**5G Vehicle-to-Everything Services in Cross-Border Environments: Standardization and Challenges**

Apostolos Kousaridas, Mikael Fallgren, Edwin Fischer, Francesca Moscatelli, Ricard Vilalta, Maciej Mühleisen, Sokratis Barmpounakis, Xavier Vilajosana, Sebastian Euler, Bruno Tossou, and Jesus Alonso-Zarate

**Abstract**

Vehicles will be wirelessly connected in the future, and they will be able to exchange information with other vehicles and their surroundings for safer and more efficient driving. 5G communication systems have introduced advanced functionalities and radio solutions to support connected, cooperative, and automated mobility (CCAM) services with demanding quality of service requirements. However, interoperability among stakeholders, seamless connectivity, and the uninterrupted delivery of real-time services across borders are issues that should be carefully analyzed for the realization of cross-border CCAM services. This article provides an overview of key standardization bodies by analyzing recent work on key technologies to provide cross-border connectivity services for CCAM. Standardization gaps and regulatory barriers that may affect fast and efficient adoption of 5G-enabled CCAM services are also discussed.

**Introduction**

Vehicles of the future will be more automated and wirelessly connected to cooperate with each other and with their surroundings, including road infrastructure, pedestrians, and so on. Wireless communication among vehicles can complement onboard sensors by extending detection ranges even when visual line of sight is not available. Wireless communication is also important for cooperative maneuvers among vehicles. Both features can contribute to safe and efficient driving, especially for higher levels of driving automation, where no or limited human interaction is needed.

Cellular vehicle-to-everything (C-V2X) communication enables the provision of both driving support and other broadband services that create added value for the end users. Connected driving support can be enabled through long-range connectivity, that is, using the Uu interface between the network infrastructure and the end-user equipment, which can bring information and thereby awareness from far away to the vehicle, and through short-range connectivity, that is, using the PC5 interface between devices without routing data through the network infrastructure, allowing the local exchange of information in the immediate surroundings of the vehicle. Hence, CV2X removes the limitation of vehicles to only rely on onboard sensor information. However, for reliable and safe V2X communication services, both connectivity and quality of service (QoS) shall be properly predicted so that vehicles can plan ahead, anticipating the future quality of connectivity as well as any potential network downtime periods. In this context, two additional important features leveraged by 5G technology are mobile edge computing (MEC) and cloud, which bring cloud service computations to the edge of the network to enable flexibility and the opportunity to reduce latency when needed, and enhanced accurate positioning to, for example, protect vulnerable road users (VRUs). It should be noted that in this article the mobile edge cloud enables MEC, so the expansion of the acronym depends on the sentence. The “M” should not stand for “multi-access,” since this would point at just one subset of MEC-related specifications, that is, the European Telecommunications Standards Institute (ETSI) ones. “Mobile” is used instead to stress the relation to mobile radio networks as specified by the Third Generation Partnership Project (3GPP).

Due to the introduction of connected, cooperative, and automated mobility (CCAM), the business models for the automotive industry are about to change. 5G could be a catalyst to enable new features in CCAM services as well as new value chains. More specifically, the value chains will change from the traditional customer/supplier roles toward a more dynamic and network-oriented paradigm. For the success of such an evolution and specifically for the faster adoption of V2X, the cooperation between the telecom and automotive industries can help to address all challenges and open issues of CCAM services.

Overall, the deployment of a complete V2X infrastructure is a complex task with several standardization, regulatory, and legal issues that involve various stakeholders, such as mobile network operators (MNOs), transport authorities, road operators, and service providers. The provi-
sion of CCAM services across different countries in Europe need harmonized solutions to support cross-border traffic, when vehicles drive through various national borders. There are technical and regulatory challenges due to the need for seamless connectivity and uninterrupted delivery of real-time services across borders. Taking into account the multi-operator, multi-country, multi-car-manufacturer, multi-telco-vendor, and cross-generation scenario of any cross-border services, it is evident that the situation becomes more challenging.

In this article we present an overview of the current status of key standardization activities as well as potential gaps (i.e., standardization, regulatory, business, and legal) that should be taken into account for the successful realization of 5G-enabled cross-border CCAM services. In particular, in the following section, we describe the current activity status of related standards and the maturity level of available communications technology. We then dwell on regulation aspects, and following that, provide a business case perspective. The final section concludes the article.

**Standardization and Technology Status**

From a technical perspective, different entities shall interact to deliver CCAM services enabled by 5G across borders. On a high level, four tiers can be identified:

- The vehicle tier, which comprises cars and other road vehicles
- The network tier, which comprises cellular networks and intelligent transportation systems (ITS) infrastructure
- The cloud tier, which comprises clouds that form back-end systems
- The application tier, which comprises applications to support CCAM services

Figure 1 presents the technical entities, technologies, and standardization bodies that are involved in the provision of 5G-enabled cross-border CCAM services. In particular, it is worth highlighting the following technologies and features, which are discussed in this article:

- Handover between borders and/or MNOs
- MEC
- Slicing
- Service continuity

The current standardization status as well as potential gaps are analyzed in the following.

**Handover across Borders and/or MNOs**

Cross-border/-MNO handover, which is called “inter public land mobile network (Inter-PLMN) handover,” has been a requirement even for 4G LTE networks. But today’s networks usually do not allow cross-MNO handovers. As analyzed below, there is an initial technical solution, but the required links for interfaces across MNOs are not in place, mainly due to the introduced complexity since each country has several MNOs that might need to be interconnected. However, it is necessary to evaluate the solution as a decision basis to deploy the links for cross-MNO interfaces, determine the QoS requirements for these links, and also to investigate further enhancements, considering the demanding QoS requirements that many V2X services have (e.g., low latency).

The network to which a user subscribes is called the home network, while the network to which the UE roams when leaving the home network is called the visited network. Experience shows that when leaving a country, a user equipment (UE) will stay connected to the network of the previous country (home network) until it is so far away that it loses synchronization to the last serving cell in the home network. For many seconds, or even minutes, radio link quality can be very low, making even simple mobile broadband (MBB) services and voice calls infeasible. After loss of synchronization, the UE will perform...
In local breakout, the user plane traffic is routed directly from the visited network to the data network, while authentication and handling of subscription processes take place at the home network. In home-routed, the visited network user plane traffic is routed to the data network via the home network.

**FIGURE 2.** Standalone 5G New Radio home-routed roaming architecture with N14 interface between AMFs.

A scan and attach to a new network in the new country (visited network). It will then establish a new connection, usually resulting in a new IP address being served by a different network than the home one. This process is called “roaming.”

Analysis performed for the delay of the registration procedure indicates that this roaming procedure is time consuming and introduces delays in the range of seconds or even longer [1]. The analysis in [1] shows that the attachment latency to a visited network may require a few tens of seconds due to the sequential process and the context transfer procedure, while toward the home network it may require up to 9 s. The required attachment time can be affected by various factors, such as roaming agreements, or the load of base stations or core networks. In a roaming procedure [2], interaction between the access and mobility management function (AMF) in the visited network, unified data management (UDM) functions in the visited and home networks, and the policy control function (PCF) in the home network is needed. According to [3], the time required to perform a single attachment procedure (without considering roaming delays) is in the range of hundreds of milliseconds (~330 ms), which is unsuitable for many time-critical V2X use cases, such as cooperative maneuvers and tele-operated driving, which have latency requirements of less than 50 ms [4].

In 5G communication systems, local breakout or home-routed roaming schemes could be used to reduce these delays. In local breakout, user plane traffic is routed directly from the visited network to the data network, while authentication and handling of subscription processes take place at the home network. In home-routed, the visited network user plane traffic is routed to the data network via the home network. Figure 2 shows the home-routed roaming architecture using a standalone 5G core communication system. In 5G, security edge protection proxies (SEPPs) are used to secure the connection between the home and visited networks.

5G communication systems can enable cross-border/-MNO radio handover by deploying the N14 interface between the AMFs of the involved operators (Fig. 2). As a result, the same handover procedures as within the same network with AMF change apply. Such a solution requires agreements between the MNOs and the deployment of particular interfaces. In this case, the user plane function (UPF) could remain unchanged in order to provide session continuity; however, the details of such operation have to be defined. It should be noted that even in the LTE communication systems, the inter-MNO handover can be enabled by employing the S10 interface between mobility management entities (MMEs) across different MNOs [5].

In either of these cases, cross-MNO handover using either N14 (in 5G communication systems) or S10 (in LTE communication systems) aims to keep session continuity and minimize interruption time. However, even though this is supported by the 3GPP specifications, to the best of our knowledge, it is not deployed in current 4G or 5G networks due to the need for interfaces across networks managed by different MNOs. Also, cross-vendor interoperability tests are necessary. According to [5], in a cross-MNO handover, the home and visited networks have to interact in order to exchange the following information:

- Static information, for example, neighbor cell lists, interconnecting traffic, and signaling links
- Dynamic information, for example, real-time signaling information related to target cell selection
For the reduction of the required time for the exchange of the information mentioned above, some particular actions (e.g., context transfer, proactive registration) can be performed in advance, that is, before the actual handover process is triggered. Nevertheless, to the best of our knowledge, this feature has rarely been evaluated in a systematic manner. However, it is important to evaluate the performance of cross-border/MNO handover in commercial networks if CCAM services, which require uninterrupted service provisioning, are to be offered.

**Mobile Edge Computing/Cloud**

MEC is a key technology to meet end-to-end latency requirements introduced by novel 5G services and aims to improve the efficiency of the whole network operation through the deployment of computing and storage resources at the edge of the network, closer to mobile users. The exploitation of edge resources offers the possibility to execute computing tasks in a distributed manner directly at the edge of a network, reducing the traffic load on the core of the infrastructure and guaranteeing faster service responses. The adoption of MEC technologies is particularly suitable for V2X use cases due to its intrinsic characteristics such as proximity to the end device as well as ultra-low latency and availability of high bandwidth.

With respect to MEC integration into 5G systems, 3GPP has defined a list of enabling functionalities that are provided in [6], where a basic application programming interface (API) for application function influence on traffic routing is specified. Further key issues and potential solutions are being studied in a corresponding Release 17 Study Item [7].

One feature, especially useful in the automotive context, was introduced in the 5G Core in Release 15. It enables a seamless change of session anchors (5G Core Protocol Data Unit Session Anchor, PSA, UPF) to have a short route between a vehicle and MEC-hosted application servers (ASs). This includes mechanisms within the 3GPP core domain like Session and Service Continuity mode 3 of the 5G Core [6]. Further adjustments might be needed for improved end-to-end solutions where challenges like server discovery, IP address changes, and connection-oriented transport layer protocols (e.g., TCP) must be supported. Even though not all of these are within the 3GPP specification domain, 3GPP might provide solutions supporting this.

The ETSI Multi-Access Edge Computing Initiative provides further specifications in the context of MEC; for example, APIs allowing applications and the network to exchange information [8]. Following this approach, applications deployed in MEC environments can benefit from real-time access to network-related context information, which can also support automotive use cases [9].

To date, one of the major challenges in the management of MEC applications remains the application portability among different platforms (i.e., technical solutions). From a commercial point of view, each MNO offers its own solution; this requires the adaptation of the application format each time, thus limiting the possibility of deploying distributed services across different administrative domains unless resorting to custom solutions. ETSI MEC ISG has specified a MEC application data model and life cycle management APIs with the purpose of defining a general and standardized approach for the orchestration of MEC application. A further important aspect is related to the dynamic and transparent management of service level agreements (SLAs) between service providers and customers, which represents a key asset toward the adoption of federated MEC ecosystems for running end-to-end services. In this direction, the TM Forum alliance is working on the specification of a business-oriented API, with several provided specifications (e.g., on SLA management [10]).

Currently, we have no reason to believe that further essential standardization efforts on MEC are required, focusing on cross-border V2X services. Instead, solutions specified in 3GPP and other fora need to be profiled. This first could be done for a specific V2X use case, due to the use-case-specific service continuity requirements, and then it could be merged to a common profile or set of profiles suitable for a larger set of V2X use cases.

**Network Slicing**

Network orchestration aims to provide functionalities and mechanisms for managing end-to-end network slices to support automotive services deployed across different geographical, administrative, and technological domains. In such a context, different challenges have to be taken into consideration for orchestrating end-to-end services and instantiating the associated slices. In particular, the end-to-end service must be decomposed into multiple service components to be instantiated in the underlying single administrative domains, where the different virtual network functions (VNFs) and ASs composing the end-to-end service chain can be placed in either a centralized public cloud or the MEC. For instance, depending on the specific service, the service decomposition can result in a set of centralized management functions plus several distributed functions running in MEC hosts for data processing in proximity to the vehicles.

Network slicing is a feature of 5G networks to provide different specific networks to different types of uses and users (e.g., end users, enterprises, public safety). It is considered a key mechanism of 5G in order to serve vertical industries with different service needs, depending on latency, capacity, or reliability. Network slicing was introduced in 3GPP Release 15, and a V2X slice suitable for the specific requirements of V2X services has been specified [6].

Road authorities are interested for V2X services such as hazard warnings and in-vehicle signage, as well as coordinating cross-border services. An ultra-reliable low-latency communication slice is required for fast and reliable reception of safety-related messages. In order to support these requirements, network resources could be allocated at the edge cloud, as close as possible to the users, or adequate transport network resources toward the central cloud should be allocated for the slice.

According to [11], a network slice is composed of a service profile, which models the
characteristics of the mobile traffic, and a network slice subnet, which contains/references NFV applications’ elements (i.e., network services and VNFs). In addition, a network slice subnet can potentially contain several other network slice subnets, enabling a recursive model, where a network slice is then composed by one or more subnets. From a cross-border scenario point of view, this recursive modeling is an important enabler for the definition of end-to-end network slices where subnets are indeed “nested” network slices provided by different operators in different administrative domains, including the possibility of sharing subnets for running services belonging to different tenants. ETSI NFV proposed integration of a network function virtualization (NFV) data model in the 3GPP network slice data model [12].

Some of the challenges that network slicing will face are related to the introduction of trusted and isolated smart connectivity services. It is envisaged that network slicing will be used end-to-end, considering the core network and radio access network (RAN). The on-demand capacity broker has been introduced by 3GPP to further improve RAN sharing flexibility. It is envisioned that it can be performed in networks by the user requesting the network slice, evolving the concept toward a smart connectivity service [13]. Cross-border scenarios also represent a research challenge for network slicing. Network slice stitching refers to a management operation consisting of creating an end-to-end network slice or a larger network slice subnet by interconnecting a set of network slice subnets together through interconnection anchors, which represent cross-domain endpoints. Furthermore, research on the relationship of network slicing and network monitoring with analytics is an ongoing work. To provide autonomous smart connectivity services, several autonomic network architectures have been considered so far.

**Quality of Service Tools for Application Adaptation**

Service adaptation to achievable performance is an important requirement for critical V2X services (e.g., safety, autonomous driving), especially in cross-border environments. On the other hand, many V2X applications can use different application-layer configurations (e.g., speed video configuration), depending on the achievable communication performance, which might be mapped to different QoS levels. This is a very useful feature, since the applications can operate with alternative QoS profiles (e.g., even lower QoS) that could be selected instead of the initial QoS profile.

The V2X AS can provide a list of alternative service requirements to the 5G system (5GS) for the V2X applications that can operate with different configurations (e.g., different latency requirements). This allows the 5GS to support alternative service requirements and apply them for the extended NG-RAN notification, as described in [6]. Improved service adaptation and the avoidance of a session interruption due to QoS degradation are the key benefits that the support of alternative QoS profiles can provide to a service.

In addition, the experienced QoS may be affected by various parameters (e.g., mobility, roaming, and channel conditions). Harsh application adjustment due to a QoS degradation is not appropriate and may affect the V2X services’ performance, since this might lead to service discontinuity and impact traffic efficiency. Hence, an application may have to adjust its configuration (e.g., increase inter-vehicle gap) according to the QoS that can be delivered. To each application-level configuration, a different QoS level (e.g., data rate, latency) may be associated. V2X applications can be promptly notified of predicted change of QoS before the actual change takes place, thus allowing the application to gracefully adapt its behavior and configuration to the expected achievable performance.
3. Cloud and Application
- Increasing automation
- e2e protection, especially cross-country
- Diverse, open, mobile ecosystem
- Responsibility, compliance
- Country specific rules/specifications

1. Vehicle
- Architecture complexity
- Missing overall standard security
- Safety-security gap

2. Network
- Increasing connectivity with vulnerable channels
- Integration IT – vehicle
- High mobility and low latency impacts also security
- Fast roaming

3. Cloud and Application
- Homologation of the whole technical chain, which
dification of an automated vehicle will require the
together, whose framework should consider future connected
moving on roads. This testing and certification
defined for autonomous vehicles
such regulation defined for autonomous vehicles
by artificial intelligence. Currently, there is no
automated vehicles has already been identified as
specification of testing procedures of standalone
for CCAM services at cross-border
data management and ownership are some of
ensure their successful mass market adoption.
the challenges of CCAM services at cross-border
topics that should be addressed for realization
3GPP has introduced an architectural solution
for notifications of potential QoS change [14].
The goal is to enable 5G communication systems
to provide analytics information regarding potential
QoS change upon request from a V2X AS.
The procedure for QoS prediction is provided by the
network data analytics function (NWDAF).
The V2X AS can provide the notification to the
vehicle side if needed in case adjustment of application behavior is handled by an in-vehicle application.
Predictive QoS support has also been identified as one of the key solutions for mobility and quality of experience (QoE) support issues, described by ETIS, in the context of the MEC framework [9]. One key example is illustrated in
Fig. 3, where the relocation of application state
information to the target MEC host is completed before connecting to the MEC host.
The above-mentioned solutions of alternative QoS profiles as well as QoS prediction analytics
have been currently standardized only for the
Uu interface, while further analysis is required
for cross-border/MNO interactions, where both
could be useful to improve service adaptation
capabilities and to maintain operational V2X service
regardless of QoS degradation.

REGULATION ASPECTS STATUS
Besides the technical challenges analyzed in the
previous section, there are also many regulatory
topics that should be addressed for realization
of 5G-enabled cross-border CCAM services and
ensure their successful mass market adoption.
Certification, liability, safety, security, as well as
data management and ownership are some of
the challenges of CCAM services at cross-border
areas that are analyzed below.

CERTIFICATION, LIABILITY, AND SAFETY
The need for certification (homologation) and
specification of testing procedures of standalone
automated vehicles has already been identified as
a real problem, especially for vehicles controlled by artificial intelligence. Currently, there is no
such regulation defined for autonomous vehicles
moving on roads. This testing and certification
framework should consider future connected vehicles with 5G connectivity capabilities, together
with the impact on V2X infrastructure. Certification of an automated vehicle will require the
homologation of the whole technical chain, which
includes vehicle, network, cloud, and application side. Moreover, the regulation of homologation
is necessary to avoid incompatible testing and certification schemes in different countries or the
need for different certification processes in specific
countries.

Cyber-resilience is needed to guarantee safety of a
distributed decision making layer highly vulnerable
to attacks. Vehicle and passenger data must also
be protected end-to-end in terms of confidentiality,
integrity, authenticity, and privacy, while being compliant with regulations, especially among different countries.

App. A - Table 1: CCAM Services Regulatory Aspects Status

| Certification, Liability, and Safety |
|-------------------------------------|
| Compliance                        |
| Liability                          |
| Safety                             |
| Security                           |
| Cross-border Interaction            |

App. A - Table 2: CCAM Services Challenges

| Challenge                                                                 |
|--------------------------------------------------------------------------|
| Network Infrastructure                                                   |
| V2X Connectivity                                                         |
| Data Management and Ownership                                            |
| Security and Privacy                                                     |
| Cloud and Application                                                    |
| Homologation and Certification                                           |

Fig. 4. Root causes of security challenges.
To address these types of challenges, a holistic vision of protection is required. A regulation for the uniform provisions concerning the approval of vehicles related to cyber security and cyber security management system is under definition by the United Nations Economic Commission for Europe and will be applied in the framework of EU Regulation starting in July 2022 for all new vehicle models.

**DATA MANAGEMENT**

Vehicles are the most essential part of a data-shaped CCAM ecosystem. Vehicle and passenger data will be collected, stored, analyzed, and shared with different stakeholders using multiple channels. Difficult trade-offs must then be found between integrity of information, safety of vehicles, and privacy of drivers and passengers.

The different CCAM stakeholders are responsible only for a part of the data, while the privacy of the vehicle driver is of utmost importance. Data ownership, data sharing, and data exchange are very important procedures. For instance, practical issues arise when video sensors capture private and sensitive data. The real-time data generated by different actors or subsystems (e.g., by the vehicular control application running on a cloud server) together with operational logs of the infrastructure (e.g., MNO) will be stored at data repositories and could be used to estimate the load in the road infrastructure among other derived applications. Other stakeholders may be interested in using the stored data, such as insurance or third-party companies that aim to exploit mobility patterns to derive other businesses (e.g., smart parking). Considering the criticality of the infrastructure and the generated data, regulators should clearly define protective laws and enforce that the storage of this data must be subject to privacy frameworks such as the General Data Privacy Regulation (GDPR).

Regulation and protection of data ownership is needed. For instance, a vehicle’s data can be used for safety purposes based on agreements signed between vehicle owners and OEMs. Also, the data that is sent from the vehicle and is stored by the road or telecom operators should preserve the highest level of privacy, as defined by the GDPR. Authorities should regulate its use, enforcing privacy at all times.

As another example, road operators that are in charge of traffic management have the mission to inform all road users when an event occurs (e.g., an accident) to protect the incident zone from any secondary incident, manage the issues related to the incident, and clean the road after the incident is closed. For that reason, interfaces for data exchange between road operators, telecom operators, service operators, and vehicles are needed. The definition of data sharing agreements among involved stakeholders, including MNOs, road authorities, vehicle manufacturers, map providers, and so on, is needed to enable various CCAM services. This will allow the monitoring, evaluation, and testing of the entire data exchange. However, the authorities responsible for the orchestration of nationwide infrastructures have not been identified yet.

Nationwide data should be exchanged between neighboring countries to support cross-border CCAM scenarios and to enable international support of V2X technologies. Once the regulation authorities of a country are defined, they will need to define the agreement policies for transnational information exchange. Cross-border data exchange becomes more challenging considering countries that use different privacy frameworks.

**BUSINESS CASE PERSPECTIVE**

The development of 5G technology needs to be sustained by economic models that can pay back the capital expenditure required to materialize the 5G deployment and ensure that its operation is maintained thanks to regular income. The cost of 5G technology deployment can be divided into the following three fractions:

- Installation costs of hardware and software for the communication components of the vehicles (capital expenditure, CAPEX)
- Infrastructure cost in terms of 5G network deployment (CAPEX)
- Maintenance costs in terms of the system operation (operating expenditure, OPEX)

These costs related to building and maintaining the system need to be compensated for by, for example, regular subscriptions of the customers/users or by inclusion in a vehicle’s selling price. The key motivation for customers to pay and contribute to the CAPEX and OPEX relies on the expected benefits of innovative features and services that allow enhanced safety, improve traffic efficiency, and provide real-time awareness and infotainment services.

The identification of the appropriate billing models for CCAM services is an open issue. For example, the services used to enable CV2X capabilities, and thereby the corresponding data bits used to enable those services, could be seen as more advanced specialized bits than the more regular broadband bits providing, for example, Internet access. In a pricing model, it could thus be reasonable to charge a premium fee for more advanced specialized bits compared to regular broadband bits, for example, when cross-border uninterrupted service provision with guaranteed QoS is needed.

Different roads have different characteristics; while network coverage in urban and inhabited areas most likely provides sufficient coverage and capacity for roads, the same cannot be taken for granted in rural or cross-border areas, where either coverage or capacity might not be sufficient to support uninterrupted 5G V2X services, also considering that different countries have different road and network infrastructure deployed. In very rural areas (e.g., where roads may have very few vehicles per day) or remote cross-border areas, it is expensive to build out full-fledged 5G coverage; therefore, there is a need to find incentives and define cooperation models to ensure that 5G-enabled CCAM services can be delivered. For this particular reason, together with urban areas, densely vehicle-populated highways are foreseen to be locations where early rollout will take place, given that these networks will deliver V2X services along with regular services such as voice and broadband data.

The identification of appropriate cooperation models between road authorities and MNOs is an
important factor that can enable the deployment and use of 5G infrastructures for CCAM. A cooperative planning model can create synergies for connectivity deployment along CCAM corridors networks in a cost-effective manner. The 5G Strategic Deployment Agenda (SDA) for CCAM services in Europe is an initiative to provide common ground among different stakeholders [15].

### Conclusion

The provision of cross-border CCAM services creates many business opportunities. On one hand, there are technical challenges (e.g., seamless communication and uninterrupted real-time services across different countries) that can be addressed via 5G technologies. But on the other hand, there are several legal, regulatory, and business issues that should be considered. Table 1 provides a summary of barriers, requirements, and gaps from the standardization, regulatory, business, and legal perspectives, which have been discussed in this article and should be addressed for fast and efficient adoption of 5G-enabled CCAM services, especially in cross-border environments. For the majority of the identified technical issues, there are either initial solutions or proposed enhancements that could be adopted. At this stage, the evolution of the regulatory framework and the coordination among involved stakeholders (e.g., for liability management, data management, and privacy and security issues) constitute probably the most important factors for the development of a consistent ecosystem that is needed for cross-border CCAM services.

### Acknowledgments

This work is part of 5GCroCo project that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 825050. The work has also been supported thanks to Spanish AURORAS (RTI2018-099178-B-I00) project.

### References

[1] S. Monshaf et al., “Cellular Network Coverage Analysis and Optimization in Challenging Smart Grid Environments,” Proc. IEEE Int’l Conf. Commun., Control, and Computing Technologies for Smart Grids, 2018.
[2] 3GPP TS 23.122, “Non-Access-Stratum (NAS) Functions Related to Mobile Station (MS) in Idle Mode,” v17.1.1, Release 17, Jan. 2021.
[3] R. Trivisonno et al., “Towards Zero Latency Software Defined 5G Networks,” Proc. IEEE Int’l Conf. Communication Wksp., 2015.
[4] 5GAA, “White Paper C-V2X Use Cases Volume II: Examples and Service Level Requirements,” Oct. 2020, https://5gaa.org/wp-content/uploads/2020/10/5GAA_White-Paper_C-V2X-Use-CasesVolume-II.pdf.
[5] 3GPP TS 22.129, “Service Aspects; Handover Requirements Between UTRAN and GERAN or Other Radio Systems,” v16.0.0, Release 16, July 2020.
[6] 3GPP TS 23.501, “System Architecture for the 5G System (5GS),” v16.7.0, Release 16, Dec. 2020.
[7] 3GPP TS 23.748, “Study on Enhancement of Support for Edge Computing in 5G Core Network (5GC),” v17.0.0, Release 17, Dec. 2020.
[8] ETSI, “Framework and Reference Architecture,” GS MEC 003 V2.1.1, Nov. 2019.

### Table 1. List of identified gaps for 5G-enabled CCAM deployment.

| Topic                                    | Identified Gaps and Challenges                                                                 |
|------------------------------------------|-----------------------------------------------------------------------------------------------|
| **Roaming and inter-MNO interaction**    | • Test and evaluate inter-MNO handover interfaces, including cross-vendor interoperability tests to identify issues that harmonize and further standardization is needed.  
• Investigate whether proactive actions (e.g., context transfer, proactive registration) are needed before the inter-MNO handover, to further reduce the time required for the exchange of this information.  
• Roaming schemes improvement for the reduction of roaming latency and determination of more detailed SLA handover, ensuring the maintenance of SLAs. |
| **Predictive and e2e QoS**               | • Specification of QoS prediction functionality in a multi-operator environment, to receive QoS prediction notifications before the handover from one MNO (home country) to another MNO (visited country).  
• Service and session continuity at country borders when switching gateways and/or MEC hosts (e.g., server discovery, IP address changes, and connection-oriented transport layer protocols). |
| **MEC**                                  | • Inter-MEC communication, considering different architectures and MEC deployment strategies in different countries by the MNOs. |
| **Network slicing**                      | • Slice selection impact during the transition from one operator to another, when accessing a service in the visited network.  
• Impacts when registering and performing slice selection in the visited network, during the transition from one MNO to another, considering that 3GPP has defined a V2X slice type that could serve as common ground for MNOs to define slices with same QoS for certain V2X services in different networks, even when roaming. |
| **Data management**                      | • Regulation and protection of data ownership.  
• Definition of data sharing agreements among involved stakeholders e.g., MNOs, road authorities, vehicle manufacturers, map providers etc to enable various CCAM services.  
• Cross-border data exchange should be regulated to enable cross-border V2X services to retrieve and process data from different countries. |
| **Liability, security, and privacy**      | • Homologation (certification) of several hardware and software components involved in V2X services is needed and also the regulation of homologation among different countries.  
• Define the regulatory and legal framework for the sharing/identification of responsibilities among V2X stakeholders (liability management), within one country and across borders.  
• Define how e2e protection of information (vehicle, network, cloud) could be provided. Considering also that different security and privacy frameworks (GDPR) may be utilized by different countries. |
| **V2X applications and traffic management** | • Standardization of advanced V2X services (e.g., cooperative manoeuvres, automated intersection management) allowing cross-OEM, cross-vendor and cross-MNO realizations is needed to accelerate development of V2X services avoiding proprietary or localized solutions.  
• Define and standardize interfaces between traffic management centers and cloud platform (e.g., MEC) for collecting and sharing road and traffic information (e.g., road warnings, road status), also across different countries. |
At this stage, the evolution of the regulatory framework and the coordination among involved stakeholders (e.g., for liability management, data management, security and privacy issues) constitute probably the most important factors for the development of a consistent ecosystem that is needed for cross-border CCAM services.

He has been involved in several international, EU, national, and industrial research projects, and currently is Project Coordinator of the 5GPPP TeraCo project. He has also authored several book chapters and technical presentations, and has three European patents.

Maciej Mühleisen received his Ph.D. on Voice over LTE from RWTH Aachen University in 2015 and worked as a group leader for vehicular communication at Hamburg University of Technology (TUHH) from 2012 until 2016, focusing on highly reliable aircraft and maritime networks. He is with Ericsson Research since 2017 and leads the architecture work package of the EU funded 5G-CroCo project on 5G for aerial and maritime environments. As “Industry Verticals Coordination” in the Research Area “Networks,” he is furthermore supporting the technical coordination of Ericsson efforts on the Automotive Edge Computing Association (AEC) and 5G Automotive Association (5GAA). His key research interest is in end-to-end design, evaluation, and approval of safety-critical communication services.

Sokratis Barmpounakis, Ph.D., is a postdoctoral research associate in the Department of Informatics and Telecommunications, at the National and Kapodistrian University of Athens (NKUA). Since 2018, he has served as an adjunct professor in the same department. He received a Ph.D. in context-based resource management and slicing for SDN-enabled 5G smart, connected environments in May 2018. He obtained his Engineering Diploma in electrical and computer engineering, from the National Technical University of Athens in 2010. He has been involved in numerous European and industrial contracts, having also undertaken managerial roles, coordinating the NKUA team.

Xavier Vilajosana (M’09, SM’15) received his B.Sc. and M.Sc. in computer science from UPC and his Ph.D. in computer science from UOC. He is CIO at WorldSensing and full professor at UOC. He has been a researcher at Orange Labs, HPL, and the University of California, Berkeley.

Sebastian Euler is a senior researcher at Ericsson Research, Sweden. He joined Ericsson in 2016 and is currently leading the work on spectrum aspects in the context of the 5G CroCo project. Besides this, his research interests are in the areas of satellite communication networks and cellular communication with aerial vehicles. He has a background in particle physics, and received his Ph.D. from RWTH Aachen University, Germany, in 2014. Before joining Ericsson, he held a postdoctoral position at Uppsala University, Sweden, during which time he worked with neutrino experiments in Antarctica.

Bruno Tonsou graduated from ISEP, an engineering school in Paris, in 2003 with a specialization in telecommunications and joined Orange Group as a research engineer. He contributed to 3GPP SA2 architecture working as Orange delegate from 2004 to 2008. Since 2010, he has been a regular Orange 3GPP SA1 delegate as well as in 5G ACIA Working Groups 1 and 3. In Orange he is involved in different internal projects on 5G deployment, edge computing, and virtualization.

Jesus Alonso-Zarate (SM), Ph.D., M.B.A., is a senior researcher at CTTIC, Barcelona. In October 2019, he was the recipient of the 2019 Young Researcher Award from the Spanish Royal Academy of Engineering. He is currently the Project Coordinator of the H2020 5GCroCo project (www.5gcroco.eu) and Chairman of the 5G-PPP Automotive Working Group. He has published more than 170 peer-reviewed scientific and technical papers in the area of wireless communications, the Internet of Things, and 5G technologies. More info can be found at www.jesusalon佐zarat.com.