Safety-Related Cooperative, Connected, and Automated Mobility Services: Interplay between Functional and Security Requirements

On the Interplay Between Functional and Security Requirements for Safety-Related CCAM Services

Journal:	*IEEE Vehicular Technology Magazine*
Manuscript ID	VTM-2020-0090.R2
Manuscript Type:	Open Call Paper
Date Submitted by the Author:	n/a
Complete List of Authors:	Centenaro, Marco; Fondazione Bruno Kessler, Berlato, Stefano; Fondazione Bruno Kessler Carbone, Roberto; Fondazione Bruno Kessler Burzio, Gianfranco; Drivesec Srl Faranda Cordella, Giuseppe; Drivesec Srl Riggio, Roberto; Fondazione Bruno Kessler, Ranise, Silvio; Fondazione Bruno Kessler
Keywords:	CCAM, 5G, C-V2X, Safety, Standardization, Regulation

On the Interplay Between Functional and Security Requirements for Safety-Related CCAM Services

Marco Centenaro, Stefano Berlato, Roberto Carbone, Gianfranco Burzio,
Giuseppe Faranda Cordella, Roberto Riggio, and Silvio Ranise

Together with the electrification of vehicles, the provision of cooperative, connected, and automated mobility (CCAM) services is a prominent recent trend in the automotive sector. Upcoming car models will be able to exchange messages between themselves and with road traffic authorities by means of vehicle-to-everything (V2X) communication – in particular, leveraging mobile network technologies for the so-called cellular V2X (C-V2X) paradigm [1]. Moreover, (part of) such exchanged messages will be processed as a whole in, e.g., edge computing servers, in order to generate a global vision of the state of a given road stretch. CCAM services will exploit vehicular information transport and processing to implement complex maneuvers in a (semi)automatic manner by interacting with the in-car network.

The undeniable benefits of CCAM services should be coupled with their security, though. Proper protection mechanisms of V2X communication as well as of edge processing must be put in place with the ultimate scope of ensuring the security of car's critical functions such as e.g., driver assistance, collision warning, and automatic emergency braking. As a matter of fact, according to the ongoing discussions in the European Union (EU) and United Nations Economic Commission for Europe (UNECE), all new vehicle models will be approved only if they fulfill the cybersecurity requirements of the General Safety Regulation[1] starting July 6, 2022.

In this article, we will overview the major standards in terms of automotive security specifications, specifically focusing on those related to the external connectivity of cars. Moreover, since not all threats may be caught at a specification level, we will perform a qualitative security assessment of safety-related CCAM services featured by the EU-funded project 5G-CARMEN, with the final aim of highlighting the delicate interplay between functional and security requirements.

Secure CCAM: A Standardization Overview

We can identify three critical domains for the security of CCAM services: i) the in-car networking, ii) the external connectivity, and iii) the treatment of vehicular data.

M. Centenaro, S. Berlato, R. Carbone, and S. Ranise are with the Center for Information and Communication Technology, Fondazione Bruno Kessler, 38123 Trento, Italy. E-mail: {mcentenaro, sberlato, carbone, rriggio, ranise}@fbk.eu.

G. Burzio and G. F. Cordella are with DriveSec S.r.l., 10121 Torino, Italy. E-mail: {gb, gfc}@drivesec.com.

R. Riggio is Research Institutes of Sweden AB (RISE). E-mail: roberto.riggio@ri.se.

[1]Regulation (EU) 2019/2144 of the European Parliament and of the Council of November 27, 2019. Available online at https://eur-lex.europa.eu/eli/reg/2019/2144/oj.

Why Is In-Car Networking at Risk?

The internal network of a vehicle typically leverages a Controller Area Network (CAN) bus that connects various electronic control units (ECUs), each one managing a given functional subsystem. In-car networks were not designed originally as *open systems*, thus they do not provide adequate protection against *external* threats. Whenever an on-board unit (OBU) providing external connectivity for i) wireless communication and ii) positioning is connected to the CAN bus, the in-car network potentially becomes subject to a plethora of new security threats. Let us mention the case of a car manufacturer that wants to perform over-the-air (OTA) updates to the embedded software of its vehicles: in case of cyber-attacks, the vehicle software as a whole could be affected. Thus, configuring gateways and firewalls to shield the internal network of sensors and actuators from external threats is a priority for the automotive industry.

In this context, the aforementioned General Safety Regulation represents the landmark for the in-car cybersecurity. Two new regulations in the framework of the General Safety Regulation are being discussed within the UNECE at the time of writing: the first one is on the cybersecurity management system,[2] the second one on remote software updates.[3] The related technical specifications will be mostly based on standards by the Society of Automotive Engineers (SAE), especially [2], which specifies the requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g., concept, design, development), production, operation, maintenance, and decommissioning. In this way, a regulatory framework that includes the requirements for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders will be clearly defined.

We observe that [2] applies to road vehicles that include electrical and electronic systems, their interfaces and their communications, but it does not prescribe specific technologies or solutions related to cybersecurity. In other words, whether such cybersecurity requirements are satisfied or not is up to the technologies that are actually leveraged to implement the

[2]Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cybersecurity and of their cybersecurity management systems. Available online at https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-19r1e.pdf

[3]Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems. Available online at https://wiki.unece.org/download/attachments/87624569/ECE-TRANS-WP29-GRVA-2020-04e.docx?api=v2

various components of the in-car network, comprising the external connectivity modules. Thus, all the players involved in the generation, exchange, and life-cycle management of vehicular data – car manufacturers, road traffic authorities, and mobile network operators (MNOs) – should work together to implement a secure communication and computing platform, again following the appropriate standards to foster interoperability.

Standards for Secure External Communication

Being the in-car network not designed to foster the cooperativeness among vehicles, it is crucial to intercept external security threats as much as possible *before* they reach the in-car network, adopting a *defense-in-depth* approach. In particular, here we focus on the external connectivity modules for vehicle communication, neglecting those involved in vehicle positioning. The vehicles exploit the communication modules to periodically exchange information regarding, e.g., position and speed, or event-triggered warnings reporting, e.g., car accidents or adverse climatic conditions, with other vehicles or road traffic authorities.

ETSI ITS Security: The Intelligent Transport Systems (ITS) technical committee of the European Telecommunications Standards Institute (ETSI) is in charge of standardizing the V2X communication in the EU. The ETSI ITS communication architecture [3] defines both the vehicles and the road-side units (RSUs) as peer ITS stations (ITS-Ss) communicating via the ETSI ITS communication protocol stack (shown in blue in Fig. 1), which features three layers: access, networking and transport, and facilities. Based on the security services for ITS-Ss identified in [4], an ETSI ITS communication *security* architecture and the related security management procedures have been specified in [5]. Two security management authorities are defined in the ETSI ITS public key infrastructure (PKI):

1) the enrollment authority (EA), which is in charge of the life-cycle management of *enrollment credentials*, and
2) the authorization authority (AA), responsible for issuing, monitoring, and withdrawing *authorization tickets*.

The EA manages *long-term* certificates for identification and accountability of an ITS-S (i.e., the enrollment certificates), allowing the bearer to apply for *short-term*, anonymized certificates (pseudonyms) for V2X communication (i.e., the authorization tickets) from the AA. After obtaining the authorization ticket, an ITS-S can securely start exchanging ITS messages, e.g., cooperative awareness messages (CAMs) and decentralized environmental notification messages (DENM).

3GPP Network Security: As shown in Fig. 1, the ETSI ITS communication protocol stack relies on other wireless communication standards for the implementation of the access layer. While originally the IEEE 802.11p standard (G5 radio interface) was leveraged, since a few years Third Generation Partnership Project (3GPP) radio access technologies represent a valid alternative. Two radio interfaces are available for C-V2X: i) the long-range Uu interface for vehicle-to-network (V2N) communication, and ii) the short-range PC5 interface for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. While the former provides end-to-end, IP-based communication between ITS-Ss or between a ITS-S and the ITS infrastructure back-end through the mobile network infrastructure [6], the latter complements it by providing an alternative, non-interoperable short-range connectivity to G5. The operational mode of the PC5 radio interface is either configured by the network or self-configuring. In the following, we will refer to C-V2X technologies only, remaining agnostic about the PC5 configuration modes.

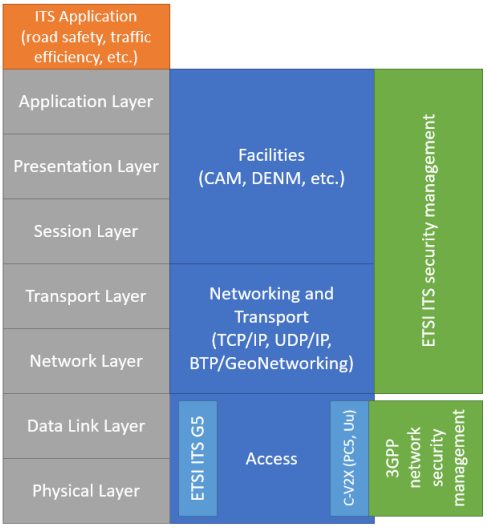

Fig. 1. Interworking between the ETSI ITS communication protocol stack (in blue) and the 3GPP protocol stack (in light blue), which implements the access layer providing long-range (Uu) and short-range (PC5) wireless connectivity. The ISO OSI protocol stack is shown as reference in grey. C-V2X access layer is alternative to ETSI ITS G5. In green, we have the security management.

As far as the security of 3GPP systems is concerned, built-in authentication, authorization, identity management, data integrity, and privacy are provided to *traditional* user equipments (UEs) (e.g., smartphones) by both the current fourth-generation Evolved Packet System (EPS) [7] and the upcoming 5G System (5GS) [8]. Moreover, further security requirements are defined for C-V2X communication, thus for *ITS-S-type* UEs [9]. In particular, 3GPP networks shall provide i) a means for the MNO to authorize or even pre-authorize a UE to perform V2X communication, ii) integrity protection of the transmission for a C-V2X application, and iii) pseudonymity and privacy of a UE using the C-V2X application.

US DoT SCMS: The United States Department of Transportation (US DoT) has been coordinating the efforts towards a PKI-based message security solution for V2V and V2I communications called Security Credentials Management System (SCMS).[4] Authorized vehicles use digital certificates to ensure authenticity and integrity of exchanged basic safety messages, which are supposed to contain no personal data to guarantee privacy.[5] Besides, the SCMS will implement a Misbehavior Authority which will collect misbehavior reports generated by vehicles.[6] After enough reports are received, the Misbehavior

[4]https://www.its.dot.gov/resources/scms.htm
[5]https://www.its.dot.gov/factsheets/pdf/Privacyfactsheet.pdf
[6]https://www.its.dot.gov/factsheets/pdf/CVSCMS.pdf

Authority will add the corresponding certificate to a certificate revocation list (CRL) and distribute them to all vehicles.

Some issues still need to be addressed. For instance, the SCMS provides that each vehicle should receive 20 certificates each week, which rotate every 5 minutes for maintaining privacy. However, managing so many certificates entails challenges such as distribution and maintenance of large CRLs and the possibility of Sybil attacks by malicious vehicles.

Treatment of Vehicular Data at the Edge Servers

While the previous communication standards enable a secure exchange of messages among ITS-Ss, the life-cycle management of vehicular data should also be taken into account, especially when a given CCAM service exploits a computing unit to process vehicular data. In case of low-latency applications, such a unit may have either an edge computing server co-located with the RSU or an ETSI multi-access edge computing (MEC) compliant server co-located with the 3GPP mobile network. In the latter scenario, multiple solutions allow tapping into the IP traffic from the UE [10]. Moreover, ad-hoc security measures are being specified to provide the users, the MNO, the CCAM application provider, the application developer, the content provider, and the platform vendor with a secure environment for the execution of CCAM services [11].

Summary

For the readers' convenience, in Tab. I we provide a brief description of the six communication security management service categories specified by ETSI ITS (i.e., enrollment, authorization, accountability, remote management, misbehavior reporting, identity management), along with the additional security features provided by the C-V2X access layer and the MEC platforms. Moreover, a graphical depiction of the relation between the involved players and the various technology enablers is outlined in Fig. 2.

A Bottom-Up Approach for CCAM Security Assessment

Despite the above-mentioned standards define a landmark for CCAM security, various details are usually *not* standardized and left to vendor implementation. In these cases, some unexpected security flaws may emerge, thus causing vulnerabilities that could affect the end-to-end vehicular communication system. For these reasons, a careful preliminary security assessment of each CCAM service should be carried out, as not all threats may have been caught both at a standardization level and development level.

In the following, we will follow a *bottom-up* approach in which we analyze some real CCAM services to identify their security threats and derive the possible countermeasures. The analyzed services are taken from one of the Horizon 2020 initiatives funded by the EU, i.e., the 5G-CARMEN project[7], which has been developing a communication and computing platform to enable CCAM services along the Bologna-Munich highway corridor crossing Italy, Austria, and Germany. The 5G-CARMEN CCAM platform employs different enabling technologies, such as 3GPP C-V2X transceivers and multi-domain orchestration, to implement four 5GS-enabled CCAM services: i) cooperative maneuvering, ii) situation awareness, iii) video streaming, and iv) green driving. The former two are *safety-related* services, that is, they aim at enhancing the awareness of status and intents among ITS-Ss (e.g., by making vehicles aware of road hazards or maneuver intents by other vehicles [5]) and have a strict relation with the safety of involved V2X users (e.g., by preventing car crashes). On the other hand, the latter two are *non-safety-related* CCAM services, concerned about enriching the passengers' experience (e.g., by providing seamless in-car entertainment). Although the security assessment is noteworthy for all CCAM services, here we focus only on safety-related ones, because these are characterized by a more tricky interplay among security and functional requirements.

Cooperative Maneuvering

In cooperative maneuvering services, each vehicle optimizes its trajectory by exchanging CAMs (containing, e.g., direction and speed) with other vehicles via C-V2X and combining this knowledge with precise positioning and information about aggregate traffic conditions. In particular, 5G-CARMEN has been implementing a cooperative lane merging (CLM) service, in which the gaps between vehicles in a cluster are managed in such a way that a vehicle that intends to move into a lane occupied by other vehicles can complete the maneuver safely and efficiently. This CCAM service is implemented by an edge application that monitors the road traffic trends as well as the intentions of the car drivers along a given road stretch: if the conditions are considered safe, the vehicles traveling along that stretch are informed via long-range Uu communication that they can perform CLM. The specific maneuver indications can be generated by the edge application itself and transmitted along with the maneuver authorization (centralized approach), otherwise, such indications can be negotiated within each cluster of vehicles, exploiting short-range PC5 communication (decentralized approach).

Situation Awareness

In situation awareness services, the car drivers are informed about nearby dangerous situations in order to increase their own safety. In this context, 5G-CARMEN has identified two variants to be implemented.

1) With back-situation awareness (BSA), each driver is notified of the expected time of arrival of an emergency vehicle, e.g., an ambulance or a police car, so that he/she can minimize road obstruction by proactively creating an emergency corridor.
2) With vehicle sensors and state sharing (VSSS), an in-advance awareness about adverse weather conditions or other detected road hazards is provided to drivers by vehicles ahead, the road infrastructure, and/or the network, thus merging information originating from different sources in the relevant area.

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

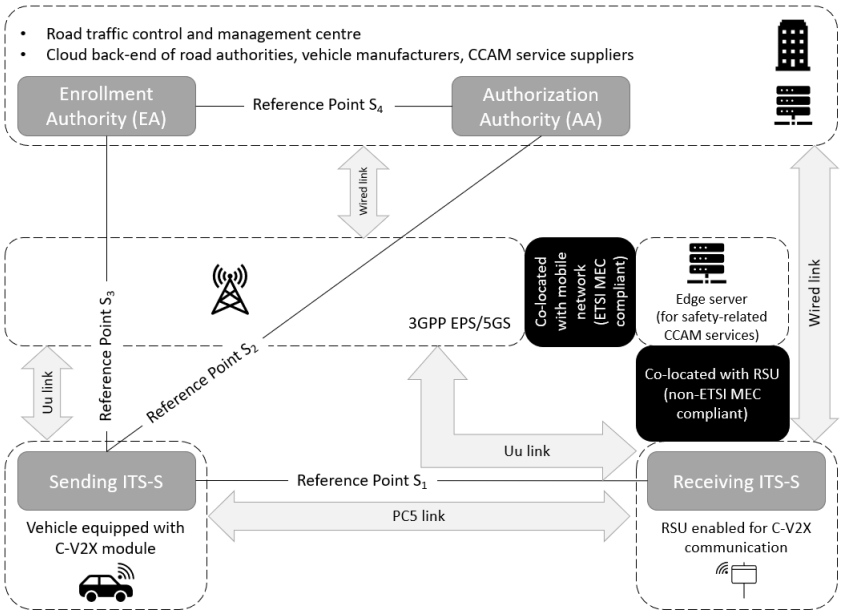

Fig. 2. A graphical mapping of the ETSI ITS communication security functional model [5, §5.3] against the players and technology enablers involved in C-V2X. In this example, the sending (receiving) ITS-S is a vehicle (RSU) equipped with C-V2X module. Through the reference points S_3 and S_2 the vehicle can apply for enrollment credentials and authorization tickets from the ITS infrastructure, respectively. Once it is admitted in the ITS system, it can perform V2N communication through the Uu interface towards CCAM services (hosted either in the remote or in the edge cloud) or distant vehicles. Moreover, through the PC5 interface, the vehicle can perform V2V/V2I communication towards vehicles in proximity/RSUs.

For both services, an edge application is exploited to dispatch the warning messages to the affected vehicles exploiting either V2V/V2I (PC5) communication or V2N (Uu) communication.

Functional and Security Requirements of Safety-Related CCAM Services

Each CCAM service entails specific *functional* requirements as well as *security* requirements, which influence each other. Moreover, the same requirement may have a different relevance across services, thus the interplay between functional and security requirements depends on the service. In the following, for each safety-related CCAM service, we briefly outline its critical functional requirements[8] and we specify the behavior of the six security service categories provided in Tab. I in terms of required security mechanisms (i.e., security requirements). Finally, we discuss the interplay between the functional requirements and the identified security requirements.

CLM Analysis

Functional Requirements: managing cooperative maneuvers requires frequent and precise input data from the involved vehicles (i.e., CAM containing position, speed, and intention) and fast elaboration of such data (e.g., by a scalable infrastructure in case of road stretches with dense traffic). Furthermore, a CLM poses a strict requirement on message reliability and latency, to prevent the exchange of aged vehicular data/maneuver indications.

[8]See, e.g., "5G-CARMEN Use Cases and Requirements," Deliverable 2.1, May 2019. Available online at https://5gcarmen.eu/wp-content/uploads/2020/03/5G_CARMEN_D2.1_FINAL.pdf

Security Requirements: as for *enrollment*, the cryptographic material (e.g., secret keys) used to guarantee confidentiality and integrity of communications toward EA shall be stored in tamper-proof secure in-car memory elements. Anyway, CRLs containing the PKI certificates of misbehaving ITS-Ss shall be kept up to date and quickly spread within the ITS infrastructure to prevent attacks from tampered/rogue ITS-Ss, which can be extremely harmful for a safety-critical CCAM service such as CLM. Also, countermeasures to physical attacks (e.g., vandalism) shall be addressed for preserving the dependability of the CLM service.

Regarding *authorization*, all involved vehicles shall obtain an "advanced CAM authorization" from the AA in order to interact with the CLM application in the edge server. The access control policy is attribute-based, and it mainly considers vehicles' location (i.e., authorization tickets shall authorize access to the closest CLM application instance only) and capabilities (e.g., sensors equipment [5]). The integrity of authorization tickets shall be preserved through cryptography (e.g., digital signatures). Privacy is based on the use of (valid and not expired) pseudonyms. However, the provisioning of pseudonyms to vehicles by AAs shall balance privacy requirements (e.g., vehicles untraceability) against possible misuses (e.g., Sybil attacks [12]). Confidentiality and integrity of communications toward AAs shall be preserved as well.

With regard to *accountability*, beside integrity, cryptography shall guarantee also the non-repudiation property on messages exchanged within the CLM service. Forensics (e.g., after a car crash) requires the possibility to resolve the pseudonym(s) used by an ITS-S. However, only relevant authorities (e.g., the police) shall be capable of linking a pseudonym to the vehicle [12]. Also, since accountability implies the retention of pseudo-

anonymized and personal data, the General Data Protection Regulation (GDPR)[9] (e.g., data minimization principle, policy on data retention [13, §4]) shall be considered. According to the GDPR, cryptography also plays a crucial role to protect user personal data (e.g., position and identity) transported in messages routinely exchanged by CCAM services. Additionally, cryptographic solutions for authentication and authorization (such as those depicted in Fig. 2) are key to developing secure and privacy-aware services; guaranteeing an appropriate level of assurance of authentication and that access control policies are appropriately enforced are mandatory for empowering users with the control of their personal data – one of the key tenets underlying the GDPR.

Referring to *remote management*, the ITS infrastructure shall be able to exclude misbehaving ITS-Ss from the CLM service, eventually interacting with the underlying 3GPP network infrastructure. In particular, there shall be security mechanisms to detect and mitigate denial of service (DoS) attacks against the CLM service at various levels: physical transmissions (e.g., jamming), multi-hop (PC5) packet routing (e.g., jellyfish attack), network topology (e.g., flooding attack), and application (e.g., memory exhaustion).

Concerning *misbehavior reporting*, ITS-Ss shall be able to report *internal* suspicious activities to the ITS infrastructure – authentication already protects against *external* misbehaving ITS-Ss. Presumed internal misbehaving ITS-Ss can be detected by complementing techniques at different levels (e.g., network, application) to combine factors which are independent of a particular use case (e.g., reputation scores, entity-based trust frameworks) with application-specific aspects to take advantage of the semantic of exchanged messages (e.g., in CLM, consistency and plausibility checks [5, §4] of a sequence of messages).

Finally, about *identity management* all V2I communications regarding CLM services shall occur through pairwise-authenticated and confidential channels. In V2V communications, the unlinkability of pseudonyms shall be guaranteed. Confidentiality, instead, is not required, as messages are broadcast [5, §4].

BSA Analysis

Functional Requirements: BSA has looser functional requirements than CLM in terms of latency and reliability. The emergency vehicles shall be authorized to broadcast their presence through CAMs, and set an adequate *priority level* to trigger support from regular ITS-Ss (e.g., by creating an emergency corridor) and the ITS infrastructure (e.g., by synchronizing traffic lights to create a 'green' wave).

Security Requirements: as for *enrollment*, since the target area may be far ahead of the emergency vehicle, the BSA service continuity across different administrative domains should be ensured. As such, the enrollment of emergency vehicle may involve different EAs. Trust establishment among PKI certification authorities (CA) requires international coordination and a proper management of CRLs. Moreover, on PKI certificate management, the same considerations as CLM services hold, for both regular and emergency vehicles.

Regarding *authorization*, only actual emergency vehicles shall be able to obtain the "authorization to claim priority rights for emergency vehicles" [5] depending on their priority level. Therefore, an access control policy shall be devised to allow for fine-grained priority levels by considering the *least privilege principle* and avoiding *privilege escalation attacks*. Also, messages broadcast by emergency vehicles shall be protected against replay attacks (e.g., through timestamp, sequence number, or location checks). Finally, we note that emergency vehicles do not need pseudonyms.

With regard to *accountability*, as in the CLM case, data shall be retained to enable later forensics. However, in BSA we envision fewer privacy requirements, as it deals with public safety services.

Referring to *remote management*, the ITS infrastructure shall be able to block stolen or misbehaving emergency vehicles from claiming priority rights.

Concerning *misbehavior reporting*, ITS-Ss shall be able to report internal suspicious activities to the ITS infrastructure. In particular, protection against message replay shall be ensured to prevent unauthorized vehicles from claiming priority privileges.

Finally, about *identity management* in BSA, neither confidentiality nor pseudonyms are needed.

VSSS Analysis

Functional Requirements: Depending on the context, VSSS messages may have latency/reliability constraints as in CLM (e.g., in case of road accident warnings) or as in BSA (e.g., adverse weather conditions warnings). When bad weather conditions or hazards are detected by a vehicle or a RSU, such ITS-Ss can notify nearby vehicles with a DENM. The warning can be then forwarded to distant vehicles through the ITS infrastructure (i.e., other RSUs preceding the dangerous road stretch), the cellular network (via Uu links), or vehicles exploiting multi-hop (PC5) routing.

Security Requirements: as for *enrollment*, similarly to BSA, the dangerous area may be far ahead from the vehicle, thus VSSS service continuity may involve multiple EA. The usual recommendations on PKI certificate management are in force.

Regarding *authorization*, only vehicles proving to have the necessary capabilities (e.g., cryptographic algorithms, sensors equipment, and quality [5]) shall be allowed to participate in the VSSS service. Since VSSS messages cannot be used for tracking [5], one pseudonym is enough to preserve drivers' privacy, with the advantage to prevent Sybil attacks [12].

With regard to *accountability* and *remote management*, as in CLM and BSA, data shall be retained to enable later forensics with the same privacy considerations and the ITS infrastructure shall be able to exclude misbehaving ITS-Ss from the VSSS service, respectively.

Concerning *misbehavior reporting*, an ITS-S shall be able to report suspicious activities. Fake road hazards (e.g., fake ice threat) could be detected by validating the data, asserting the reputation of the sending vehicle, or having multiple vehicles confirming the same road hazard.

[9]https://gdpr.eu/

Finally, about *identity management*, while (at least one) pseudonym is needed to preserve privacy, confidentiality is not needed as VSSS messages are broadcast.

Interplay Between Functional and Security Requirements

Both functional and the identified security requirements of the analyzed CCAM services (which are summarized in a tabular format in Tab. II) aim at preserving and enhancing their safety but with different objectives, thus their fulfillment should be thoroughly balanced in order to avoid *interference* between them. In the following, we will describe some situations in which such an interference between functional and security requirements yields negative impacts on safety.

Preserving the integrity of messages (security requirement) exchanged by ITS-S involved in CLM and VSSS is crucial for preventing potentially dramatic safety issues (e.g., due to wrong maneuvering suggestions or an altered environmental perception). On the other hand, given the typically low computational capabilities of cars' ECUs, robust and secure cryptographic primitives used to protect messages may degrade the system performance and break the strict latency constraint (functional requirement), potentially leading to safety issues as well (e.g., vehicle position is outdated by the time the message is read). Therefore, the level of robustness of cryptographic primitives needs to be carefully chosen. We note that attacks to message integrity at the edge computing platforms are more complex but not impossible, e.g., by exploiting the complexity and possible subtle dependencies between the modules in which the software runs. Also, deploying enrollment and authorization services in a real-time and dynamic scenario is a challenging task [14]. These services require several cryptographic operations and V2N communication for the validation of PKI certificates against CRLs. Ensuring a high level of security may again affect the latency, with negative impacts on safety.

Beside overall integrity, also the content of the messages should be checked to prevent an internal attacker from spreading fake information. In VSSS, vehicles are notified of road hazards through DENMs. The content of these messages can be validated through reputation or trust scores [15]. A simple solution is to aggregate DENMs from different vehicles and compare their content to ensure consistency (security requirement). For instance, we could assume that at least two DENMs are required to validate the presence of a road hazard. However, waiting for the second DENM may delay vehicles' reaction like steering or breaking (functional requirement), affecting safety again. Thus, the trust threshold needs to be carefully chosen, e.g., as a function of the current traffic condition. Nonetheless, we note that a misbehaving ITS-S could exploit the (several) pseudonyms provided by the AA to subvert the correct information through a Sybil attack. On the other hand, a scant supply of pseudonyms could lead to potential privacy issues [12].

Another example is that of scalability, which, as a functional requirement, fosters decentralized approaches like, e.g., in CLM. Nonetheless, this has a negative effect on security, since there is no central entity with global state awareness that can become aware of misbehaving vehicles (security requirement) that can alter other vehicles awareness and impact safety.

The dependability of the edge computing platforms should also be taken into account. Even modest attempts to perform a DoS attack may have dramatic consequences on safety due to the strict latency requirements of the examined CCAM services. The deployment of redundant instances of a CCAM service may mitigate the impact of a Memory Exhaustion attack (security requirement) at the expenses of reducing virtualization resources available for other services (functional requirement).

As a final remark, we note that safety fallback mechanisms should be devised and deployed to avoid the worst-case scenario. Each service should have a fail-safe design so that ITS-Ss can adjust their functional characteristics to the new situation and fall back to secure states. For instance, the CLM service is very sensible to attacks to messages integrity or availability, thus it is advisable to implement fallback mechanisms to ensure drivers' safety even under adverse conditions (e.g., attacks or communication errors). Let us think at a DoS attack to the centralized CLM service, which prevents the edge server from generating maneuvering indications. The vehicles themselves could issue a warning to their driver and provide the safest advice based on the current context (e.g., slow down, do not merge).

Conclusions

In this article, we surveyed the ongoing regulation and standardization activities aimed at specifying the security procedures for vehicle cybersecurity. Moreover, we performed a security assessment of three safety-related CCAM services under study in the UE-funded project 5G-CARMEN, focusing on the interplay between functional and security requirements. The discussions provided in this work are beneficial, e.g., to the Data Protection Impact Assessment (DPIA) mandated by Art. 35 of the GDPR. Indeed, stakeholders (in particular, data controllers) must evaluate the likelihood and impact of privacy risks on the rights and freedom of data subjects; in the context of certain CCAM services such as the CLM, safety is one of the most important rights.

Acknowledgment

This work has been performed in the framework of the European Union Horizon 2020 project 5G-CARMEN co-funded by the EU under grant agreement No. 825012. The views expressed are those of the authors and do not necessarily represent the project. The Commission is not liable for any use that may be made of any of the information contained therein.

References

[1] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, Feb. 2020.
[2] "Road vehicles — Cybersecurity Engineering," Vehicle Cybersecurity Systems Engineering Committee, ISO/SAE standard 21434, Feb. 2020.
[3] "Communications Architecture," ETSI TC ITS European Std. EN 302 665 V1.1.1, Sep. 2010.
[4] "Security; Security services and architecture," ETSI TC ITS Tech. Spec. 102 731 V1.1.1, Sep. 2010.

[5] "Security; ITS communications security architecture and security management," ETSI TC ITS Tech. Spec. 102 940 V1.3.1, Apr. 2018.
[6] "Framework for Public Mobile Networks in Cooperative ITS (C-ITS)," ETSI TC ITS Tech. Rep. 102 962 V1.1.1, Feb. 2012.
[7] "Service requirements for the Evolved Packet System (Release 17)," 3GPP TSG-SA Tech. Spec. 22.278 V17.1.0, Dec. 2019.
[8] "Service requirements for the 5G system; Stage 1 (Release 17)," 3GPP TSG-SA Tech. Spec. 22.261 V17.1.0, Dec. 2019.
[9] "Service requirements for V2X services; Stage 1 (Release 15)," 3GPP TSG-SA Tech. Spec. 22.185 V15.0.0, Jun. 2018.
[10] "MEC deployments in 4G and evolution towards 5G," ETSI ISG MEC Whitepaper #24, Feb. 2018.
[11] "Multi-access edge computing; Phase 2: Use cases and requirements," ETSI ISG MEC Group Spec. MEC002 V2.1.1, Oct. 2018.
[12] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," in *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228-255, Firstquarter 2015.
[13] "Critical security controls for effective cyber defence; Part 5: Privacy enhancement," ETSI TC CYBER Tech. Rep. 103 305-5 V1.1.1, Sep. 2018.
[14] A. Patwary, A. Fu, R. Naha, S. Battula, S. Garg, M. Patwary, and E. Aghasian "Authentication, Access Control, Privacy, Threats and Trust Management Towards Securing Fog Computing Environments: A Review", ArXiV, Mar. 2020. [Online]. Available: https://arxiv.org/abs/2003.00395
[15] M. Hasan, S. Mohan, T. Shimizu, H. Lu "Securing Vehicle-to-Everything (V2X) Communication Platforms", ArXiV, Mar. 2020 [Online]. Available: https://arxiv.org/abs/2003.07191

Marco Centenaro (marco.centenaro.it@ieee.org) is an Expert Researcher at Fondazione Bruno Kessler, Trento, Italy. His research is focused on telecommunication standards as well as Internet of Things technologies.

Stefano Berlato (sberlato@fbk.eu) is a Research Assistant at Fondazione Bruno Kessler, Trento, Italy. His current research interests include the analysis of security in ITS and edge computing solutions.

Roberto Carbone (carbone@fbk.eu) is a Researcher of the Security&Trust research unit of Fondazione Bruno Kessler in Trento, Italy, since 2010. He received his PhD from the University of Genova in 2009. His research mainly focuses on digital identity management and formal analysis of security protocols and services.

Gianfranco Burzio (gb@drivesec.com) was born in Carmagnola, Italy, on 14 September 1956. Graduated in Electrical Engineering in 1980, with a final vote of 110/110 cum laude. Specialization in Industrial Automation. After two years of experience as a software system engineer, he joined the FIAT Research Centre in 1982. He worked initially in industrial automation and robotics, from 1990 his activities moved to development of driving assistance systems (anti-collision, lane keeping, overtaking warning). Executive manager in 1995 he managed the development teams of on-board information systems, driver assistance, telematics and vehicle-driver interface. Coordinator of several European funded research projects. Between 2003 and 2006 he coordinated the participation of FIAT Group to the Torino Wireless regional project. In 2012 he was appointed Safety Director at ACEA, the European association of vehicle manufacturers, in Brussels. Back in Fiat Chrysler Automotive in 2016, until October 2017. Automotive safety and security advisor for Drivesec since November 2017.

Giuseppe Faranda Cordella (gfc@drivesec.com) got a master degree in Computer Science at Turin University and he is a senior executive with an experience of over 25 years in the design and development of automotive electronics, connected car services and vehicle cybersecurity. In his career he is been working in different roles in leading automotive companies either as an OEM or a Tier1 suppliers. In recent years he served as head of research and development and VP of infotainment for a large OEM in Europe. In the last few years he was appointed head of Vehicle Cybersecurity for leading OEM in EMEA, managing the introduction of digital protection countermeasures in connected cars.

Roberto Riggio (roberto.riggio@ri.se) is Senior Researcher in the Connected Intelligence Group at RISE AB in Stockholm, Sweden. He received his PhD from the University of Trento (Italy), after that he was postdoc at University of Florida, Researcher/Chief Scientist at CREATE-NET in Trento (Italy), Head of Unit at FBK in Trento (Italy), and Senior 5G Researcher at the i2CAT Foundation in Barcelona (Spain). His research interests revolve around optimization and algorithmic problems in networked and distributed systems. His current fields of applications are edge automation platforms, intelligent networks, and human-driven networking. Roberto Riggio has published more than 130 papers in internationally refereed journals and conferences. He is a Senior Member of the IEEE.

Silvio Ranise (ranise@fbk.eu) received a joint Phd from the University of Genova (Italy) and Université Henri Poincaré (Nancy, France). He was researcher at INRIA (the french National Institute for Computer Science and Automation), visiting professor at the University of Milano (Italy) and researcher at the University of Verona (Italy). He is now the Head of the Security and Trust research unit in Fondazione Bruno Kessler (Trento, Italy). His main research interests are digital identity management, risk assessment and legal compliance (e.g., for privacy and finance), and security analysis of complex ecosystems combining different technologies such as APIs, IoT, mobile and cloud computing. He has published more than 100 papers in international conferences and journals and regularly serves as PC member of several international conferences in cybersecurity. He is or has been involved in many European and industrial projects.

TABLE I
LIST OF ETSI ITS COMMUNICATION SECURITY MANAGEMENT SERVICES CATEGORIES [5, TAB. 4], WITH ADDITIONAL FEATURES PROVIDED BY C-V2X RADIO ACCESS TECHNOLOGIES [9] AND VEHICULAR DATA PROCESSING INFRASTRUCTURE [11].

SERVICE CATEGORY	DESCRIPTION AND FUNDAMENTAL FEATURES	ADDITIONAL FEATURES
Enrollment	Management of enrollment credentials through reference point S_3. An ITS-S shall request enrollment credentials to the EA such that it can be trusted to function correctly by another ITS-S. Fundamental features: • establishment of enrollment trust via secure handling and storage of cryptographic keys (PKI certificates) at the ITS-S • enrollment trust management based on certificate provisioning by the EA	• The EPS/5GS shall support information authenticity between the UE and the EPS/5GS • Appropriate traffic protection measures should be provided by the EPS/5GS • The EPS/5GS shall ensure that no unauthorized user can obtain a legitimate IP address that can be used to establish communication or enable malicious attacks on EPS/5GS entities
Authorization	Management of authorization tickets through reference points S_4 and S_2. An enrolled ITS-S shall request authorization tickets to the AA to get specific permissions (e.g., to access to a specific service/resource). Fundamental features: • trust management of the authorization tickets based on certificate provisioning and privacy management based on pseudonyms provisioning by the AA • privacy management of the authorization tickets based on pseudonyms provisioning by the AA • access control policies	• The 3GPP network shall provide a means for the MNO to authorize a UE supporting V2X application to perform V2X communication when served by E-UTRAN supporting V2X communication • The 3GPP network shall provide a means (e.g., pre-authorization) for the MNO to authorize a UE supporting V2X application to perform V2X communication when not served by E-UTRAN supporting V2X communication • The 3GPP network shall provide a means for the MNO to authorize UEs supporting V2X application separately to perform V2N communication • The 3GPP system shall support integrity protection of the transmission for a V2X application • The MEC platform shall only provide a MEC application with the information for which the application is authorized
Accountability	Records incoming/outgoing messages such that the ITS-S can be held accountable.	• The EPS shall be able to store information of third-party applications necessary for performing security and charging functions • The 5GS shall support a secure mechanism to store cached data • Implement measures for meeting the NFV retained data problem set (secure logging, access control, post-incident analysis)
Remote management	Enable the ITS infrastructure to remotely manage a misbehaving ITS station, e.g., by remotely activating/deactivating the transmission of messages on a specific ITS station.	• Subject to regional or national regulatory requirements, the 5GS shall support a secure mechanism for allowing an authorized entity to disable from normal operation of a UE reported as stolen
Misbehavior reporting	Enable an ITS-S to report a suspicious activity (e.g., a misbehaving ITS-S) to the ITS infrastructure.	• Subject to regional or national regulatory requirements, the 5GS shall support mechanisms to detect tampering and spoofing attempts on the production of the user location information and the user position-related data
Identity management	Provide services supporting the simultaneous change of communication identifiers, i.e., station ID (facility layer), network ID (network/transport layer), and MAC address (access layer), and credentials used for secure communications, within the ITS-S. Provides features allowing the disabling of ID change. Fundamental features: • communication privacy management, entailing anonimity/pseudonimity, unlinkability/unobservability • assurance of transmitted information confidentiality	• The EPS/5GS shall provide several appropriate levels of user privacy including communication confidentiality, location privacy, and identity protection • Subject to regional regulatory requirements and/or operator policy for a V2X application, the 3GPP system shall support pseudonymity and privacy of a UE using the V2X application, by ensuring that a UE identity cannot be tracked or identified by any other UE beyond a certain short time-period required by the V2X application • Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the 3GPP system shall support pseudonymity and privacy of a UE in the use of a V2V/V2I application, such that no single party (operator or third party) can track a UE identity in that region

TABLE II
MAPPING BETWEEN ETSI ITS COMMUNICATION SECURITY SERVICE CATEGORIES AND SAFETY-RELATED 5G-CARMEN CCAM SERVICES.

SECURITY SERVICE		CLM	BSA	VSSS
Enrollment	Secure storage of cryptographic material at the ITS-S	yes	yes	yes
	Enrollment checked against CRLs	yes	yes	yes
	Management of enrollment credentials across (trusted) administrative domains	no need	yes	yes
	Security Properties	**integrity, privacy**	**integrity**	**integrity, privacy**
Authorization	Vehicle Authorization	Advanced CAM authorization [5]	Authorization to claim priority rights for emergency vehicles [5]	Basic CAM authorization [5]
	Access Control	Based on ITS-S location and capabilities [5]	Based on priority levels (least privilege principle)	Based on ITS-S capabilities (e.g., cryptographic algorithms, sensors equipment and quality [5])
	Pseudonyms	(balanced) provisioning [12]	no need	provisioning limited to one pseudonym [5]
	Security Properties	**confidentiality, integrity, safety**	**integrity**	**confidentiality, integrity**
Accountability	ITS-Ss and MEC platforms shall store logs (e.g., received messages) to enable forensics.	yes	yes	yes
	Relevant authorities only shall be capable of linking a pseudonym to a vehicle in case of necessity [12].	yes	no need (no pseudonyms to solve)	yes
	Consideration of GDPR, Data Minimization principle and policy on data retention [13, § 4].	yes	no need (no personal or sensitive data)	yes
	Security Properties	**availability, integrity**	**availability, integrity**	**availability, integrity**
Remote Management	The ITS infrastructure shall be able to	exclude misbehaving ITS-S from the service.	block stolen or misbehaving emergency vehicles from claiming priority rights.	exclude misbehaving ITS-S from the service.
	The ITS infrastructure shall be able to revoke PKI certificates of misbehaving ITS-S through CRLs.	yes	yes	yes
	Security Properties	**integrity, safety**	**integrity, safety**	**integrity, safety**
Misbehaviour Reporting	ITS-Ss shall be able to report internal suspicious activities to the ITS infrastructure (e.g., fake messages or data tampering).	yes	yes	yes
	Service misuse protection	Too many CLM requests from a vehicle shall be reported.	Messages broadcast by emergency vehicles shall be protected against replay attacks.	Too many CLM requests from a vehicle shall be reported.
	Security Properties	**integrity, safety**	**integrity, safety**	**integrity, safety**
Identity Management	Communication confidentiality	All V2I communications happen through pairwise-authenticated and confidential channels.	The V2I communication between the emergency vehicle and the ITS infrastructure happens through pairwise-authenticated and confidential channels. Then, confidentiality is not required for broadcast messages [5, §4].	Confidentiality is not required for broadcast messages [5, §4].
	Privacy	The ITS infrastructure shall support the simultaneous change of communication identifiers.	No need	One pseudonym shall be used to preserve privacy.
	Security Properties	**confidentiality, privacy**	**none – Neither confidentiality nor pseudonyms are needed.**	**privacy**

Authors' Replies To Comments

Manuscript ID VTM-2020-0090.R1, "Trade-Off Between Functionality and Security in 5G-Enabled Safety-Related CCAM Services"

Cover Letter

2021-04-20

Dear Editor,

We thank the Reviewers for the valuable feedback on the revised manuscript. We have carefully gone through the received comments and replied to them, applying several changes throughout the manuscript. We hope that these modifications satisfy the expectations of the Editor and the Reviewers.

Please find below the detailed replies; we have also provided a difference file between the newly submitted manuscript and the previous one in order to ease spotting out the applied changes.

We are looking forward to your feedback.

Best regards,

Marco Centenaro (corresponding author), on behalf of the authors

Replies to Reviewer 1's Comments

1. Authors not GDPR but fail to describe the effect on security, e.g., privacy vs functionality.

Authors' Reply: We agree with the Reviewer's observation. Thus, we have added some lines at the beginning of page 5, first column, when we mention the role of GDPR on accountability:

"According to the GDPR, cryptography also plays a crucial role to protect user personal data (e.g., position and identity) transported in messages routinely exchanged by CCAM services. Additionally, cryptographic solutions for authentication and authorization (such as those depicted in Fig. 2) are key to developing secure and privacy-aware services; guaranteeing an appropriate level of assurance of authentication and that access control policies are appropriately enforced are mandatory for empowering users with the control of their personal data – one of the key tenets underlying the GDPR."

Another aspect of our work related to the GDPR concerns the Data Protection Impact Assessment (DPIA) of data processing activities in safety-related CCAM services. Indeed, safety may be a crucial aspect to consider while conducting such a DPIA and the observations in the manuscript may help. We have added the following sentence in the conclusions:

"The discussions provided in this work are beneficial, e.g., to the Data Protection Impact Assessment (DPIA) mandated by Art. 35 of the GDPR. Indeed, stakeholders (in particular, data controllers) must evaluate the likelihood and impact of privacy risks on the rights and freedom of data subjects; in the context of certain CCAM services such as the CLM, safety is one of the most important rights."

2. 5G is conflated with C-V2X. This may be the case with 5G-Carmen but the C-V2X in deployment at this writing is all LTE-V2X and not 5G NR sidelink as is implied with this conflation.

Authors' Reply: We agree with the Reviewer; C-V2X is currently based on the LTE standard only, while 5G-based C-V2X is still yet to come. To clear out any possible misunderstanding, we hereby propose to reduce the focus on "5G" by

- *Mentioning "mobile network technologies" in a general way as enablers of C-V2X in the introductory section;*
- *dropping the "5G" term from the title, which we propose to change to "On the Interplay Between Functional and Security Requirements for Safety-Related CCAM Services."*

We also remark that both specifications of 4G systems and 5G systems are cited in the manuscript under "3GPP Network Security" (see [7] and [8], respectively, at page 2, second column), and reported in Table 1 as well.

3. USDOT is attributed to be the source of US SCMS. That may have been true 4 years ago, but at this writing given no mandate there is no US involvement with the private SCMS.

Authors' Reply: We agree with the Reviewer, and we propose to rephrase the sentence related to the role of US DoT as follows:

"The US DoT has been coordinating the efforts towards a PKI-based message security solution for V2V and V2I communications called SCMS."

In this way, rather than ascribing the design of the SCMS to the US DoT, we highlight its role in leading and funding the activities related to that solution.

Replies to Reviewer 2's Comments

1. The authors have adequately addressed the issues raised in my original review.

***Authors' Reply**: We sincerely thank the Reviewer for the positive comment about the revised manuscript.*

Replies to Reviewer 3's Comments

1. Article title is about tradeoffs, but it is unclear what is the conclusion in terms of compromises for different implementations/concepts/.

***Authors' Reply**: We agree with the Reviewer's comment. As a matter of fact, the aim of the paper is to identify the potential security threats that could arise in safety-related CCAM services which are characterized by stringent functional requirements. In order to avoid misunderstanding also to the readers, we have modified the title of the paper as follows:*

"On the Interplay Between Functional and Security Requirements for Safety-Related CCAM Services."

Moreover, we have clearly stated the scope of the manuscript, mentioning the analysis of the interplay *between functional requirements and security requirements rather their* trade-off*. Our analysis can be useful in several context, including the Data Protection Impact Assessment (DPIA) preparation by the stakeholders involved in the design of safety-related CCAM services. Thus, we have mentioned this contribution of our manuscript in the conclusions:*

"The discussions provided in this work are beneficial, e.g., to the Data Protection Impact Assessment (DPIA) mandated by Art. 35 of the GDPR. Indeed, stakeholders (in particular, data controllers) must evaluate the likelihood and impact of privacy risks on the rights and freedom of data subjects; in the context of certain CCAM services such as the CLM, safety is one of the most important rights."

~~Trade-Off~~ On the Interplay Between ~~Functionality~~ Functional and Security ~~in 5G-Enabled~~ Requirements for Safety-Related CCAM Services

Marco Centenaro, Stefano Berlato, Roberto Carbone, Gianfranco Burzio,
Giuseppe Faranda Cordella, Roberto Riggio, and Silvio Ranise

Together with the electrification of vehicles, the provision of cooperative, connected, and automated mobility (CCAM) services is a prominent recent trend in the automotive sector. Upcoming car models will be able to exchange messages between themselves and with road traffic authorities by means of vehicle-to-everything (V2X) communication – in particular, leveraging ~~the upcoming fifth-generation (5G) cellular networks~~ mobile network technologies for the so-called cellular V2X (C-V2X) paradigm [1]. Moreover, (part of) such exchanged messages will be processed as a whole in, e.g., edge computing servers, in order to generate a global vision of the state of a given road stretch. CCAM services will exploit vehicular information transport and processing to implement complex maneuvers in a (semi)automatic manner by interacting with the in-car network.

The undeniable benefits of CCAM services should be coupled with their security, though. Proper protection mechanisms of V2X communication as well as of edge processing must be put in place with the ultimate scope of ensuring the security of car's critical functions such as e.g., driver assistance, collision warning, and automatic emergency braking. As a matter of fact, according to the ongoing discussions in the European Union (EU) and United Nations Economic Commission for Europe (UNECE), all new vehicle models will be approved only if they fulfill the cybersecurity requirements of the General Safety Regulation[1] starting July 6, 2022.

In this article, we will overview the major standards in terms of automotive security specifications, specifically focusing on those related to the external connectivity of cars. Moreover, since not all threats may be caught at a specification level, we will perform a qualitative security assessment of safety-related CCAM services featured by the EU-funded project 5G-CARMEN, with the final aim of highlighting the delicate ~~trade-off~~ interplay between functional and security requirements.

M. Centenaro, S. Berlato, R. Carbone, and S. Ranise are with the Center for Information and Communication Technology, Fondazione Bruno Kessler, 38123 Trento, Italy. E-mail: {mcentenaro, sberlato, carbone, rriggio, ranise}@fbk.eu.

G. Burzio and G. F. Cordella are with DriveSec S.r.l., 10121 Torino, Italy. E-mail: {gb, gfc}@drivesec.com.

R. Riggio is Research Institutes of Sweden AB (RISE). E-mail: roberto.riggio@ri.se.

[1]Regulation (EU) 2019/2144 of the European Parliament and of the Council of November 27, 2019. Available online at https://eur-lex.europa.eu/eli/reg/2019/2144/oj.

Secure CCAM: A Standardization Overview

We can identify three critical domains for the security of CCAM services: i) the in-car networking, ii) the external connectivity, and iii) the treatment of vehicular data.

Why Is In-Car Networking at Risk?

The internal network of a vehicle typically leverages a Controller Area Network (CAN) bus that connects various electronic control units (ECUs), each one managing a given functional subsystem. In-car networks were not designed originally as *open systems*, thus they do not provide adequate protection against *external* threats. Whenever an on-board unit (OBU) providing external connectivity for i) wireless communication and ii) positioning is connected to the CAN bus, the in-car network potentially becomes subject to a plethora of new security threats. Let us mention the case of a car manufacturer that wants to perform over-the-air (OTA) updates to the embedded software of its vehicles: in case of cyber-attacks, the vehicle software as a whole could be affected. Thus, configuring gateways and firewalls to shield the internal network of sensors and actuators from external threats is a priority for the automotive industry.

In this context, the aforementioned General Safety Regulation represents the landmark for the in-car cybersecurity. Two new regulations in the framework of the General Safety Regulation are being discussed within the UNECE at the time of writing: the first one is on the cybersecurity management system,[2] the second one on remote software updates.[3] The related technical specifications will be mostly based on standards by the Society of Automotive Engineers (SAE), especially [2], which specifies the requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g., concept, design, development), production, operation, maintenance, and decommissioning. In this way, a regulatory framework that includes the requirements for a cybersecurity process and a common language

[2]Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cybersecurity and of their cybersecurity management systems. Available online at https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-19r1e.pdf

[3]Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems. Available online at https://wiki.unece.org/download/attachments/87624569/ECE-TRANS-WP29-GRVA-2020-04e.docx?api=v2

for communicating and managing cybersecurity risk among stakeholders will be clearly defined.

We observe that [2] applies to road vehicles that include electrical and electronic systems, their interfaces and their communications, but it does not prescribe specific technologies or solutions related to cybersecurity. In other words, whether such cybersecurity requirements are satisfied or not is up to the technologies that are actually leveraged to implement the various components of the in-car network, comprising the external connectivity modules. Thus, all the players involved in the generation, exchange, and life-cycle management of vehicular data – car manufacturers, road traffic authorities, and mobile network operators (MNOs) – should work together to implement a secure communication and computing platform, again following the appropriate standards to foster interoperability.

Standards for Secure External Communication

Being the in-car network not designed to foster the cooperativeness among vehicles, it is crucial to intercept external security threats as much as possible *before* they reach the in-car network, adopting a *defense-in-depth* approach. In particular, here we focus on the external connectivity modules for vehicle communication, neglecting those involved in vehicle positioning. The vehicles exploit the communication modules to periodically exchange information regarding, e.g., position and speed, or event-triggered warnings reporting, e.g., car accidents or adverse climatic conditions, with other vehicles or road traffic authorities.

ETSI ITS Security: The Intelligent Transport Systems (ITS) technical committee of the European Telecommunications Standards Institute (ETSI) is in charge of standardizing the V2X communication in the EU. The ETSI ITS communication architecture [3] defines both the vehicles and the road-side units (RSUs) as peer ITS stations (ITS-Ss) communicating via the ETSI ITS communication protocol stack (shown in blue in Fig. 1), which features three layers: access, networking and transport, and facilities. Based on the security services for ITS-Ss identified in [4], an ETSI ITS communication *security* architecture and the related security management procedures have been specified in [5]. Two security management authorities are defined in the ETSI ITS public key infrastructure (PKI):

1) the enrollment authority (EA), which is in charge of the life-cycle management of *enrollment credentials*, and
2) the authorization authority (AA), responsible for issuing, monitoring, and withdrawing *authorization tickets*.

The EA manages *long-term* certificates for identification and accountability of an ITS-S (i.e., the enrollment certificates), allowing the bearer to apply for *short-term*, anonymized certificates (pseudonyms) for V2X communication (i.e., the authorization tickets) from the AA. After obtaining the authorization ticket, an ITS-S can securely start exchanging ITS messages, e.g., cooperative awareness messages (CAMs) and decentralized environmental notification messages (DENM).

3GPP Network Security: As shown in Fig. 1, the ETSI ITS communication protocol stack relies on other wireless communication standards for the implementation of the access layer. While originally the IEEE 802.11p standard (G5 radio interface) was leveraged, since a few years Third Generation Partnership Project (3GPP) radio access technologies represent a valid alternative. Two radio interfaces are available for C-V2X: i) the long-range Uu interface for vehicle-to-network (V2N) communication, and ii) the short-range PC5 interface for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. While the former provides end-to-end, IP-based communication between ITS-Ss or between a ITS-S and the ITS infrastructure back-end through the mobile network infrastructure [6], the latter complements it by providing an alternative, non-interoperable short-range connectivity to G5. The operational mode of the PC5 radio interface is either configured by the network or self-configuring. In the following, we will refer to C-V2X technologies only, remaining agnostic about the PC5 configuration modes.

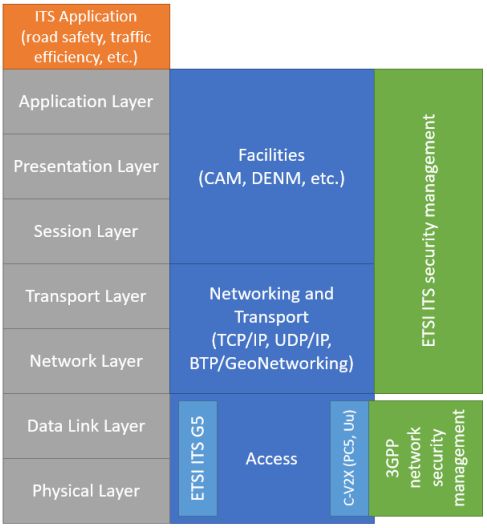

Fig. 1. Interworking between the ETSI ITS communication protocol stack (in blue) and the 3GPP protocol stack (in light blue), which implements the access layer providing long-range (Uu) and short-range (PC5) wireless connectivity. The ISO OSI protocol stack is shown as reference in grey. C-V2X access layer is alternative to ETSI ITS G5. In green, we have the security management.

As far as the security of 3GPP systems is concerned, built-in authentication, authorization, identity management, data integrity, and privacy are provided to *traditional* user equipments (UEs) (e.g., smartphones) by both the current fourth-generation Evolved Packet System (EPS) [7] and the upcoming 5G System (5GS) [8]. Moreover, further security requirements are defined for C-V2X communication, thus for *ITS-S-type* UEs [9]. In particular, 3GPP networks shall provide i) a means for the MNO to authorize or even pre-authorize a UE to perform V2X communication, ii) integrity protection of the transmission for a C-V2X application, and iii) pseudonymity and privacy of a UE using the C-V2X application.

US DoT SCMS: The United States Department of Transportation (US DoT) has ~~also proposed~~ been coordinating the efforts towards a PKI-based message security solution for V2V and V2I communications ~~,~~called Security Credentials Management System (SCMS).[4] Authorized vehicles use digital certificates

[4]https://www.its.dot.gov/resources/scms.htm

to ensure authenticity and integrity of exchanged basic safety messages, which are supposed to contain no personal data to guarantee privacy.[5] Besides, the SCMS will implement a Misbehavior Authority which will collect misbehavior reports generated by vehicles.[6] After enough reports are received, the Misbehavior Authority will add the corresponding certificate to a certificate revocation list (CRL) and distribute them to all vehicles. ~~Even though SCMS may be considered as a reference in 5G-enabled C-V2X use cases, some~~

Some issues still need to be addressed. For instance, ~~SCMS states~~ the SCMS provides that each vehicle should receive 20 certificates each week, which ~~should~~ rotate every 5 minutes for maintaining privacy. However, ~~the management of~~ managing so many certificates entails challenges such as distribution and maintenance of large CRLs and the possibility of ~~sybil~~ Sybil attacks by malicious vehicles.

Treatment of Vehicular Data at the Edge Servers

While the previous communication standards enable a secure exchange of messages among ITS-Ss, the life-cycle management of vehicular data should also be taken into account, especially when a given CCAM service exploits a computing unit to process vehicular data. In case of low-latency applications, such a unit may have either an edge computing server co-located with the RSU or an ETSI multi-access edge computing (MEC) compliant server co-located with the 3GPP mobile network. In the latter scenario, multiple solutions allow tapping into the IP traffic from the UE [10]. Moreover, ad-hoc security measures are being specified to provide the users, the MNO, the CCAM application provider, the application developer, the content provider, and the platform vendor with a secure environment for the execution of CCAM services [11].

Summary

For the readers' convenience, in Tab. I we provide a brief description of the six communication security management service categories specified by ETSI ITS (i.e., enrollment, authorization, accountability, remote management, misbehavior reporting, identity management), along with the additional security features provided by the C-V2X access layer and the MEC platforms. Moreover, a graphical depiction of the relation between the involved players and the various technology enablers is outlined in Fig. 2.

A Bottom-Up Approach for CCAM Security Assessment

Despite the above-mentioned standards define a landmark for CCAM security, various details are usually *not* standardized and left to vendor implementation. In these cases, some unexpected security flaws may emerge, thus causing vulnerabilities that could affect the end-to-end vehicular communication system. For these reasons, a careful preliminary security assessment of each CCAM service should be carried out, as not all threats may have been caught both at a standardization level and development level.

In the following, we will follow a *bottom-up* approach in which we analyze some real CCAM services to identify their security threats and derive the possible countermeasures. The analyzed services are taken from one of the Horizon 2020 initiatives funded by the EU, i.e., the 5G-CARMEN project[7], which has been developing a communication and computing platform to enable CCAM services along the Bologna-Munich highway corridor crossing Italy, Austria, and Germany. The 5G-CARMEN CCAM platform employs different enabling technologies, such as 3GPP C-V2X transceivers and multi-domain orchestration, to implement four ~~5G~~5GS-enabled CCAM services: i) cooperative maneuvering, ii) situation awareness, iii) video streaming, and iv) green driving. The former two are *safety-related* services, that is, they aim at enhancing the awareness of status and intents among ITS-Ss (e.g., by making vehicles aware of road hazards or maneuver intents by other vehicles [5]) and have a strict relation with the safety of involved V2X users (e.g., by preventing car crashes). On the other hand, the latter two are *non-safety-related* CCAM services, concerned about enriching the passengers' experience (e.g., by providing seamless in-car entertainment). Although the security assessment is noteworthy for all CCAM services, here we focus only on safety-related ones, because these are characterized by a more tricky interplay among security and functional requirements.

Cooperative Maneuvering

In cooperative maneuvering services, each vehicle optimizes its trajectory by exchanging CAMs (containing, e.g., direction and speed) with other vehicles via C-V2X and combining this knowledge with precise positioning and information about aggregate traffic conditions. In particular, 5G-CARMEN has been implementing a cooperative lane merging (CLM) service, in which the gaps between vehicles in a cluster are managed in such a way that a vehicle that intends to move into a lane occupied by other vehicles can complete the maneuver safely and efficiently. This CCAM service is implemented by an edge application that monitors the road traffic trends as well as the intentions of the car drivers along a given road stretch: if the conditions are considered safe, the vehicles traveling along that stretch are informed via long-range Uu communication that they can perform CLM. The specific maneuver indications can be generated by the edge application itself and transmitted along with the maneuver authorization (centralized approach), otherwise, such indications can be negotiated within each cluster of vehicles, exploiting short-range PC5 communication (decentralized approach).

Situation Awareness

In situation awareness services, the car drivers are informed about nearby dangerous situations in order to increase their own safety. In this context, 5G-CARMEN has identified two variants to be implemented.

[5]https://www.its.dot.gov/factsheets/pdf/Privacyfactsheet.pdf
[6]https://www.its.dot.gov/factsheets/pdf/CVSCMS.pdf
[7]https://5gcarmen.eu/

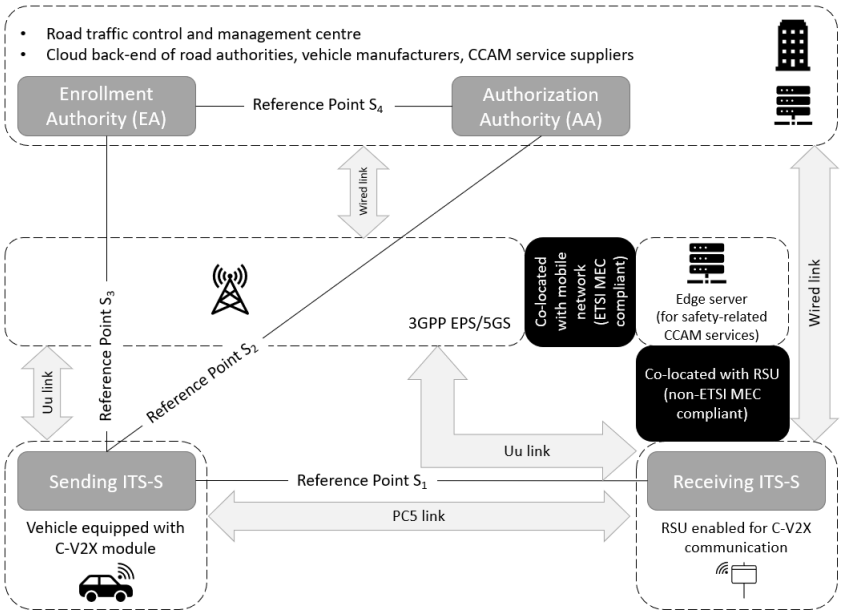

Fig. 2. A graphical mapping of the ETSI ITS communication security functional model [5, §5.3] against the players and technology enablers involved in C-V2X. In this example, the sending (receiving) ITS-S is a vehicle (RSU) equipped with C-V2X module. Through the reference points S_3 and S_2 the vehicle can apply for enrollment credentials and authorization tickets from the ITS infrastructure, respectively. Once it is admitted in the ITS system, it can perform V2N communication through the Uu interface towards CCAM services (hosted either in the remote or in the edge cloud) or distant vehicles. Moreover, through the PC5 interface, the vehicle can perform V2V/V2I communication towards vehicles in proximity/RSUs.

1) With back-situation awareness (BSA), each driver is notified of the expected time of arrival of an emergency vehicle, e.g., an ambulance or a police car, so that he/she can minimize road obstruction by proactively creating an emergency corridor.
2) With vehicle sensors and state sharing (VSSS), an in-advance awareness about adverse weather conditions or other detected road hazards is provided to drivers by vehicles ahead, the road infrastructure, and/or the network, thus merging information originating from different sources in the relevant area.

For both services, an edge application is exploited to dispatch the warning messages to the affected vehicles exploiting either V2V/V2I (PC5) communication or V2N (Uu) communication.

~~Trade-Off Between~~ Functional and Security Requirements of Safety-Related CCAM Services

Each CCAM service entails specific *functional* requirements as well as *security* requirements, which influence each other. Moreover, the same requirement may have a different relevance across services, thus the interplay between functional and security requirements depends on the service. In the following, for each safety-related CCAM service, we briefly outline its critical functional requirements[8] and we specify the behavior of the six security service categories provided in Tab. I in terms of required security mechanisms (i.e., security requirements). Finally, we discuss the interplay between the functional requirements and the identified security requirements.

[8]See, e.g., "5G-CARMEN Use Cases and Requirements," Deliverable 2.1, May 2019. Available online at https://5gcarmen.eu/wp-content/uploads/2020/03/5G_CARMEN_D2.1_FINAL.pdf

CLM Analysis

Functional Requirements: managing cooperative maneuvers requires frequent and precise input data from the involved vehicles (i.e., CAM containing position, speed, and intention) and fast elaboration of such data (e.g., by a scalable infrastructure in case of road stretches with dense traffic). Furthermore, a CLM poses a strict requirement on message reliability and latency, to prevent the exchange of aged vehicular data/maneuver indications.

Security Requirements: as for *enrollment*, the cryptographic material (e.g., secret keys) used to guarantee confidentiality and integrity of communications toward EA shall be stored in tamper-proof secure in-car memory elements. Anyway, CRLs containing the PKI certificates of misbehaving ITS-Ss shall be kept up to date and quickly spread within the ITS infrastructure to prevent attacks from tampered/rogue ITS-Ss, which can be extremely harmful for a safety-critical CCAM service such as CLM. Also, countermeasures to physical attacks (e.g., vandalism) shall be addressed for preserving the dependability of the CLM service.

Regarding *authorization*, all involved vehicles shall obtain an "advanced CAM authorization" from the AA in order to interact with the CLM application in the edge server. The access control policy is attribute-based, and it mainly considers vehicles' location (i.e., authorization tickets shall authorize access to the closest CLM application instance only) and capabilities (e.g., sensors equipment [5]). The integrity of authorization tickets shall be preserved through cryptography (e.g., digital signatures). Privacy is based on the use of (valid and not expired) pseudonyms. However, the provisioning of pseudonyms to vehicles by AAs shall balance privacy requirements (e.g., vehicles untraceability) against possible

misuses (e.g., Sybil attacks [12]). Confidentiality and integrity of communications toward AAs shall be preserved as well.

With regard to *accountability*, beside integrity, cryptography shall guarantee also the non-repudiation property on messages exchanged within the CLM service. Forensics (e.g., after a car crash) requires the possibility to resolve the pseudonym(s) used by an ITS-S. However, only relevant authorities (e.g., the police) shall be capable of linking a pseudonym to the vehicle [12]. Also, since accountability implies the retention of pseudo-anonymized and personal data, the General Data Protection Regulation (GDPR)[9] (e.g., data minimization principle, policy on data retention [13, §4]) shall be considered. According to the GDPR, cryptography also plays a crucial role to protect user personal data (e.g., position and identity) transported in messages routinely exchanged by CCAM services. Additionally, cryptographic solutions for authentication and authorization (such as those depicted in Fig. 2) are key to developing secure and privacy-aware services; guaranteeing an appropriate level of assurance of authentication and that access control policies are appropriately enforced are mandatory for empowering users with the control of their personal data – one of the key tenets underlying the GDPR.

Referring to *remote management*, the ITS infrastructure shall be able to exclude misbehaving ITS-Ss from the CLM service, eventually interacting with the underlying 3GPP network infrastructure. In particular, there shall be security mechanisms to detect and mitigate denial of service (DoS) attacks against the CLM service at various levels: physical transmissions (e.g., jamming), multi-hop (PC5) packet routing (e.g., jellyfish attack), network topology (e.g., flooding attack), and application (e.g., memory exhaustion).

Concerning *misbehavior reporting*, ITS-Ss shall be able to report *internal* suspicious activities to the ITS infrastructure – authentication already protects against *external* misbehaving ITS-Ss. Presumed internal misbehaving ITS-Ss can be detected by complementing techniques at different levels (e.g., network, application) to combine factors which are independent of a particular use case (e.g., reputation scores, entity-based trust frameworks) with application-specific aspects to take advantage of the semantic of exchanged messages (e.g., in CLM, consistency and plausibility checks [5, §4] of a sequence of messages).

Finally, about *identity management* all V2I communications regarding CLM services shall occur through pairwise-authenticated and confidential channels. In V2V communications, the unlinkability of pseudonyms shall be guaranteed. Confidentiality, instead, is not required, as messages are broadcast [5, §4].

BSA Analysis

Functional Requirements: BSA has looser functional requirements than CLM in terms of latency and reliability. The emergency vehicles shall be authorized to broadcast their presence through CAMs, and set an adequate *priority level* to trigger support from regular ITS-Ss (e.g., by creating an emergency corridor) and the ITS infrastructure (e.g., by synchronizing traffic lights to create a 'green' wave).

Security Requirements: as for *enrollment*, since the target area may be far ahead of the emergency vehicle, the BSA service continuity across different administrative domains should be ensured. As such, the enrollment of emergency vehicle may involve different EAs. Trust establishment among PKI certification authorities (CA) requires international coordination and a proper management of CRLs. Moreover, on PKI certificate management, the same considerations as CLM services hold, for both regular and emergency vehicles.

Regarding *authorization*, only actual emergency vehicles shall be able to obtain the "authorization to claim priority rights for emergency vehicles" [5] depending on their priority level. Therefore, an access control policy shall be devised to allow for fine-grained priority levels by considering the *least privilege principle* and avoiding *privilege escalation attacks*. Also, messages broadcast by emergency vehicles shall be protected against replay attacks (e.g., through timestamp, sequence number, or location checks). Finally, we note that emergency vehicles do not need pseudonyms.

With regard to *accountability*, as in the CLM case, data shall be retained to enable later forensics. However, in BSA we envision fewer privacy requirements, as it deals with public safety services.

Referring to *remote management*, the ITS infrastructure shall be able to block stolen or misbehaving emergency vehicles from claiming priority rights.

Concerning *misbehavior reporting*, ITS-Ss shall be able to report internal suspicious activities to the ITS infrastructure. In particular, protection against message replay shall be ensured to prevent unauthorized vehicles from claiming priority privileges.

Finally, about *identity management* in BSA, neither confidentiality nor pseudonyms are needed.

VSSS Analysis

Functional Requirements: Depending on the context, VSSS messages may have latency/reliability constraints as in CLM (e.g., in case of road accident warnings) or as in BSA (e.g., adverse weather conditions warnings). When bad weather conditions or hazards are detected by a vehicle or a RSU, such ITS-Ss can notify nearby vehicles with a DENM. The warning can be then forwarded to distant vehicles through the ITS infrastructure (i.e., other RSUs preceding the dangerous road stretch), the cellular network (via Uu links), or vehicles exploiting multi-hop (PC5) routing.

Security Requirements: as for *enrollment*, similarly to BSA, the dangerous area may be far ahead from the vehicle, thus VSSS service continuity may involve multiple EA. The usual recommendations on PKI certificate management are in force.

Regarding *authorization*, only vehicles proving to have the necessary capabilities (e.g., cryptographic algorithms, sensors equipment, and quality [5]) shall be allowed to participate in the VSSS service. Since VSSS messages cannot be used for tracking [5], one pseudonym is enough to preserve drivers' privacy, with the advantage to prevent Sybil attacks [12].

With regard to *accountability* and *remote management*, as in CLM and BSA, data shall be retained to enable later forensics

[9]https://gdpr.eu/

with the same privacy considerations and the ITS infrastructure shall be able to exclude misbehaving ITS-Ss from the VSSS service, respectively.

Concerning *misbehavior reporting*, an ITS-S shall be able to report suspicious activities. Fake road hazards (e.g., fake ice threat) could be detected by validating the data, asserting the reputation of the sending vehicle, or having multiple vehicles confirming the same road hazard.

Finally, about *identity management*, while (at least one) pseudonym is needed to preserve privacy, confidentiality is not needed as VSSS messages are broadcast.

Interplay Between Functional and Security Requirements

Both functional and the identified security requirements of the analyzed CCAM services (which are summarized in a tabular format in Tab. II) aim at preserving and enhancing their safety but with different objectives, thus their fulfillment should be thoroughly balanced in order to avoid *interference* between them. In the following, we will describe some situations in which such an interference between functional and security requirements yields negative impacts on safety.

Preserving the integrity of messages (security requirement) exchanged by ITS-S involved in CLM and VSSS is crucial for preventing potentially dramatic safety issues (e.g., due to wrong maneuvering suggestions or an altered environmental perception). On the other hand, given the typically low computational capabilities of cars' ECUs, robust and secure cryptographic primitives used to protect messages may degrade the system performance and break the strict latency constraint (functional requirement), potentially leading to safety issues as well (e.g., vehicle position is outdated by the time the message is read). Therefore, the level of robustness of cryptographic primitives needs to be carefully chosen. We note that attacks to message integrity at the edge computing platforms are more complex but not impossible, e.g., by exploiting the complexity and possible subtle dependencies between the modules in which the software runs. Also, deploying enrollment and authorization services in a real-time and dynamic scenario is a challenging task [14]. These services require several cryptographic operations and V2N communication for the validation of PKI certificates against CRLs. Ensuring a high level of security may again affect the latency, with negative impacts on safety.

Beside overall integrity, also the content of the messages should be checked to prevent an internal attacker from spreading fake information. In VSSS, vehicles are notified of road hazards through DENMs. The content of these messages can be validated through reputation or trust scores [15]. A simple solution is to aggregate DENMs from different vehicles and compare their content to ensure consistency (security requirement). For instance, we could assume that at least two DENMs are required to validate the presence of a road hazard. However, waiting for the second DENM may delay vehicles' reaction like steering or breaking (functional requirement), affecting safety again. Thus, the trust threshold needs to be carefully chosen, e.g., as a function of the current traffic condition. Nonetheless, we note that a misbehaving ITS-S could exploit the (several) pseudonyms provided by the AA to subvert the correct information through a Sybil attack. On the other hand, a scant supply of pseudonyms could lead to potential privacy issues [12].

Another example is that of scalability, which, as a functional requirement, fosters decentralized approaches like, e.g., in CLM. Nonetheless, this has a negative effect on security, since there is no central entity with global state awareness that can become aware of misbehaving vehicles (security requirement) that can alter other vehicles awareness and impact safety.

The dependability of the edge computing platforms should also be taken into account. Even modest attempts to perform a DoS attack may have dramatic consequences on safety due to the strict latency requirements of the examined CCAM services. The deployment of redundant instances of a CCAM service may mitigate the impact of a Memory Exhaustion attack (security requirement) at the expenses of reducing virtualization resources available for other services (functional requirement).

As a final remark, we note that safety fallback mechanisms should be devised and deployed to avoid the worst-case scenario. Each service should have a fail-safe design so that ITS-Ss can adjust their functional characteristics to the new situation and fall back to secure states. For instance, the CLM service is very sensible to attacks to messages integrity or availability, thus it is advisable to implement fallback mechanisms to ensure drivers' safety even under adverse conditions (e.g., attacks or communication errors). Let us think at a DoS attack to the centralized CLM service, which prevents the edge server from generating maneuvering indications. The vehicles themselves could issue a warning to their driver and provide the safest advice based on the current context (e.g., slow down, do not merge).

CONCLUSIONS

~~The increasing demand for CCAM services is pushing car manufacturers to release new vehicle models to fill the gap of their current offer. Together with the development of CCAM services, however, proper security mechanisms should be adopted in order to ensure the drivers' safety.~~ In this article, we surveyed the ongoing ~~EU~~ regulation and standardization activities aimed at specifying the security procedures for vehicle cybersecurity. ~~Then~~Moreover, we performed a security assessment of three safety-related CCAM services under study in the UE-funded project 5G-CARMEN, focusing on the interplay between functional and security requirements. The discussions provided in this work are beneficial, e.g., to the Data Protection Impact Assessment (DPIA) mandated by Art. 35 of the GDPR. Indeed, stakeholders (in particular, data controllers) must evaluate the likelihood and impact of privacy risks on the rights and freedom of data subjects; in the context of certain CCAM services such as the CLM, safety is one of the most important rights.

ACKNOWLEDGMENT

This work has been performed in the framework of the European Union Horizon 2020 project 5G-CARMEN co-funded by the EU under grant agreement No. 825012. The views

expressed are those of the authors and do not necessarily represent the project. The Commission is not liable for any use that may be made of any of the information contained therein.

REFERENCES

[1] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, Feb. 2020.
[2] "Road vehicles — Cybersecurity Engineering," Vehicle Cybersecurity Systems Engineering Committee, ISO/SAE standard 21434, Feb. 2020.
[3] "Communications Architecture," ETSI TC ITS European Std. EN 302 665 V1.1.1, Sep. 2010.
[4] "Security; Security services and architecture," ETSI TC ITS Tech. Spec. 102 731 V1.1.1, Sep. 2010.
[5] "Security; ITS communications security architecture and security management," ETSI TC ITS Tech. Spec. 102 940 V1.3.1, Apr. 2018.
[6] "Framework for Public Mobile Networks in Cooperative ITS (C-ITS)," ETSI TC ITS Tech. Rep. 102 962 V1.1.1, Feb. 2012.
[7] "Service requirements for the Evolved Packet System (Release 17)," 3GPP TSG-SA Tech. Spec. 22.278 V17.1.0, Dec. 2019.
[8] "Service requirements for the 5G system; Stage 1 (Release 17)," 3GPP TSG-SA Tech. Spec. 22.261 V17.1.0, Dec. 2019.
[9] "Service requirements for V2X services; Stage 1 (Release 15)," 3GPP TSG-SA Tech. Spec. 22.185 V15.0.0, Jun. 2018.
[10] "MEC deployments in 4G and evolution towards 5G," ETSI ISG MEC Whitepaper #24, Feb. 2018.
[11] "Multi-access edge computing; Phase 2: Use cases and requirements," ETSI ISG MEC Group Spec. MEC002 V2.1.1, Oct. 2018.
[12] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," in *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228-255, Firstquarter 2015.
[13] "Critical security controls for effective cyber defence; Part 5: Privacy enhancement," ETSI TC CYBER Tech. Rep. 103 305-5 V1.1.1, Sep. 2018.
[14] A. Patwary, A. Fu, R. Naha, S. Battula, S. Garg, M. Patwary, and E. Aghasian "Authentication, Access Control, Privacy, Threats and Trust Management Towards Securing Fog Computing Environments: A Review", ArXiV, Mar. 2020. [Online]. Available: https://arxiv.org/abs/2003.00395
[15] M. Hasan, S. Mohan, T. Shimizu, H. Lu "Securing Vehicle-to-Everything (V2X) Communication Platforms", ArXiV, Mar. 2020 [Online]. Available: https://arxiv.org/abs/2003.07191

Marco Centenaro (marco.centenaro.it@ieee.org) is an Expert Researcher at Fondazione Bruno Kessler, Trento, Italy. His research is focused on telecommunication standards as well as Internet of Things technologies.

Stefano Berlato (sberlato@fbk.eu) is a Research Assistant at Fondazione Bruno Kessler, Trento, Italy. His current research interests include the analysis of security in ITS and edge computing solutions.

Roberto Carbone (carbone@fbk.eu) is a Researcher of the Security&Trust research unit of Fondazione Bruno Kessler in Trento, Italy, since 2010. He received his PhD from the University of Genova in 2009. His research mainly focuses on digital identity management and formal analysis of security protocols and services.

Gianfranco Burzio (gb@drivesec.com) was born in Carmagnola, Italy, on 14 September 1956. Graduated in Electrical Engineering in 1980, with a final vote of 110/110 cum laude. Specialization in Industrial Automation. After two years of experience as a software system engineer, he joined the FIAT Research Centre in 1982. He worked initially in industrial automation and robotics, from 1990 his activities moved to development of driving assistance systems (anti-collision, lane keeping, overtaking warning). Executive manager in 1995 he managed the development teams of on-board information systems, driver assistance, telematics and vehicle-driver interface. Coordinator of several European funded research projects. Between 2003 and 2006 he coordinated the participation of FIAT Group to the Torino Wireless regional project. In 2012 he was appointed Safety Director at ACEA, the European association of vehicle manufacturers, in Brussels. Back in Fiat Chrysler Automotive in 2016, until October 2017. Automotive safety and security advisor for Drivesec since November 2017.

Giuseppe Faranda Cordella (gfc@drivesec.com) got a master degree in Computer Science at Turin University and he is a senior executive with an experience of over 25 years in the design and development of automotive electronics, connected car services and vehicle cybersecurity. In his career he is been working in different roles in leading automotive companies either as an OEM or a Tier1 suppliers. In recent years he served as head of research and development and VP of infotainment for a large OEM in Europe. In the last few years he was appointed head of Vehicle Cybersecurity for leading OEM in EMEA, managing the introduction of digital protection countermeasures in connected cars.

Roberto Riggio (~~rriggio~~roberto.riggio@~~fbk.eu) head of the Wireless and Networked System~~ ri.se) is Senior Researcher in the Connected Intelligence Group at RISE AB in Stockholm, Sweden. He received his PhD from the University of Trento (Italy), after that he was postdoc at University of Florida, Researcher/Chief Scientist at CREATE-NET in Trento (Italy), Head of Unit at FBK ~~CREATE-NET~~in Trento (Italy), and Senior 5G Researcher at the i2CAT Foundation in Barcelona (Spain). His research interests ~~include software-defined mobile networks, network slicing, and distributed management and orchestration of network services. He~~ revolve around optimization and algorithmic problems in networked and distributed systems. His current fields of applications are edge automation platforms, intelligent networks, and human-driven networking. Roberto Riggio has published more than ~~100 papers and has generated more than 2.7 million Euros in competitive funding. He has received several awards including the IEEE CNSM 2015 Best Paper Award. He serves on the TPC/OC of leading conferences in networking and is an Associate Editor of several journals including IEEETransactions on Network and Service Management.~~ 130 papers in internationally refereed journals and conferences. He is a Senior Member of the IEEE.

Silvio Ranise (ranise@fbk.eu) received a joint Phd from the University of Genova (Italy) and Université Henri Poincaré (Nancy, France). He was researcher at INRIA (the french National Institute for Computer Science and Automation), visiting professor at the University of Milano (Italy) and researcher at the University of Verona (Italy). He is now the Head of the Security and Trust research unit in Fondazione Bruno Kessler (Trento, Italy). His main research interests are digital identity management, risk assessment and legal compliance (e.g., for privacy and finance), and security analysis of complex ecosystems combining different technologies such as APIs, IoT, mobile and cloud computing. He has published more than 100 papers in international conferences and journals and regularly serves as PC member of several international conferences in cybersecurity. He is or has been involved in many European and industrial projects.

TABLE I
LIST OF ETSI ITS COMMUNICATION SECURITY MANAGEMENT SERVICES CATEGORIES [5, TAB. 4], WITH ADDITIONAL FEATURES PROVIDED BY C-V2X RADIO ACCESS TECHNOLOGIES [9] AND VEHICULAR DATA PROCESSING INFRASTRUCTURE [11].

SERVICE CATEGORY	DESCRIPTION AND FUNDAMENTAL FEATURES	ADDITIONAL FEATURES
Enrollment	Management of enrollment credentials through reference point S_3. An ITS-S shall request enrollment credentials to the EA such that it can be trusted to function correctly by another ITS-S. Fundamental features: • establishment of enrollment trust via secure handling and storage of cryptographic keys (PKI certificates) at the ITS-S • enrollment trust management based on certificate provisioning by the EA	• The EPS/5GS shall support information authenticity between the UE and the EPS/5GS • Appropriate traffic protection measures should be provided by the EPS/5GS • The EPS/5GS shall ensure that no unauthorized user can obtain a legitimate IP address that can be used to establish communication or enable malicious attacks on EPS/5GS entities
Authorization	Management of authorization tickets through reference points S_4 and S_2. An enrolled ITS-S shall request authorization tickets to the AA to get specific permissions (e.g., to access to a specific service/resource). Fundamental features: • trust management of the authorization tickets based on certificate provisioning and privacy management based on pseudonyms provisioning by the AA • privacy management of the authorization tickets based on pseudonyms provisioning by the AA • access control policies	• The 3GPP network shall provide a means for the MNO to authorize a UE supporting V2X application to perform V2X communication when served by E-UTRAN supporting V2X communication • The 3GPP network shall provide a means (e.g., pre-authorization) for the MNO to authorize a UE supporting V2X application to perform V2X communication when not served by E-UTRAN supporting V2X communication • The 3GPP network shall provide a means for the MNO to authorize UEs supporting V2X application separately to perform V2N communication • The 3GPP system shall support integrity protection of the transmission for a V2X application • The MEC platform shall only provide a MEC application with the information for which the application is authorized
Accountability	Records incoming/outgoing messages such that the ITS-S can be held accountable.	• The EPS shall be able to store information of third-party applications necessary for performing security and charging functions • The 5GS shall support a secure mechanism to store cached data • Implement measures for meeting the NFV retained data problem set (secure logging, access control, post-incident analysis)
Remote management	Enable the ITS infrastructure to remotely manage a misbehaving ITS station, e.g., by remotely activating/deactivating the transmission of messages on a specific ITS station.	• Subject to regional or national regulatory requirements, the 5GS shall support a secure mechanism for allowing an authorized entity to disable from normal operation of a UE reported as stolen
Misbehavior reporting	Enable an ITS-S to report a suspicious activity (e.g., a misbehaving ITS-S) to the ITS infrastructure.	• Subject to regional or national regulatory requirements, the 5GS shall support mechanisms to detect tampering and spoofing attempts on the production of the user location information and the user position-related data
Identity management	Provide services supporting the simultaneous change of communication identifiers, i.e., station ID (facility layer), network ID (network/transport layer), and MAC address (access layer), and credentials used for secure communications, within the ITS-S. Provides features allowing the disabling of ID change. Fundamental features: • communication privacy management, entailing anonimity/pseudonimity, unlinkability/unobservability • assurance of transmitted information confidentiality	• The EPS/5GS shall provide several appropriate levels of user privacy including communication confidentiality, location privacy, and identity protection • Subject to regional regulatory requirements and/or operator policy for a V2X application, the 3GPP system shall support pseudonymity and privacy of a UE using the V2X application, by ensuring that a UE identity cannot be tracked or identified by any other UE beyond a certain short time-period required by the V2X application • Subject to regional regulatory requirements and/or operator policy for a V2V/V2I application, the 3GPP system shall support pseudonymity and privacy of a UE in the use of a V2V/V2I application, such that no single party (operator or third party) can track a UE identity in that region

TABLE II
MAPPING BETWEEN ETSI ITS COMMUNICATION SECURITY SERVICE CATEGORIES AND SAFETY-RELATED 5G-CARMEN CCAM SERVICES.

SECURITY SERVICE		CLM	BSA	VSSS
Enrollment	Secure storage of cryptographic material at the ITS-S	yes	yes	yes
	Enrollment checked against CRLs	yes	yes	yes
	Management of enrollment credentials across (trusted) administrative domains	no need	yes	yes
	Security Properties	**integrity, privacy**	**integrity**	**integrity, privacy**
Authorization	Vehicle Authorization	Advanced CAM authorization [5]	Authorization to claim priority rights for emergency vehicles [5]	Basic CAM authorization [5]
	Access Control	Based on ITS-S location and capabilities [5]	Based on priority levels (least privilege principle)	Based on ITS-S capabilities (e.g., cryptographic algorithms, sensors equipment and quality [5])
	Pseudonyms	(balanced) provisioning [12]	no need	provisioning limited to one pseudonym [5]
	Security Properties	**confidentiality, integrity, safety**	**integrity**	**confidentiality, integrity**
Accountability	ITS-Ss and MEC platforms shall store logs (e.g., received messages) to enable forensics.	yes	yes	yes
	Relevant authorities only shall be capable of linking a pseudonym to a vehicle in case of necessity [12].	yes	no need (no pseudonyms to solve)	yes
	Consideration of GDPR, Data Minimization principle and policy on data retention [13, § 4].	yes	no need (no personal or sensitive data)	yes
	Security Properties	**availability, integrity**	**availability, integrity**	**availability, integrity**
Remote Management	The ITS infrastructure shall be able to	exclude misbehaving ITS-S from the service.	block stolen or misbehaving emergency vehicles from claiming priority rights.	exclude misbehaving ITS-S from the service.
	The ITS infrastructure shall be able to revoke PKI certificates of misbehaving ITS-S through CRLs.	yes	yes	yes
	Security Properties	**integrity, safety**	**integrity, safety**	**integrity, safety**
Misbehaviour Reporting	ITS-Ss shall be able to report internal suspicious activities to the ITS infrastructure (e.g., fake messages or data tampering).	yes	yes	yes
	Service misuse protection	Too many CLM requests from a vehicle shall be reported.	Messages broadcast by emergency vehicles shall be protected against replay attacks.	Too many CLM requests from a vehicle shall be reported.
	Security Properties	**integrity, safety**	**integrity, safety**	**integrity, safety**
Identity Management	Communication confidentiality	All V2I communications happen through pairwise-authenticated and confidential channels.	The V2I communication between the emergency vehicle and the ITS infrastructure happens through pairwise-authenticated and confidential channels. Then, confidentiality is not required for broadcast messages [5, §4].	Confidentiality is not required for broadcast messages [5, §4].
	Privacy	The ITS infrastructure shall support the simultaneous change of communication identifiers.	No need	One pseudonym shall be used to preserve privacy.
	Security Properties	**confidentiality, privacy**	**none – Neither confidentiality nor pseudonyms are needed.**	**privacy**