW and HW (e.g. vehicles, network components, OBUs, RSUs, Applications, Key Performance Indicators (KPI) logging mechanisms, etc.) to enable the trials is actively ongoing while field deployments and trial site preparations are ongoing, despite the somewhat impacted timeline due to COVID-19 measures and travel ban.

All three projects (with slight scheduling differentiations) are now entering the beginning of their trial phase, starting from initial local trials in controlled environments and moving towards the full-scale cross border experiments. As the results will start coming in from the initial trials, all projects will move towards the evaluation and impact assessment phase (technical, business and user acceptance) while large scale demonstrations take place involving all relevant stakeholders at the respective cross-border sites. A rough timeline of the ICT-18 projects' phases is depicted in Figure 6[7].

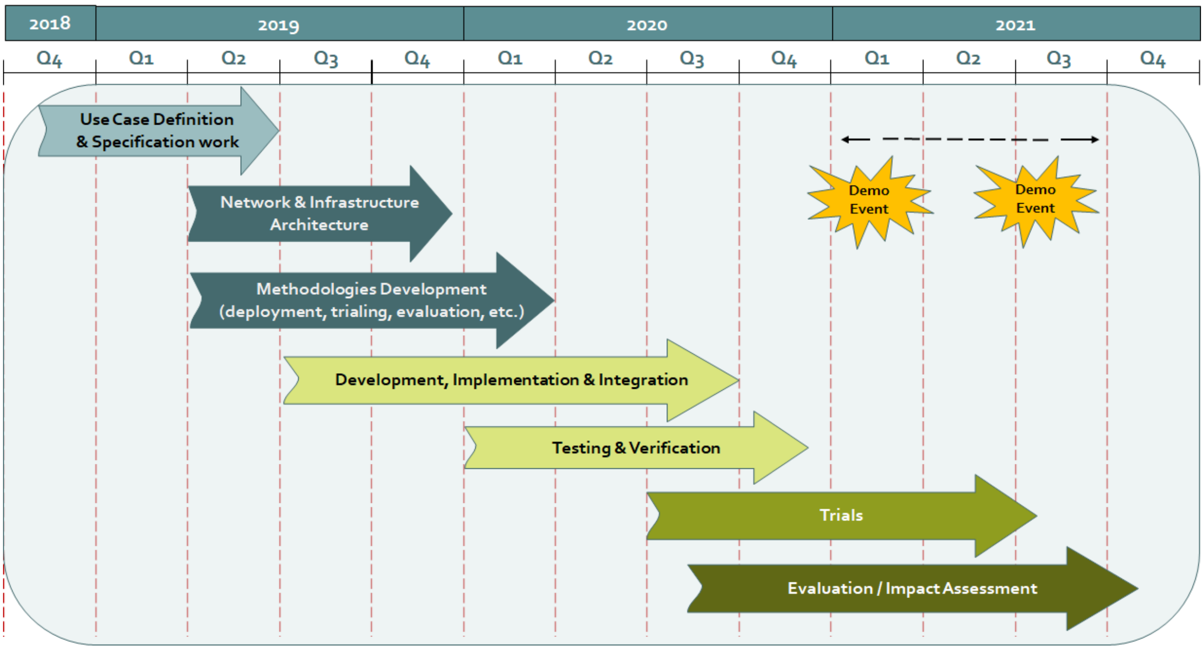


Figure 6: High-level roadmap of the ICT-18 projects' phases

5G networks have been targeted to meet the requirements of a highly mobile and fully connected society. The coexistence of human-centric and machine type applications will define very diverse functional and performance requirements that 5G networks will have to support. Within the 5G System (5GS), end-to-end network slicing, service-based architecture (SBA), Software-Defined Networking (SDN), and Network Functions Virtualisation (NFV) are seen as the fundamental pillars to support the heterogeneous KPIs of the new use cases in a cost-efficient way. The 5GS gives mobile network operators the unique opportunities to offer new services to consumers, enterprises, verticals, and third-party tenants by addressing their respective requirements. To this end, 5G Infrastructure Public Private Partnership (5G PPP) Phase I/II collaborative research projects as well as standardisation bodies have specified and developed the main elements of the 5G architecture.

---

[7] The exact timelines of each project are slightly different that the scheduling presented in Figure 6, as each project follows its own activities roadmap

3 Cross-border Challenges & Considerations

Achieving continuity of data services for vehicles, such as those introduced in Section 2, while meeting a certain expectation of service quality depends on a variety of factors. To start with, cellular change of serving network across multiple MNO domains may result in major interruptions in connectivity between a vehicle and the network infrastructure. Moreover, whereas the handover of a User Equipment (UE) between radio base stations -evolved NodeB/eNB(4G), next generation NodeB/gNB(5G)- and the re-selection of network functions on the mobility control- and data plane, such as a Packet Data Network Gateway (PGW) in 4G (not shown below) or a User Plane Function (UPF) serving as data plane anchor, is entirely under control of the mobility management system (N3, N9 reference points in the 5G architecture per Figure 7), the treatment of data plane traffic in between the mobile data plane anchor and the service instance in a data network (N6 reference point) is not standardized and rather handled per operators' proprietary policy and associated configuration, or not controlled at all. However, in the 3GPP 5G system architecture [6], the characteristics of the network segments in between a UE's current UPF and the service's data network can have a large impact on the service quality.

In this context, MNOs are moving towards the deployment of decentralized cloud resources, network/service function virtualization (NFV), and MEC platforms, which host virtualized service instances, aiming at the provisioning of services topologically closer to the UEs at the network infrastructure edge, herewith introducing more flexibility and reducing the topological distance between a service in the infrastructure and UEs as service clients.

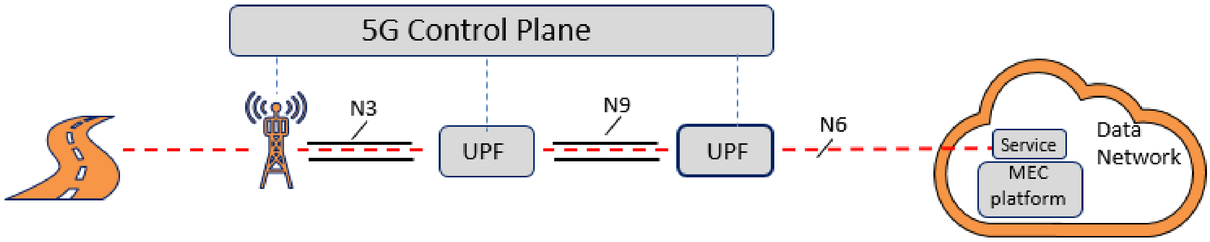


Figure 7: End-to-end data plane between vehicle and MEC service instance

On the other hand, the mobility of UEs results in changes in the routing path between the service and a mobile client due to the continuous change of the serving radio base station. Routing impact is even stronger in case of cross-border movements and the resulting change of MNO, which can result in very long communication paths (and hence increased latency) if a roaming vehicle, as typically done today, continues using a gateway with its home MNO (Home Routing). Looking at the complete end-to-end data plane path between a virtualized service instance on a MEC platform and a UE, configuration and policy enforcement on the multiple data plane segments is under control of multiple and de-coupled control and management planes, such as the 5G control plane, the MEC platform manager and the NFV management and orchestration system. As a result, providing service continuity for V2X applications during inter-PLMN HO at border environments is a significant, multi-aspect challenge.

Especially regarding the availability of V2X Application Servers (V2X-AS) for providing time critical ITS applications with a high reliability, the deployment of V2X-ASs across multiple MNO domains and/or good connectivity between MNOs is essential for both capacity and cost/investment reasons. Along with the vehicles[8]' path across national borders, the (MEC) application moves across different edge cloud instances administrated by different operators. This requires continuous monitoring, rapid discovering and deciding on the optimum MEC instance for best serving the vehicles [14].

---

[8] UEs as far as a 5G network is concerned

In order to guarantee uninterrupted CCAM service provisioning in a heterogeneous, multi-stakeholder, cross-border environment comprising 5G networks, MEC/Edge and cloud resources and RSI, ***five Key Challenges*** need to be addressed. These challenges have been labelled as [**Ch.1]** to **[Ch.5]** by the experts of the three 5G PPP Phase 3 ICT-18 corridor projects. These challenges are summarized in Table 2, and are further elaborated in the following sections.

Table 2: Key Challenges for CCAM service provisioning in cross-border environments

Challenge ID	Name / Title	Short description
Ch.1	**Cellular coverage and radio access aspects**	A fundamental requirement is cellular radio coverage and sufficient capacity to meet minimum bandwidth and maximum latency constraints. This is equally relevant in the area of country borders, where network coverage and a smooth transition of a UE between different networks of different MNOs need to be ensured but can be particularly challenging and onerous to be achieved. Network reselection and UE re-configuration issues also have to be taken into account Without careful radio planning at the border, cellular connectivity can be greatly impaired due to a high level of interference in areas where coverage from neighbouring MNOs overlap or may even not be available at all when coverage gaps are present. A more detailed analysis is presented in Section 3.1.
Ch.2	**Service and Session continuity aspects**	Mobility Management (MM) across borders is especially challenging as the agreed upon QoS/QoE needs to be guaranteed for CCAM users. This means that even during the inter-PLMN HO (i.e., when a UE/vehicle detaches from its Home network/PLMN to attach to the Visiting network/PLMN), service and session continuity needs to be provisioned. An Application Server (AS), irrespective of its location, which can be for example in one MNO's data centre or be MEC-hosted, needs to be changed mid-session to keep the AS topologically close to the mobile client to keep the network impact towards QoS/QoE low. Practically, the mid-session change of an AS, serving a mobile client, requires the transfer of a client's session state (in case of stateful services) and the update of data routing through the network(s). This relocation procedure should take place seamlessly, guaranteeing the Service Level Agreement (SLA) based end-to-end QoS. In addition, to keep service relocation transparent to the mobile client, service name and network address should be maintained. A more detailed analysis is presented in Section 3.2.
Ch.3	**MNO collaboration & Data Plane routing**	The smooth collaboration and inter-play between neighbouring MNOs at the borders are critical for the successful transition of the CCAM services from one country to the other. Besides tackling radio frequency and coverage requirements, per Ch.1, MNOs need to collaborate by leveraging protocol interfaces and additional semantics to share information about mobile clients and their services, aiming at smooth transition and continuity of services. Whereas solutions related to Ch.2 enable continuity on AS level during service relocation, MNOs need to contribute to optimize end-to-end data plane routes by the (re-)selection of suitable data plane anchors, such as the UPF serving as Protocol Data Unit (PDU) session anchor or as Uplink Classifier and enable local breakout of data plane traffic. A more detailed analysis is presented in Section 3.3.

Ch.4	**Data management & protection**	Besides the technical aspects, the provisioning of CCAM services across borders also entails significant data management, security and privacy issues that need to be resolved with a realistic approach. As most CCAM services operate on at least some sensitive (personal) data, such as vehicle attributes (make, model, license plate/ID), location and more, the handling of these data and the related processes become even more complicated in cross-border scenarios. How to abide by the General Data Protection Regulation (GDPR) rules, which subscriber data can and cannot be shared and under how strict anonymization procedures, how to secure this sensitive data exchange among MNOs and MECs as well as liability issues, are only a few examples of such challenges. A more detailed analysis is presented in Section 3.4.
Ch.5	**Non-functional aspects & business enablers**	Besides the technical and data management aspects that have to be addressed for a successful deployment of CCAM services across national borders, there is a number of non-functional, business and regulatory challenges that will also have to be resolved. The proper engagement of stakeholders at the right stages of development including national and regional authorities, regulatory bodies, traffic and road authorities and more will enable the development of a realistic plan for deployment of the necessary infrastructure to serve the challenging CCAM use cases. Moreover, the development of realistic and effective business plans, including potential sharing of resources/expenses, is considered critical for the engagement of the proper stakeholders and the assurance of the investor's interest, while significant consideration has to be given to regulatory aspects as neighbouring nations may adhere to different rules and guidelines. A more detailed analysis is presented in Section 3.5.

3.1 Cellular coverage and radio access aspects (Ch.1)

In order to understand the current radio network implementation situation and issues, we need to take a step back and describe the underlying proceedings for network coverage. This is followed by a brief explanation of network handovers and the current situation in Europe.

3.1.1 Radio Planning and Cellular Network coverage at the borders

Cellular networks are a very important part of the connectivity-based solutions – and connectivity is indispensable for coordinated, efficient and altruistic mobility. Although other connectivity solutions may be available at some locations, the most promising possibility to ensure seamless network coverage and sufficient capacity to meet future bandwidth and latency requirements are cellular networks. This multi-service/multi-functional communication network, enhanced with new 5G possibilities and applications for ITS use cases, can assure connectivity with vehicles and road agents in general (such as pedestrians for instance).

In cross-border areas however, coverage between foreign MNOs' networks may be conflicting (especially in cities close to the border, but also in sparsely populated rural areas). Roads in the vicinity of denser population areas, where significant 5G deployments are foreseen due to a predicable higher customer demand, will have no problem achieving the necessary 5G-cellular connectivity. On the other hand, areas with a lower population density, such as cross-borders, will have to be considered differently, so that the communication infrastructure investment is justified. It should also be noted that it is not uncommon for cross-borders to be located in geographically challenging areas, where it can be particularly onerous to provide coverage (e.g. mountains, valleys, etc.), or difficult from a radio planning point of view (e.g. along rivers, with roads following the border and moving in areas where the coverage of MNOs from different countries overlap and blur).

The individual frequency usage of each MNO depends firstly on the general EU Electronic Communications Committee (ECC)[9] regulation, who then tasks each national Federal Network Agency to execute and supervise the implementation (e.g. spectrum auctions, dispute resolution etc), and finally the individual MNO radio network planning. Currently, the radio coordination between neighbouring countries – and thus several neighbouring MNOs, since each country normally has several MNOs – is only governed by the legal aspect of frequency bands and radio emission control. As MNOs always operate under individual member state jurisdictions, by (national) law they are only allowed to cover national territory (national law and operations cannot be applied to foreign countries), and thus the overlapping coverage at country borders is supposed to be as minimal as possible. In practice, the national laws and the thorough application of the laws by the different National Federal Network Agencies varies for each country. Also, a European HCM (Harmonized Coordination Model) agreement exists[10], however it currently does not involve neither all member states nor all MNOs – and its processes, e.g. in relation to national validations of base station/antenna sites and spectrum constraints, are not taking into account any service continuity requirement.

Despite industry efforts, uncontrolled and uncoordinated planning and operation of the frequency spectrum at the borders can lead to inconsistent connectivity and even radio interference due to missing knowledge of the essential Radio Access Network (RAN) data of neighbouring MNOs. The consequences may infer a degradation of the network quality and related CCAM Services.

3.1.2 Inter-PLMN Handover

Inter-PLMN Handover i.e., the process during which a UE changes its network service from one country (Home PLMN) to a neighbouring country (Visiting PLMN), is exceedingly challenging compared to an intra-PLMN HO [7]. The execution of a smooth, low-latency inter-PLMN HO is perhaps the most critical aspect for ensuring service continuity and low latency to CCAM applications, when crossing the borders. The inter-PLMN HO is significantly affected by the radio coverage conditions at the border areas. The following HO situations may arise:

- *HO with overlapping coverage:* As MNOs attempt to provide full coverage even at the borders of their country, it frequently occurs that gNB (or pre-5G base stations) radio coverage from neighbouring MNOs are overlapping (also mentioned as ‘spill-over’ in cross-border scenarios). Despite best efforts from MNOs to avoid such situations it is extremely difficult from a technical perspective to eliminate all spill-overs, which potentially result in the actual HO taking place well before or after the actual border. A high level of overlapping coverage may lead to multiple unwanted effects such as interference among gNBs and consequently low SINR leading to QoS degradation, disturbance of the UE connection stability, i.e. ping-pong effect, unbalanced traffic load and more. Consequently, CCAM applications will suffer negative impacts from the resulting QoS degradation.
- *HO with coverage gaps:* The distance among the eNBs/gNBs of different MNOs and the (uncoordinated) radio planning of the two neighbouring MNOs may result in areas close to the border where no MNO can provide network services or the UE connection to a network is not even possible. These areas with no coverage are identified as coverage gaps and result in complete service interruption, until wireless connectivity can be re-established with one of the networks. Such an interruption of connectivity has severe consequences for any application, but especially so for CCAM functionality where critical application for safety may require connectivity, so it is of at

---

[9] https://cept.org/ecc/topics/

[10] http://www.hcm-agreement.eu/http/englisch/verwaltung/index_europakarte.htm

most importance to deal with such coverage gaps. In such cases vehicles may continue to communicate with each other via V2V communication until network connectivity is re-established, however CCAM application depending on external information (e.g. sensor/camera data from road side infrastructure, warning messages and communication with cloud/MEC platforms) will experience severe service degradation or even complete inability to perform their design purposes.

Besides the coverage conditions during a HO, another important factor which affects performance during HOs is the transition to a different technology, the so-called *hybrid HO*. This involves the handover between cellular network communication technologies with different performance capabilities, i.e. different RAN and core technologies. This will be particularly common when combining 5G NR with currently available 4G LTE networks. Both cases of HO between a 5G Non-Standalone (5G NR + Evolved Packet Core (EPC)) and a 4G LTE and 5G SA (5G NR + 5G Core (5GC)) and a 4G LTE network need to be considered. Performance degradation in terms of throughput (impact on enhanced Mobile Broad-Band (eMBB) services), delay (impact on Ultra Reliable Low Latency Communication (URLLC) services) and potential period of disconnection during the execution of a HO are some of the most severe anticipated consequences.

3.1.3 Network Reselection

For the standard seamless handover procedure, interconnected Core Networks and the exposure of essential functions are required – however, in reality, the latter is not the case because it is not a simple question of technological feasibility. Apart from the costs, business and security (including legal obligations) considerations play a major stake and the non-technical issues of practical integrations into the (inter-)MNO business are not covered by standardization bodies, but rather (if at all) by individual agreements and proprietary developments. More technical descriptions about the standard 3GPP network handover and network reselection procedures are currently under discussion in 5GAA, while relevant contributions have already taken place by the three projects (e.g. [11]), or will take place after the first trial results.

Concerning the network reselection procedure and its long connectivity gaps, accelerations are possible, but for example ePLMNs are currently hardly configured in European live networks. And since 5G will not be available everywhere in Europe at the same time (especially rural border regions are not a rollout priority), different Radio Access Technologies (RAT) at different sides of the border is habitual. In addition, detailed information about the RAN or at least the used frequencies of the cells of neighbouring foreign MNOs are left to individual scans of each UE (and therefore long connectivity gaps), instead of sharing and managing this data on the network infrastructure side. As long as the – for a large part non-Technical (see Section 3.5) – burdens are not remediated at a European level, network reselection applies at all European borders and Service Continuity is difficult to assure.

3.2 Service and Session continuity aspects (Ch.2)

The content of this section initially points out the challenges related to session and service continuity, especially when Edge Computing is applied. It initially states cross-border specific challenges before more generically describing Edge Computing specifics concerning low latency connections between end-users (typically the vehicle) and Edge Servers. This needs to be maintained within an MNO, but the challenge is equally in particular across MNOs, e.g. when crossing country borders. A prerequisite for Edge Computing is the availability of data plane breakouts between the 3GPP-specified mobile radio network and Edge Servers.

3.2.1 Service Continuity and End-to-End QoS Across Borders

Edge Computing is considered an essential component of the solutions in the three cross-border corridor projects. It should logically also be applied in cross-border scenarios when vehicles roam to mobile radio networks that are not their home network. Today, typically Home Routing (HR) is applied where the gateway[11] between mobile radio network and other networks, such as Edge Computing facilities and the public Internet are located within the home network of the vehicle. Resulting end-to-end routes between the vehicle and the application servers it communicates with, can become very long (see Figure 8). This contradicts the Edge Computing goal of short end-to-end routes.

In cross-border scenarios those would be MEC hosts on the different sides of the border. Solving this, is ongoing work but solutions must assure that application servers on MEC hosts from different MNOs can communicate, which is a particular challenge if Network Address Translation (NAT) is used or MEC hosts have no public Internet Access at all. Even if this is solved using the best effort public Internet, it will not provide the desired SLA guarantees, which were a driver for MEC deployment in the first place.

3.2.2 Keeping Short End-to-End Routes as the Vehicle Moves

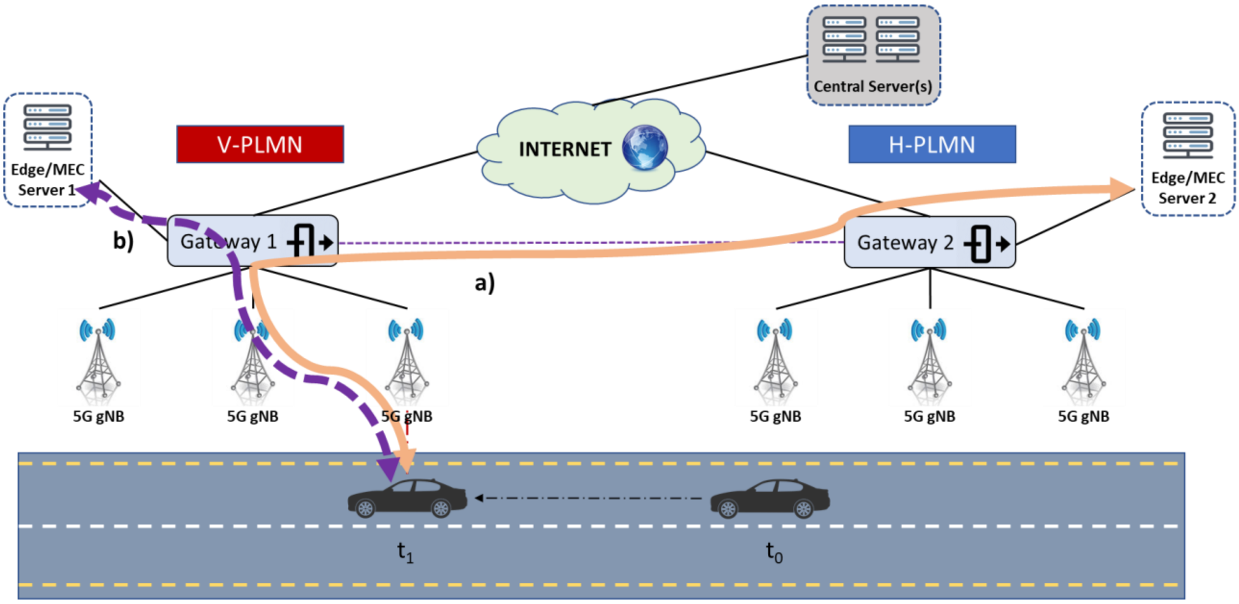


Figure 8: A vehicle communicating with an Edge Server that is accessed via a) a far away gateway (HR concept) and b) a near gateway (LBO concept)

Figure 8 depicts today's situation where a vehicle is connected to Edge Server 2 through Gateway 2 (route a). As the vehicle moves to the left, Edge Server 1 becomes more suitable and it should be reached through Gateway 1, as is depicted via route b) in Figure 8. The challenge of changing the gateway is called "session continuity" in 5G Core specification TS 23.501 [6] while also switching the application server and host providing it is called service continuity. The question if service continuity was really achieved depends on the application. A connection-less application using User Datagram Protocol (UDP) and only sporadically communicating might not be affected by gateway and edge server changes causing temporary communication interruption, as the UE might very likely not be communicating during that time.

After switching the gateway, which is under control of the mobility control plane (Challenge 3 discussed in Section 3.3), also the Edge Server should be changed for a short end-to-end route. Several challenges need to be addressed for this to happen. First of all, switching the gateway can also result in changing the IP address that is visible towards the Edge Server. In case of NAT it is the gateway, not the vehicle client IP address that changes from point of view of the Edge Servers. A NAT server at the new gateway has no state information about the vehicle and would not know what to do when receiving data from an Edge Server directed towards the vehicle. Moving higher up in the protocol stack, a connection-oriented transport layer protocol like TCP (Transmission Control Protocol) would normally also have to reset a connection or

---

[11] P-GW in 4G Evolved Packet Core or PDU Session Anchor (PSA) User Plane Function (UPF) in 5G Core

establish a new one. IP addresses are used as unique identifiers for TCP connections and according to what was described before, they would need to be updated. Furthermore, the new Edge Server has no context associated to a TCP connection that was established with the previous Edge Server. For connectionless transport protocols, continuity of an Edge Server or edge service IP address as communication endpoint from the vehicle client helps to avoid additional interaction and signalling with the vehicle client, which may be required to enforce the use of the new communication endpoint IP address (Edge Server or edge service IP address). On the other hand, service IP address continuity across different networks moves such IP address from a topologically correct network address to a topologically incorrect address in the target network. Routing uplink packets from a vehicle client to the new edge service requires policy routes, as default routes will not be applicable. Such policy routes apply to the network segments in between the vehicle client's local gateway and the relocated, local edge service.

Lastly, also the server-side application itself can have context associated with the ongoing connection with the vehicle, which the new Edge Server does not have although required for seamless service continuity from a vehicle application client point of view. The precise challenge is application dependent as this depends on the protocols used and the stored context information. It is also important to state that more than one applications could be active and transition between Edge Servers would therefore have to assure service continuity for all active applications that require it.

3.3 MNO collaboration & Data Plane routing (Ch.3)

3.3.1 Roaming Impact to Service and Session Continuity

The Roaming Regulation EU 2015/2120 regulates the imposition of roaming charges within the European Economic Area; however, it does not substitute the individual agreements or governance between mobile network operators. Roaming agreements typically cover technical aspects, charging, security (including fraud), legal aspects and associated processes, and these agreements are often facilitated via organizations such as the GSMA. International roaming support for V2X communication use cases is required to provide a pan-European functionality. Specifically, when a UE (e.g., automated vehicle) crosses the border into another country, thus switching to another MNO, service migration needs to be performed in an optimum way aiming to fulfil the strict requirements of the CCAM use cases and applications in terms of latency and service continuity. Roaming agreements between the MNOs is a prerequisite. The underlying network technology that each MNO uses may differentiate such agreements. Three distinct cases of 5G roaming can be foreseen:

- *Roaming between MNOs with 5G non-standalone (NSA) network solutions support*: Taking into account vendors' roadmap, this scenario seems to be the most likely to happen at the first phase of 5G deployments, exploiting the existing LTE roaming agreements. Such solutions are expected to inherit the 4G-LTE roaming performance (as the 4G core would still be used), which means that there is a certain limit in terms of service interruption and end-to-end latency which might not be suitable for the very stringent CCAM applications (e.g., requiring less than 100 ms of service interruption time). Customized solutions would need to be applied to mitigate the impact on performance while roaming.
- *Roaming between MNOs with 5G standalone (SA) core network solutions support*: Taking into account vendors' roadmap and the standardization status, this scenario will occur at a later phase. Specialized SA features such as end-to-end slicing and SSC (Session and Service Continuity) mode 3 (make before break approach – see also Section 4.1.1) have the potential to improve roaming performance and seamlessly support CCAM applications. However, besides the fact that such solutions require significant 5G SA penetration (which will take years), inter-PLMN HO solutions would still need to be specified as part of the 5G Core specifications.
- *Roaming between a 5G NSA network and a 5G SA network*: Interworking functionalities need to be supported at this scenario; roaming extensions or new roaming interfaces (i.e. N26 interface [6])

will be required, while performance for CCAM services is expected to degrade unless pro-active measures are taken. This case is expected to be an intermediate step between the first roll-out of 5G-NSA networks and the migration towards more advanced 5G-SA networks.

For NSA deployments, long roaming latency is expected since currently the roaming user traffic is Home Routed, meaning that subscribers always obtain service from the home packet gateway (i.e. traffic is always routed back to the home network). As the service is always managed through the Home network, service continuity while roaming can be ensured, but nevertheless with increased latency (long route back to the Home network). Local breakout solutions would help decrease the latency (i.e. route user plane traffic locally via the Visited network and not through the Home network), however session and service continuity challenges described in Section 3.2 must be resolved. Since this work has a specific focus, it is to be mentioned (without going into details) that a local breakout scenario also entails various other considerations, including customer and subscription data availability (in visited networks), security, lawful interception, business strategies, connection (tariff) control and billing.

3.3.2 Need for Local Breakout support across MNO domains

Today, a mobile data plane anchor (PGW) is selected according to the data network, which hosts a UE's service. In the view of MEC, a data plane anchor or a local gateway in the proximity of the edge network , which hosts the MEC service instance to which a UE connects, enables local breakout of traffic to access the edge service, resulting in an optimized end-to-end routing of data plane traffic. In case the MEC platform and the edge network is re-selected and re-configured for a UE, e.g. due to the UE's mobility, the UE's data plane anchor needs to be re-selected and re-configured too, to avoid sub-optimal routing.

The 3GPP standard covers different SSC modes, whereas SSC mode 3 considers mid-session re-location of a UE's UPF serving as data plane anchor. In the view of service relocation between different MNO domains, MNOs need to share information about roaming UEs as well as ongoing data sessions and associated services. The target MNO needs to assess which data network hosts the required service(s) and select a suitable local data plane anchor (local gateway, UPF) to serve as data plane breakout point.

3.4 Data Management & Protection (Ch.4)

Besides the network/MNO oriented challenges that need to be addressed for a successful deployment of CCAM services at cross-border areas, the change of national and administrative domain imposed by an inter-PLMN HO also poses several security, privacy and data management challenges. This section addresses the most prominent of them.

3.4.1 Data Management

Proper data management and interoperability become major issues in cross-border vehicular environments, as data is exchanged across multiple vehicle vendors, network domains, infrastructure systems and/or federated service providers, potentially with inconsistent data schemes. Moreover, in such a multi-stakeholder environment data ownership, data management rights, data access and liability for data leaks/breaches become blurred as there is an overlapping area of concern among the different actors.

On the technical aspects of this issue, due to different information sources (e.g., from different manufacturers' equipment or different application / functionality developers, different vehicles, different road side infrastructure) two integrated CCAM applications or even the two countries' ITS centres may have different information at a given time. Such a mismatch may lead to an inconsistent view at the border area, for example in terms of the number of vehicles, their exact location and their trajectory. In turn this creates an additional trust issue (which of the two "views" should be trusted?) which would be catastrophic for CCAM operations at the borders.

Moreover, the operational and legal issues regarding data ownership, data sharing and data exchange that arise from cross-border CCAM functionalities, also need to be addressed. CCAM applications supporting cross-border functionality will eventually have to process data from citizens of different countries. The management of personal data leaking incidents increases the complexity of this issue, which could cause severe security concerns and render a CCAM application unsuitable for cross-border functionality.

Another major concern is how to achieve trusted and secure communications between vehicles and the infrastructure of different trust domains. Without a common trust domain between the EU (EU C-ITS security Credential Management System - CCMS) and non-EU neighbouring countries, trusted and secure communication between the vehicles and/or network or application entities, could not be achieved when the vehicles from different trust domains are to communicate. As a consequence, the message exchange cannot be authenticated by the neighbouring infrastructure/vehicles and incoming vehicles may potentially not be allowed in the other trust domain (country). This issue becomes even more severe when discussing cross-border operation at the external EU borders, where GDPR principals may not be enforced by the non-EU country. The trust and privacy management guidelines that European Telecommunications Standards Institute (ETSI) has put forth [15] are a first step in the right direction but a comprehensive framework addressing all aspects of this issue is still missing.

Finally, different approaches to data processing procedures utilized by neighbouring countries and MNOs, may introduce additional challenges. For instance, the technical mechanisms that are applied in order to support the legal requirements on lawful data processing could encounter difficulties in a cross-border scenario, as neighbouring countries may need to comply to different legal frameworks regarding the capabilities and permissions of these mechanisms. Disputed data processing procedures may include: encryption, data minimization/anonymization, privacy by design mechanism and informed consent. Such processes could be incompatible between EU and non-EU countries, which could result on more difficult handover procedures or limited functionality of a CCAM application, once the border is crossed.

3.4.2 Security/Privacy and Regulatory compliance

Certain aspects of the end-to-end CCAM chain are not regulated at all, such as the message formatting for autonomous vehicles. Even though DENM (Decentralized Environmental Notification Message) and CAM (Cooperative Awareness Message) are well-defined messages, automotive manufacturers rely on proprietary solutions i.e. for the internal communication of their system and all of its components (e.g. sensors, applications, ECU). Similarly, there is no consensus on how privacy frameworks, such as GDPR, should be implemented, which means that different manufacturers may rely on different proprietary implementations regarding security and privacy mechanisms or even target specific automotive market for deployment. Some of the specifications or rules implemented for one market/country may not be applicable/valid for a different country [16]. This poses a significant obstacle in cross-border operations, as proper CCAM functionality must be ensured when crossing any border and local and European regulations must be respected at all times. A regulation for automotive cybersecurity is under definition by UN-ECE (United Nations Economic Commission for Europe) and will be applied in the framework of EU Regulation 2019/2144[12], General Safety Regulation, starting from July 2022 for all new vehicle models.

Cybersecurity in the automotive industry raises distinct challenges around the connected vehicle, the surrounding infrastructure and across connected IT systems and backends. It is very likely that cybersecurity, which is heavily connected to safety, is one of the major challenges facing the entire automotive industry. Like in many other industries, these challenges appear at each stage of its ecosystems lifecycle (plan, build and run).

---

[12] https://eur-lex.europa.eu/eli/reg/2019/2144/oj

3.5 Non-functional Aspects & Business Enablers (Ch.5)

Various non-functional aspects such as regulatory, standardization and business (impact) related issues need to be addressed before the successful deployment of CCAM services can be offered at cross-border environments.

3.5.1 Protocol Interoperability

V2X communications and CCAM applications are dependent on the smooth integration and interoperability among multiple components designed and developed by various manufacturers. The end-to-end chain of connected HW and SW potentially comprises among others 5G network radio and core components (physical or virtual), MEC/Edge and Cloud infrastructure, RSIs, vehicles, OBUs, platforms and application servers. It can be understood that even if one of these components cannot function or properly communicate with any of the others, the end-to-end functionality could be reduced or break down. Hence, interoperability and compatibility among the various components of the CCAM ecosystem is of paramount importance. This means that the architecture, interfaces, configuration, message formatting and input/output of each of the components must be well-established, known and compatible with the rest of the components.

To a certain degree this is addressed by standardization bodies for the telecommunications infrastructure and components, and by major vehicle manufacturers and Tier-1 suppliers for the automotive parts, which provide the guidelines for the design of various components. This is the case for instance for 5G networks where 3GPP is defining the design, interfaces and messaging of key components in order to ensure interoperability among different networks and MNOs; or for MEC where, among others, 3GPP, Linux Foundation, and ETSI have defined the guidelines for the MEC functionality and integration to mobile networks, as well as the CAM and DENM messages for V2X communication. However, they do not cover all aspects of the network / MEC functionality leaving enough room for network equipment vendors and other developers to apply their custom solutions which in turn introduces potential interoperability issues between third party implementations. Several additional fora and working groups exist for practical alignments and implementation/utilization decisions, which in turn may also take non-technical collaboration aspects into consideration.

3.5.2 Spectrum Harmonization

In November 2016 the Radio Spectrum Policy Group (RSPG) provided the first indications on the frequency bands that can be used for the development of 5G systems, identifying, together with the 700 MHz band, the 3.4-3.8 GHz band and the 26 GHz band (24.25-27.5 GHz) as priority bands to support the introduction of 5G systems. In the latest International Telecommunication Union (ITU) World Radiocommunication Conference (WRC-19), held in Egypt[13] in November 2019, new radio frequency bands for International Mobile Telecommunication (IMT) have been identified (4.25-27.5 GHz, 37-43.5 GHz, 45.5-47 GHz, 47.2-48.2 GHz and 66-71 GHz). This represents more than 17 GHz spectrum available for future 5G deployments, where 85% of it has been harmonized worldwide.

Inside the EU Digital Single Market (DSM) initiative, there is a policy definition for the spectrum[14] with four main areas: the identification of needs, the harmonization, the policy priorities and the regulatory environment. As a result, the European Union has defined the plan of spectrum harmonization for the three first relevant bands for 5G. Since then, as the spectrum market is managed locally in each country, the state governments have launched different frequency band auctions. The European Union is clearly leading 5G band auctions worldwide, with more than ten countries' bandwidth awarded in the last two years, but the planning of these auctions is not aligned and will be a risk in cross-borders situations, due to the fact of the

---

[13] https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/

[14] https://ec.europa.eu/digital-single-market/en/content/eus-spectrum-policy-framework

time needed to deploy the 5G infrastructure after being awarded. Moreover, the deployment requirements for the MNOs are different in each country, without a minimal commitment about coverage in road environments. Germany and France are examples where important coverage and throughput conditions have been defined in terms of surface or roads and no longer based on population. This is crucial for mobility services, but there are no common pan-European requirements, and this may definitely result in problems for cross-border scenarios.

In the same direction, the re-farming of frequencies which are currently being used in 2G/3G and 4G is under consideration in many countries. The main candidates to be used for 5G are the 3G bands of 2.1 and 2.6 GHz since the allowed bandwidth in these bands is a good fit for 5G services. This process is not coordinated by the EU and will impose new risks for the service continuity between different countries.

3.5.3 Road and Traffic related regulation

Currently, there are no national or international regulations specified for the roads and the corresponding autonomous vehicles moving on these roads. For instance, different vehicles will have different safety distance levels for emergency braking situations. In case of handing over the control of the driving from vehicle to driver, there should be standardized driver warning systems (which are not in place currently). A situation where a connected and automated vehicle has been homologated for the source country but not for the destination country may also occur. As an example, an Autonomous vehicle A has successfully passed the minimum tests required to drive in autonomous mode in country A, but it has not passed the tests on country B, or the tests are different in both countries; therefore, autonomous vehicle A is not authorized to be driven in autonomous mode in country B. These tests ensure that the vehicle is safe on that country, e.g. it takes into account the local laws, it has installed the maps for the route, etc. Lack of regulations may affect the vehicular hardware selection and its specifications; hence, compliance to several different systems of different brands can be costly from the perspective of OEMs.

Besides traffic and manufacturing regulations, the interaction of autonomous vehicles with local law enforcement agencies per country, is another significant concern. The rapid deployment of autonomous vehicle technology will undoubtedly have a significant impact on public safety services, including law enforcement agencies. In fact, connected and automated vehicles will reshape the nature of the interactions concerning traffic management emergency, police and other authorities.

3.5.4 Business models for cross-border environments

The building blocks of 5G-enabled CCAM solutions, especially in cross-border environments integrate multiple telecommunication and computing technologies. From a business point of view, these elements are developed and/or managed by different stakeholders that will participate in the value chain (e.g., Automotive Suppliers, Telecom Equipment vendors OEMs, MNOs), as also highlighted in [17]. New roles and business opportunities will be identified for different V2X use cases, including cross border scenarios. Use cases are some of the main drivers for the development of business models, business cases, value chains, and strategic decisions. Different EU-funded projects and European initiatives have started to analyse different aspects for business modelling of the emerging CCAM ecosystem., without a clear dominant option or direction.

In a cross-border environment, new relations between market players will be established [18]. For instance, new services definition and how connectivity can affect them by enhancing or enabling them for deployment. Business model examples, where the evolution from a linear value chain to a multi-linear relationship model might be expected. New neutral operators for dedicated AD and network functions (e.g. MEC service, RAN sharing, ToD) may erase, as well as adaptation of accounting and payment models in an inter-operator environment for mixed markets and different use cases.

The cost of deployment of the 5G technology to be used in any CCAM use case shall be divided in three fractions:

- Cost of 5G network deployment (Capital Expenditure - CAPEX)
- Cost of HW and SW for the embedded telco system in the cars (CAPEX)

- System operation (Operational Expenditure - OPEX)

In order to have a good profitability, these costs shall be balanced and compensated by, for example, the subscription of the customers, or by inclusion in the price of the vehicle. Other alternatives may exist, and these have to be explored. Currently, there is no clear model for CAPEX/OPEX sharing. The adoption of new business models for CCAM will help to identify appropriate financing schemes for 5G-enabled transportation solutions, revenue allocation and procurement models.

4 Technological Enablers for Cross Border Solutions

A set of potential solutions that could ensure that CCAM services can be supported efficiently in cross-border scenarios by addressing the above-mentioned challenges, are briefly presented in this section. Faster and more reliable handover of a data connection from one operator to another, inter-edge node coordination, QoS prediction and enhanced MNO collaboration schemes are some of the solutions investigated within the three 5G PPP ICT-18 corridor projects, that could mitigate the uncertainties during a real 5G cross-border scenario. The main technological enablers that allow for the implementation of such solutions in cross border environments and their impact on one or more of the identified key challenges are discussed below.

4.1 Edge Computing

Two challenges need to be solved in this context and they equally apply even to MNOs within a single country. This is related to Challenge 2 and 3 identified in Section 3. With Home Routing (HR) it is not possible to have a short route to MEC hosts associated with the currently visited MNO. They might not be reachable at all. With no inter-PLMN HO in place the challenge was actually easier to solve (at the cost of service continuity). When registering to the visited network, Local Breakout (LBO) routing, instead of home routing, can be selected. But with the targeted seamless handover across MNOs enabled, the vehicle will remain connected to the gateway of the previous MNO (HR). To change that, the mechanisms for changing the gateway, as described under Section 4.1.1 below, must be used.

The second challenge is related to information exchange across application servers deployed to MEC hosts related to different MNOs. There must be a solution assuring some kind of “managed latency” between MEC infrastructure related to different MNOs. One such solution is a service agreement with wide-area network providers for beyond best effort connectivity between MNO data centres.

4.1.1 Session/service continuity

This section provides further details about ***[Ch.2]*** described in Section 3 and discussed solutions in both 5G SA and NSA networks. ***The terms session/service continuity*** were introduced in the 5G Core specifications [6], but similar mechanisms exist with the 4G EPC and will be described first. It has to be distinguished where the decision of gateway and server switching is done. For every 4G network the modem control software can request the Packet Data Network (PDN) connection to be released and established again. This will trigger the mechanism to select a new gateway and the selection algorithm can be configured to select the closest one. This will also result in getting a new IP address from the IP address pool of that gateway. When implemented and enabled, the Selective IP Traffic Offload (SIPTO) [19] above RAN feature can be used to allow the network to take this decision. In this case, e.g., a radio handover to a cell belonging to a different Tracking Area could trigger a gateway change. But the mechanisms are the same and results in first disconnecting from the old gateway and then connecting again. So, there is a temporary communication outage.

The 5G Core introduces three SSC modes. SSC mode 1 corresponds to above described 4G EPC solution where a gateway change is triggered by the modem control software in the vehicle by releasing and immediately establishing a session. SSC mode 2 corresponds to SIPTO above RAN for 4G EPC. The advantage of SSC mode 2 over mode 1 is the possibility to exploit network internal information, especially on gateway placement, to trigger the reselection process. With the modem control software-based SSC mode 1 approach the vehicle would have to know when to trigger the reselection process in order to actually be connected to a different gateway than before. Both, SSC mode 1 and 2, result in temporary loss of connectivity when the previous connection is released but the new one is not established yet.

SSC mode 3 is introduced in the 5G Core allowing gateway switching without temporary loss of connectivity. The connection to a new gateway is established before the old one is released. The Application Function (AF) influence on traffic routing Application Programming Interfaces (API) can support information exchange between the 5G Core and application to negotiate when and/or where to trigger the gateway switching process or to make an application aware that such switching took place. The above described solutions for gateway switching only cover IP connectivity within the scope of the 3GPP network. In the end-to-end path between vehicle and MEC application further challenges need to be solved, as described in Section 3.2.2. It has to be noted that a gateway change will also result in a change of the IP address of the vehicle. It is an open question if/how this could change with IPv6 where the vehicle might have several IPv6 prefixes that can be used to avoid address changes.

Solving these challenges is ongoing work in the three corridor projects, but the following solution ideas are considered, so far: It is already a common paradigm to design and implement cloud applications in a way to have no or limited impact on the service when e.g. the IP address and/or TCP connection changes. Key to this is avoiding stateful context in the application and/or have the context in the vehicle software allowing to be reused across different application servers. One example are authorization tokens issued by a server to the client and then reused with different servers by submitting the information with every request. Alternatively, or complementarily, application servers can perform a context transfer between each other. A prerequisite is that they can communicate with each other. This is not trivial as MEC hosts from different MNOs might be located in different local networks with no public IP address.

4.1.2 Connecting MEC to the 3GPP network

Methods how to connect Edge Servers to 3GPP networks are similar for the 5G Core and the 4G EPC, but terms usage can be different. Figure 9 provides an overview of the relevant part of the 3GPP network architecture and provides 4G EPC (red), 5GC (blue) and commonly used terms (black).

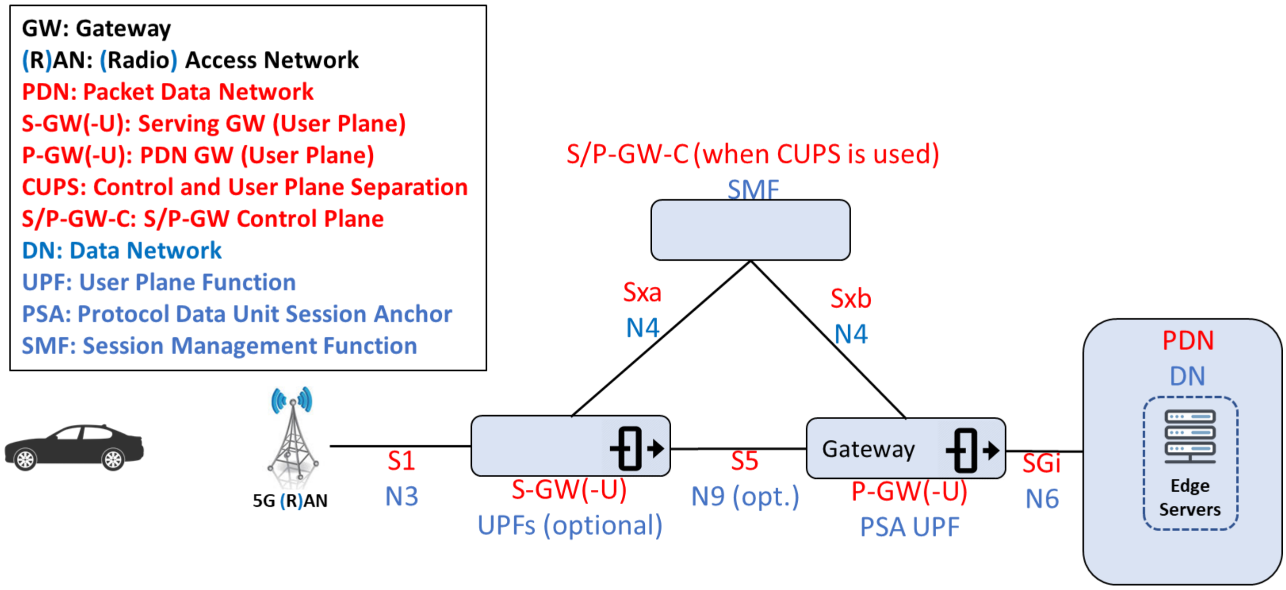


Figure 9: Mapping of 5G Core to 4G Evolved Packet Core (EPC) terms

One discussed option to connect MEC hosts to 3GPP networks [20][21] is through the S1 / N3 interface. This is also called “bump-in-the-wire”. 3GPP architectures do not explicitly mention this option but it is possible as the underlying transport network is built on standard IP (e.g. routers) and lower layer components (e.g. Ethernet switches). Traffic with certain characteristics can be therefore rerouted to MEC hosts. Problems when applying this option are applicability of identifying traffic to be rerouted when encryption is used. Furthermore, 3GPP security, lawful interception and charging functions were not designed for this [6].

With a 5G Core available, the preferred option of connecting MEC hosts is through "local"[15] PDU Session Anchor User Plane Functions (PSA UPFs) [22] [23]. Control and User Plane Separation (CUPS) is always applied in the 5G Core so there is no need to also deploy an extra Session Management Function (SMF).

In case of 4G Evolved Packet Core, as it is used for non-standalone 5G networks, CUPS is available from 3GPP Release 14 onwards. This enables the same options as for 5G Core to connect MEC hosts to the 3GPP networks but with less session/service continuity options, as SSC mode 3 is not supported (see Section 4.1.1). In case CUPS is not available or enabled, complete local S-/P-GWs, not just S-/P-GW-Us for user plane can be deployed. This makes no difference from an end-user performance point of view but requires more computational, memory and storage resources than for the more lightweight CUPS solution that only deploy local user planes.

The ETSI-MEC whitepaper [21] also includes the option of deploying a full 4G EPC with Mobility Management Entity (MME) and Home Subscriber Server (HSS). While this might make sense in some domains, e.g. industrial campus networks, it has no extra value for automotive use cases (continuity issues remaining) and just consumes more computational, memory and storage resources.

Such implementations of edge computing and their effect on session and service continuity as well as the direct exchange of data via interconnected MECs have the potential to (at least partially) address some of the roaming and data routing issues presented as part of ***[Ch.3]***, as the MNO collaboration among neighbouring MNOs would be enhanced and the information flow would be pre-determined and facilitated. The discussed solutions will be put to the test during the planned trials by all projects and further conclusions regarding the advantages and disadvantages of each one will be drawn.

4.1.3 Collaborating Systems: MEC – 5G – NFV Management and Orchestration

The treatment of isolated systems in a highly dynamic environment, such as CCAM, leads to problems as summarized in ***[Ch.2]*** and ***[Ch.3]***. Whereas the 5G System enables mobility management and handover, as well as session continuity, a change in a user's anchor UPF (PSA UPF) or additional UPF needs to be aligned with traffic treatment in the remaining network segments that the mobile data plane traverses between the user's UPF(s) and the Application Servers (AS), which is placed into the network infrastructure. Since first MEC solutions are available, services can be placed topologically closer to clients while leveraging the MEC value adding services. Most MEC platforms apply NFV technology to enable network function and service instance placement and scaling per demand. Whereas the ETSI ISG MEC is investigating the integration of MEC with the ETSI's NFV Management and Orchestration (MANO) architecture [24], a recently started study is analysing options to integrate MEC platforms into the 5G System [24].

In the view of ***[Ch.2]*** and ***[Ch.3]*** in particular, the projects are investigating platform solutions for mobile service provisioning and continuity in CCAM, leveraging and extending recent specifications and developments for MEC, 5G and NFV, in support of optimized service continuity for handover within as well as between MNOs. The projects' efforts address in particular gaps in recent specifications and deployments, including the following:

- Lack in the integration and inter-working of MEC and associated MEC platform management with hierarchical and de-centralized orchestration
- Lack in coupling MEC and NFV management with the 5G system to coordinate runtime changes in the setup and configuration to continue services for mobile users with the expected quality

---

[15] It is assumed that "central" PSA UPFs already exist and typically provide Internet connectivity. "Local" ones are used to provide further gateways, but it is not precluded that existing "central" ones are also used for that purpose, e.g. serving geographical areas close to existing "central" gateways.

- Lack in optimization for low-latency *edge-to-edge* CCAM service continuity. State of the art mainly focuses on *end-to-end* setup and management of services, as considered for network slices.

The design of an orchestrated platform for CCAM is taking strong alignment with the directions of various standards tracks into account, in particular with the ETSI MEC, ETSI NFV, and 3GPP. The current status and directions in the developed orchestrated platform for CCAM represents a well-integrated ecosystem made out of the 5G system, MEC, as well as NFV MANO. While the platform specification extends the current standard's semantic in support of CCAM platform specific operations, the key design focuses on the detailed functional architecture of the MEC network domain and associated integration of the MEC architecture with the 5G System and NFV orchestration as well as platform and network control and management functions.

In-line with the previously described CCAM use cases and the specified operations, which leverage in particular edge networks and the presence of MEC platforms, the specified CCAM platform addresses mainly operations at and between MEC platforms. In alignment with various associated standard track studies and directions [21]-[24], such as in the ETSI and 3GPP, the MEC platform (MEC PF) and an associated MEC Platform Manager (MEC PF Mgr) represent an integral part of the designed orchestrated platform for CCAM. The use of defined interfaces between the CCAM platform and the 5G system for loose coupling of the two systems is investigated, in support of proper service provisioning and continuation across international borders. Such solutions leverage the 3GPP's AF, which can be used to align user and traffic treatment policies between the 5G System and the MEC System levels. Early results of such integration and operational aspects have been disseminated to suitable standards tracks, such as the ETSI MEC group [24]. Figure 10 depicts an abstract view of an option for the integration of the MEC, NFV MANO and 5G systems.

In the view of cross-border operation, associated federation interfaces on orchestration layers as well as on 5G System layers are being leveraged. In alignment with the NIS Cooperation Group's 5G Risk Assessment, the projects analysed security and privacy threats associated with the defined use cases and are following, as an ongoing process, the design of the CCAM platform to identify and counteract potential risks. An identity management framework is being specified and developed, which can leverage the underlying technology, such as secure elements and other hardware components to establish trusted identities between vehicles and services.

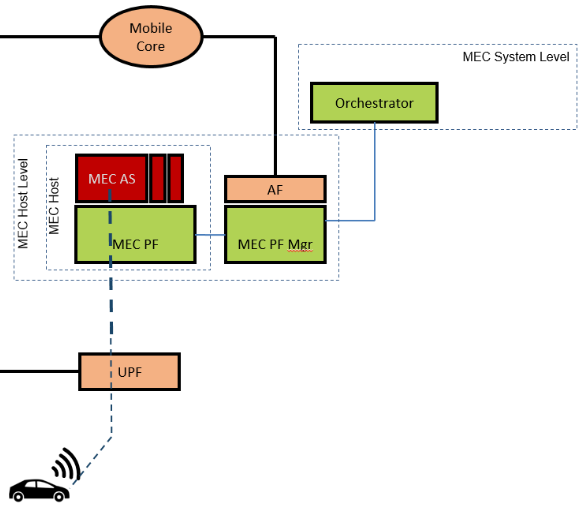


Figure 10: Abstract view of integrated 5G, MEC and NFV MANO systems [24]

4.2 QoS Prediction

In 4G and 5G mobile radio networks various methods are available to ensure QoS for applications, but they are only enforced by the scheduler based on the available radio-resources that can change over location and time. The geographical environment (e.g. tunnels, mountains), the weather conditions or even technical failures can create coverage gaps. Prediction enables in-advance information of the expected network quality for a given location and time to a specific subscriber of the network.

A QoS prediction scheme targets the assessment of the experienced QoS for each client and the early identification of a QoS degradation. It monitors different parameters of the network and environment from present and past to obtain a prediction. Furthermore, prediction algorithms can learn from past decisions to improve their accuracy or be trained. A notification is provided to the V2X application in case the minimum required QoS cannot be met, in terms of specific KPIs (e.g., data rate, packet loss, end-to-end delay). In the context of cross-border scenarios, the QoS prediction will be of crucial value. Since the coverage of multiple MNOs overlaps in border areas, a prediction about expected QoS change after the handover from one MNO to another can help a V2X application to adapt accordingly, ensuring service continuity and efficient driving behaviour. In 3GPP Service Architecture Working Group (WG), an architectural solution has been introduced about the notifications on potential QoS change [25]. The procedure for QoS prediction (or "QoS Sustainability" analytics, which is the term used in 3GPP) is provided by Network Data Analytics Function (NWDAF) and is described in 3GPP TS 23.288 [26].

QoS prediction can become a catalyst for CCAM operation at the borders over 5G connectivity, as it can enable pre-emptive actions to mitigate the effect of limited coverage or an imminent inter-PLMN HO (**[*Ch.1*]** and **[*Ch.3*]**). Such actions could be a HO preparation procedure being triggered earlier or resources pre-allocation at the visiting PLMN taking place, based on predictions of reduced QoS due to the vehicle's mobility as it approaches the borders. Such mechanisms could result in reduced HO interruption time and/or reduced attachment time and guaranteed QoS at the visiting PLMN, hence contributing towards the smoother cross-border functionality of stringent CCAM applications.

4.3 V2X Message routing

4.3.1 Sidelink

3GPP standardized C-V2X in Release 14 while an update specification is defined with Release 16 [25]. C-V2X supports two interfaces for communication, namely the PC5 interface and Uu interface. PC5 interface, based on 3GPP Device to Device (D2D) specified in Release 12 [27], supports direct communication between devices. It allows vehicles to directly exchange messages with each other (V2V) with roadside infrastructure (V2I) or pedestrians (V2P). C-V2X introduces sidelink transmission mode 3 (network coordinated V2V communication) and mode 4 (radio resource utilization decided by vehicles) and uses the 5.9 GHz ITS band. The direct communication mode in Release 16, 5G NR C-V2X sidelink offers major enhancements in terms of new short-range features in the form of higher throughput, lower latency, enhanced reliability, and improved positioning enabling advanced applications to complement the early basic ITS safety use cases.

5G NR C-V2X sidelink also moves the default mode of operation from broadcast to reliable multicast communication which is enabled by some fundamental new innovations. 5G NR C-V2X sidelink is probably the first wireless system to introduce distance as a dimension at the physical layer. This helps in getting a uniform communication range across widely varying radio environments — for both line-of-sight and non-line-of-sight scenarios. Introducing distance as a dimension also enables formation of "on-the-fly" multicast groups based on distance and applications. Such multicast groups require little or no overhead for group formation and dismantling.

With 5G NR C-V2X sidelink, vehicles reach a more sophisticated level of coordinated driving through intent sharing. 5G NR C-V2X is designed to facilitate negotiated intersection crossings (resolving the ambiguity that occurs at a four-way stop through intent sharing, thus improving traffic efficiency), coordinated lane changes leveraging lower latency communication, better positioning accuracy, and on-the-fly distance-based group formations.

While Uu interface supports communication between the device and the cellular network and related computation entities, PC5 interface supports direct communication between the devices. As such, this interface is ideally suited to support local low latency use cases like basic safety, cooperative manoeuvring and more. Uu interface can be used to communicate over wider geographical area, thus the communication on the two interfaces is complementary. Solutions based on V2X sidelink communication could help mitigate the effects of limited connectivity to the infrastructure or communication gaps due to the inter-PLMN HO (and hence help with addressing **[*Ch.1*]** and **[*Ch.3*]**) as they can provide vehicles with communication capabilities even when no connection to a 5G network is available. However, the smooth transition between V2N and V2V/V2I connectivity and the simultaneous assurance of service and session continuity during such an operation is a challenge on its own right and should be further investigated.

4.3.2 Cross-border Message Broker

In the automotive field, message brokers are used for dispatching Cooperative Intelligent Transportation Messages (C-ITS) messages (e.g., according to ETSI-ITS specification [28] or DATEX-II [29]) to and from road authorities, road operators, service providers and connected vehicles. Message brokers allow the implementation of the multicasting (availability of messages to a set of vehicles) and its special form called geo-casting (messages sent only to the vehicles present in a particular, service and/or vehicle preference specific area). The most common message broker platforms (such as MQ Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP) but also proprietary, tailor made ones) can be accessed by “producers” and “consumers”. The producers send information, the consumers receive it according to their interest and/or the recipient selection done by the broker. The message broker is use case independent and can be used in every C-ITS use case. But as many different message formats and broker types exist, interoperability becomes a challenge. So far, two solution concepts to overcome this are considered in the projects:

- Multi-format / -broker support: For example, the ACCA use case may support MQTT message brokers but also proprietary ones. Some vehicles encode the information in JSON while others use ETSI-ITS CAMs and DENMs. The message brokers, as part of the so-called “geoservice” support both and translate between the two.
- Interchange Functions: The above example for multi-format / -broker only considers two different solutions with some nuances. Changes in one solution often have consequences for the translation to and from the other one. Rather than unifying all potential solutions and/or creating translation function for all combinations, the concept of Interchange Functions was developed e.g. in the NordicWay [30] and InterCor [31] projects (there called Interface 2 (IF2)). It is being standardized by the C-Roads platform as “IP Based Interface” [32]. The idea is to have a well-defined channel between different solutions where information can be sent and received. The so-called “Improved Interface” is meant as control plane to e.g. discover what information a backend for a particular solution is interested in and where it wants to provide information to. Its specification is in an early stage. The “Basic Interface” defines how quadtree (see Appendix A of [32]) should be used for aligned georeferencing and defines AMQP as protocol and broker to be used. Currently, only support for ETSI-ITS messages and related payload format is defined in full detail, but the underlying AMQP protocol is agnostic to payload formats. The challenge for this is to cope with the fact that some attached meta-information, that can be used to filter within the possibilities of AMQP, can be message format dependent, like e.g. the service type or specification version.

The message broker is also network independent and can be accessed from every data network (mobile 4G/5G or fixed) with TCP/IP protocol.

Such a solution would help mitigate the effects of inter-PLMN HO **[*Ch.3]*** as it can assist with the direct and correct connectivity of neighbouring brokers as well as with proper data management procedures **[*Ch.4*]** involving data from users and vehicles of both countries.

4.4 MNO Collaboration Framework

One of the common themes for all three corridor projects is lack of common MNO cross-border (radio) network data, tools and processes. Although bilateral exchanges between MNOs exist, the radio network domain is in pressing need of alignment in order to establish 5G and its features everywhere in Europe. Since the non-technical aspect of collaboration take place between organizations, currently the 5GAA plays a big role by maintaining a dedicated activity on harmonized interoperability across multiple MNOs and car manufacturers with respect to the Automotive use cases. Nevertheless, a standardized, secure and automated collaboration between all European MNOs can only work with the governance of the European Commission.

Concerning the network handover/redirection, simply knowing detailed information about the used RATs in neighbouring countries minimizes the connectivity gap (and this might be sufficient for many use cases). A shared database, under common framework rules, with all base stations, radio cells, frequencies etc. likewise facilitates other radio network related inter-MNO constraints, including radio planning and optimization. This can be an indisputable, always up-to-date system of truth, interconnected with the 5G (and legacy) MNO radio network management systems. In such kind of digital collaboration framework, regulatory bodies and states can also easily participate, interact (e.g. for compliance audits or dispute resolution) and benefit from costs savings through integrated automated processes.

Such a framework of collaboration among neighbouring MNOs, may have multiple aspects and serve a multitude of targets, as with a generic implementation, any data can be securely exchanged, including roaming agreements and potential details about the network quality, SLAs, MNO capacities and resources, user and device identities etc. Such a solution could be assisted by AI mechanisms and predictive analytics where autonomous negotiations algorithms may agree on a minimum set of commonly agreeable configurations / settings for the functionality of the various CCAM applications.

Market self-regulation does not assure a coherent, non-discriminatory and controlled ecosystem, however once initiated and managed on a European level, the inter-MNO collaboration will constitute one of the fundamentals of the digital economy. As an example, from adjacent areas the GSMA also asks the governments for more policies[16].

Such a framework has the potential to address and/or mitigate the effect of many of the challenges mentioned in Section 3 and especially **[*Ch.1]***, **[*Ch.3]*** and **[*Ch.4]***. Coordinated exchange of data in a similar format may allow for more precise cellular coverage planning, taking into account interference from neighbouring countries, as well as roaming and HO configuration optimization among neighbouring MNOs and enable pre-allocation of resources. Moreover, the structured fashion of data exchange would follow strict rules which would be obeyed by both operators and hence the compliance to any applicable data, security and privacy regulations would be a given.

---

[16] https://www.gsma.com/newsroom/press-release/gti-gsma-call-for-governments-to-facilitate-the-5g-era/

4.5 Business & Deployment Enablers

4.5.1 Developing and fostering 5G-CCAM business models

Coordination between MNOs will be required to ensure high level reliability, as well as advanced mechanisms allowing real time handover between MNO(s) and this could change the business status compared to today's eMBB deployments for mass market. Network sharing, as well as slicing has been identified as possible solutions [25]. But this could create many challenges in terms of responsibility sharing between MNOs in order to achieve high availability of the overall system, in an end-to-end fashion. Indeed, if an accident occurs due to infrastructure breakdown at the time when vehicles are connected to shared MNO infrastructure, then the exact liability and responsibilities of each MNO are not clear. This could change the commercial relationship between MNOs and the risk will likely be integrated in the pricing. Furthermore, the revenues will have to be shared considering the level of investment of each MNO, as well as the quality of infrastructure which will have to be measured in real time. This will include complex mechanisms involving several MNOs. The same principles apply to MEC platforms in the respective MNO networks for enabling ITS applications, as these applications require interworking cross-MNO in both domestic and cross-border constellations.

Specific business models for CCAM operations over 5G connectivity including cross-border environments can be also helpful to combat / mitigate data management and security/privacy and regulatory challenges ***[Ch.4]***. By nature such models, include strict rules on what is and isn't allowed to take place in specific environments, who is responsible (and hence also has the liability) for certain operations, who has the rights to perform certain tasks (and corresponding obligations) and also define the manner in which the different stakeholders interact.

4.5.2 Strategic Deployment Agenda (SDA) for CCAM in Europe

The establishment of 5G and 5G-related Services is a priority for the European Union. In particular the Mobility Corridors on the road (and with the next wave of projects e.g. also waterway and other corridors) are in focus and thus, pave the ground for necessary infrastructure adaptations.

The Strategic Deployment Agenda for Connected and Automated Mobility in Europe (SDA) [18] presents the shared view of a wide group of stakeholders on the topic connected, automated driving and especially the role of 5G in this context. It promotes the rollout of 5G networks along transport paths to provide the necessary bandwidth required for the digitization of the automotive, mobility and transport sector going along with increased investments in future technologies such as artificial intelligence, cybersecurity, supercomputing and cloud computing.

5G communication technology is considered as one crucial part contributing to a combination of technologies that together assure total reliability and safety for fully automated vehicles. Other parts mentioned are sensors and positioning systems.

Eight principles are listed as common vision in the SDA. The first one stresses the importance of an evolutionary path throughout different technologies and their different generations stressing that even with 4G some services are possible but more demanding ones will be enabled with 5G. The second principle underlines the importance of service continuity across country borders, MNOs and many other stake holders, which is also the key topic of this white paper. According to the SDA, CCAM will only become reality if all relevant stake holders together form an overall ecosystem with boundless connectivity. Finally, the SDA hints to the fact that a 5G deployment according to the vision pointed out above will cost billions. It therefore suggests that the EU Connecting Europe Facilities (CEF) Digital program co-finances the rollout. An indicative list of 5G corridors to be prioritized is provided and includes the cross-border locations where the three 5G PPP ICT-18 projects conduct their 5G cross-border trials.

4.6 Standardization, security and regulation alignment

Many of the challenges mentioned in Section 3 can be addressed through the standardization of commonly accepted solutions which will consequently also standardize the way in which the various stakeholders interact. This applies to both technical aspects, e.g. network reselections rules as well as non-technical aspects such as data management, security/privacy issues, etc. **[*Ch.4*]**. Moreover, the inherent heterogeneity of the rules around border areas would be mitigated through the common understanding and mutual European agreements on traffic regulation, vehicular protocols/messages, conditions for network operations etc.

4.6.1 Cross-Border Regulatory Framework

The V2X infrastructure needs to support vehicles roaming independently of the manufacturer or on-board technology provider, while ensuring coexistence of V2X technologies and interoperability [33]. Authorities and civil infrastructure operators need to ensure that the nation-wide infrastructures support the roaming of vehicles without influencing its operation. Regulations will be required to ensure that infrastructures are being updated and compatibility is maintained.

In order to cope with the differentiated road and traffic regulation in neighbouring countries, the vehicle software needs to be adapted to the target location, so that it knows how to behave to respect local traffic laws. Even for the same country, the rules might vary depending on the type of road, e.g., speed limit or overtaking behaviour on urban vs. highway. In addition, roadside units of a specific region may need to supply different message types that may not be understandable by vehicles homologated in a different country. In such cases the vehicle might break the law if this has not been taken into account in the design of the algorithm, or the autonomous driving function might be restricted to certain road types, e.g., highway chauffeur. The lack of understanding of safety related messages may lead to dangerous traffic conditions for all road users.

On the radio network side, the planning and (inter-)operation must be adapted to the needs and practical usage instead of only considering historic national territories. The legal framework, regulation and governance of mobile networks have to be adapted on a European level (e.g. permitting extended coverage, joint networks, streamlined international administrative procedures etc.), otherwise the industry can adapt and provide the necessary networks and network services in a cross-border environment.

4.6.2 Data Ownership and Data Exchange

Data ownership, as well as data protection is one of the most challenging aspects to address [20]. Data ownership needs to be regulated and protected. Agreements between vehicle owners and manufacturers should be signed when vehicles are acquired so their data can be used to improve the safety of the vehicle. Laws should enforce that users have the rights of this data being able to remove it at all times. The data that leaves the vehicle and is stored by the road or telecom operator should preserve the highest level of privacy as defined by the GDPR. Authorities should regulate its use enforcing privacy at all times.

Stakeholders in the value chain, including car manufacturers, telco operators, road/city/highway infrastructure operators, navigation and map providers and protection authorities should define data sharing agreements so the entire infrastructure can be monitored, evaluated or tested. It is, however, not clear today which are the authorities that should take responsibility for orchestrating nationwide and even pan-European infrastructures. Nationwide data should be exchanged to nearby countries, first to cover cross-border scenarios but also to enable international support for V2X technologies and CCAM use cases.

4.6.3 Cyber-Security Measures

The plan, build and run stages (see Section 3.4.2) need to be addressed in order to prevent, detect and respond to cybersecurity threats. All connected services have to support end-to-end security and should be designed around the Defence-in-Depth paradigm. Proactive measures must be implemented from the start instead of reacting to problems in a production environment. These measures include:

- Threat modelling;
- Secure architecture design;
- Secure software development;
- Patch and vulnerability management;
- Technical security assessments (pen-tests etc.).

The same applies to data protection, as proper organizational procedures must be put in place to handle data protection. These mechanisms could include (but are not limited to):

- Data processing cartography;
- Privacy risk assessment;
- Data breach procedures;
- Documentation

Liability management with MNOs, Public Authorities, Road Operators, Service Providers and other relevant stakeholders should also be a part of the generic collaboration framework, while in order to ensure the necessary levels of security and privacy, the communication links from and to the vehicles should support the following requirements:

- Trusted and secure communications in different trust domains (supporting vehicle discovery, federation, etc.);
- End to end protection of information, including anonymization/ pseudonymization;
- Privacy by design;

Many of the challenges mentioned in Section 3 can be addressed through the standardization of commonly accepted solutions which will consequently also standardize the way in which the various stakeholders interact. This applies to both technical aspects, e.g. network reselections rules ***[Ch.3]*** as well as non-technical aspects such as data management and security/privacy issues **[*Ch.4*]**. Moreover, the inherent heterogeneity of the rules around border areas would be mitigated through the common understanding and mutual agreement on spectrum and protocol harmonization, regulatory frameworks, etc **[Ch.5]**.

4.7 Challenges / Solutions Overview

Throughout the three ICT-18 projects the several identified challenges were included in use cases or user stories in order to verify and evaluate solutions that are being developed by the several partners in all projects. Yet, as there isn’t a one-to-one correspondence between each challenge identified in Section 3 and the solutions suggested in Section 4, due to a significant overlap in some areas of actuation, Table 3 establishes this relation where the several challenges were addressed with potential solutions/enablers.

Table 3: Overview of challenges and potential solutions for effective cross-border CCAM service provisioning over 5G networks

Challenge	Potential Solution based on Technology Enablers
Cellular coverage and radio access aspects [Ch.1]	
Radio Planning and Cellular Network coverage at cross-borders	• MNO Collaboration Framework • Standardization and Regulation • V2X sidelink • 5G-CCAM Business models
Inter-PLMN HO	• Standardization and Regulation • QoS prediction • MEC utilization
Network Reselection	• MNO Collaboration Framework • Standardization and Regulation • QoS prediction
Service and Session continuity aspects [Ch.2]	
Cross-border message routing	• MEC utilization • V2X sidelink • Cross-border message broker
Data session continuity	• MEC utilization • Service Orchestration • QoS prediction
MNO collaboration & Data Plane routing [Ch.3]	
Isolated MNO planning	• MNO collaboration Framework • Cross-Border Regulatory Framework
Roaming / Data routing	• Security and Standardization • MNO collaboration Framework
Data management & protection [Ch.4]	
Data Management	• Cross-border message broker • MNO collaboration Framework • 5G-CCAM Business models • Security and Standardization
Security/Privacy and Regulatory compliance	• Security and standardization • 5G-CCAM Business models • Cross-Border Regulatory Framework
Non-functional aspects & business enablers [Ch.5]	
Spectrum Harmonization	• MNO collaboration framework • Security and Standardization • Cross-Border Regulatory Framework
Road, traffic, network and data regulation	• Standardization and Regulation • Cross-Border Regulatory Framework

5 Conclusions

5G officially starts with Release 15, approved in December 2017. While during 2019 the first smartphones have arrived in the market, more than 50 MNOs in more than 30 countries worldwide have launched one or more 5G services (compliant with 3GPP Release 15). According to the latest GSMA report [34], 1 billion 5G devices will be in circulation worldwide by 2024, while by 2025 the penetration of 5G subscriptions will reach 46% in North America, around 40% in China, Japan and South Korea and 30% for Europe. In terms of coverage, a third of the world population will be 5G covered by 2025, however the surface area coverage will be more limited than that, as initial deployments will focus on heavily populated urban areas. This aspect might be quite relevant for the provisioning of CCAM and V2X services, as 5G coverage will not be ubiquitous, especially in rural and cross-border areas.

The full potential of 5G will only be available when the networks will deploy the SA architecture; however, the added value for the connected vehicle is already demonstrated in the 5G cross-border projects. Concerning the massive adaptation, at the time of writing, only BMW has officially announced the arrival of 5G in its future vehicles, starting in 2021 with the iNEXT model[17]. Unresolved challenges when attempting to roll-out ubiquitous 5G services all over Europe will act as a deterrent for any further investments and will slow down the adoption and penetration of CCAM solutions. Hence, it becomes critically important to address currently unresolved as well as future cross-border challenges.

In this work (Section 3), several prominent cross-border challenges have been identified and categorized into ***five main categories***, which jeopardize the CCAM roll out and adoption at cross border areas, both technical and non-technical in nature. The importance of the proper ***interconnection of operator networks and edge computing sites*** across countries (neighbouring PLMNs), and its significant role in ***service and session continuity*** has been highlighted. Closely related, well-known issues with ***inter-PLMN handover, data routing*** across different data networks, ***radio planning and resource allocation*** as well as ***roaming*** challenges have been discussed and analysed. This was complemented by analysing the ***data management and security situation,*** as well as the existing concerns regarding ***privacy, GDPR and regulatory compliance*** for CCAM operations in multi-disciplinary/multi-stakeholder cross-border environments. An important insight is that besides the technical and operational aspects, there are also significant ***non-functional, business and regulatory (beyond standardization)*** aspects which need to be resolved in order to enable smooth and sustainable cross-border CCAM functionality.

In Section 4, various potential solutions to these barriers were discussed, based on available technological enablers and the research directions followed by the three ICT-18 corridor projects. In order to avoid the service continuity problems linked to the cross border scenarios, the ***components from different entities need to collaborate*** for mutual exposure of data and events, such as ***radio network information***, decisions to re-configure the network, ***UPF-assignments to a UE***, or the ***re-location of the complete MEC platform and service instances***. For inter-domain and cross-border service continuity, the ***coordination between the different 5G control- and management planes needs to be enabled both locally and federated***, based on clear ***MNO-collaboration guidelines and SLAs***. Especially the dynamic network adaptations and usage of local resources (i.e. edge cloud, MEC platform, service instances and UPF) may be required for service- and quality continuity after a failover or handover to a different network. Direct communication enabled by the V2X sidelink may also help address issues arising from the potential network connectivity interruptions during inter-PLMN HO.

The significantly ***improved performance of 5G*** and its novel features are also capable of mitigating several known barriers as they were previously evoked; however, additional measures will further increase the overall performance. For instance, in order to address the roaming and handover issues, ***proactive planning and resource allocation*** should be considered, taking into account the coverage and performance of the targeted network (e.g. handover to a 4G network could be handled by overprovisioning resources). ***URLLC***

---

[17] https://www.richmondbmwmidlothian.com/blog/2020/january/29/bmw-inext-will-be-first-5g-luxury-vehicle.htm

resource discovery and allocation may take place within the visited PLMN before the roaming takes place, hence partially dealing with the latency concerns. However, the best roaming performance is expected from the ***5G SA deployments*** thanks to their flexibility, ***slice management capabilities*** and the availability of specialized features (e.g. ***SSC mode 3 based mobility***).

Another enhancement example is the ***radio network data sharing among all MNOs***, a fundamental aspect not only for the ***network management***, but for many infrastructure aspects, ***administrative processes*** (e.g. for new base stations and its validation processes) and especially for the urgent problem of network outages at cross-country highways. Currently, in practise network reselection applies: UEs perform time-consuming frequency scans instead of rather being directly redirected to a foreign cell. A digitized, ***common reference system among all European MNOs***, for example in the form of a distributed database, would progress the MNO collaboration. Such an approach also reduces process times and costs, while laying the ground for further ***joint operations in areas like spectrum management***.

Despite any features which may be in place, service continuity and low latencies when roaming will always require diligent network resource configuration from the MNOs. The provision of intelligent and proactive network mobility solutions to ***anticipate performance degradation*** will further optimize the handover performance. As it is always possible to experience a complete loss of connectivity, it is critically important to also introduce '*fail-safes*' in all CCAM applications where in the worst-case scenario control would be passed back to the driver in a smooth transition (no last minute actions).

Orchestrated and collaborating cloud computing- and networking platforms for the deployment of ***virtualized CCAM services*** at network edges are investigated in alignment with the directions of various relevant bodies, in particular 3GPP, 5GAA, ETSI ISG MEC and ETSI ISG NFV. These platforms complement handover optimization techniques with service provisioning and continuity enablers and enable solutions in accordance with the ecosystem made out of the 5G system, MEC, NFV and NFV MANO. The projects are investigating the use and extension of defined interfaces between components of the orchestrated platform for CCAM and with the 5G system in support of ***proper service provisioning and continuation across international borders***.

5GCroCo, 5G-CARMEN and 5G-MOBIX partners are heavily involved in multiple standardization bodies (3GPP RAN and SA groups, ETSI, IETF) and are committed to disseminating critical project results which will help push towards a broader standardization of CCAM aspects and specific interoperability guidelines. At the same time, partners from all three projects are actively contributing to the various 5G PPP Working Groups, forming a common strategy with industry, academia and research, and providing further input to relevant regulatory and standardization bodies.

References

[1] 5G for Europe Action Plan: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

[2] 5G Automotive Association (5GAA), “A visionary roadmap for advanced driving use cases, connectivity technologies, and radio spectrum needs”, White paper, September 2020. https://5gaa.org/wp-content/uploads/2020/09/A-Visionary-Roadmap-for-Advanced-Driving-Use-Cases-Connectivity-Technologies-and-Radio-Spectrum-Needs.pdf

[3] Designews.com article, “Automakers Are Rethinking the Timetable for Fully Autonomous Cars”, May 2019, https://www.designnews.com/electronics-test/automakers-are-rethinking-timetable-fully-autonomous-cars/93993798360804

[4] NGMN, “*V2X White Paper*”, v1.0, July 2018, https://5gaa.org/wp-content/uploads/2018/08/V2X_white_paper_v1_0.pdf

[5] 3GPP TS36.300, “*Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2*”, v16.1.0, April 2020

[6] 3GPP TS23.501, “*System architecture for the 5G System (5GS)*”, v16.5.0, July 2020.

[7] 3GPP TS23.502, “*Procedures for the 5G System (5GS)*”, v 16.5.1, August 2020

[8] “Levels of Driving Automation,” Society of Automotive Engineers (SAE), https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles

[9] 3GPP TS 22.186, “*Service requirements for enhanced V2X scenarios*”, v16.1.0, December 2018

[10] 5G-MOBIX Deliverable D2.1, “5G-enabled CCAM use cases specifications”, April 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.1-Use-case-specifications-v1.0.pdf

[11] 5G- MOBIX Deliverable D2.2, “5G architecture and technologies for CCAM specifications” , July 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.2-5G-architecture-and-technologies-for-CCAM-specifications-V1.0.pdf

[12] 5G-MOBIX Deliverable D2.3, “Specification of roadside and cloud infrastructure and applications to support CCAM”, July 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.3-Specification-of-roadside-and-cloud-infrastructure-and-applications-to-support-CCAM-V2.0.pdf

[13] 5G-MOBIX Deliverable D2.4, “Specification of Connected and Automated Vehicles”, July 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.4-Specification-of-Connected-and-Automated-Vehicles-V1.0.pdf

[14] 5GAA Cellular V2X Conclusions based on “Evaluation of Available Architectural Options”, White Paper, 2020, https://5gaa.org/wp-content/uploads/2019/02/5GAA_White_Paper_on_C-V2X_Conclusions_based_on_Evaluation_of_Available_Architectural_Options.pdf

[15] ETSI TS 102 941 V1.2.1, “Intelligent Transport Systems (ITS); Security; Trust and Privacy Management”, May 2018, https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

[16] Silvia Giampaolo, “Regulatory and legal framework for automated vehicles”, Lexology article, https://www.lexology.com/library/detail.aspx?g=62f2bcbf-91ac-4dee-bb11-7666b1d1d9a0

[17] 5G PPP Automotive WG, “*Business Feasibility Study for 5G V2X Deployment*”, February 2019, https://bscw.5G PPP.eu/pub/bscw.cgi/d293672/5G%20PPP%20Automotive%20WG_White%20Paper_Feb2019.pdf

[18] 5G Strategic Deployment Agenda for Connected and Automated Mobility in Europe, October 2020, https://5G PPP.eu/wp-content/uploads/2020/10/20201002_5G_SDA_for_CAM_Final.pdf

[19] 3GPP TR23.829, "*Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)*", v10.0.1, October 2011.

[20] 5GCroCo Deliverable D5.1, "Description of 5GCroCo Business Potentials", September 2019, https://5gcroco.eu/images/templates/rsvario/images/5GCroCo_D5_1.pdf

[21] ETSI White Paper No.24, "MEC Deployments in 4G and Evolution Towards 5G", February 2018, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf

[22] Automotive Edge Computing Consortium (AECC), Technical Report v2.0, "Driving Data to the Edge: The Challenge of Data Traffic Distribution", https://aecc.org/wp-content/uploads/2020/07/AECC_WG2_TR_v2.0_July2020.pdf

[23] ETSI White Paper No.28, "MEC in 5G Networks", June 2018 https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[24] ETSI ISG MEC 0031, "Multi-access Edge Computing (MEC) MEC 5G Integration", July 2020.

[25] 3GPP, TS 23.287, "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services (Release 16)", March 2020.

[26] 3GPP TS 23.288, "Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 16)", March 2020.

[27] 3GPP TR 36.785, "Vehicle to Vehicle (V2V) services based on LTE sidelink; User Equipment (UE) radio transmission and reception", v14.0.0, October 2016.

[28] ETSI EN 302 665 V1.1.1, "Intelligent Transport Systems (ITS); Communications Architecture", September 2010, https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf

[29] European Committee for Standardization, CEN/TC 278, "Intelligent transport systems", January 2011, https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:31061,6259&cs=1AD0E6D5BFD62AC9653A3746374D70EE9

[30] NORDIC WAY 2, Deliverable 21:1, "Architecture, Draft", February 2019, https://uploads-ssl.webflow.com/5c487d8f7febe4125879c2d8/5ca71cee5f97516d05b07204_NW2_A2_D21_1_Architecture%20and%20Service%20Definition_Draft_190225_ver1.0.pdf

[31] INTERCOR, "Milestone 4 - Common set of upgraded specifications for hybrid communication", January 2019, https://intercor-project.eu/wp-content/uploads/sites/15/2019/03/InterCor_M4-Upgraded-Specifications-Hybrid_v2.1-final_INEA-1.pdf

[32] C-Roads Platform, "C-ITS IP Based Interface Profile", Version 1.7, June 2020, https://www.c-roads.eu/platform/about/news/News/entry/show/release-17-of-c-roads-harmonised-c-its-specifications.html

[33] 5GCroCo Deliverable D6.1, "Intermediate Report on Standardization, Dissemination and Exploitation Activities", April 2020, https://5gcroco.eu/images/templates/rsvario/images/5GCroCo_D6_1.pdf

[34] GSMA Report, "Realising 5G's full potential: Setting policies for success", March 2020, https://www.gsma.com/publicpolicy/wp-content/uploads/2020/03/Realising_5Gs_full_potential_setting_policies_for_success_MARCH20.pdf

List of Contributors

Name	Company / Institute / University	Country
Editorial Team		
Trichias, Konstantinos	WINGS ICT SOLUTIONS	Greece
Fernández Barciela, Antonio	Groupe PSA	Spain
Heider-Aviet, Andreas	Deutsche Telekom AG	Germany
Contributors		
Alonso-Zarate, Jesus	CTTC	Spain
Cantarero, Ana	BMW	Germany
Capato, Silvia	SWM	Italy
Centenaro, Marco	Fondazione Bruno Kessler - FBK	Italy
Fallgren, Mikael	Ericsson	Sweden
Fantini, Roberto	TIM	Italy
Fernández Barciela, Antonio	Groupe PSA	Spain
Fernandez Ferreira, Luis	Groupe PSA	Spain
Fischer, Edwin	Deutsche Telekom AG	Germany
Gavazzi, Roberto	TIM	Italy
Harutyunyan, Davit	Fondazione Bruno Kessler - FBK	Italy
Heider-Aviet, Andreas	Deutsche Telekom AG	Germany
Hetzer, Dirk	Deutsche Telekom AG	Germany
Katsaros, Konstantinos	ICCS	Greece
Kousaridas, Apostolos	HUAWEI	Germany
Liebsch, Marco	NEC Laboratories Europe GmbH	Germany
Martin, Angel	VICOMTECH	Spain
Moutinho, Joao	CCG	Portugal
Muehleisen, Maciej	Ericsson	Germany
Riggio, Roberto	Fondazione Bruno Kessler - FBK	Italy
Trichias, Konstantinos	WINGS ICT SOLUTIONS PC	Greece
Velez, Gorka	VICOMTECH	Spain

Contributing 5G PPP Projects

Phase 3 Projects

https://5G PPP.eu/5G PPP-phase-3-projects/

Acknowledgements

This work is part of the 5GCroCo, 5G-CARMEN and 5G-MOBIX projects. These projects have received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreements No 825050, 825012 and 825496, respectively. Content reflects only the authors’ views and the European Commission is not responsible for any use that may be made of the information it contains.